

JP1 Version 11

**JP1/Integrated Management - Manager
Administration Guide**

3021-3-A09-30(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 - Manager and JP1/Integrated Management - View, see the release notes for the relevant product.

JP1/Integrated Management - Manager (for Windows):

P-2A2C-8EBL JP1/Integrated Management - Manager 11-50

The above product includes the following:

P-CC2A2C-9MBL JP1/Integrated Management - Manager 11-50 (for Windows Server 2016, Windows Server 2012, Windows Server 2008 R2)

P-CC2A2C-6HBL JP1/Integrated Management - View 11-50 (for Windows Server 2016, Windows 10, Windows 8.1, Windows 8, Windows Server 2012, Windows 7, Windows Server 2008 R2)

JP1/Integrated Management - Manager (for AIX):

P-1M2C-8EBL JP1/Integrated Management - Manager 11-50

The above product includes the following:

P-CC1M2C-9MBL JP1/Integrated Management - Manager 11-50 (for AIX)

P-CC2A2C-6HBL JP1/Integrated Management - View 11-50 (for Windows Server 2016, Windows 10, Windows 8.1, Windows 8, Windows Server 2012, Windows 7, Windows Server 2008 R2)

JP1/Integrated Management - Manager (for Linux):

P-812C-8EBL JP1/Integrated Management - Manager 11-50

The above product includes the following:

P-CC812C-9MBL JP1/Integrated Management - Manager 11-50 (for Linux 7, Linux 6 (x64), Oracle Linux 7, Oracle Linux 6 (x64), CentOS 7, CentOS 6 (x64))

P-CC9W2C-9MBL JP1/Integrated Management - Manager 11-50 (for SUSE Linux 12)

P-CC2A2C-6HBL JP1/Integrated Management - View 11-50 (for Windows Server 2016, Windows 10, Windows 8.1, Windows 8, Windows Server 2012, Windows 7, Windows Server 2008 R2)

■ Trademarks

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

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

IBM, AIX are trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide.

AMD, AMD Opteron, and combinations thereof, are trademarks of Advanced Micro Devices, Inc.

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

Linux^(R) is the registered trademark of Linus Torvalds in the U.S. and other countries.

Microsoft and Hyper-V are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

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

Red Hat is a trademark or a registered trademark of Red Hat Inc. in the United States and other countries.

RSA and BSAFE are either registered trademarks or trademarks of EMC Corporation in the United States and/or other countries.

All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc., in the United States and other countries. Products bearing SPARC trademarks are based upon an architecture developed by Sun Microsystems, Inc.

SUSE is a registered trademark or a trademark of SUSE LLC in the United States and other countries.

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

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

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

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

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

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

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

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

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

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

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

This product includes software developed by 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/>)



This product includes RSA BSAFE Cryptographic software of EMC Corporation.

■ 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 7		Microsoft ^(R) Windows ^(R) 7 Enterprise
		Microsoft ^(R) Windows ^(R) 7 Professional
		Microsoft ^(R) Windows ^(R) 7 Ultimate
Windows 8		Windows ^(R) 8 Enterprise
		Windows ^(R) 8 Pro
Windows 8.1		Windows ^(R) 8.1 Enterprise
		Windows ^(R) 8.1 Pro
Windows 10		Windows ^(R) 10 Enterprise 32-bit
		Windows ^(R) 10 Enterprise 64-bit
		Windows ^(R) 10 Home 32-bit
		Windows ^(R) 10 Home 64-bit
		Windows ^(R) 10 Pro 32-bit
		Windows ^(R) 10 Pro 64-bit
Windows Server 2008		Microsoft ^(R) Windows Server ^(R) 2008 Datacenter
		Microsoft ^(R) Windows Server ^(R) 2008 Enterprise
		Microsoft ^(R) Windows Server ^(R) 2008 Standard
Windows Server 2008 R2		Microsoft ^(R) Windows Server ^(R) 2008 R2 Datacenter

Abbreviation		Full name or meaning
		Microsoft ^(R) Windows Server ^(R) 2008 R2 Enterprise
		Microsoft ^(R) Windows Server ^(R) 2008 R2 Standard
Windows Server 2012	Windows Server 2012	Microsoft ^(R) Windows Server ^(R) 2012 Datacenter
		Microsoft ^(R) Windows Server ^(R) 2012 Standard
	Windows Server 2012 R2	Microsoft ^(R) Windows Server ^(R) 2012 R2 Datacenter
		Microsoft ^(R) Windows Server ^(R) 2012 R2 Standard
Windows Server 2016		Microsoft ^(R) Windows Server ^(R) 2016 Datacenter
		Microsoft ^(R) Windows Server ^(R) 2016 Standard

Windows is sometimes used generically, referring to Windows Server 2016, Windows 10, Windows 8.1, Windows 8, Windows Server 2012, Windows 7, and Windows Server 2008 R2.

■ 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

Nov. 2017: 3021-3-A09-30(E)

■ Copyright

Copyright (C) 2016, 2017, Hitachi, Ltd.

Copyright (C) 2017, Hitachi Solutions, Ltd.

Summary of amendments

The following table lists changes in this manual (3021-3-A09-30(E)) and product changes related to this manual.

Changes	Location
The configuration file for incident inheritance information was added to the list of files to back up.	<i>1.1.1, 1.1.3</i>
A description about the exclusion history and definition history of common exclusion-conditions was added to the section about using historical reports.	<i>1.4.3</i>
The detailed information of JP1 events displayed in the Event Details window now includes the following items: <ul style="list-style-type: none"> • Common exclude conditions group ID • Common exclude conditions group name • Common exclude conditions group target-for-exclusion 	<i>5.2</i>
A common exclusion-condition in extended mode can now exclude a JP1 event that satisfies the condition from automated-action execution.	<i>5.5.4</i>
The maximum number of hosts that can be set in a business group or monitoring group was increased to 2,500.	<i>8.7.2(5), 8.7.2(6)</i>
The following files were added to the lists of log files and directories: <ul style="list-style-type: none"> • Common exclusion history file • Common exclusion-conditions definition history file 	<i>10.2.4</i>
The following files were added to the lists of data to be collected for troubleshooting: <ul style="list-style-type: none"> • Common exclusion history file • Common exclusion-conditions definition history file 	<i>10.3.1, 10.3.2</i>
A corrective action for cases where a common exclusion-condition is used in extended mode was added to the actions to take when no JP1 event is displayed in the Event Console window.	<i>10.5.1(24)</i>
A description was added for actions to take when an automated action is not executed.	<i>10.5.1(63)</i>

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

Preface

This manual explains administration, operations, and troubleshooting for JP1/Integrated Management - Manager and JP1/Integrated Management - View. In this manual, JP1/Integrated Management - Manager and JP1/Integrated Management - View are generically referred to as *JP1/Integrated Management* or *JP1/IM*.

■ Intended readers

This manual is intended for professionals who use JP1/IM to manage and operate infrastructures developed for administering open platform systems. More specifically, it is intended for:

- System administrators who implement centralized monitoring of events that occur in the system
- System administrators who implement centralized monitoring of the system by associating the status of the infrastructure used to manage the system with the events that occur in the system.
- Those who have knowledge of operating systems and applications

■ Organization of this manual

This manual is organized into the following parts:

PART 1. Administration

This part explains the tasks necessary for maintaining a JP1/Integrated Management system, along with system evaluation methods.

PART 2. Operation

This part explains how to operate monitoring jobs that use JP1/Integrated Management.

PART 3. Linking with Other Products

This part provides an overview of monitoring tasks when linking with products other than integrated management products. It also describes the functionality that allows linkage to take place, how to build and use the monitoring environment, aspects of the user interface that relate to product linkage, and the command options used when linking with other products.

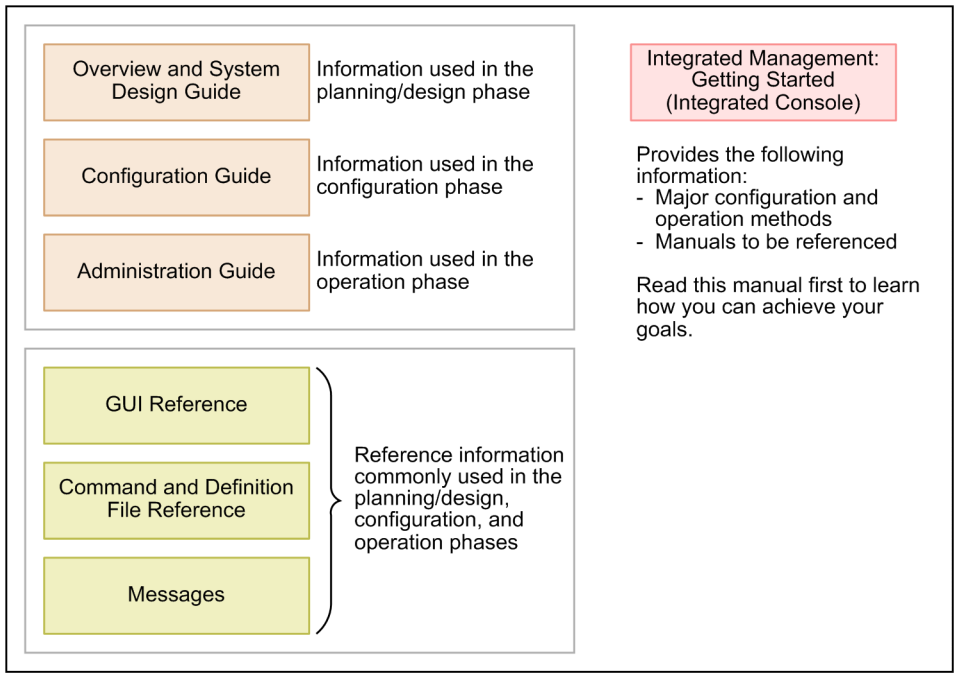
PART 4. Troubleshooting

This part explains the actions to take when problems occur in JP1/Integrated Management.

■ Manual suite






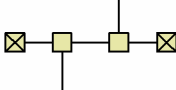


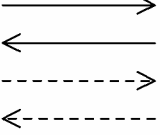
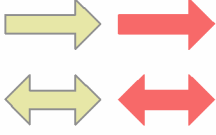


JP1/IM manuals provide necessary information according to the phase in the system life cycle (the phases include planning/design, configuration, and operation). Read the manual appropriate for the purpose.

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



■ Conventions: Diagrams

This manual uses the following conventions in diagrams:

- Computer (terminal) 
- Computer 
- Disk device, file 
- Screen 
- WAN 
- Network 
- Communication channel 
- Program 
- Flow of control 
- Flow of data 
- Flow of process or task 
- Error 

■ Conventions: Fonts and symbols

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

Text formatting	Convention
Bold	<p>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:</p> <ul style="list-style-type: none"> From the File menu, choose Open. Click the Cancel button. In the Enter name entry box, type your name.
<i>Italic</i>	<p>Italic characters indicate a placeholder for some actual text to be provided by the user or system. For example:</p> <ul style="list-style-type: none"> Write the command as follows: <code>copy source-file target-file</code> The following message appears: <code>A file was not found. (file = file-name)</code> <p>Italic characters are also used for emphasis. For example:</p> <ul style="list-style-type: none"> Do <i>not</i> delete the configuration file.
Monospace	<p>Monospace characters indicate text that the user enters without change, or text (such as messages) output by the system. For example:</p> <ul style="list-style-type: none"> At the prompt, enter <code>dir</code>. Use the <code>send</code> command to send mail. The following message is displayed: <code>The password is incorrect.</code>

The following table explains the symbols used in this manual:

Symbol	Convention
	<p>In syntax explanations, a vertical bar separates multiple items, and has the meaning of OR. For example: <code>A B C</code> means A, or B, or C.</p>
{ }	<p>In syntax explanations, curly brackets indicate that only one of the enclosed items is to be selected. For example: <code>{A B C}</code> means only one of A, or B, or C.</p>
[]	<p>In syntax explanations, square brackets indicate that the enclosed item or items are optional. For example: <code>[A]</code> means that you can specify A or nothing. <code>[B C]</code> means that you can specify B, or C, or nothing.</p>
...	<p>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: <code>A, B, B, . . .</code> means that, after you specify A, B, you can specify B as many times as necessary.</p>
Δ	<p>Indicates a space. Δ₀: Zero or more spaces (space can be omitted). Δ₁: One or more spaces (space cannot be omitted).</p>
▲	<p>Indicates a tab. Example:</p>

Symbol	Convention
	▲ A means that a tab character precedes A.

Conventions for mathematical expressions

This manual uses the following symbols in mathematical expressions:

Symbol	Meaning
x	Multiplication sign
/	Division sign

■ 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	<i>View-path</i>	<i>system-drive</i> : \Program Files\Hitachi\JP1CoView
JP1/IM - Manager	<i>Manager-path</i>	<i>system-drive</i> : \Program Files\Hitachi\JP1IMM
	<i>Console-path</i>	<i>system-drive</i> : \Program Files\Hitachi\JP1Cons
	<i>Scope-path</i>	<i>system-drive</i> : \Program Files\Hitachi\JP1Scope
JP1/Base	<i>Base-path</i>	<i>system-drive</i> : \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*.

■ 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**.

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.

Contents

Notices	2
Summary of amendments	6
Preface	7

Part 1: Administration

1	JP1/IM System Maintenance	18
1.1	Managing the configuration information	19
1.1.1	Backup (in Windows)	19
1.1.2	Recovery (in Windows)	25
1.1.3	Backup (in UNIX)	25
1.1.4	Recovery (in UNIX)	29
1.2	Managing the databases	30
1.2.1	Database reorganization	30
1.2.2	Database backup and recovery	32
1.2.3	Re-creating a database and changing its settings	38
1.3	Managing the disk capacity	48
1.3.1	Managing the IM database capacity	48
1.3.2	Managing the log file size	49
1.3.3	Managing dump files	49
1.4	Using historical reports	50
1.4.1	Outputting events to a CSV file	50
1.4.2	Correlation event generation history	50
1.4.3	Exclusion history and definition history of common exclusion conditions	51
1.5	Migrating the configuration information and databases	52
1.5.1	Configuration information and databases to be migrated	52
1.6	Managing certificates for the communication encryption function	54
1.6.1	Managing the effective duration of the server certificate	54
1.6.2	Managing keystores	54
2	Changing the Configuration of JP1/IM	56
2.1	Changing the JP1/IM settings information	57
2.2	Tasks necessary when a host name is changed	58
2.2.1	Tasks necessary immediately after the host name of a manager or agent is changed	58
2.2.2	Tasks to be performed when the host name of a manager or agent is changed	58
2.2.3	Procedure for re-distributing the system configuration when the host name of a manager or agent is changed	60

- 2.2.4 Tasks to be performed when the host name of a mail server is changed 60
- 2.2.5 Tasks to be performed before a logical host name is changed in a cluster system 60
- 2.3 Tasks necessary when an IP address is changed 62
 - 2.3.1 Tasks necessary immediately after the IP address of a manager or agent is changed 62
 - 2.3.2 Tasks to be performed when the IP address of a manager or agent is changed 62
 - 2.3.3 Procedure for restarting the system when the IP address of a manager or agent is changed 62
 - 2.3.4 Tasks to be performed when the IP address of a mail server is changed 63
- 2.4 Tasks necessary when the date of a manager or agent is changed 64
 - 2.4.1 Resetting the date/time of a manager or agent to a past date/time 64
 - 2.4.2 Advancing the system time 66
- 2.5 Tasks necessary when the date of a monitored host in a remote monitoring configuration is changed 67
 - 2.5.1 Resetting the date/time of a monitored host in a remote monitoring configuration to a past date/time 67
 - 2.5.2 Advancing the date/time of a monitored host in a remote monitoring configuration 67
- 2.6 Tasks necessary when the passwords of a monitored host in a remote monitoring configuration are changed 68
- 2.7 Notes on changing the monitoring configuration from remote to agent 69
 - 2.7.1 Notes on log file traps 69
 - 2.7.2 Notes on event log traps 69

Part 2: Operation

3 Starting and Stopping JP1/IM - Manager 70

- 3.1 Starting JP1/IM - Manager 71
 - 3.1.1 In Windows 71
 - 3.1.2 In UNIX 72
 - 3.1.3 Operations in a cluster system 73
 - 3.1.4 Operating a logical host in a non-cluster system 74
- 3.2 Stopping JP1/IM - Manager 75
 - 3.2.1 In Windows 75
 - 3.2.2 In UNIX 75
 - 3.2.3 Operations in a cluster system 76
 - 3.2.4 Operating a logical host in a non-cluster system 76
- 3.3 Automatic startup and automatic stop setting examples when a logical host operates in a non-cluster system 77
 - 3.3.1 Setting up automatic startup and automatic stop when a logical host operates in a non-cluster system (for Windows) 77
 - 3.3.2 Setting up automatic startup and automatic stop when a logical host operates in a non-cluster system (for AIX) 77
 - 3.3.3 Setting up automatic startup and automatic stop when a logical host operates in a non-cluster system (for Linux) 78
 - 3.3.4 Setting up automatic startup and automatic stop on both the physical host and the logical host 79
- 3.4 Notes on starting and stopping 81

4	JP1/IM - Manager Login and Logout	82
4.1	Logging in to JP1/IM - Manager	83
4.1.1	Using the GUI to log in to JP1/IM - Manager	83
4.1.2	Using a command to log in to JP1/IM - Manager	84
4.2	Logging out of JP1/IM - Manager	86
5	System Monitoring from Central Console	87
5.1	Viewing JP1 events	88
5.1.1	Items displayed in the events list	88
5.1.2	Events displayed in the events list in the Event Console window	92
5.1.3	Applying a filter	96
5.2	Displaying detailed JP1 event information	97
5.2.1	Editing JP1 memo entries	99
5.3	Setting JP1 event response statuses	100
5.3.1	Settings for JP1 event response statuses	100
5.3.2	Setting a response status for JP1 events from the events list	101
5.3.3	Deleting severe events from the Severe Events page	101
5.4	Operating JP1 events from the Related Events window	102
5.4.1	Checking detailed information about repeated events and changing the response status	102
5.4.2	Checking detailed information about a correlation event and changing the response status	103
5.5	Applying a JP1/IM filter	106
5.5.1	Enabling a view filter to display only certain JP1 events	106
5.5.2	Displaying only severe events	106
5.5.3	Switching the event acquisition filter to be applied	107
5.5.4	Setting an additional common exclusion-condition to exclude a JP1 event from the monitoring target or action execution	111
5.6	Displaying an event by specifying an event display start-time	113
5.7	Narrowing the JP1 events to be displayed by specifying a time period	114
5.8	Searching for JP1 events	116
5.8.1	Search method	116
5.8.2	Displaying the search results	118
5.9	Customizing JP1 event information by operation	121
5.9.1	Displaying program-specific extended attributes of JP1 events (displaying program-specific extended attributes)	121
5.9.2	Displaying extended attributes of JP1 events (mapping of event information)	121
5.9.3	Adding a user-defined extended attribute to JP1 events that match a condition	124
5.9.4	Changing the severity level of JP1 events	125
5.9.5	Changing the message displayed for a JP1 event	128
5.10	Taking actions for the generation of a large number of events	132
5.10.1	General procedures and preparation for handling occurrence a large number of events	132
5.10.2	Preparing to suppress event forwarding from an agent	134

- 5.10.3 Handling the occurrence of a large number of events by suppressing event forwarding from an agent 137
- 5.10.4 Handling the occurrence of a large number of events by consolidating them on the manager 141
- 5.10.5 Setting a threshold for automatically suppressing event forwarding on an agent 142
- 5.10.6 Specifying repeated event conditions 143
- 5.10.7 Stopping, on the manager, a log file trap that issues a large numbers of events 148
- 5.10.8 Consolidated display when events with the same attributes occur consecutively 149
- 5.11 Handling JP1 events by linking with other products 151
- 5.11.1 Registering JP1 events as incidents in JP1/IM - Service Support (linking with JP1/IM - Service Support) 151
- 5.11.2 Displaying operating procedures for JP1 events (linking with JP1/Navigation Platform) 152
- 5.11.3 Checking the rule startup request status and making a rule startup request (linking with JP1/IM - Rule Operation) 152
- 5.11.4 Opening a monitor window of the application that issued JP1 events 155
- 5.11.5 Displaying performance reports for JP1 events when linking with JP1/PFM 156

6 System Monitoring from Central Scope 157

- 6.1 Monitoring from the Monitoring Tree window 158
- 6.1.1 Changing the status of monitoring nodes 158
- 6.1.2 Changing the monitoring status of monitoring nodes 159
- 6.1.3 Searching for monitoring nodes 160
- 6.1.4 Searching for status-change events 160
- 6.1.5 Displaying the attributes of monitoring nodes 161
- 6.1.6 Displaying guide information 161
- 6.1.7 Opening the Visual Monitoring window 162
- 6.1.8 Displaying a login user list 162
- 6.1.9 Saving the information in the Monitoring Tree window on the local host 162
- 6.2 Monitoring from the Visual Monitoring window 163
- 6.2.1 Opening the Monitoring Tree window from the Visual Monitoring window 163
- 6.2.2 Changing the status of monitoring nodes 164
- 6.2.3 Changing the monitoring status of monitoring nodes 164
- 6.2.4 Searching for monitoring nodes 165
- 6.2.5 Searching for status-change events 165
- 6.2.6 Displaying the attributes of monitoring nodes 166
- 6.2.7 Displaying guide information 166

7 System Operation Using JP1/IM 168

- 7.1 Executing a command 169
- 7.1.1 Executing a command by using Command Execution 169
- 7.1.2 Executing a command by using the Command button 171
- 7.1.3 User that executes commands 173
- 7.1.4 Checking command execution status and deleting a command 173
- 7.2 Executing automated actions and taking necessary steps 175

- 7.2.1 Checking the execution status of an automated action 175
- 7.2.2 Checking the execution results of automated actions 176
- 7.2.3 Checking the operating status of the automated action function 181
- 7.3 Opening other application windows from the Tool Launcher 183
- 7.3.1 Operations in the Tool Launcher window 183
- 7.3.2 Functions that can be operated from the Tool Launcher window 184

8 Managing the System Hierarchy Using IM Configuration Management 187

- 8.1 Managing hosts 188
- 8.2 Managing the system hierarchy 189
- 8.3 Managing the configuration of a virtual system 190
- 8.3.1 Registering a virtual system host 190
- 8.3.2 Displaying host information in a virtual system 190
- 8.3.3 Applying the management information to the Central Scope monitoring tree 190
- 8.4 Managing business groups 192
- 8.5 Managing profiles 193
- 8.6 Managing service operation status 194
- 8.6.1 Collecting service operation information 194
- 8.6.2 Service operation information display 195
- 8.7 Exporting and importing management information of IM Configuration Management 196
- 8.7.1 Exporting management information of IM Configuration Management 196
- 8.7.2 Importing management information of IM Configuration Management 200
- 8.7.3 Applying the imported management information of IM Configuration Management to a system 210

Part 3: Linking with Other Products

9 Linking with BJEX or JP1/AS 213

- 9.1 Overview of BJEX and JP1/AS linkage 214
- 9.1.1 System configuration when linking JP1/IM with a batch job execution system 214
- 9.2 JP1/IM functionality for BJEX and JP1/AS linkage 217
- 9.2.1 Handling response-waiting events in JP1/IM 217
- 9.2.2 Monitoring response-waiting events 219
- 9.2.3 Accumulation of response-waiting events 222
- 9.2.4 Responding to response-waiting events 223
- 9.2.5 Canceling response-waiting events 225
- 9.3 Configuring JP1/IM to link with BJEX and JP1/AS 227
- 9.3.1 Configuring JP1/IM - Manager 227
- 9.3.2 Configuring JP1/IM - View 228
- 9.3.3 Configuring JP1/Base 229
- 9.3.4 Communication settings between BJEX or JP1/AS and JP1/IM - Manager 229
- 9.3.5 Configuring BJEX or JP1/AS 230

9.4	Working with response-waiting events	231
9.4.1	Flow of tasks for responding to response-waiting events	231
9.4.2	Responding to response-waiting events	234
9.4.3	Manually releasing response-waiting events from the hold-and-accumulate state	234
9.4.4	Resuming monitoring of events in the hold-and-accumulate state	235
9.5	Command usage when linking with BJEX or JP1/AS	236
9.5.1	jcoimdef	236
9.5.2	jim_log.bat (Windows only)	236
9.5.3	jim_log.sh (UNIX only)	237

Part 4: Troubleshooting

10 Troubleshooting 238

10.1	Troubleshooting procedure	239
10.2	Log information types	240
10.2.1	Common message log	240
10.2.2	Integrated trace log	240
10.2.3	Operation log	242
10.2.4	Log files and directory list	242
10.3	Data that needs to be collected when a problem occurs	269
10.3.1	In Windows	269
10.3.2	In UNIX	280
10.4	Collecting data	293
10.4.1	In Windows	293
10.4.2	In UNIX	300
10.5	Troubleshooting	305
10.5.1	Dealing with common problems	305

Index 364

1

JP1/IM System Maintenance

This chapter explains JP1/IM system maintenance.

To ensure stable operation of JP1/IM, which forms the basis for system administration and operations, we recommend that you plan regular maintenance activities, including backing up definition files and maintaining the database.

1.1 Managing the configuration information

This section explains how to back up and recover a JP1 system.

If the system no longer operates due to a disk failure, it might not be possible to restore data used in JP1/IM. As a precaution in the event the unexpected occurs, certain types of files need to be backed up.

According to the explanation provided here, consider backup and recovery of JP1 as part of a backup plan for the entire system.

Note that you cannot use backup and recovery procedures for moving files between servers.

When you perform backup and recovery, all of the following items must match on the backup source and the recovery destination:

- Host name
- IP address
- PP model name
- PP version (match the format of *VVRRZZ*)
- Directory structure used by the product (permissions and the like must match)

It is assumed that OS and hardware on the source and the destination are able to perform the same operations.

If the above conditions are not met, you will need to move files.

See [1.5 Migrating the configuration information and databases](#) and perform the operations described there.

OS commands or backup software can be used for a full backup of the entire system. However, we recommend that you back up or recover data by using the commands provided with individual JP1/IM - Manager functions that do not depend on the OS commands or backup software. If you use OS commands or backup software, the following conditions must be met:

- Data is backed up when all JP1/IM - Manager services, including the IM database, have been stopped.
- Data is backed up when all file and registry information, including the information registered in the OS, is consistent.
- The backup target files are not sparse files.

If you back up and recover the definition information, also back up and recover the database.

Stop JP1/IM - View when you perform backup and recovery.

1.1.1 Backup (in Windows)

This subsection explains how to back up JP1/IM configuration information.

If you change the JP1/IM configuration, make a backup. When you make a backup of JP1/IM, be sure to make a backup of JP1/Base at the same time. For details about how to back up the definition files that are configured by JP1/Base users, see the *JP1/Base User's Guide*.

Make a backup using a method of your choice, such as copying files. If at all possible, perform backup procedures while the JP1/IM services are not running. If you must make a backup while these services are running, note the following:

- The definition files may be modified during execution in some cases. If a backup is made while a definition file is being modified, the backup file will be corrupted.
Immediately following the backup operation, compare the collected backup file with the original file to make sure their contents match.
- When you make a backup, do not lock the target file. If you need to lock the file, first log out from all viewers that are connected, and then copy the target file to another file. After you have copied it, compare the copied file with the original file to make sure their contents match, and then back up the copied file.
- When you restore the backed-up configuration information, the configuration is simply modified with the restored content, and the events that have already arrived at JP1/IM - Manager are not re-evaluated.

Of the files shown in the table below, back up all those that exist. If only some of the existing files are backed up, interaction with the remaining files might become inconsistent, preventing the system from operating correctly.

Also, if the system operates in a cluster configuration, back up each environment in the order of physical hosts, then logical hosts.

The table below shows the JP1/IM files to back up. For a logical host, replace *Console-path* in the table with *shared-folder\JP1Cons*, replace *Scope-path* with *shared-folder\JP1Scope*.

Table 1–1: JP1/IM files to back up

Product name	File name	Description
Common to all products	Backup files created in <i>6.3.4 Copying the common definition information during new installation (for Windows)</i> in the <i>JP1/Integrated Management - Manager Configuration Guide</i>	Common definition information backup file#1
JP1/IM - Manager	<i>user-selected-file-name</i>	<p>Private key used by the communication encryption function File specified for the following common definition information: JP1_DEFAULT \JP1BASE\SSL \PRIVATEKEYFILE \#2</p> <p>Server certificate used by the communication encryption function File specified for the following common definition information: JP1_DEFAULT \JP1BASE\SSL \CERTIFICATEFILE# 2</p> <p>Root certificate used by the communication encryption function File specified for the following common definition information: JP1_DEFAULT \JP1BASE\SSL \CACERTIFICATEFILE# E#2</p>

Product name		File name	Description
JP1/IM - Manager	Central Console	<i>Console-path</i> \conf\jplco_env.conf	IM environment definition file
		<i>Console-path</i> \conf\jplco_param.conf	IM parameter definition file
		<i>Console-path</i> \conf\jplco_param_V7.conf	IM parameter definition file
		<i>Console-path</i> \conf\jplco_service.conf	Extended startup process definition file
		<i>Console-path</i> \conf\jplco_system.conf	IM server system environment settings file
		<i>Console-path</i> \conf\action\actdef.conf	Automated action definition file
		<i>Console-path</i> \conf\console\actprofile\actprofile_ <i>JP1-user-name</i>	Action profile
		<i>Console-path</i> \conf\console\actprofile\actprofile2_ <i>JP1-user-name</i>	
		<i>Console-path</i> \conf\console\actprofile\actprofile_0950_ <i>JP1-user-name</i>	
		<i>Console-path</i> \conf\console\attribute*.conf	Definition file for extended event attributes
		<i>Console-path</i> \conf\console\attribute\extend*.conf	Definition file for extended event attributes (extended file)
		<i>Console-path</i> \conf\console\filter*.conf	Filter definition file
		<i>Console-path</i> \conf\console\filter\attr_list\common_exclude_filter_attr_list.conf	Common-exclusion-conditions display item definition file
		<i>Console-path</i> \conf\console\filter\auto_list\common_exclude_filter_auto_list.conf	Common-exclusion-conditions auto-input definition file
		<i>Console-path</i> \conf\console\mapping\mapping.conf	Event information mapping definition file
		<i>Console-path</i> \conf\console\monitor*.conf	Definition file for opening monitor windows
		<i>Console-path</i> \conf\console\object_type*	Definition file for object types
		<i>Console-path</i> \conf\console\profile\.system	System profile
		<i>Console-path</i> \conf\console\profile\defaultUser	JP1/IM - View user profile (default)
		<i>Console-path</i> \conf\console\profile\profile_ <i>JP1-user-name</i>	JP1/IM - View user profile
<i>Console-path</i> \conf\console\profile\systemColor.conf	System color definition file		
<i>Console-path</i> \www\console.html# ³	Web-based operation definition file		

Product name	File name	Description
	<i>Console-path</i> \default\console.conf#3	Communication environment definition file
	<i>Console-path</i> \conf\console\correlation\view_cor.conf	Settings file for the consolidated display of repeated events
	<i>Console-path</i> \conf\console\correlation\view_cor_JP1-user-name.conf	Settings file for the consolidated display of repeated events
	<i>Console-path</i> \conf\console\rmtcmd\cmdbtn.conf	Command button definition file
	<i>Console-path</i> \conf\health\jcohc.conf	Health check definition file
	<i>Console-path</i> \conf\hostmap\user_hostmap.conf	Event-source-host mapping definition file
	<i>Console-path</i> \conf\action\actnotice.conf	Automatic action notification definition file
	<i>Console-path</i> \conf\processupdate\processupdate.conf	Status event definition file
	<i>Console-path</i> \conf\guide\jco_guide.txt	Event guide information file
	<i>Console-path</i> \conf\system\event_storm*.conf	Repeated event condition definition file
	<i>Console-path</i> \conf\console\event_storm\attr_list\event_storm_attr_list.conf	Display item definition file for repeated event condition
	<i>Console-path</i> \conf\console\event_storm\auto_list\event_storm_auto_list.conf	Auto-input definition file for repeated event condition
	<i>Console-path</i> \conf\console\incident\incident.conf	Definition file for manually registering incidents
	<i>Console-path</i> \conf\console\incident\incident_info.conf	Configuration file for incident inheritance information
	<i>user-selected-folder</i> \ <i>user-selected-file-name</i>	Event guide message file
	All files under <i>Console-path</i> \conf\evgen\	Definition files for correlation event generation
	<i>user-selected-folder</i> \ <i>file-name.conf</i>	Correlation event generation definition file
	<i>Console-path</i> \conf\action\attr_list\attr_list.conf	File that defines which items are displayed for event conditions
	<i>Console-path</i> \conf\chsev\jcochsev.conf	Severity changing definition file

Product name	File name	Description
	<i>Console-path</i> \conf\chsev\attr_list\chsev_attr_list.conf	Display item definition file for severity change definition
	<i>Console-path</i> \conf\chsev\auto_list\chsev_auto_list.conf	Automatic input definition file for severity change definition
	<i>Console-path</i> \conf\mail\jimmail.conf	Email environment definition file
	<i>Console-path</i> \conf\chattr\jcochmsg.conf	Display message change definition file
	<i>Console-path</i> \conf\chattr\attr_list\chmsg_attr_list.conf	Display item definition file for a display message change definition
	<i>Console-path</i> \conf\chattr\auto_list\chmsg_auto_list.conf	Automatic input definition file for a display message change definition
Central Scope	<i>Scope-path</i> \conf\jcs_guide*.txt	Guide information file
	<i>Scope-path</i> \conf\jcs_hosts	Host information file
	<i>Scope-path</i> \conf\action_complete_on.conf	Settings file for completed-action linkage function
	<i>Scope-path</i> \conf\action_complete_off.conf	
	<i>user-selected-folder</i> \ <i>user-selected-file-name</i>	Definition file for automatic delete mode of status change event
	<i>user-selected-folder</i> \ <i>user-selected-file-name</i>	Definition file for monitoring object initialization mode
	<i>Scope-path</i> \conf\auto_dbbackup_on.conf	Backup recovery settings file for monitored object database
	<i>Scope-path</i> \conf\auto_dbbackup_off.conf	
	<i>Scope-path</i> \conf\evhist_warn_event_on.conf	Settings file for the maximum number of status change events
	<i>Scope-path</i> \conf\evhist_warn_event_off.conf	
	<i>user-selected-folder</i> \ <i>user-selected-file-name</i>	Guide message file
	<i>user-selected-folder</i> \ <i>user-selected-file-name</i>	Definition file for on memory mode of status change condition
IM Configuration Management	<i>Manager-path</i> \conf\imcf\jplcf_applyconfig.conf	Apply-IM-configuration-method definition file
	<i>Manager-path</i> \conf\imcf\jplcf_treedefaultpolicy.csv	Default monitoring policy definition file
	All files under <i>Manager-path</i> \data\imcf	System management information
	All files under <i>shared-folder</i> \JP1IMM\data\imcf	
	<i>Manager-path</i> \conf\agtless\targets\wmi.ini	Definition files regarding WMI authentication information
	<i>shared-folder</i> \JP1IMM\conf\agtless\targets\wmi.ini	

Product name	File name	Description
	<i>Manager-path</i> \conf\agtlless\targets\ssh.ini	Definition files regarding SSH authentication information
	<i>shared-folder</i> \JP1IMM\conf\agtlless\targets\ssh.ini	
JP1/IM - View	<i>View-path</i> \conf\webdata\en*.html	Web page call definition file
	<i>View-path</i> \conf\tuning.conf	IM - View settings file
	<i>View-path</i> \conf\ssl\nosslhost.conf	Non-encryption communication host configuration file
	<i>View-path</i> \default\view.conf.update	Communication environment definition file
	<i>View-path</i> \default\tree_view.conf.update	
	<i>View-path</i> \conf\sovtoolexec\en\!JP1_CS_APP0.conf	Start program definition file
	<i>View-path</i> \conf\sovtoolitem\en\!JP1_CS_FTOOL0.conf	Toolbar definition file
	<i>View-path</i> \conf\sovtoolitem\en\!JP1_CS_FTREE0.conf	Icon operation definition file
	<i>View-path</i> \conf\appexecute\en*.conf	Definition file for executing applications
	<i>View-path</i> \conf\function\en*.conf	Definition file for the tool launcher
	<i>user-selected-folder</i> \ <i>user-selected-file-name</i>	Configuration file for monitoring tree
	Files under <i>View-path</i> \image\icon\	Icon file
	Files under <i>View-path</i> \image\visual\	Visual icon file ^{#4}
	Files under <i>View-path</i> \image\map\	Background-image-file-name
	<i>View-path</i> \conf\jcfview\jcfview.conf	Operation definition file for IM Configuration Management - View
	<i>View-path</i> \conf\jrmview\jrmview.conf	Operation definition file for Rule Operation - View ^{#5}
<i>View-path</i> \default\jrmview_reg.conf	Common definition settings file ^{#5}	

#1: The common definition information backup file backs up the definition information of a logical host in a cluster system. This backup file is created during setup of the cluster system. This backup file backs up the definition information of JP1/IM as well as JP1/Base, JP1/AJS, and Version 06-02 and later of JP1/Power Monitor. For details, see 6.1.3(5) *Setting common definition information* in the *JP1/Integrated Management - Manager Configuration Guide*.

#2: On a logical host, JP1_DEFAULT is the logical host name.

#3: This file exists only on a physical host.

#4: Files added by the user are backed up.

#5: This file is used by JP1/IM - View (the part linked to JP1/IM - Rule Operation).

1.1.2 Recovery (in Windows)

This subsection explains how to recover JP1/IM configuration information.

Before you recover JP1/IM backup information, you must first recover JP1/Base. Make sure that the following prerequisite conditions are met, and then recover the backup files to their original locations.

Prerequisite conditions:

- JP1/Base has already been installed.
- JP1/IM - Manager has already been installed.
- To recover a logical host environment, JP1 must already be set up in the logical host environment.
- JP1/Base and JP1/IM - Manager are stopped.

Backup information is recovered only for the host of the environment that was backed up. To recover backup information, you must perform a recovery operation in each environment.

If the system operates in a cluster configuration, recover each environment in the order of physical hosts, then logical hosts.

1.1.3 Backup (in UNIX)

This subsection explains how to back up JP1/IM configuration information.

If you change the JP1/IM configuration, make a backup. When you make a backup of JP1/IM, be sure to make a backup of JP1/Base at the same time. For details about how to back up the definition files that are configured by JP1/Base users, see the *JP1/Base User's Guide*.

The available backup methods include the `tar` and `cpio` commands. You can also use a backup tool such as JP1/OmniBack II to make a backup. Make a backup using a method of your choice, such as copying files. If at all possible, perform backup procedures when JP1/IM daemons are not running. If you must make a backup while these daemons are running, note the following:

- The definition files may be modified during execution in some cases. If a backup is made while a definition file is being modified, the backup file will be corrupted.
Immediately following the backup operation, compare the collected backup file with the original file to make sure their contents match.
- When you make a backup, do not lock the target file. If you need to lock the file, first log out from all viewers that are connected, and then copy the target file to another file. After you have copied it, compare the copied file with the original file to make sure their contents match, and then back up the copied file.
- When you restore the backed-up configuration information, the configuration is simply modified with the restored content, and the events that have already arrived at JP1/IM - Manager are not re-evaluated.

Of the files shown in the table below, back up all those that exist. If only some of the existing files are backed up, interaction with the remaining files might become inconsistent, preventing the system from operating correctly.

Also, if the system operates in a cluster configuration, back up each environment in the order of physical hosts, then logical hosts.

The table below shows the JP1/IM files to back up. For a logical host, replace `/etc/opt` in the table with *shared-directory*.

Table 1–2: JP1/IM files to back up

Product name	File name	Description	
Common to all products	Backup files created in 7.3.4 <i>Copying the common definition information during new installation (for UNIX) in the JP1/Integrated Management - Manager Configuration Guide</i>	Common definition information backup file ^{#1}	
JP1/IM - Manager	<i>user-selected-file-name</i>	Private key used by the communication encryption function File specified for the following common definition information: JP1_DEFAULT\JP1BASE\SSL\PRIVATEKEYFILE\#2	
		Server certificate used by the communication encryption function File specified for the following common definition information: JP1_DEFAULT\JP1BASE\SSL\CERTIFICATEFILE#2	
		Root certificate used by the communication encryption function File specified for the following common definition information: JP1_DEFAULT\JP1BASE\SSL\CACERTIFICATEFILE#2	
JP1/IM - Manager	Central Console	/etc/opt/jplcons/conf/jplco_env.conf	IM environment definition file
		/etc/opt/jplcons/conf/jplco_param.conf	IM parameter definition file
		/etc/opt/jplcons/conf/jplco_param_v7.conf	IM parameter definition file
		/etc/opt/jplcons/conf/jplco_service.conf	Extended startup process definition file
		/etc/opt/jplcons/conf/jplco_system.conf	IM server system environment settings file
		/etc/opt/jplcons/conf/action/actdef.conf	Automated action definition file
		/etc/opt/jplcons/conf/console/actprofile/actprofile_ <i>JP1-user-name</i>	Action profile
		/etc/opt/jplcons/conf/console/actprofile/actprofile2_ <i>JP1-user-name</i>	
		/etc/opt/jplcons/conf/console/actprofile/actprofile_0950_ <i>JP1-user-name</i>	
		/etc/opt/jplcons/conf/console/attribute/*.conf	Definition file for extended event attributes
		/etc/opt/jplcons/conf/console/attribute/extend/*.conf	Definition file for extended event attributes (extended file)
/etc/opt/jplcons/conf/console/filter/*.conf	Filter definition file		

Product name	File name	Description
	/etc/opt/jplcons/conf/console/filter/attr_list/common_exclude_filter_attr_list.conf	Common-exclusion-conditions display item definition file
	/etc/opt/jplcons/conf/console/filter/auto_list/common_exclude_filter_auto_list.conf	Common-exclusion-conditions auto-input definition file
	/etc/opt/jplcons/conf/console/mapping/mapping.conf	Event information mapping definition file
	/etc/opt/jplcons/conf/console/monitor/*.conf	Definition file for opening monitor windows
	/etc/opt/jplcons/conf/console/object_type/*	Definition file for object types
	/etc/opt/jplcons/conf/console/profile/.system	System profile
	/etc/opt/jplcons/conf/console/profile/defaultUser	JP1/IM - View user profile (default)
	/etc/opt/jplcons/conf/console/profile/profile_ <i>JP1-user-name</i>	JP1/IM - View user profile
	/etc/opt/jplcons/conf/console/profile/systemColor.conf	System color definition file
	/opt/jplcons/www/console.html ^{#3}	Web-based operation definition file
	/etc/opt/jplcons/default/console.conf ^{#3}	Communication environment definition file
	/etc/opt/jplcons/conf/console/correlation/view_cor.conf	Settings file for the consolidated display of repeated events
	/etc/opt/jplcons/conf/console/correlation/view_cor_ <i>JP1-user-name</i> .conf	Settings file for the consolidated display of repeated events
	/etc/opt/jplcons/conf/console/rmtcmd/cmdbtn.conf	Command button definition file
	/etc/opt/jplcons/conf/health/jcohc.conf	Health check definition file
	/etc/opt/jplcons/conf/hostmap/user_hostmap.conf	Event-source-host mapping definition file
	/etc/opt/jplcons/conf/action/actnotice.conf	Automatic action notification definition file
	/etc/opt/jplcons/conf/processupdate/processupdate.conf	Status event definition file
	/etc/opt/jplcons/conf/guide/jco_guide.txt	Event guide information file
	/etc/opt/jplcons/conf/console/incident/incident.conf	Definition file for manually registering incidents
	/etc/opt/jplcons/conf/console/incident/incident_info.conf	Configuration file for incident inheritance information
	/etc/opt/jplcons/conf/system/event_storm/*.conf	Repeated event condition definition file
	/etc/opt/jplcons/conf/console/event_storm/attr_list/event_storm_attr_list.conf	Display item definition file for repeated event condition

Product name	File name	Description	
	/etc/opt/jplcons/conf/console/event_storm/ auto_list/event_storm_auto_list.conf	Auto-input definition file for repeated event condition	
	<i>user-selected-directory/user-selected-file-name</i>	Event guide message file	
	All files under /etc/opt/jplcons/conf/evgen/	Definition files for correlation event generation	
	<i>user-selected-directory/file-name.conf</i>	Correlation event generation definition file	
	/etc/opt/jplcons/conf/chsev/jcochsev.conf	Severity changing definition file	
	/etc/opt/jplcons/conf/action/attr_list/ attr_list.conf	File that defines which items are displayed for event conditions	
	/etc/opt/jplcons/conf/chsev/attr_list/ chsev_attr_list.conf	Display item definition file for severity change definition	
	/etc/opt/jplcons/conf/chsev/auto_list/ chsev_auto_list.conf	Automatic input definition file for severity change definition	
	/etc/opt/jplcons/conf/chattr/jcochmsg.conf	Display message change definition file	
	/etc/opt/jplcons/conf/chattr/attr_list/ chmsg_attr_list.conf	Display item definition file for a display message change definition	
	/etc/opt/jplcons/conf/chattr/auto_list/ chmsg_auto_list.conf	Automatic input definition file for a display message change definition	
	Central Scope	/etc/opt/jplscope/conf/jcs_guide*.txt	Guide information file
		/etc/opt/jplscope/conf/jcs_hosts	Host information file
		/etc/opt/jplscope/conf/ action_complete_on.conf	Settings file for completed-action linkage function
		/etc/opt/jplscope/conf/ action_complete_off.conf	
		<i>user-selected-directory/user-selected-file-name</i>	Definition file for automatic delete mode of status change event
		<i>user-selected-directory/user-selected-file-name</i>	Definition file for monitoring object initialization mode
		/etc/opt/jplscope/conf/auto_dbbackup_on.conf	Backup recovery settings file for monitored object database
		/etc/opt/jplscope/conf/ auto_dbbackup_off.conf	
	/etc/opt/jplscope/conf/ evhist_warn_event_on.conf	Settings file for the maximum number of status change events	
	/etc/opt/jplscope/conf/ evhist_warn_event_off.conf		
	<i>user-selected-directory/user-selected-file-name</i>	Guide message file	
	<i>user-selected-directory/user-selected-file-name</i>	Definition file for on memory mode of status change condition	
IM Configuration Management	/etc/opt/jplimm/conf/imcf/ jplcf_applyconfig.conf	Apply-IM-configuration -method definition file	

Product name	File name	Description
	/etc/opt/jplimm/conf/imcf/ jplcf_treedefaultpolicy.csv	Default monitoring policy definition file
	All files under /var/opt/jplimm/data/imcf/	System management information
	All files under <i>shared-directory</i> /jplimm/data/imcf/	
	/etc/opt/jplimm/conf/agtless/targets/ssh.ini	Definition files regarding SSH authentication information
	<i>shared-directory</i> /jplimm/conf/agtless/targets/ssh.ini	

#1: The common definition information backup file backs up the definition information of a logical host in a cluster system. This backup file is created during setup of the cluster system. This backup file backs up the definition information of JP1/IM as well as JP1/Base, JP1/AJS, and Version 06-02 and later of JP1/Power Monitor. For details, see 6.1.3(5) *Setting common definition information* in the *JP1/Integrated Management - Manager Configuration Guide*.

#2: On a logical host, JP1_DEFAULT is the logical host name.

#3: This file exists only on a physical host.

1.1.4 Recovery (in UNIX)

This subsection explains how to recover the JP1/IM configuration information.

Before you recover JP1/IM backup information, you must first recover JP1/Base. Make sure that the following prerequisite conditions are met, and then recover the backup files to their original locations.

Prerequisite conditions:

- JP1/Base has been installed, and the setup command has already been executed.
- JP1/IM - Manager has been installed, and the setup command has already been executed.
- To recover a logical host environment, JP1 must already be set up in the logical host environment.
- JP1/Base and JP1/IM - Manager are stopped.

Backup information is recovered only for the host of the environment that was backed up. To recover backup information, you must perform a recovery operation in each environment.

If the system operates in a cluster configuration, recover each environment in the order of physical hosts, then logical hosts.

1.2 Managing the databases

The JP1/IM system uses the following databases:

- Command execution log
- Monitored object database
- Host information database
- Event database
- File for accumulated response-waiting events
- IM database

The monitored object database and the host information database are used when the Central Scope functions are used. The file for accumulated response-waiting events is used by the response-waiting event management function. This section explains the procedure for backing up and recovering these databases, and the procedure for re-creating them.

1.2.1 Database reorganization

(1) Reorganization of the command execution log

There is no need to reorganize the command execution log.

(2) Reorganization of the monitored object database and the host information database

There is no need to reorganize the monitored object database or the host information database.

(3) Reorganization of the event database

There is no need to reorganize the event database.

(4) Reorganization of the file for accumulated response-waiting events

There is no need to reorganize the file for accumulated response-waiting events.

(5) Reorganization of the IM databases

This subsection explains the procedure for reorganizing the IM databases.

Among the IM databases, the integrated monitoring database does not have the problem of free space becoming fragmented. Therefore, reorganization of the IM database is not necessary if only the integrated monitoring database is used.

When data is repeatedly added to and deleted from the IM Configuration Management database, the free space in the IM database can become fragmented. This can prevent additional items from being registered before the maximum number of hosts or properties has been reached. In addition, registering, updating, and deleting database entries might take extra time.

To prevent such occurrences, reorganize the IM databases at times such as the following.

- When JP1/IM - Manager is stopped for regular backup operations
- During annual creation and implementation of a reorganization execution plan
- When the message KFPH00212-I or KFPH00213-W is output to the Windows Event Log (`syslog`)

When issues like the above occur, use the procedure below to release free space in the database. To release the free space in the database:

1. In Windows, check whether the IM database service (JP1/IM - Manager DB Server) is running.
2. Using the `jimdbreclaim` command, release the free space in the database.
3. Check whether any host information or profiles registered in the IM database are unnecessary, and delete those that are not needed.

If this procedure does not eliminate the occurrence of problems, you need to reorganize the IM database. The following describes the procedures for reorganizing the IM database on a physical host, and in a cluster environment.

(a) Reorganizing the IM database on a physical host

To reorganize the IM database on a physical host:

1. Check the service status.
 - In Windows, check whether the IM database service (JP1/IM - Manager DB Server) is running.
 - Check whether the JP1/IM-Manager service is stopped.
 - If JP1/IM - MO is being used, check whether the JP1/IM - Message Optimizer service of JP1/IM - MO on the connection source is stopped.
2. Stop the JP1/IM - Manager service.
If JP1/IM - MO is being used, also stop the JP1/IM - Message Optimizer service of JP1/IM - MO on the connection source.
3. Using the `jimdbroorg` command, reorganize the database.
For details about the `jimdbroorg` command, see *jimdbroorg* (in *Chapter 1. Commands*) in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.
4. Start the JP1/IM - Manager service.
If JP1/IM - MO is being used, also start the JP1/IM - Message Optimizer service of JP1/IM - MO on the connection source.

(b) Reorganizing the IM database in a cluster environment

In a cluster environment, execute the reorganization process on the executing host. Furthermore, the shared directory must be accessible.

To reorganize the IM database in a cluster environment:

1. Check the service status.
 - In Windows, check whether the IM database service (JP1/IM - Manager DB Server) is running.
 - Check whether the JP1/IM-Manager service and the cluster service (JP1/IM-Manager DB Cluster Service) of the IM database are stopped.

- If JP1/IM - MO is being used, check whether the JP1/IM - Message Optimizer service of JP1/IM - MO on the connection source is stopped.
2. Stop the JP1/IM - Manager service and the cluster database service.
If JP1/IM - MO is being used, also stop the JP1/IM - Message Optimizer service of JP1/IM - MO on the connection source.
 3. Using the `jimdborg` command, reorganize the database.
For details about the `jimdborg` command, see `jimdborg` (in *Chapter 1. Commands*) in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.
 4. Start the JP1/IM - Manager service and the cluster database service that you stopped in Step 1.
If JP1/IM - MO is being used, also start the JP1/IM - Message Optimizer service of JP1/IM - MO on the connection source.

1.2.2 Database backup and recovery

When you perform backup and recovery, all of the following items need to match on the backup source and the recovery destination:

- Host name
- IP address
- PP model name
- PP version (match the format of *VVRRZZ*)
- Directory structure used by the product (permissions and the like must match)

It is assumed that the OS and hardware on the source and the destination are able to perform the same operations.

If the above conditions are not met, you will need to move files.

See *1.5 Migrating the configuration information and databases* and perform the operations described there.

You can use OS commands or backup software to make a full backup of the entire system. However, we recommend that you back up or recover data by using the commands provided with individual JP1/IM - Manager functions that do not depend on OS commands or backup software. If you use OS commands or backup software, the following conditions must be met:

- Data is backed up when all JP1/IM - Manager services, including the IM database, have been stopped.
- Data is backed up when all file and registry information, including the information registered in the OS, is consistent.
- The backup target files are not sparse files.

Databases cannot be partially backed up and recovered. If a database is partially backed up or recovered, database associations become contradictory. In this case, incorrect data could be referenced.

Back up and recover definition information in addition to the database itself. If you back up only the database, relationships with the definition information might become inconsistent.

Stop JP1/IM - View when you perform backup and recovery.

(1) Command execution log backup and recovery procedures

The following explains the procedures for backing up and recovering the command execution log.

(a) Backup procedure

To back up the command execution log:

1. Stop JP1/IM - Manager.
2. Stop JP1/Base.
3. Back up the target files.
For details about which files to back up, see [1.2.2\(1\)\(c\) Files to back up](#).
4. Start JP1/Base.
5. Start JP1/IM - Manager.

(b) Recovery procedure

To recover the command execution log:

1. Stop JP1/IM - Manager.
2. Stop JP1/Base.
3. Place the backup files in their respective directories.
4. Start JP1/Base.
5. Start JP1/IM - Manager.



Important

When the log is recovered, the history of the automated actions taken and the commands executed from the Command Execution window between the time of backup and the time of recovery cannot be viewed.

(c) Files to back up

The files to back up are listed below.

In Windows:

Table 1–3: Files to back up (Windows)

Information type	Files to back up
Command execution log file	All files under <i>Base-path</i> \log\COMMAND\
	All files under <i>shared-folder</i> \jplbase\log\COMMAND\
Action information file	<i>Console-path</i> \log\action\actinf.log
	<i>shared-folder</i> \jplcons\log\action\actinf.log
Action hosts file	<i>Console-path</i> \log\action\acttxt{1 2}.log
	<i>shared-folder</i> \jplcons\log\action\acttxt{1 2}.log

In UNIX:

Table 1–4: Files to back up (UNIX)

Information type	Files to back up
Command execution log file	All files under <code>/var/opt/jplbase/log/COMMAND/</code>
	All files under <code>shared-directory/jplbase/log/COMMAND/</code>
Action information file	<code>/var/opt/jplcons/log/action/actinf.log</code>
	<code>shared-directory/jplcons/log/action/actinf.log</code>
Action hosts file	<code>/var/opt/jplcons/log/action/acttxt{1 2}.log</code>
	<code>shared-directory/jplcons/log/action/acttxt{1 2}.log</code>

For details about the command execution log file, see the *JP1/Base User's Guide*.

(2) Monitored object database backup and recovery procedures

The following explains the procedures for backing up and recovering the monitored object database. The monitored object database is used when the Central Scope functions are used.

(a) Backup procedure

To back up the monitored object database:

1. Stop JP1/IM - Manager.

2. Back up the target files.

The table below shows the files to back up.

Table 1–5: Files to back up

OS	Information type	Files to back up
Windows	Monitored object database	All files under <code>Scope-path\database\jcsdb\</code>
		All files under <code>shared-folder\jplscope\database\jcsdb\</code>
UNIX	Monitored object database	All files under <code>/var/opt/jplscope/database/jcsdb/</code>
		All files under <code>shared-directory/jplscope/database/jcsdb/</code>

3. Start JP1/IM - Manager.

(b) Recovery procedure

To recover the monitored object database:

1. Stop JP1/IM - Manager.

2. Place the backup files in directories.

3. Start JP1/IM - Manager.

(3) Host information database backup and recovery procedures

The following explains the procedures for backing up and recovering the host information database. The host information database is used when the Central Scope functions are used.

(a) Backup procedure

To back up the host information database:

1. Stop JP1/IM - Manager.
2. Back up the target files.

The table below shows the files to back up.

Table 1–6: Files to back up

OS	Information type	Files to back up
Windows	Host information database	All files under <i>Scope-path</i> \database\jcshosts\
		All files under <i>shared-folder</i> \jp1scope\database\jcshosts\
UNIX	Host information database	All files under /var/opt/jp1scope/database/jcshosts/
		All files under <i>shared-directory</i> /jp1scope/database/jcshosts/

3. Start JP1/IM - Manager.

(b) Recovery procedure

To recover the host information database:

1. Stop JP1/IM - Manager.
2. Place the backup files in directories.
3. Start JP1/IM - Manager.

(4) Event database backup and recovery procedures

For details about the procedures for backing up and recovering the event database, see the explanation on backup and recovery in the *JP1/Base User's Guide*.

When you are recovering the event database of a JP1/IM - Manager host, you must also back up and recover the command execution log at the same time. For details about the procedures for backing up and recovering the command execution log, see *1.2.2(1) Command execution log backup and recovery procedures*.

Important

When you are backing up and recovering the event database, you must also back up and recover the command execution log at the same time.

If you back up and recover only the event database, an inconsistency will occur in the association of JP1 event execution results and automated actions inside the event database.

The results of automated actions executed before the event database recovery may be displayed as the execution results of automated actions for JP1 events registered after the event database recovery.

(5) Backup and recovery procedures for the file for accumulated response-waiting events

The following explains the procedures for backing up and recovering the file for accumulated response-waiting events. This file is used by the response-waiting event management function.

(a) Backup procedure

1. Stop JP1/IM - Manager.

2. Back up the target files.

The table below shows the files to back up.

Table 1–7: Files to back up

OS	Files to back up
Windows	<i>Console-path</i> \log\response\resevent.dat
	<i>shared-folder</i> \jplcons\log\response\resevent.dat
UNIX	/var/opt/jplcons/log/response/resevent.dat
	<i>shared-directory</i> /jplcons/log/response/resevent.dat

3. Start JP1/IM - Manager.

(b) Recovery procedure

1. Stop JP1/IM - Manager.

2. Place the backup files in the appropriate directories.

3. Start JP1/IM - Manager.

(6) IM database backup and recovery procedures

This subsection explains the procedures for backing up and recovering the IM database on a physical host, and in a cluster environment.

Important

When you back up and recover the IM database, you must also back up and recover the event database. For details about the procedure for backing up and recovering the event database, see [1.2.2\(4\) Event database backup and recovery procedures](#).

Important

Depending on the method used to recover the event database, you might need to re-create the event database. Depending on the method used to re-create the event database, you might also need to re-create the IM database. In such a case, do not recover the IM database. If the IM database is recovered, information in the IM database might no longer match the information in the event database, resulting in an unexpected change to the JP1 event handling status when the handling status is changed.

Important

Do not recover the backup data that was acquired before `jimdbupdate` command execution from the pre-update IM database to the IM database after `jimdbupdate` command execution.

After you have executed the `jimdbupdate` command, use the `jimdbbackup` command again to acquire a backup.

(a) Procedures for backing up and recovering the IM database on a physical host

To back up the IM database on a physical host:

1. In Windows, check whether the IM database service (JP1/IM - Manager DB Server) is running.
2. Stop the following services:
 - JP1/IM-Manager service
 - In Windows, the cluster service (JP1/IM-Manager DB Cluster Service) of the IM database
 - If JP1/IM - MO is being used, the JP1/IM - Message Optimizer service of JP1/IM - MO on the connection source
3. Use the `jimdbbackup` command to make a backup of the target database.
For details about the `jimdbbackup` command, see *jimdbbackup* (in *Chapter 1. Commands*) in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.
4. Back up the target files.
For details about which files to back up, see *1.1.1 Backup (in Windows)* and *1.1.3 Backup (in UNIX)*.
5. Start the services that were stopped in step 2.

To recover the IM database on a physical host:

1. In Windows, check whether the IM database service (JP1/IM - Manager DB Server) is running.
2. Stop the following services:
 - JP1/IM-Manager service
 - In Windows, the cluster service (JP1/IM-Manager DB Cluster Service) of the IM database
 - If JP1/IM - MO is being used, the JP1/IM - Message Optimizer service of JP1/IM - MO on the connection source
3. Using the `jimdbrecovery` command, recover the target database.
For details about the `jimdbrecovery` command, see *jimdbrecovery* (in *Chapter 1. Commands*) in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.
4. Place the backed up files in their respective directories.
With IM configuration management enabled, place the backed up files in their respective directories.
5. Start the services that were stopped in step 2.

(b) Procedures for backing up and recovering the IM database in a cluster environment

The procedure for backing up the IM database in a cluster environment is described below. In the case of a cluster environment, execute the backup process on the executing host. Furthermore, the shared directory must be accessible.

To back up the IM database in a cluster environment:

1. Stop the JP1/IM - Manager service and the cluster database service.
If JP1/IM - MO is being used, also start the JP1/IM - Message Optimizer service of JP1/IM - MO on the connection source.
2. Using the `jimdbbackup` command, make a backup of the target database.
For details about the `jimdbbackup` command, see *jimdbbackup* (in *Chapter 1. Commands*) in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.
3. Back up the target files.
For details about which files to back up, see *1.1.1 Backup (in Windows)* and *1.1.3 Backup (in UNIX)*.
4. Start the JP1/IM - Manager service and the cluster database service that was stopped in Step 1.
If JP1/IM - MO is being used, also start the JP1/IM - Message Optimizer service of JP1/IM - MO on the connection source.

To recover the IM database in a cluster environment. If the system operates in a cluster configuration, perform recovery on the active host. You will also need to be able to access shared directories.

1. Stop the JP1/IM - Manager service and the cluster database service.
If JP1/IM - MO is being used, also stop the JP1/IM - Message Optimizer service of JP1/IM - MO on the connection source.
2. Using the `jimdbrecovery` command, recover the target database.
For details about the `jimdbrecovery` command, see *jimdbrecovery* (in *Chapter 1. Commands*) in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.
3. Place the backed up files in their respective directories.
With IM configuration management enabled, place the backed up files in their respective directories.
4. Start the JP1/IM - Manager service and the cluster database service that was stopped in Step 1.
If JP1/IM - MO is being used, also start the JP1/IM - Message Optimizer service of JP1/IM - MO on the connection source.

1.2.3 Re-creating a database and changing its settings

(1) Re-creating the command execution log

To re-create the command execution log:

1. Stop JP1/IM - Manager.
2. Stop JP1/Base.
3. Delete the command execution log file, the action information file, and the action hosts file shown in the table below.

In Windows:

Table 1–8: Files to delete (Windows)

Information type	Files to delete
Command execution log file	All files under <i>Base-path</i> \log\COMMAND\
	All files under <i>shared-folder</i> \jplbase\log\COMMAND
Action information file	<i>Console-path</i> \log\action\actinf.log
	<i>shared-folder</i> \jplcons\log\action\actinf.log
Action hosts file	<i>Console-path</i> \log\action\acttxt{1 2}.log
	<i>shared-folder</i> \jplcons\log\action\acttxt{1 2}.log

In UNIX:

Table 1–9: Files to delete (UNIX)

Information type	Files to delete
Command execution log file	All files under /var/opt/jplbase/log/COMMAND/
	All files under <i>shared-directory</i> /jplbase/log/COMMAND/
Action information file	/var/opt/jplcons/log/action/actinf.log
	<i>shared-directory</i> /jplcons/log/action/actinf.log
Action hosts file	/var/opt/jplcons/log/action/acttxt{1 2}.log
	<i>shared-directory</i> /jplcons/log/action/acttxt{1 2}.log

4. Start JP1/Base.
5. Start JP1/IM - Manager.

Restarting JP1/Base and JP1/IM - Manager and executing a command from JP1/IM - View or an automated action re-creates the command execution log.

(2) Procedure for re-creating the monitored object database and the host information database

To re-create the monitored object database and the host information database:

1. Stop JP1/IM - Manager.
2. Back up the files.
Back up the *Scope-path*\database\ folder.
3. Re-create the monitored object database.
Executing the `jcsdbsetup -f` command deletes the existing monitored object database, and then re-creates the object database.
4. Re-create the host information database.
First, delete the files from the *Scope-path*\database\jcs\hosts\ folder, and then execute the following command:
`jcshostsimport -r host-information-file (jcs_hosts)`

5. Start JP1/IM - Manager.

(3) Procedure for re-creating the event database

The procedure differs depending on the version of JP1/Base that is installed on the target host whose event database you are re-creating.

(a) Manager (JP1/Base 09-00 or later)

The procedure differs depending on whether the integrated monitoring database is used.

If the integrated monitoring database for JP1/IM - Manager is not used

Using the `jevdbinit` command of JP1/Base, initialize the event database.

For details about how to initialize the event database of JP1/Base, see the description about initializing the event database in the chapter that explains how to set up the Event Service environment in the *JP1/Base User's Guide*.

If you changed the serial numbers by executing the `jevdbinit` command with the `-s` option, you must re-create the command execution log.

For details about how to re-create the command execution log, see [1.2.3\(1\) Re-creating the command execution log](#).

If the integrated monitoring database for JP1/IM - Manager is used

You can use the following procedure to initialize the event database:

1. Stop JP1/IM - Manager.
2. Execute the JP1/Base `jevdbinit` command without the `-s` option.

If you execute the `jevdbinit` command without the `-s` option, the serial numbers in the pre-initialization event database are inherited.

If you changed the serial numbers by executing the `jevdbinit` command with the `-s` option, you must set up the integrated monitoring database again and re-create the command execution log.

Before setting up the integrated monitoring database again, unset up the database by executing the `jcodbunsetup` command.

For details about how to re-create the command execution log, see [1.2.3\(1\) Re-creating the command execution log](#).

For details about the `jevdbinit` command, see the chapter on commands in the *JP1/Base User's Guide*.

Note that if you execute the `jevdbinit` command with the `-s` option specified, you must use Central Scope to select the root monitoring node, change the status, and delete the status change event logs.

(b) Agent (JP1/Base 07-51 or earlier)

Using the `jevdbinit` command of JP1/Base, initialize the event database. There is no need to delete and re-create the event database.

For details about how to initialize the event database of JP1/Base, see the description about initializing the event database in the chapter that explains how to set up the Event Service environment in the *JP1/Base User's Guide*.

Important

If an agent initializes the event database, JP1/Base discards the events without registering them in the event database. Consequently, if the correct procedure is not followed, it might become impossible to transfer some of the events after the event database is initialized.

(c) Agent (JP1/Base 07-00 or earlier)

When an event database is re-created, the following problem occurs:

- At the JP1 event forwarding destination host, the processing performance for accepting, registering, and acquiring JP1 events deteriorates.

This is because re-creation initializes the event database at the forwarding source, creating a mismatch with the management information in the event database at the forwarding destination.

Important

If an agent initializes the event database, JP1/Base discards the events without registering them in the event database. Consequently, if the correct procedure is not followed, it might become impossible to transfer some of the events after the event database is initialized.

To prevent this problem from occurring, re-create event databases using the following procedure.

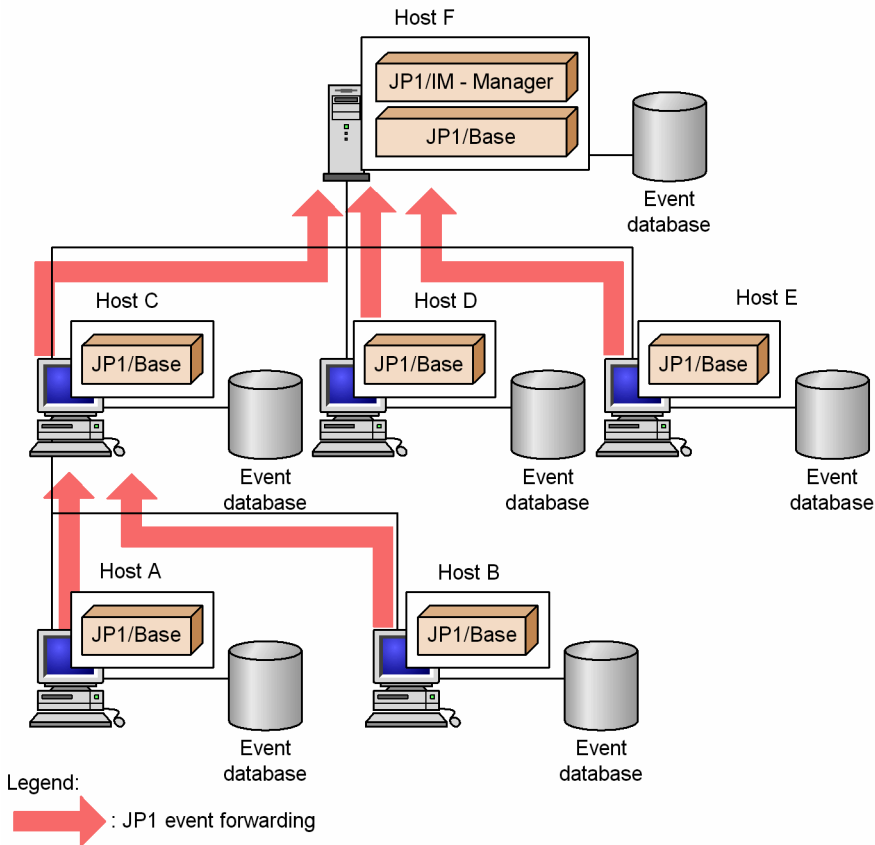
To re-create event databases:

1. Stop JP1/Base.
2. Stop JP1/Base at all forwarding destination hosts defined in the forwarding setting file (`forward`) of the JP1/Base you stopped in Step 1.
If data is forwarded from the JP1/Base at the forwarding destination host to yet another host, stop this forwarding destination as well. If JP1/IM - Manager has been installed on the host that is to be stopped, stop JP1/IM - Manager beforehand.
For details about the forwarding setting file (`forward`), see the sections that describe the settings for JP1 event forwarding in the chapter that explains how to set up an Event Service environment in the *JP1/Base User's Guide*.
3. Delete the event databases of the JP1/Bases you stopped in Steps 1 and 2.
If you need to view the content of the event databases, use the `jvexport` command of JP1/Base to output this content to a CSV file. Note that you cannot re-create an event database from an output CSV file.
For details about the `jvexport` command, see the chapter on commands in the *JP1/Base User's Guide*.
4. Start the JP1/Base (and JP1/IM - Manager) that you stopped in Step 2.
5. Start the JP1/Base that you stopped in Step 1.

Starting JP1/Base in Steps 4 and 5 re-creates the event databases.

For this example, assume that event databases will be re-created in the system configuration shown in the following figure.

Figure 1–1: Example showing hosts and forwarding destination hosts on which event databases are to be re-created



To re-create (delete) the event database of host A, it is necessary to delete the event databases of Hosts C and F, which are the forwarding destination hosts for JP1 events.

(4) Procedure for re-creating the file for accumulated response-waiting events

1. Stop JP1/IM - Manager.
2. Delete the file for accumulated response-waiting events.

Table 1–10: Files to delete

OS	Files to delete
Windows	<i>Console-path</i> \log\response\resevent.dat
	<i>shared-folder</i> \jplcons\log\response\resevent.dat
UNIX	<i>/var/opt/jplcons/log/response/resevent.dat</i>
	<i>shared-directory</i> /jplcons/log/response/resevent.dat

3. Start JP1/IM - Manager.

(5) Procedures for expanding the IM database size

This subsection explains how to expand the IM database size on a physical host, and in a cluster environment. If you create the IM database with `L` specified for the database size in the setup information file (`jimdbsetupinfo.conf`), the IM database size cannot be expanded.

(a) Procedure for expanding the IM database size on a physical host

The procedure for expanding the IM database size differs depending on whether you need to continue system monitoring without using the IM database during the expansion process. The procedure for each scenario is described below.

- Procedure when monitoring events without using the IM database during the expansion process
 1. Isolate the integrated monitoring database and the IM Configuration Management database.

Isolate the integrated monitoring database and the IM Configuration Management database so that Central Console only uses the JP1/Base event database.

Execute the following command, and then restart JP1/IM - Manager:

```
jcoimdef -db OFF
```

For details about the `jcoimdef` command, see `jcoimdef` (in *Chapter 1. Commands*) in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

If JP1/IM - MO is being used, also stop the JP1/IM - Message Optimizer service of JP1/IM - MO on the connection source.
 2. Back up the database.

Execute the `jimdbbackup` command with the `-m EXPAND` option specified.

For details about the `jimdbbackup` command, see `jimdbbackup` (in *Chapter 1. Commands*) in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.
 3. Unset up both the integrated monitoring database and the IM Configuration Management database.

Unset up only those databases that have been set up.
 4. Edit the setup information file.

Change the size specified in the database size (`IMDBSIZE`) of the setup information file.
 5. Set up both the integrated monitoring database and the IM Configuration Management database.

Set up only those databases that were unset up in Step 3.

During setup, you need to specify a database size that is larger than the backup size and the same database directory that was used during the backup.
 6. Recover the database.

Execute the `jimdbrecovery` command with the `-m EXPAND` option specified.

For details about the `jimdbrecovery` command, see `jimdbrecovery` (in *Chapter 1. Commands*) in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.
 7. Restart the JP1/IM - Manager service.

Execute the following command and then restart JP1/IM - Manager:

```
jcoimdef -db ON
```

For details about the `jcoimdef` command, see `jcoimdef` (in *Chapter 1. Commands*) in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

If JP1/IM - MO is being used, also start the JP1/IM - Message Optimizer service of JP1/IM - MO on the connection source.

- Procedure when stopping system monitoring via Central Console

1. Stop the JP1/IM - Manager service.

2. Back up the database.

Execute the `jimdbbackup` command with the `-m EXPAND` option specified.

For details about the `jimdbbackup` command, see *jimdbbackup* (in *Chapter 1. Commands*) in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

3. Unset up the integrated monitoring database and the IM Configuration Management database.

Unset up only those databases that have been set up.

4. Edit the setup information file.

Change the size specified in the database size (`IMDBSIZE`) parameter in the setup information file.

5. Set up the integrated monitoring database and the IM Configuration Management database.

Set up only those databases that you unset up in Step 3.

During setup, you need to specify a database size that is larger than the size of the database you backed up, and the same database directory that was used during the backup.

6. Recover the database.

Execute the `jimdbrecovery` command with the `-m EXPAND` option specified.

For details about the `jimdbrecovery` command, see *jimdbrecovery* (in *Chapter 1. Commands*) in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

7. Start the JP1/IM - Manager service.

(b) Procedure for expanding the IM database size in a cluster environment

The procedure for expanding the database size differs depending on whether you need to continue system monitoring via Central Console during the expansion process. The procedure for each scenario is described below.

- Procedure when continuing system monitoring via Central Console (with limited functionality)

1. Isolate the integrated monitoring database and the IM Configuration Management database.

Isolate the integrated monitoring database and the IM Configuration Management database so that Central Console only uses the JP1/Base event database.

Execute the following command, and then restart JP1/IM - Manager:

```
jcoimdef -db OFF -h logical-host-name
```

For details about the `jcoimdef` command, see *jcoimdef* (in *Chapter 1. Commands*) in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

If JP1/IM - MO is being used, also stop the JP1/IM - Message Optimizer service of JP1/IM - MO on the connection source.

2. Stop the cluster database service.

Stop the cluster database service registered in the cluster software.

3. Back up the database.

Execute the `jimdbbackup` command with the `-m EXPAND` option specified.

For details about the `jimdbbackup` command, see *jimdbbackup* (in *Chapter 1. Commands*) in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

4. Unset up the integrated monitoring database and the IM Configuration Management database.
Unset up only those databases that have been set up.
 5. Edit the cluster setup information file.
Change the size specified in the database size (`IMDBSIZE`) of the cluster setup information file.
 6. Set up the integrated monitoring database and the IM Configuration Management database.
Set up only those databases that were unset up in Step 4.
During setup, you need to specify a database size that is larger than the backup size and the same database directory that was used during the backup.
 7. Recover the database.
Execute the `jimdbrecovery` command with the `-m EXPAND` option specified.
For details about the `jimdbrecovery` command, see *jimdbrecovery* (in *Chapter 1. Commands*) in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.
 8. Start the cluster database service.
Start the cluster database service you stopped in Step 2.
 9. Restart the JP1/IM - Manager service.
Execute the following command and then restart JP1/IM - Manager:
`jcoimdef -db ON -h logical-host-name`
For details about the `jcoimdef` command, see *jcoimdef* (in *Chapter 1. Commands*) in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.
If JP1/IM - MO is being used, also start the JP1/IM - Message Optimizer service of JP1/IM - MO on the connection source.
- Procedure when stopping system monitoring via Central Console
 1. Stop the JP1/IM - Manager service and the cluster database service.
Stop the JP1/IM - Manager service and the cluster database service registered in the cluster software.
 2. Back up the database.
Execute the `jimdbbackup` command with the `-m EXPAND` option specified.
For details about the `jimdbbackup` command, see *jimdbbackup* (in *Chapter 1. Commands*) in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.
 3. Unset up the integrated monitoring database and the IM Configuration Management database.
Unset up only those databases that have been set up.
 4. Edit the cluster setup information file.
Change the size specified in the database size (`IMDBSIZE`) parameter in the cluster setup information file.
 5. Set up the integrated monitoring database and the IM Configuration Management database.
Set up only those databases you unset up in Step 3.
During setup, you need to specify a database size that is larger than the size of the database you backed up, and the same database directory that was used during the backup.
 6. Recover the database.
Execute the `jimdbrecovery` command with the `-m EXPAND` option specified.

For details about the `jimdbrecovery` command, see *jimdbrecovery* (in *Chapter 1. Commands*) in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

7. Start the JP1/IM - Manager service and the cluster database service.

Start the JP1/IM - Manager service and cluster database service you stopped in Step 1.

(6) Procedure for changing the IM database port

To change the IM database port:

1. Stop JP1/IM - Manager service.

If JP1/IM - MO is being used, also stop the JP1/IM - Message Optimizer service of JP1/IM - MO on the connection source.

2. Back up the database.

Execute the `jimdbbackup` command with the `-m MAINT` option specified.

For details about the `jimdbbackup` command, see *jimdbbackup* (in *Chapter 1. Commands*) in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

3. Unset up both the integrated monitoring database and the IM Configuration Management database.

Unset up only those databases that have been set up.

4. Edit the setup information file.

Change the port number described in the setup information file.

5. Set up both the integrated monitoring database and the IM Configuration Management database.

Set up only those databases that were unset up in Step 3.

6. Recover the database.

Execute the `jimdbrecovery` command with the `-m MAINT` option specified.

For details about the `jimdbrecovery` command, see *jimdbrecovery* (in *Chapter 1. Commands*) in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

7. Start JP1/IM - Manager.

If JP1/IM - MO is being used, also start the JP1/IM - Message Optimizer service of JP1/IM - MO on the connection source.

(7) Procedure for rebuilding the IM database

The procedure below explains the procedure for rebuilding the IM database that is required when you change the manager's host name. After you change the host name of a physical or logical host, you need to rebuild the IM database. Note that when the host name of a logical host is changed, you need to re-register the service created in this procedure in the IM database service to be registered in the cluster software.

To rebuild the IM database:

1. Stop JP1/IM - Manager service.

If JP1/IM - MO is being used, also stop the JP1/IM - Message Optimizer service of JP1/IM - MO on the connection source.

2. Unset up both the integrated monitoring database and the IM Configuration Management database.

Unset up only those databases that have been set up.

3. Change the name of the host on which JP1/IM - Manager has been installed.
4. This step is not necessary if the host name is not changed.
5. Set up both the integrated monitoring database and the IM Configuration Management database.
Set up only those databases that were unset up in Step 2.
When you are setting up a logical host, you need to edit the logical host name in the cluster setup information file.
6. Start JP1/IM - Manager.
Start the JP1/IM - Manager of the host to be changed.
If JP1/IM - MO is being used, also start the JP1/IM - Message Optimizer service of JP1/IM - MO on the connection source.

 **Important**

If you rebuild the IM database after changing the host name, you cannot recover the database. Therefore, as needed, use the `jcoevtreport` command to output and save JP1 events, and use the `jcfexport` command to save the IM configuration management information. For details about commands, see *Chapter 1. Commands* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

If you do not change the host name, you can recover the database. For details, see [1.2.2 Database backup and recovery](#).

1.3 Managing the disk capacity

To ensure stable operation of JP1/IM, check the available disk space regularly.

1.3.1 Managing the IM database capacity

The integrated monitoring databases used by JP1/IM are designed not to increase invalid areas, even during continued use. As long as the required capacity is secured, there is no need to check the database during operations.

Because data is written to the database created at setup, you basically do not have to consider capacity increase if the capacity is properly estimated at setup.

For details about increasing the log file size, see [1.3.2 Managing the log file size](#).

When the number of JP1 events exceeds the storage limit of the integrated monitoring database, JP1 events are automatically deleted. Therefore, you need to output and save JP1 event information regularly to prevent data loss.

To manage the disk capacity using the output-and-save operation:

1. View the information related to output-and-save operations.

Executing the `jcoevtreport -showsv` command displays the information related to output-and-save operations. Based on this information, estimate the output-and-save frequency and the free space required for outputting and saving information.

The following table shows the items that are displayed.

Table 1–11: Displayed items

Displayed item	Description
Percentage of events that have not been saved	Shows the percentage of JP1 events within the integrated monitoring database that have not been output or saved (the ratio relative to the maximum number of entries in the integrated monitoring database).
Size of events that are have not been saved	Shows the data size of JP1 events within the integrated monitoring database that have not been output or saved (in megabytes). The size displayed is the size within the integrated monitoring database. CSV output will require 1.2 times the size of the displayed events that have not been output.
Settings for deletion warning notification	Shows the value set as the deletion warning notification level. If the deletion warning notification is set to OFF, a hyphen (-) is displayed.

2. Output and save the events that have not been output.

Executing the `jcoevtreport -save` command outputs to a CSV file all JP1 events that have not been output and saved.

For details about the `jcoevtreport` command, see *jcoevtreport* (in *Chapter 1. Commands*) in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

If too many JP1 events occurred and regular output-and-save operations were too late for them, you can issue a deletion warning notification event. A deletion warning notification event reports when the percentage of JP1 events that have not been output and saved exceeds the deletion warning notification level.

To set up a deletion warning notification:

1. Enable the issuance of deletion warning notification events.

Executing the `jcoimdef -dbntc ON` command enables the function that issues a deletion warning notification event when the percentage of JP1 events not output and saved within the integrated monitoring database exceeds the deletion warning notification level. This percentage is the ratio relative to the maximum number of entries in the integrated monitoring database. The default for the deletion warning notification event is `OFF`.

2. Specify a deletion warning notification level.

Executing the `jcoimdef -dbntcpos 70` command sets the percentage of JP1 events for issuing a deletion warning notification event to 70%.

For details about the `jcoimdef` command, see *jcoimdef* (in *Chapter 1. Commands*) in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

For details about when the IM Configuration Management database is used, see *1.2.1(5) Reorganization of the IM databases*.

1.3.2 Managing the log file size

One of the factors that can cause insufficient disk capacity is an increase in the size of log files.

In the case of JP1/IM and JP1/Base, if you estimate the log file size in advance, there is no need to consider the possibility of increasing the log file size. This is because JP1/IM and JP1/Base use a method that outputs log files by switching between multiple log files.

For the OS and other products on the same host, check their specifications and make sure that their log file size will not increase.

1.3.3 Managing dump files

If JP1/IM, JP1/Base, or a user program terminates abnormally because of a problem, a dump file such as a core dump file (in UNIX) might be output in some cases.

These dump files are large. Therefore, when a problem occurs, collect the necessary data and then delete the dump files.

In Windows, if an application error occurs in a process, the Windows Error Reporting dialog box opens. When this dialog box opens, the system goes into a response-waiting state and cannot restart. Therefore, you need to disable error reporting based on the screen display.

For details about collecting data for troubleshooting, see *10. Troubleshooting*.

1.4 Using historical reports

JP1/IM manages historical information, such as information about JP1 events that occur during operations and JP1/IM processing information. This historical information is useful during maintenance of JP1/IM.

1.4.1 Outputting events to a CSV file

The function that outputs JP1 events to a CSV file is called the *event report output*. The following three methods are available for outputting JP1 events to a CSV file:

- Outputting a snapshot of event information to a CSV file
A snapshot means extraction of information at a specific time. The snapshot of event information displayed in JP1/IM - View can output JP1 events that are filtered according to the operation. For example, a snapshot showing the host or product where a problem has occurred, or a snapshot showing the corrective action being taken can be used as a system problem report.
For details about how to output to a CSV file the events list displayed in the Event Console window, see [5.1 Viewing JP1 events](#).
- Outputting the content of the event database to a CSV file
Using the `jvlexport` command, you can output the content of the event database managed by JP1/Base to a CSV file. If you wish to use as historical or statistical information JP1 events that need not be forwarded to the manager, such as normal termination of JP1/AJS jobs, you can use the `jvlexport` command to output the content of the agent's event database to a CSV file.
For details about the `jvlexport` command, see the chapter that explains commands in the *JP1/Base User's Guide*.
- Outputting the content of the integrated monitoring database to a CSV file
Using the `jcoevtreport` command, you can output the JP1 events registered in the integrated monitoring database to a CSV file. You can use this method when you wish to output the JP1 events registered in the integrated monitoring database, such as a list of JP1 events that occurred last week, or specified events only.
For details about the `jcoevtreport` command, see `jcoevtreport` (in *Chapter 1. Commands*) in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

1.4.2 Correlation event generation history

The correlation event generation history file shows the status of the correlation event generation service and the content of the correlation event generation process.

By viewing the correlation event generation history file, you can check whether correlation events are being generated according to the defined correlation event generation condition. For example, if a large number of historical reports have been issued in which a certain generation condition was not met, the combination of JP1 events for which correlation events are to be generated may not be appropriate, or the timeout period may be too short.

During regular reassessment of the generation condition, refer to the correlation event generation history file.

1.4.3 Exclusion history and definition history of common exclusion conditions

The history of common exclusion conditions is logged into the following files:

- Common exclusion history file

This file contains the information of JP1 events that were not collected or included in automated-action execution due to common exclusion-conditions and the information of common exclusion-conditions that caused the exclusion. This file also contains the history of operations to apply or change common exclusion definitions. The contents of common exclusion-conditions definitions that caused exclusion can be found in the common exclusion-conditions definition history file.

- Common exclusion-conditions definition history file

This file contains the history of operations to apply or change common exclusion-conditions definitions and the contents of the applied or changed common exclusion-conditions definitions.

You can view the common exclusion history file to check that JP1 events are excluded by common exclusion-conditions as intended.

For example, if an expected JP1 event does not appear in the event console or an expected automated action is not executed, a common exclusion-condition might unexpectedly exclude the JP1 event from the target to be collected or automated-action execution. Check the common exclusion history file to know whether any JP1 event is excluded unexpectedly.

For details about the files, see *3.2.7(5) Information included in a common exclusion history file* and *3.2.7(6) Information included in a common exclusion-conditions definition history file* of the manual *JP1/Integrated Management - Manager Overview and System Design Guide*.

1.5 Migrating the configuration information and databases

1.5.1 Configuration information and databases to be migrated

The configuration information of JP1/IM needs to be migrated when one of the items listed below is different at the migration-destination host. Note that you cannot migrate a database.

- Host name
- IP address
- PP version
- Directory structure used by the product (including permissions)

This subsection explains the configuration information of JP1/IM that is migrated.

(1) JP1/IM - Manager (Central Console)

During migration to another host, the definitions in the automated action definition file are the only definitions that can be migrated.

Other definitions must be re-created on the host at the migration destination.

(2) JP1/IM - Manager (Central Scope)

You can use the `jcsdbexport` and `jcsdbimport` commands to migrate the information of the monitored object database.

Other definitions must be re-created on the host at the migration destination.

Before migrating the information of the monitored object database, make sure that the host name and IP address of the local host, which are set in the status change condition and common condition of the monitored object, are correct.

(3) JP1/IM - Manager (IM Configuration Management)

You can use the `jcfexport` and `jcfimport` commands to migrate the information of IM configuration management.

To apply the imported IM configuration management information to the system, see [8.7.3 Applying the imported management information of IM Configuration Management to a system](#).

If the manager host name of the migration source is set in the profile information of the imported setting file, review the profile settings.

(4) JP1/IM - View

The definition file of JP1/IM - View must be re-created on the host at the migration destination.

(5) IM database

The IM database cannot be migrated. You need to rebuild the IM database on the host at the migration destination. For details about how to rebuild the IM database, see [1.2.3\(7\) Procedure for rebuilding the IM database](#).

(6) Event database

The event database cannot be migrated. You need to rebuild the event database on the host at the migration destination. For details about how to rebuild the event database, see the *JP1/Base User's Guide*.

1.6 Managing certificates for the communication encryption function

When you use the communication encryption function, you need to manage certificates and private keys.

To ensure continued stable operation of JP1/IM, you need to renew the server certificate before its effective duration expires.

Additionally, you need to correctly set the access permissions to the certificate and private key.

1.6.1 Managing the effective duration of the server certificate

The communication encryption function of JP1/IM is designed not to work if the server certificate of the manager host expires.

To ensure continued stable operation of JP1/IM, you need to renew the server certificate before its effective duration expires.

For details about how to update the server certificate, see *8.4.2 Changing configured certificates* in the *JP1/Integrated Management - Manager Configuration Guide*.

To check the effective duration of the server certificate, use the `openssl` command. Executing this command displays the server certificate information. Based on this information, consider when to update the server certificate.

For details about the settings required for executing the `openssl` command and related notes, see the *JP1/Base User's Guide*.

1.6.2 Managing keystores

When the communication encryption function is enabled, JP1/IM - Manager deletes and creates keystores when it starts, and deletes keystores when it stops. If the communication encryption function is disabled, JP1/IM - Manager deletes keystores when it starts.

The keystores for JP1/IM - Manager store the following files:

- Private key
- Server certificate
- Certificate issued by an intermediate certificate authority (if used)

If the keystores were not able to be deleted when JP1/IM - Manager was starting or stopping, manually delete them. Perform the following procedure to manually delete the unnecessary keystores:

1. Make sure that JP1/IM - Manager is stopped.
2. Delete the unnecessary keystores.

For details about the keystore storage destination, see *8.4.4(3) Keystores for JP1/IM - Manager* in the *JP1/Integrated Management - Manager Configuration Guide*.

 **Important**

When a private key or a keystore for JP1/IM - Manager is obtained, someone might be able to decrypt encrypted communication data. Therefore, the JP1/IM - Manager administrator must strictly manage the private key and the keystore for JP1/IM - Manager. The folder that stores the private key or the keystore for JP1/IM - Manager must be set so that it cannot be accessed by ordinary users.

2

Changing the Configuration of JP1/IM

This chapter explains the tasks necessary for changing the configuration of a JP1/IM system.

2.1 Changing the JP1/IM settings information

Before you change the JP1/IM operating environment by, for example, increasing the number of hosts monitored or operated by JP1/IM or by improving the efficiency of JP1/IM jobs (system operation monitoring) by making changes in JP1/IM operations, you need to clearly understand the purposes for making these changes. You also need to identify what setting tasks will be necessary as a result of changes in the operating environment.

For details about the reasons for changing the operating environment and about the setting tasks, see the *JP1/Integrated Management - Manager Overview and System Design Guide*. For details about how to carry out setting tasks, see the *JP1/Integrated Management - Manager Configuration Guide* and the *JP1/Base User's Guide*.

2.2 Tasks necessary when a host name is changed

This subsection explains the tasks you must perform when the host name of a manager or agent is changed, and the procedure for distributing the system configuration.

Some tasks might also become necessary when the host name of a mail server or the logical host name of a cluster system is changed. Perform these tasks based on the explanation provided here.

2.2.1 Tasks necessary immediately after the host name of a manager or agent is changed

This subsection explains the tasks you must perform immediately after the host name of a manager or agent is changed.

(1) Tasks necessary in JP1/Base

You must first terminate JP1/Base on the manager or agent whose host name has been changed, and then restart it.

(2) Tasks necessary in the IM database

When a manager's host name is changed, see [1.2.3\(7\) Procedure for rebuilding the IM database](#) and rebuild the IM database.

2.2.2 Tasks to be performed when the host name of a manager or agent is changed

(1) Host name that was set in the filtering condition

If the registered host name defined in the Severe Event Definitions window, the Settings for View Filter window, or the Detailed Settings for Event Receiver Filter window needs to be changed, you must change the registered host name settings in each setting window.

(2) Host name that was set in the Action Parameter Definitions window or in the automated action definition file

If the executing host name that was defined in the Action Parameter Definitions window or in the automated action definition file needs to be changed, you must change the executing host name settings in the Action Parameter Definitions window or in the automated action definition file.

After setting the host name, perform either of the following tasks:

- When starting JP1/IM - Manager, in the Action Parameter Definitions window of JP1/IM - View, click the **Apply** button to enable the definition.
- Reload the definition by executing the `jcachange` command.

(3) Host name that was set using a status change condition for the monitored object

If a host name that was set in the Status Change Condition Settings window or in the Common Condition Detailed Settings window needs to be changed, you must change the host name settings in each setting window.

After setting the host name, re-distribute the system configuration. For details, see *2.2.3 Procedure for re-distributing the system configuration when the host name of a manager or agent is changed*.

(4) Host name that was set in the correlation event generation definition file

If a host name defined as a condition for generating a correlation event in the correlation event generation definition file needs to be changed, you must change the host name settings in the correlation event generation definition file.

After setting the host name in the correlation event generation definition file, enable the correlation event generation definition by executing the `jcoegschange` command.

(5) Host name that was set in the severity changing definition file

If a host name defined as a severity changing condition in the severity changing definition file needs to be changed, you must change the host name settings in the severity changing definition file.

If the severity changing function is enabled for an event, enable the host name change by performing one of the following tasks:

- Execute the `jco_spm�_reload` command.
- Start JP1/IM - Manager.
- In the Add Severity Change Definition Settings window, click the **OK** button.
- In the View Severity Change Definitions window, click the **Apply** button.

(6) Host name that is set in the display message change definition file

If a host name defined as a display message change condition in the display message change definition file needs to be changed, you must change the host name that is set in the display message change definition file.

If the display message change function is enabled for an event, enable the host name change by performing one of the following tasks:

- Execute the `jco_spm�_reload` command.
- Start JP1/IM - Manager.
- In the Add Display Message Change Definitions window, click the **OK** button.
- In the Display Message Change Definitions window, click the **Apply** button.

(7) Host name described in CN and SAN of a server certificate

If the communication encryption function is enabled and the host name described in CN and SAN of a server certificate needs to be changed, you need to re-create the server certificate.

For details about how to re-create a server certificate, see *8.4.2 Changing configured certificates in the JP1/Integrated Management - Manager Configuration Guide*.

2.2.3 Procedure for re-distributing the system configuration when the host name of a manager or agent is changed

If the host name of a manager or agent is changed, you need to re-distribute the system configuration. The procedure is as follows:

1. Terminate all JP1/IM - Views that are connected to JP1/IM - Manager.
2. Terminate JP1/IM - Manager.
3. Execute the `jbsrt_distrib` command and redistribute the system configuration.
4. Start JP1/IM - Manager.
5. Start all JP1/IM - Views that are connected to JP1/IM - Manager.

For details about the system configuration distribution methods, see *1.8 Setting the system hierarchy (when IM Configuration Management is used) (for Windows)*, *1.9 Setting the system hierarchy (when IM Configuration Management is not used) (for Windows)*, or *2.8 Setting the system hierarchy (when IM Configuration Management is not used) (for UNIX)* in the *JP1/Integrated Management - Manager Configuration Guide*.

2.2.4 Tasks to be performed when the host name of a mail server is changed

(1) Host name that is set in the mail environment definition file

If the name of the host defined as the SMTP server and POP3 server in the mail environment definition file needs to be changed, you must change the host name in the mail environment definition file.

After changing the host name in the mail environment definition file, execute the `jimmail` command to enable the changed host name.

2.2.5 Tasks to be performed before a logical host name is changed in a cluster system

Before changing a logical host name in an environment in which a cluster system is running, firstly delete the logical host environment you want to change. Then, set up a new logical host so that the cluster system can work.

In Windows:

For details about how to delete a logical host, see *6.6.1 Deleting logical hosts (for Windows)* in the *JP1/Integrated Management - Manager Configuration Guide*. For details about how to set up a logical host, see *6.3 Installing and setting up logical hosts (new installation and setup) (for Windows)* or *6.5 Upgrade installation and setup of logical hosts (for Windows)* in the *JP1/Integrated Management - Manager Configuration Guide*.

In UNIX:

For details about how to delete a logical host, see *7.6.1 Deleting logical hosts (for UNIX)* in the *JP1/Integrated Management - Manager Configuration Guide*. For details about how to set up a logical host, see *7.3 Installing and setting up logical hosts (new installation and setup) (for UNIX)* or *7.5 Upgrade installation and setup of logical hosts (for UNIX)* in the *JP1/Integrated Management - Manager Configuration Guide*.

Important

In the case of a cluster system, after a host name is changed, JP1 events that were issued under the old host name are processed as follows:

- **Source host** in JP1/IM - View shows the old host name.
- When you search for an event, the result will be matched to the old host name.
- When the Event Details window is opened, an error message may be issued, such as The specified JP1 event could not be found.
- You cannot display the JP1/AJS - View monitor from a JP1 event that was issued under the old host name.
- In **Host** in the Action Log window, the Action Log Details window, and the List of Action Results window, the old host name is displayed.

2.3 Tasks necessary when an IP address is changed

This subsection explains the tasks you must perform when the IP address of a manager or agent is changed. It also explains the procedure for distributing the system configuration.

Some tasks might also become necessary when the IP address of a mail server is changed. Perform these tasks based on the explanation provided here.

2.3.1 Tasks necessary immediately after the IP address of a manager or agent is changed

This subsection explains the tasks you must perform immediately after the IP address of a manager or agent is changed.

(1) Necessary tasks in JP1/Base

You must first terminate JP1/Base on the manager or agent whose IP address has been changed, and then restart it.

(2) Necessary tasks related to the IM database

When a manager's IP address is changed, you must first terminate the IM database, and then restart it.

2.3.2 Tasks to be performed when the IP address of a manager or agent is changed

(1) IP address that was set using a status change condition for the monitoring object

If an IP address that was set in the Status-Change Condition Settings window or the Common Condition Detailed Settings window needs to be changed, you must change the IP address specification in each setting window.

If you are using IM Configuration Management, start IM Configuration Management - View before collecting host information.

After setting the IP address, restart the system. For details, see [2.3.3 Procedure for restarting the system when the IP address of a manager or agent is changed](#).

2.3.3 Procedure for restarting the system when the IP address of a manager or agent is changed

If the IP address of a manager or agent is changed, you need to restart JP1/IM - Manager and JP1/IM - View. The procedure is as follows:

1. Terminate all instances of JP1/IM - View that are connected to JP1/IM - Manager.
2. Terminate JP1/IM - Manager.

3. Start JP1/IM - Manager.

4. Start JP1/IM - View.

2.3.4 Tasks to be performed when the IP address of a mail server is changed

(1) IP address that was set in the mail environment definition file

If a host name defined as the SMTP server and POP3 server in the mail environment definition file needs to be changed, you must change the host name setting in the mail environment definition file.

After you change the IP address in the mail environment definition file, execute the `jimmail` command to enable the changed IP address.

2.4 Tasks necessary when the date of a manager or agent is changed

This subsection provides notes related to changing the date of a manager or agent while JP1/IM is running, along with the procedure. If the date of a monitored host in a remote monitoring configuration is being changed, see [2.5 Tasks necessary when the date of a monitored host in a remote monitoring configuration is changed](#).

Important

If you are using the communication encryption function, check whether the changed date is within the effective duration of the certificate being used. If the changed date is past the effective duration of the certificate, obtain a certificate whose effective duration accommodates the changed date.

2.4.1 Resetting the date/time of a manager or agent to a past date/time

When you change the date/time of a manager or agent, do not return it to a past date/time, as a rule. On a host where JP1/IM is running, resetting the system clock of the operating system to a past date/time affects the database significantly, which requires JP1/IM to be re-installed or the database to be set up again.

Even when you are correcting a system clock that is too fast or slow, setting the system time back may disrupt the order in which the execution results of automated actions are displayed, or it may cause a problem in the way the monitoring tree status change date/time is displayed. Such problems occur when resetting the system time causes inconsistencies in the data managed by JP1/IM - Manager and JP1/Base. JP1/IM - View is not affected.

Furthermore, if the system time is set back, events may not be correctly searched when you search for events by specifying the arrival time.

If you intentionally set the system date/time forward to a future date/time for testing purposes, and you then need to return the system date/time to the original settings, use the procedure below.

Important

If you are using a method to set the server's system date/time that does not reset it to a past date/time, such as a method using a Network Time Protocol (NTP) server, you can change the date/time without following the procedure described below. In this case, there is no need to stop JP1/Base.

(1) Resetting the manager's date/time back to the original date/time

1. Stop JP1/IM - Manager.
2. If the IM database is being used, stop the IM database.
3. Stop JP1/Base.
4. Reset the system to an earlier time.
5. When the system reaches the original time, start JP1/IM - Manager.
For example, if the system was reset from 02:00 to 01:00 in step 2, start JP1/IM - Manager when the system reaches 02:00.
However, if the IM database is being used, perform the following steps to start JP1/IM - Manager in step 4.

1. JP1/Base
2. IM database
3. JP1/IM - Manager

! Important

If you inadvertently start a service before the system time has reached the original time before the reset (that is, before 02-00 in step 5), the integrated monitoring database might become corrupted. If such corruption occurs, you need to rebuild the system.

Before resetting the time, back up the configuration information and database so that they can be recovered after the system is rebuilt.

The files that can be recovered are those that were backed up at a system time that was before the system time at the time of recovery. If the system time during the backup was not prior to the system time at the time of recovery, recover the files after the system time is past the backup time.

Alternatively, you can use the method described below to reset the system date and time. However, note that if you use this method, the information shown in step 5 and the event and host information in the IM database must be deleted.

Steps 3 and 6 are required only if you are using the IM database. To reset the date/time back to the original date/time:

1. Stop JP1/IM - Manager.

2. Stop JP1/Base.

3. Perform unsetup for the IM database.

For Windows, you need to start the JP1/IM-Manager DB Server service beforehand.

If the integrated monitoring database and IM Configuration Management database have been set up, you must remove both of those setups.

4. Reset the system date/time to the current date/time.

5. Delete the action information file, action hosts file, event database, and command execution log file.

The tables below show where the files to delete are stored.

In Windows:

Table 2–1: Files to delete (Windows)

File name	Storage location
Action information file	<i>Console-path</i> \log\action\actinf.log
	<i>shared-folder</i> \jplcons\log\action\actinf.log
Action hosts file	<i>Console-path</i> \log\action\acttxt{1 2}.log
	<i>shared-folder</i> \jplcons\log\action\acttxt{1 2}.log
Command execution log file	All files under <i>Base-path</i> \log\COMMAND\
	All files under <i>shared-folder</i> \jplbase\log\COMMAND\
Event database	IMEvent*.* files under <i>Base-path</i> \sys\event\servers\default\#
	IMEvent*.* files under <i>shared-folder</i> \jplbase\event\#

#: If a different path was specified in the event server index (index) file, the files under the specified path need to be deleted.

In UNIX:

Table 2–2: Files to delete (UNIX)

File name	Storage location
Action information file	/var/opt/jp1cons/log/action/actinf.log
	<i>shared-directory</i> /jp1cons/log/action/actinf.log
Action hosts file	/var/opt/jp1cons/log/action/acttxt{1 2}.log
	<i>shared-directory</i> /jp1cons/log/action/acttxt{1 2}.log
Command execution log file	All files under /var/opt/jp1base/log/COMMAND/
	All files under <i>shared-directory</i> /jp1base/log/COMMAND/
Event database	IMEvent*.* files under /var/opt/jp1base/sys/event/servers/default/#
	IMEvent*.* files under <i>shared-directory</i> /jp1base/event/#

#: If a different path was specified in the event server index (*index*) file, the files under the specified path need to be deleted.

6. Set up the IM database.
7. Start JP1/Base.
8. Start JP1/IM - Manager.

This completes resetting of the system data/time of the manager. If you are using Central Scope, perform the following tasks.

1. From JP1/IM - View, log in to JP1/IM - Manager (Central Scope).
2. From the Monitoring Tree window, choose the highest-order monitoring group and set its state to the initial state. Resetting all monitored nodes to their initial states eliminates inconsistencies in the data managed by Central Scope.

(2) Resetting the agent's date/time to the original date/time

When you reset the agent's date/time to the original date/time, you must also reset both the event database of JP1/Base on the applicable host and the JP1/Base date/time on the host at the event forwarding destination. For details such as the relevant procedure, see the explanation on necessary tasks when the system date and time is changed in the chapter about changing settings during operation of JP1/Base in the *JP1/Base User's Guide*.

2.4.2 Advancing the system time

Unlike in the case of resetting the system clock back, there is no need to stop JP1/IM or delete files in order to set the system clock forward.

If the IM database is used, do not change the time while starting or stopping the IM database.

2.5 Tasks necessary when the date of a monitored host in a remote monitoring configuration is changed

This subsection provides notes related to changing the date of a monitored host in a remote monitoring configuration, along with the procedure.

2.5.1 Resetting the date/time of a monitored host in a remote monitoring configuration to a past date/time

If you want to reset the date/time of a monitored host in a remote monitoring configuration after intentionally changing the date/time to a point in the future for testing or other purposes, you must delete the event log for the future date/time and the file that contains the collection status for remote monitoring on the host.

To reset the date/time:

1. If there is a remote monitoring event log trap that is running on the host, stop it.
2. Change the date/time of the host.
3. Confirm that the host does not have an event log whose date/time is later than the current date/time on the host. If there is such a log, delete the corresponding event log.
4. Back up the following file that contains the collection status, and then delete the original file:

- For a physical host

Manager-path\log\imcf\profiles*monitored-host-name*\al\event_log_trap\evt.wdef

- For a logical host

shared-folder\JP1IMM\log\imcf\profiles*monitored-host-name*\al\event_log_trap\evt.wdef

If you delete the wrong file by mistake, restore the file from the backup.

5. Restart the stopped remote monitoring event log trap.

If the date and time of the monitored host do not match the date and time of the machine where JP1/IM - Manager is running, remote-monitoring event log traps cannot be used for monitoring. When changing the date/time of a monitored host, also check the date/time of the host on which JP1/IM is running.

2.5.2 Advancing the date/time of a monitored host in a remote monitoring configuration

No tasks are necessary for setting the date/time of a monitored host in a remote monitoring configuration for a reason such as a clock delay.

2.6 Tasks necessary when the passwords of a monitored host in a remote monitoring configuration are changed

If you change the password of the manager that manages monitored hosts in a remote monitoring configuration, and the password of a monitored remote host, you must review and, if necessary, revise the settings in the Remote Monitoring Settings window or the System Common Settings window.

If you change the user name or domain name of a monitored remote host, you must review the settings in the Remote Monitoring Settings window or the System Common Settings window.



Note

When registering or changing a monitored remote host, you can store and manage the OS communication settings information as common settings of the system. To do so, use the System Common Settings window rather than the Remote Monitoring Settings window.

For details about the settings in the Remote Monitoring Settings window and the System Common Settings window, see *3.1.5 Changing the attributes of host information* in the *JP1/Integrated Management - Manager Configuration Guide*.

For details about the Remote Monitoring Settings window and the System Common Settings window, see the following sections in the manual *JP1/Integrated Management - Manager GUI Reference*.

- *4.7 Remote Monitoring Settings window*
- *4.20 System Common Settings window*

2.7 Notes on changing the monitoring configuration from remote to agent

This section provides notes on changing the monitoring configuration from a remote monitoring configuration using a log file trap (remote monitoring log file trap) and an event log trap (remote monitoring event log trap) to an agent configuration using a log file trap and event log trap.

For an overview of managing a monitored remote host, see *6.6 Managing remotely monitored hosts* in the *JP1/Integrated Management - Manager Overview and System Design Guide*.

2.7.1 Notes on log file traps

If you are changing the monitoring configuration of log file traps from a remote monitoring configuration to an agent monitoring configuration, note the following:

- Enable the extended regular expression in the common definition information.
- If a file monitoring interval (`-t` option) is not specified, the monitoring interval becomes shorter.
- When migrating the remote monitoring for a logical host, specify the name of the destination event server (`-s` option).

2.7.2 Notes on event log traps

If you are changing the monitoring configuration of event log traps from a remote monitoring configuration to an agent monitoring configuration, note the following:

- Enable the extended regular expression in the common definition information.
- When migrating the remote monitoring for a logical host, specify the event server name (`server`) in the JP1/Base event log trap action-definition file.
For details about the JP1/Base event log trap action-definition file, see the chapter on definition files in the *JP1/Base User's Guide*.
- When the specified `trap-interval` is 181 or more, change the value to 180 or less.
When the version of JP1/Base is 11-00 or later, `trap-interval` is not required to be set.
- If `trap-interval` is not specified, the monitoring interval becomes shorter.
When the version of JP1/Base is 11-00 or later, `trap-interval` is not required to be set.
- If you want a JP1 event to be issued when event log acquisition fails during event log monitoring (as in remote monitoring), define `jplevent-send` as 1 (notify).

3

Starting and Stopping JP1/IM - Manager

This chapter explains how to start and stop JP1/IM - Manager.

3.1 Starting JP1/IM - Manager

This section explains how to start JP1/IM - Manager.

Before you start JP1/IM - Manager, start all JP1/Base services required for monitoring. Before you restart JP1/Base services, JP1/IM - Manager must be stopped. If JP1/IM - Manager is not stopped, a problem might occur (for example, events cannot be displayed).

For details about starting JP1/Base services, see the chapter about starting and stopping JP1/Base in the *JP1/Base User's Guide*.

Furthermore, you must stop JP1/IM - Manager before you can restart the Event Service of JP1/Base. If you do not restart JP1/IM - Manager, you will have problems displaying events, for example.

The startup method varies depending on the OS that is being used. For details, see [3.1.1 In Windows](#) or [3.1.2 In UNIX](#).

3.1.1 In Windows

This subsection explains how to start JP1/IM - Manager when the host is a physical host whose OS is Windows.

The startup method when the IM database is being used is as follows.

To start up when the IM database is being used:

1. Start the IM database.
Start the JP1/IM - Manager DB Server service.
2. Start JP1/IM - Manager.
Start the JP1/IM - Manager service.

The startup method when the IM database is not being used is as follows.

To start up when the IM database is not being used:

1. Start JP1/IM - Manager.
Start the JP1/IM - Manager service.

To start the IM database and JP1/IM - Manager, you can use either a method that uses JP1/Base startup control or one that does not use startup control.

Startup control is a function that starts services according to a preset sequence. If startup control is set up, it first starts JP1/Base Control Service during Windows startup, and then it starts various services such as JP1/Base and JP1/IM - Manager.

If you want to automatically start individual services at system startup, use startup control of JP1/Base to control the start sequence of those services.

Before you can use startup control to start services, you must choose **Control Panel**, then **Administrative Tools**, and then **Services** in Windows. In the Services dialog box, you must set the startup method for the JP1/IM - Manager DB Server service and JP1/IM - Manager service to **Manual**. For details about startup control, see the chapter on setting up the service startup and stopping sequence (Windows only) in the *JP1/Base User's Guide*.

Starting the IM database

The default setting is that the IM database is not started using JP1/Base startup control.

To start the IM database without using startup control, choose **Control Panel** and then **Administrative Tools**, and then start the JP1/IM - Manager DB Server service from **Services**.

To start the IM database using startup control, delete # from the lines shown below in the start sequence definition file of JP1/Base. Also, replace *JP1/IM - Manager-path* in StopCommand with *Manager-path*.

```
# [Jp1IM-Manager DB]
#Name=JP1/IM-Manager DB Server
#ServiceName=HiRDBEmbeddedEdition_JM0
#StopCommand=Manager-path\bin\imdb\jimdbstop.exe
```

For details about startup control, see the chapter on setting up the service startup and stopping sequence (Windows only) in the *JP1/Base User's Guide*.

Starting JP1/IM - Manager

The default setting is that JP1/IM - Manager is started using the startup control of JP1/Base.

To start JP1/IM - Manager without using startup control, choose **Control Panel** and then **Administrative Tools**, and then start the JP1/IM - Manager DB Server service and JP1/IM - Manager service from **Services**.

Important

- When you use JP1/Power Monitor to start or stop the host on which JP1/IM - Manager starts, specify a command such as a batch file for executing `net stop IM-database-service-name` in the StopCommand parameter of the start sequence definition file of JP1/Base.
- If you are using the integrated monitoring database, set it up; if you are using IM Configuration Management, set up the IM Configuration Management database. If you are using Central Scope, set up the monitoring object database, and then start JP1/IM - Manager.

3.1.2 In UNIX

In UNIX, an OS function starts JP1/IM - Manager (if the automatic startup script is set).

If the IM database is used, the automatic startup script is executed during system startup and starts JP1/Base, JP1/IM - Manager, and IM database in that order. Note that the `pdprcd` process is started during system startup whether or not the automatic startup script is enabled.

If the IM database is not used, the automatic startup script is executed during system startup and starts JP1/Base, followed by JP1/IM - Manager.

For details about how to set the automatic startup script, see 2.17.2 *Setting automatic startup and automatic stop (for UNIX)* in the *JP1/Integrated Management - Manager Configuration Guide*. For details about the automatic startup script, see `jco_start (UNIX only)` (in *Chapter 1. Commands*) in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

To start JP1/IM - Manager without setting up the automatic startup script, execute the `/etc/opt/jplcons/jco_start.model` script or a file into which this script has been copied.

Before starting JP1/IM - Manager, start all JP1/Base services required for monitoring. To use the IM database, you must also start the IM database when you start JP1/IM - Manager. Before you restart JP1/Base services, JP1/IM - Manager must be stopped. If JP1/IM - Manager is not stopped, a problem might occur (for example, events cannot be displayed).

For details about starting JP1/Base services, see the chapter about starting and stopping JP1/Base in the *JP1/Base User's Guide*.

Important

If you are using the integrated monitoring database, set it up; if you are using IM Configuration Management, set up the IM Configuration Management database. If you are using Central Scope, set up the monitoring object database, and then start JP1/IM - Manager.

(1) Notes for cases where the automatic startup and automatic stop of JP1/IM - Manager are enabled in Linux

To start JP1/IM - Manager manually after enabling the automatic startup and automatic stop, execute the commands listed below.

To check the status (started or stopped) of JP1/IM - Manager processes, you can use the `jco_spmd_status` command. When the IM database is used, you can use the `jimdbstatus` command to check the operating status of the IM database.

- To start JP1/IM - Manager:

Physical hosts:

```
systemctl start jpl_cons.service
```

Logical hosts:

```
systemctl start jpl_cons_logical-host-name.service
```

Even when the automatic startup and automatic stop are enabled, JP1/IM - Manager does not stop automatically after it is started or stopped by using a command other than the `systemctl` command, for example, the `jco_start` or `jco_start.cluster` command or the `jco_stop` or `jco_stop.cluster` command. In such a case, the automatic startup and automatic stop remain enabled although the stop script does not start when the system stops.

To allow JP1/IM - Manager to stop automatically when the system stops, start JP1/IM - Manager again by using the `systemctl` command. To know whether JP1/IM - Manager stops automatically, execute one of the following commands to check whether `active` is returned:

Physical hosts:

```
systemctl is-active jpl_cons.service
```

Logical hosts:

```
systemctl is-active jpl_cons_logical-host-name.service
```

3.1.3 Operations in a cluster system

Regardless of the platform (OS and cluster software type) being used, to operate JP1/IM - Manager of a logical host in a cluster system, use the cluster software controls to start JP1/IM - Manager.

In a cluster system, applications are registered in the cluster software and are started and stopped by the cluster software; therefore, these applications are executed by the executing server and moved to the standby server through a failover when an error such as a system failure occurs. When you operate JP1/IM - Manager in a cluster operation system, you must also register JP1/IM - Manager in the cluster software so that the cluster software controls it.

When JP1/IM - Manager is running in a cluster operation system, it must be started and stopped by cluster software operations. If you start or stop JP1/IM - Manager manually, such as by executing a command, the status of the JP1/IM - Manager being managed by the cluster software will not match the actual status, which may be judged as an error.

For details about the start sequence, see *6.4 Registering into the cluster software during new installation and setup (for Windows)* or *7.4 Registering into the cluster software during new installation and setup (for UNIX)* in the *JP1/Integrated Management - Manager Configuration Guide*.

3.1.4 Operating a logical host in a non-cluster system

On a logical host in a non-cluster system, start JP1/Base and JP1/IM - Manager according to the following sequence:

1. JP1/Base
2. JP1/IM - Manager

If you are using the IM database, start JP1/Base and JP1/IM -Manager according to the following sequence:

1. JP1/Base
2. IM database
Start JP1/IM-Manager DB Cluster Service *_logical-host-name*.
3. JP1/IM - Manager

For details about automatic startup and automatic stop when a logical host is operated in a non-cluster system, see *3.3 Automatic startup and automatic stop setting examples when a logical host operates in a non-cluster system*.

3.2 Stopping JP1/IM - Manager

This section explains how to stop JP1/IM - Manager.

You must stop JP1/IM - Manager before you stop JP1/Base. If you are using the IM database, you must stop the IM database when you stop JP1/IM - Manager.

The stopping method differs depending on the OS that is being used.

3.2.1 In Windows

If you are using the IM database, start JP1/Base, the IM database service, and JP1/IM - Manager in that order.

If JP1/Power Monitor has been installed, you can use the startup control of JP1/Base to stop a service. For details about how to set up startup control, see the chapter on setting up the service startup and stopping sequence (Windows only) in the *JP1/Base User's Guide*.

To stop a service without using startup control, choose **Control Panel** and then **Administrative Tools**, and then stop the JP1/IM - Manager service from **Services**.

3.2.2 In UNIX

If you are using the IM database and you have set up the automatic termination script, JP1/IM - Manager, the IM database, and JP1/Base stop in that order when the system stops. Although the `pdprcd` process continues running even when JP1/IM - Manager and the IM database have stopped, it is not necessary to stop it.

If you are not using the IM database but have set up the automatic termination script, JP1/IM - Manager and JP1/Base stop in that order when the system stops.

For details about how to set the automatic startup script, see *2.17.2 Setting automatic startup and automatic stop (for UNIX)* in the *JP1/Integrated Management - Manager Configuration Guide*. For details about the automatic termination script, see *jco_stop (UNIX only)* (in *Chapter 1. Commands*) in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

To stop JP1/IM - Manager without setting up the automatic termination script, execute the `/etc/opt/jplcons/jco_stop.model` script or a file into which this script has been copied.

(1) Notes for cases where the automatic startup and automatic stop of JP1/IM - Manager are enabled in Linux

To stop JP1/IM - Manager manually after enabling the automatic startup and automatic stop, execute the commands listed below.

To check the status (started or stopped) of JP1/IM - Manager processes, you can use the `jco_spmc_status` command. When the IM database is used, you can use the `jimdbstatus` command to check the operating status of the IM database.

- To stop JP1/IM - Manager:
Physical hosts:

```
systemctl stop jpl_cons.service
```

Logical hosts:

```
systemctl stop jpl_cons_logical-host-name.service
```

Even when the automatic startup and automatic stop are enabled, JP1/IM - Manager does not stop automatically after it is started or stopped by using a command other than the `systemctl` command, for example, the `jco_start` or `jco_start.cluster` command or the `jco_stop` or `jco_stop.cluster` command. In such a case, the automatic startup and automatic stop remain enabled although the stop script does not start when the system stops.

To allow JP1/IM - Manager to stop automatically when the system stops, start JP1/IM - Manager again by using the `systemctl` command. To know whether JP1/IM - Manager stops automatically, execute one of the following commands to check whether `active` is returned:

Physical hosts:

```
systemctl is-active jpl_cons.service
```

Logical hosts:

```
systemctl is-active jpl_cons_logical-host-name.service
```

3.2.3 Operations in a cluster system

Regardless of the platform (OS and cluster software type) being used, to operate JP1/IM - Manager of a logical host in a cluster system, use the cluster software controls to stop JP1/IM - Manager.

In a cluster system, applications are registered in the cluster software and are started and stopped by the cluster software, so that these applications are executed by the executing server and moved to the standby server through a failover when an error such as a system failure occurs. When you operate JP1/IM - Manager in a cluster operation system, you must also register JP1/IM - Manager in the cluster software so that the cluster software controls it.

When JP1/IM - Manager runs in a cluster operation system, it must be started and stopped by cluster software operations. If you start or stop JP1/IM - Manager manually, such as by executing a command for example, the status of the JP1/IM - Manager being managed by the cluster software will not match the actual status, which may be judged as an error.

3.2.4 Operating a logical host in a non-cluster system

On a logical host in a non-cluster system, stop JP1/Base and JP1/IM - Manager according to the following sequence:

1. JP1/IM - Manager
2. JP1/Base

If you are using the IM database, stop JP1/Base and JP1/IM - Manager according to the following sequence:

1. JP1/IM - Manager
2. IM database
Stop JP1/IM-Manager DB Cluster Service_ *logical-host-name*.
3. JP1/Base

For details about automatic startup and automatic stop when a logical host is operated in a non-cluster system, see [3.3 Automatic startup and automatic stop setting examples when a logical host operates in a non-cluster system](#).

3.3 Automatic startup and automatic stop setting examples when a logical host operates in a non-cluster system

To automatically start and stop JP1 services for a logical host at system startup or stop, you must follow the setup sequence described below. The setup method differs depending on the OS supported by JP1/IM - Manager. The setup method for each OS is described below.

3.3.1 Setting up automatic startup and automatic stop when a logical host operates in a non-cluster system (for Windows)

1. Use a text editor to add the following description to the start sequence definition file (JP1SVPRM.DAT):

Storage destination: *Base-path*\conf\boot\JP1SVPRM.DAT

```
[Jp1BaseEvent_logical-host-name]
Name=JP1/BaseEvent_logical-host-name
ServiceName=JP1_Base_Event_logical-host-name

[Jp1Base_logical-host-name]
Name=JP1/Base_logical-host-name
ServiceName=JP1_Base_logical-host-name
StopCommand=jbs_spm�_stop.exe -h logical-host-name

[JP1/IM-Manager DB Cluster Service_logical-host-name]
Name=JP1/IM-Manager DB Cluster Service_logical-host-name
ServiceName=HiRDBClusterService_JMn
StopCommand=Manager-path\bin\imdb\jimdbstop.exe -h logical-host-name

[Jp1IM-Manager_logical-host-name]
Name=JP1/IM-Manager_logical-host-name
ServiceName=JP1_Console_logical-host-name
StopCommand=jco_spm�_stop.exe -h logical-host-name
```

JMn: For *n*, specify the same value as that specified for LOGICALHOSTNUMBER in the cluster setup information file.

The command specified by the *StopCommand* parameter is executed when JP1/Power Monitor shuts down the host.

Important

When you use JP1/Power Monitor to start or stop the host on which JP1/IM - Manager starts, specify a command such as a batch file for executing `net stop IM-database-service-name` in the *StopCommand* parameter of the start sequence definition file of JP1/Base.

3.3.2 Setting up automatic startup and automatic stop when a logical host operates in a non-cluster system (for AIX)

1. Use the `mkinitab` command to add the following description to the `/etc/inittab` file:

```
# mkitab -i hntr2mon "jplbase:2:wait:/etc/opt/jplbase/jbs_start.cluster
logical-host-name"
# mkitab -i jplbase "jplcons:2:wait:/etc/opt/jplcons/jco_start.cluster
logical-host-name"
```

Adding this description executes JP1 service startup processing during system startup.

2. Use a text editor to add the following description after the description of the product that requires JP1/Base and JP1/IM - Manager in `/etc/rc.shutdown`:

```
test -x /etc/opt/jplcons/jco_stop.cluster && /etc/opt/jplcons/
jco_stop.cluster logical-host-name
test -x /etc/opt/jplbase/jbs_stop.cluster && /etc/opt/jplbase/
jbs_stop.cluster logical-host-name
test -x /opt/hitachi/HNTRLlib2/etc/D002stop &&
/opt/hitachi/HNTRLlib2/etc/D002stop
```

Adding this description executes JP1 service stop processing during system stop.

3.3.3 Setting up automatic startup and automatic stop when a logical host operates in a non-cluster system (for Linux)

1. Create a script for automatic startup and automatic stop for the logical host.

Storage destination: `/usr/lib/systemd/system/jpl_cons_logical-host-name.service`

Automatic startup and automatic stop script example

```
[Unit]
Description=JP1/Integrated Management - Manager logical-host-name Service
Requires=jpl_base_logical-host-name.service
After=jpl_base_logical-host-name.service
ConditionFileIsExecutable=/etc/opt/jplcons/jco_start.cluster
ConditionFileIsExecutable=/etc/opt/jplcons/jco_stop.cluster

[Service]
ExecStart=/etc/opt/jplcons/jco_start.cluster logical-host-name
ExecStop=/etc/opt/jplcons/jco_stop.cluster logical-host-name

Type=forking
KillMode=none
StandardOutput=null
StandardError=null

[Install]
WantedBy=multi-user.target graphical.target
```

`logical-host-name` indicates the name of the logical host to be started. For details about the `Unit` file of a JP1/Base logical host, follow the settings in JP1/Base.

2. Use the following command to register the created script for automatic startup and automatic stop.

```
# systemctl --system enable jpl_cons_logical-host-name
```

3. To edit the script for automatic startup and automatic stop, use the following command to apply the change to `systemd`:

Important

In Linux, to start or stop JP1/IM - Manager manually when the automatic start and automatic stop of JP1/IM - Manager are enabled, execute the commands listed below. To start or stop JP1/IM - Manager manually, you can use the commands listed below. To check the status (started or stopped) of JP1/IM - Manager processes, you can use the `jco_spmc_status` command. When the IM database is used, you can use the `jimdbstatus` command to check the operating status of the IM database.

- Starting JP1/IM - Manager

Physical hosts:

```
systemctl start jpl_cons.service
```

Logical hosts:

```
systemctl start jpl_cons_logical-host-name.service
```

- Stopping JP1/IM - Manager

Physical hosts:

```
systemctl stop jpl_cons.service
```

Logical hosts:

```
systemctl stop jpl_cons_logical-host-name.service
```

Even when automatic startup and stop is set to enabled, JP1/IM - Manager does not stop automatically after it is started or stopped by using a command other than the `systemctl` command, for example, by using the `jco_start` or `jco_start.cluster` command to start, or the `jco_stop` or `jco_stop.cluster` command to stop. (In such a case, automatic startup and stop remains enabled although the stop script does not start when the system stops.)

To allow JP1/IM - Manager to stop automatically when the system stops, start it again by using the `systemctl` command. To know whether JP1/IM - Manager will stop automatically, execute the following commands to check whether `active` is returned.

Physical hosts:

```
systemctl is-active jpl_cons.service
```

Logical hosts:

```
systemctl is-active jpl_cons_logical-host-name.service
```

3.3.4 Setting up automatic startup and automatic stop on both the physical host and the logical host

To implement automatic startup and automatic stop on both the physical and the logical hosts, you must use the settings described below, in addition to the settings for automatic startup and automatic stop on the logical host.

The setup method differs depending on the OS. The setup method for each OS is described below.

In the Windows environment:

Startup control sequentially executes startup and stop processes as described in the startup sequence definition file (`JP1SVPRM.DAT`), starting at the top. To change the startup sequence of the physical host and logical host, define

a new startup and stop sequence for the physical host and logical host in the startup sequence definition file (JP1SVPRM.DAT).

In the Linux environment:

The automatic startup and stop sequences are determined based on the value of the numerical portion (** portion in S** and K**) in the automatic startup and automatic stop script. The greater the numerical value, the later the execution. The symbolic link to the automatic startup and automatic stop script for the physical host is automatically created during installation. To implement automatic startup and stop on both the physical and logical hosts, change the name of the symbolic link created for the logical host, and adjust the startup and stop sequences of the physical and logical hosts.

Note that the automatic startup and automatic stop scripts for the physical host are already provided. The following table lists the symbolic links to the automatic startup and automatic stop scripts for the physical host.

Table 3–1: List of symbolic links to the automatic startup and automatic stop scripts for the physical host

Startup script	Stop script
/etc/rc.d/rc3.d/S99_JP1_20_CONS	/etc/rc.d/rc0.d/K01_JP1_80_CONS
/etc/rc.d/rc5.d/S99_JP1_20_CONS	/etc/rc.d/rc6.d/K01_JP1_80_CONS

Adjust the physical and logical host startup sequence by varying the size relationship between the value of the ** portion in S** and K** in the symbolic link list, and the value of the ** portion in S** and K** in the symbolic link to the automatic startup and stop script for the logical host.

For example, to start the logical host first, set the number in the symbolic name S** for the automatic startup script to be created for the logical host to a value smaller than 99 (for Linux).

In the AIX environment:

To automatically start and stop the physical host, you must use additional settings.

For details about the additional settings, see *2.17.2 Setting automatic startup and automatic stop (for UNIX)* in the *JP1/Integrated Management - Manager Configuration Guide*.

3.4 Notes on starting and stopping

- Do not change the **System account** initial settings in the JP1/IM - Manager service's **Logon** settings. In addition, do not select the **Allow service to interact with desktop** option. If this option is selected, the service might not function normally.

For details about the JP1/IM - Manager service, see 2.6 *JP1/IM - Manager service* in the *JP1/Integrated Management - Manager Overview and System Design Guide*.

- If you restart Event Service of JP1/Base, you must also restart JP1/IM - Manager. In addition, you must restart the JP1/IM - View that was connected. If you do not restart it, you will have problems displaying events, for example.
- If a process does not stop even after you have stopped all services of JP1/IM - Manager for a logical host, you can execute the `jco_killall.cluster` command to forcibly stop the process. Use this command for stopping a process only when a process does not stop after you have used a normal method and stopped the JP1/IM - Manager services.
- If you collect a large number^{#1} of events during startup of JP1/IM - Manager, the startup time^{#2} will lengthen in proportion to the number of events that are collected. Consequently, the JP1/IM - Manager service (in Windows) or the `jco_start` command (in UNIX) may time out^{#3} and return an error value. In such a case, JP1/IM - Manager may appear not to be starting, but startup will be completed after a while.

#1

The number will vary depending on the event collection filtering condition and the number of events that have accumulated in the event database.

#2

The startup time will vary depending on the machine's performance.

#3

The timeout period for the JP1/IM - Manager service (in Windows) or the `jco_start` command (in UNIX) is 2 minutes.

- If the IM database fails to start, it may be unstable because it is in restart suspension (after the IM database fails to start, 8 is returned as the return value when the `jimdbstatus` command is executed).

Factors that cause the IM database to be in restart suspension and to become unstable are as follows:

- Insufficient disk capacity (not insufficient IM database capacity)
- Insufficient memory

If the IM database is in restart suspension and is unstable, you cannot normally stop the IM database by stopping services or executing a command. To avoid this state, you must execute the `jimdbstop` command with the `-f` option specified to forcibly stop the IM database.

- If you are using the IM database, start JP1/Base, the IM database service, and JP1/IM - Manager in that order.
- If you are using the IM database, stop JP1/IM - Manager, the IM database service, and JP1/Base in that order. If JP1/IM - MO is being used, stop the JP1/IM - Message Optimizer service of JP1/IM - MO on the connection source before stopping JP1/IM - Manager.

4

JP1/IM - Manager Login and Logout

To use JP1/IM - View, you must log in to JP1/IM - Manager. This chapter explains how to log in to and log out of JP1/IM - Manager.

4.1 Logging in to JP1/IM - Manager

To use JP1/IM - View and IM Configuration Management - View, you must log in to JP1/IM - Manager from the viewer. You can log in to JP1/IM - Manager by using the GUI or by executing the `jcoview` or `jcfview` command.

If you register a shortcut for the `jcoview` or `jcfview` command at Windows startup, you can start JP1/IM - View and IM Configuration Management - View when you log on to Windows. You can also register a shortcut for the `jcoview` or `jcfview` command in the Quick Launch bar displayed next to the **Start** button in Windows, or you can create a shortcut for the `jcoview` or `jcfview` command for each host or user.

4.1.1 Using the GUI to log in to JP1/IM - Manager

(1) Using JP1/IM - View

To use JP1/IM - View to log in to JP1/IM - Manager via a GUI:

1. From the Windows **Start** menu, choose **All Programs**, then **JP1_Integrated Management - View**, and then **Integrated View**.

The Login window opens.

2. In the Login window, enter a user name, a password, and the name of the host to which you want to connect.

You can use alphanumeric characters, 1 to 31 bytes, for the user name. The user name is not case sensitive.

The password is case-sensitive.

For the host to which to connect, specify the name of the host where the JP1/IM - Manager to which you are logging in is located. Specify a host name defined in the viewer or an IP address.

For details about the Login window, see *1.2.1 Login window of Central Consol and Central Scope* in the manual *JP1/Integrated Management - Manager GUI Reference*.

If you want to log in to Central Scope, advance settings for using the Central Scope functions are required.

3. Select the check boxes according to the functions you wish to use.

You can select either one or both of them.

If you select the **Central Console** check box, you will be connected to JP1/IM - Manager (Central Console).

If you select the **Central Scope** check box, you will be connected to JP1/IM - Manager (Central Scope).

4. Click **OK**.

If you are connecting to JP1/IM - Manager (Central Console), the Event Console window opens. If you are connecting to JP1/IM - Manager (Central Scope), the Monitoring Tree window opens.

The user name you use for login must be registered in advance. For details about user registration, see the chapter on setting up the user management function in the *JP1/Base User's Guide*.

When logging in to JP1/IM - Manager, you can log in to a maximum of three different Managers from a single viewer.

Using the Web version of JP1/IM - View:

To use a Web browser to log in to JP1/IM - Manager:

1. Open a Web browser and specify the following URL:

`http://name-of-host-to-which-to-connect/JP1IM/console.html`

The Login window opens.

2. Enter your user name and password.

The host name specified in the URL is displayed as the host to which you are connecting. You cannot change the host in this window.

3. Click **OK**.

The Event Console window opens.

When you are logging in from a Web browser, you can log in to only one manager from a single viewer. Furthermore, when you are using a Web browser, you can log in to JP1/IM - Manager (Central Console) only, and you cannot use JP1/IM - Manager (Central Scope).

(2) Using IM Configuration Management - View

To use IM Configuration Management - View to log in to JP1/IM - Manager via a GUI:

1. From the Windows **Start** menu, choose **All Programs**, then **JP1_Integrated Management - View**, and then **Configuration Management**.

The Login window opens.

If you want to start IM Configuration Management - View from the Windows **Start** menu, you must first execute the `jcovcfsetup` command and add **Configuration Management** to the Windows **Start** menu. For details about how to add **Configuration Management** to the Windows **Start** menu, see *1.19.3 Setting up and customizing IM Configuration Management - View (for Windows)* in the *JP1/Integrated Management - Manager Configuration Guide*.

2. In the Login window, enter a user name, a password, and the name of the host to which you want to connect.

You can use only lower-case letters for the user name. If you enter upper-case letters, they will be recognized as lower-case letters.

The password is case-sensitive.

For the host to which to connect, specify the name of the host where the JP1/IM - Manager to which you are logging in is located. Specify a host name defined in the viewer or an IP address.

3. Click **OK**.

You are connected to IM Configuration Management, and the IM Configuration Management window opens.

The user name to be used for login must be registered in advance. For details about user registration, see the chapter on setting up the user management function in the *JP1/Base User's Guide*.

When you log in to JP1/IM - Manager, you can log in to a maximum of three different managers from a single viewer.

4.1.2 Using a command to log in to JP1/IM - Manager

(1) Using JP1/IM - View

This subsection explains how to use the `jcoview` command to log in to JP1/IM - Manager and use JP1/IM - View.

Execute the following command:

- To open the Login window

```
jcoview [-c] [-s] [-h name-of-host-to-which-to-connect] [-u user-name]
```

If no argument is specified, the Login window opens with the information from the previous login entered.

If arguments are specified, the Login window opens with the specified values entered.

- To log in

```
jcoview [-c] [-s] [-h name-of-host-to-which-to-connect] [-u user-name] [-p password]
```

If you specify all arguments, you will be logged in to both Central Console and Central Scope of JP1/IM - Manager.

If you specify only the `-c` argument, you will be logged in to Central Console. If you specify only the `-s` argument, you will be logged in to Central Scope. If you omit both the `-c` and `-s` arguments, you will be logged in to Central Console.

Once the user is authenticated, the Login window will not be displayed. The Event Console window and the Monitoring Tree window open according to the arguments that are specified.

For details about how to log in via the GUI, see [4.1.1 Using the GUI to log in to JP1/IM - Manager](#). For details about the `jcoview` command, see *jcoview (Windows only)* (in *Chapter 1. Commands*) in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

(2) Using IM Configuration Management - View

This subsection describes the method of using the `jcfview` command to log in to JP1/IM - Manager and use IM Configuration Management - View.

Execute the following command:

- To open the Login window

```
jcfview -h [name-of-host-to-connect] -u [user-name]
```

If no argument is specified, the Login window opens with the information from the previous login entered.

If arguments are specified, the Login window starts with the specified values entered.

- To log in

```
jcfview -h [name-of-host-to-connect] -u [user-name] -p [password]
```

If you specify all arguments, you will be logged in to IM Configuration Management of JP1/IM - Manager.

Once the user is authenticated, the Login window will not be displayed. The IM Configuration Management window opens according to the arguments that are specified.

For details about how to log in via the GUI, see [4.1.1 Using the GUI to log in to JP1/IM - Manager](#). For details about the `jcfview` command, see *jcfview (Windows only)* (in *Chapter 1. Commands*) in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

4.2 Logging out of JP1/IM - Manager

To log out of JP1/IM - Manager, use the following methods.

To log out of JP1/IM - Manager (Central Console):

- In the Event Console window, from the **File** menu, choose **Exit, Logout**.
- Click the × button in the upper right corner of the Event Console window.

To log out of JP1/IM - Manager (Central Scope):

- In the Monitoring Tree window, from the **File** menu, choose **Exit, Logout**.
- Click the × button in the upper right corner of the Monitoring Tree window.

To log out of JP1/IM - Manager (IM Configuration Management):

- In the IM Configuration Management window, from the **File** menu, choose **Exit, Logout**.
- Click the × button in the upper right corner of the IM Configuration Management window.

The above methods close the active windows. Note, however, that windows and monitoring windows that were started from Tool Launcher will not be closed. You must close these windows individually.

The logout procedure is the same regardless of whether you use a Web browser or a command to log in. If you close an application without logging out, the login information remains in the manager, ultimately causing a resource shortage for the manager. Therefore, remember to end your session by logging out.

Once you log out from JP1/IM - Manager (Central Console), the user profile is updated and the event console's user environment, such as column width and view filter enable/disable settings, is saved.

5

System Monitoring from Central Console

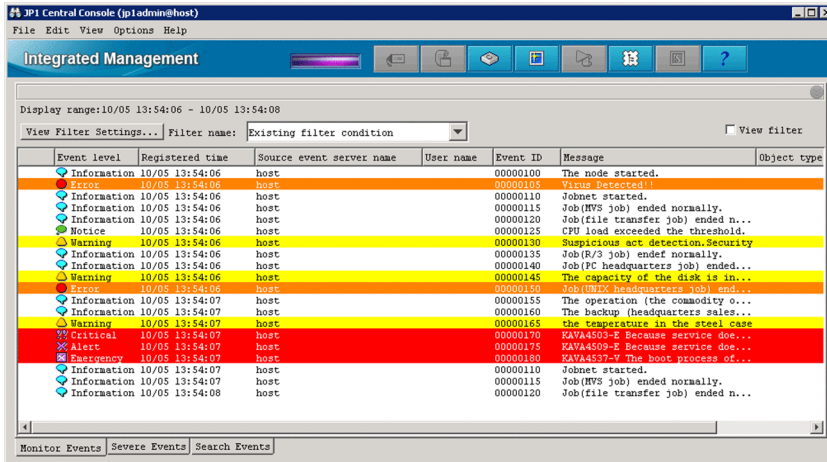
This chapter explains how to use JP1/IM - View to monitor JP1 events.

5.1 Viewing JP1 events

Received JP1 events are displayed in the Event Console window. The Event Console window opens when you log in to JP1/IM - Manager (Central Console).

The following figure shows a display example of the Event Console window.

Figure 5–1: Event Console window (Monitor Events page) display example



The screenshot shows the JP1 Central Console (jp1admin@host) window. The main area displays a table of events with columns for Event level, Registered time, Source event server name, User name, Event ID, Message, and Object type. The events are sorted by time, with the most recent at the bottom. The table includes various event levels such as Information, Warning, Error, and Critical, with corresponding icons. The messages describe system operations, job completions, and hardware warnings.

Event level	Registered time	Source event server name	User name	Event ID	Message	Object type
Information	10/05 13:54:06	host		00000100	The node started.	
Information	10/05 13:54:06	host		00000103	Jobnet started.	
Information	10/05 13:54:06	host		00000110	Jobnet started.	
Information	10/05 13:54:06	host		00000115	Job(MVS job) ended normally.	
Information	10/05 13:54:06	host		00000120	Job(file transfer job) ended n...	
Notice	10/05 13:54:06	host		00000125	CPU load exceeded the threshold.	
Warning	10/05 13:54:06	host		00000130	Suspicious act detection.Security	
Information	10/05 13:54:06	host		00000135	Job(R/3 job) ended normally.	
Information	10/05 13:54:06	host		00000140	Job(PC headquarters job) ended...	
Warning	10/05 13:54:06	host		00000145	The capacity of the disk is in...	
Error	10/05 13:54:06	host		00000150	Job(UNIX headquarters job) end...	
Information	10/05 13:54:07	host		00000155	The operation (the commodity o...	
Information	10/05 13:54:07	host		00000160	The backup (headquarters sales...	
Warning	10/05 13:54:07	host		00000165	the temperature in the steel case	
Critical	10/05 13:54:07	host		00000170	KAWA4503-E Because service doe...	
Alert	10/05 13:54:07	host		00000175	KAWA4509-E Because service doe...	
Emergency	10/05 13:54:07	host		00000180	KAWA4532-E The boot process of...	
Information	10/05 13:54:07	host		00000110	Jobnet started.	
Information	10/05 13:54:07	host		00000115	Job(MVS job) ended normally.	
Information	10/05 13:54:08	host		00000120	Job(file transfer job) ended n...	

The Event Console window displays the JP1 events registered in the logged-in manager's event database. New JP1 events are added at the bottom of the events list. The JP1 event with the most recent arrival date/time is displayed at the very bottom of the events list.

Note

You can use a CSV file to save a snapshot of the events list displayed in the Event Console window. To save a snapshot in a CSV file, in the Event Console window, choose **File** and then **Save Displayed Events**.

You can also copy selected parts of JP1 event information and action execution results to the clipboard in CSV format. For details about the information that can be copied to the clipboard in CSV format, see [3.15.3 Copying JP1 event information and action execution results to the clipboard](#) in the *JP1/Integrated Management - Manager Overview and System Design Guide*.

Saving information to a CSV file and copying information to the clipboard in CSV format are not supported by the Web version of JP1/IM - View.

5.1.1 Items displayed in the events list

The events list displays the attributes of JP1 events and their handling status. For the event attributes, you can also display basic attributes, common extended attributes, and program-specific extended attributes.

You can change the column width of the items displayed in the events list by holding the mouse button down on a column edge and dragging. If you change a column width on one page (on the **Monitor Events** page, for example), it is also changed on the other two pages (**Severe Events** and **Search Events** pages).

You can set up the **Monitor Events**, **Severe Events**, and **Search Events** pages so that background colors are added to specific events displayed in these pages. You can add background colors to events with the following levels of severity: Emergency, Alert, Critical, Error, and Warning.

If you use the severity changing function to change a severity level, set up a background color for the events at the changed severity level.

You can set the severity changing function if you are using the integrated monitoring database.

For details about how to set up the integrated monitoring database, see *1.4.2 Setting up the integrated monitoring database (for Windows)* or *2.4.2 Setting up the integrated monitoring database (for UNIX)* in the *JP1/Integrated Management - Manager Configuration Guide*.

For details about how to set up the severity changing function, see *4.13 Setting the severity changing function* in the *JP1/Integrated Management - Manager Configuration Guide*.

In the Preferences window, you can specify whether to save the column width for each display item when you log out, and whether to add background colors for specific events. For details about the Preferences window, see *2.24 Preferences window* in the manual *JP1/Integrated Management - Manager GUI Reference*.












(1) Basic attributes, common extended attributes, and program-specific extended attributes of JP1 events



The events list displays the attributes (basic attributes, common extended attributes, or program-specific extended attributes) of each event. The default is that the severity level, registered time, registered host name, user name, event ID, message, object type, and action are displayed. You can change the items displayed in the events list from the Preferences window. For details about how to change displayed items, see *2.24 Preferences window* in the manual *JP1/Integrated Management - Manager GUI Reference*.

The items that can be displayed (columns) in the events list are those event attributes that are listed in the table below.

Table 5–1: Items displayed in the events list

Attribute	Explanation
Response status display item	Displays information (Processed, Processing, Held, or Unprocessed) that indicates the response status of JP1 events. If the response status of a consolidated event is different from the response status of repeated events, ! is displayed.
Consolidation status	This attribute shows the number of times a consolidated event is repeated. It is only displayed when monitoring of repeated events is suppressed or the display of repeated events is consolidated. For events that are being consolidated, + is displayed after the repetition count, indicating that consolidation is in progress.
Severity	This attribute indicates the urgency of a JP1 event, in the following descending order: Emergency, Alert, Critical, Error, Warning, Notice, Information, and Debug. When you are using the integrated monitoring database, if you use the severity changing function to change a severity level, this attribute indicates the urgency of the JP1 event after the change.
Registered time	Time at which a JP1 event was registered in the event database of the event-issuing host.
Registered host name	Name of the agent (event server) that registered the JP1 event.
User name	Name of the user that issued the JP1 event.
Event ID	Value that indicates the source program of the event that occurred.
Message	Message text that shows the content of the JP1 event.

Attribute	Explanation
Object type	Character strings, such as JOB and JOBNET, that indicate the type of object where the event that triggered event generation occurred.
Action	<p>When automated actions are set up and if an event becomes the target of action execution, an action icon  (action that was not suppressed)  (action that was suppressed), or  (action that was partially suppressed) is displayed.</p> <p>If a large number of events occur while the corresponding action is suppressed by the repeated event monitoring suppression function,  is displayed in the Event Console window.</p> <p>When monitoring of repeated events is suppressed or the display of repeated events is consolidated, and the action status of a consolidated event is different from the action status of repeated events, ! is displayed.</p> <p>When an event is not the target of action execution due to the common exclusion-conditions,  (Action-excluded event) is displayed.</p>
Product name	Name of the program that issued the JP1 event.
Object name	Name of the object (job, jobnet, etc.) where the event that triggered event generation occurred.
Root object type	Object type. The root object type is normally the same as the object type, but the highest-order object type is displayed for multi-level jobs, such as jobnets and jobs.
Root object name	Object name. The root object name is normally the same as the object name, but the highest-order object name is displayed for multi-level jobs, such as jobnets and jobs.
Arrival time	<p>Time at which the JP1 event arrived at the event database of the connected manager.</p> <p>For the Search Events page, this attribute shows the time at which the JP1 event was registered in the event database of the search-target host.</p>
Start time	Shows the time zone in which the execution started.
End time	Shows the time zone in which the execution ended.
Occurrence	Shows the phenomena (execution start, definition creation, etc.) that occurred for the object.
Serial number	Order in which the JP1 event arrived at this event server, regardless of the source.
Source process ID	Process ID of the source application program.
Source user ID	Source process user ID. The ID is -1 if the event comes from Windows.
Source group ID	Source process group ID. The ID is -1 if the event comes from Windows.
Source user name	Source process user name.
Source group name	Source process group name. The name is left blank if the event comes from Windows.
Source serial number	Serial number at the source host (the value does not change through forwarding).
Type	<p>JP1 event type.</p> <p>Either the correlation succeeded icon  or the correlation failed icon  is displayed.</p> <p>If a large number of events occur that are suppressed by the repeated event monitoring suppression function,  is displayed on each page of the Event Console window to indicate that a large number of events have occurred.</p>
Action type	<p>Action type.</p> <p>An icon indicating the action type  (command) or  (rule) is displayed.</p>
Severity (before change)	<p>Severity level before the change.</p> <p>This attribute can be set when the integrated monitoring database is used and the severity changing function is enabled.</p>
Severity changing	When the severity level is changed, the icon  is displayed.

Attribute	Explanation
	This attribute is displayed when the integrated monitoring database is used and the severity changing function is enabled.
Changed display message	Displays a message after the change. This attribute is displayed when the integrated monitoring database is used and the display message change function is enabled. After an upgrade from version 10-50 or earlier, this attribute can only be used if the IM database has been updated using the <code>jimdbupdate</code> command. This attribute is not displayed in the Web-based JP1/IM - View.
New display message	When the display message is changed,  is displayed. This attribute is displayed when the integrated monitoring database is used and the display message change function is enabled. After an upgrade from version 10-50 or earlier, this attribute can only be used if the IM database has been updated using the <code>jimdbupdate</code> command. This attribute is not displayed in the Web-based JP1/IM - View.
Display message change definition	Definition name of display message change. This attribute is displayed when the integrated monitoring database is used and the display message change function is enabled. After an upgrade from version 10-50 or earlier, this attribute can only be used if the IM database has been updated using the <code>jimdbupdate</code> command. This attribute is not displayed in the Web-based JP1/IM - View.
Memo	When there are memo entries for the JP1 event, the icon  is displayed. This attribute can be set when the integrated monitoring database is used and the function for setting memo entries is enabled.
Source host name	Name of the host on which an event generating a JP1 event occurs. A name is displayed when the integrated monitoring database is used, and source host mapping is enabled.
Source IP address	IP address of the source event server.
Object ID	Serial number of the event that triggered an action.
Return code	Command execution result.
Relation Event serial number	Serial number of correlation source event database.
Correlation event generation condition name	Name of a correlation event generation condition that is satisfied.
Suppressed event ID	Serial number (unique number in the event database) of a repeated event that occurs more frequently than the threshold.
Repeated event condition name	Name of a repeated event condition that determined that the event was a repeated-event.
Monitoring ID	Log file trap ID.
Monitoring name	Log file trap name.
Program-specific extended attribute	Displays the content of a program-specific extended attribute. The program-specific extended attributes defined in the definition file for extended event attributes (extended file) are displayed.

(2) Program-specific extended attributes of JP1 events (displaying program-specific extended attributes)

When you set up a definition file for extended event attributes (extended file), you can display the content of a program-specific extended attribute in the column of the events list with a specified item name. For example, when you specify

`System Name` as the item name for the `E.SYSTEM` program-specific extended attribute, you can display the attribute value of the `E.SYSTEM` program-specific extended attribute under an item called *System Name* in the events list.

Note that the Web-based JP1/IM - View cannot display in the events list the item names defined in the definition file for extended event attributes (extended file).

(3) Program-specific extended attributes of JP1 events (event information mapping)

When you set up event information mapping, you can display the content of a program-specific extended attribute in the display item (basic attribute or common extended attribute) column of the events list. For example, when an SNMP trap is converted into a JP1 event to be displayed in the events list, you can display the SNMP trap source host name in the registered host column.

When a program-specific extended attribute is displayed using event information mapping, it is preceded by the hash mark and a space (#).

To display a program-specific extended attribute using event information mapping, you need to map a display item to the program-specific extended attribute. For details about event information mapping, see [5.9.2 Displaying extended attributes of JP1 events \(mapping of event information\)](#).

(4) JP1 event response status



You can display a response status icon indicating the event's response status (Processed, Processing, or Held) in the far-left column of the events displayed in the events list. For details about how to display response status icons, see [5.3.1 Settings for JP1 event response statuses](#).

If you are using the repeated event monitoring suppression function or the consolidated display of repeated events function, and the response status of a consolidated event is different from the response status of repeated events, ! is displayed.

5.1.2 Events displayed in the events list in the Event Console window

Types of events displayed on the screen:

Events displayed on the screen are normal JP1 events, consolidated events (including events being consolidated and consolidation completion events), and correlation events.

- Consolidated events
The number of repetitions or a plus sign (+) indicating that consolidation is in progress appears in **Summary status**.
For details about displaying consolidated events, see [5.1.2\(1\) Displaying consolidated events in the events list](#).
- Correlation events
The icon  or  is displayed in **Type**.
For details about displaying correlation events, see [5.1.2\(2\) Displaying correlation events in the events list](#).

Number of events that can be displayed on the screen:

The number of events that can be displayed on the screen is the value specified in **Scroll Buffer** in the Preferences window. The maximum number of JP1 events that can be displayed is 2,000.

If you use the integrated monitoring database, you can display all events saved in the integrated monitoring database. You can use the slider to adjust the event display start-time located in the event display start-time specification area, or by specifying a date and time. For details about how to set up the integrated monitoring database, see *1.4.2 Setting up the integrated monitoring database (for Windows)* or *2.4.2 Setting up the integrated monitoring database (for UNIX)* in the *JP1/Integrated Management - Manager Configuration Guide*.

When the number of JP1 events exceeds the number of JP1 events that can be displayed, the following operation takes place:

Monitor Events page

Regardless of its response status, the JP1 event with the earliest arrival time is erased.

Severe Events page

Even if its response status is Processed, the JP1 event with the earliest arrival time is erased.

If there are Processed severe events, the JP1 event with the earliest arrival time is erased regardless of its response status.

Even those JP1 events that are erased from the screen are registered in the event database. To view the JP1 events that have been erased from the screen, search for JP1 events. For details about how to search for JP1 events, see *5.8 Searching for JP1 events*.

JP1 events that are displayed when the screen starts:

JP1 events that are displayed when the screen is started are the latest JP1 events that satisfy either of the following conditions:

- JP1 events that occurred after the logged-in manager started but before the screen was started
- JP1 events that were acquired from the event database beginning from the event acquisition start time set by the `jcoimdef` command until startup of the currently logged-in manager.

The number of JP1 events that are displayed when the screen is started is limited to one of the following values, whichever is smaller:

- The value specified in **Event Buffer** in the System Environment Settings window (event buffer count)
- The value specified in **Scroll Buffer** in the Preferences window (scroll buffer count)

Note that the JP1 event count also includes the communication events[#] used internally. Therefore, during the initial display, the number of JP1 events displayed may not reach the upper limit.

[#]: Communication event

A communication event is internally generated when the response status of a severe event is changed or deleted, or when an automated action is executed and is not displayed on the screen.

Updating the events list:

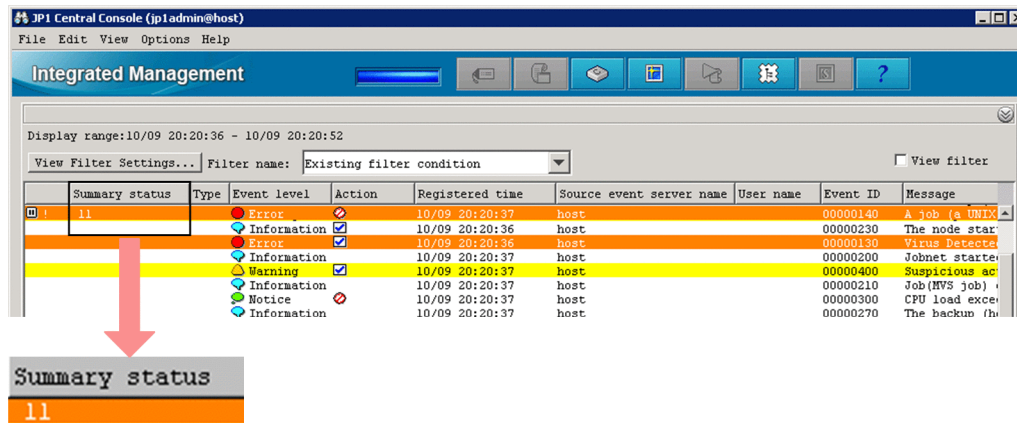
The events list is updated at a user-specified updating interval, and displays the latest JP1 events. However, if automatic updating is not set up, the latest JP1 events are not displayed even when the screen is started. To display the latest JP1 events in such a case, from the **View** menu, choose **Refresh**.

Specify whether to automatically refresh the screen, and the automatic refresh interval, in the Preferences window.

(1) Displaying consolidated events in the events list

After JP1 events have been consolidated by the repeated event monitoring suppression function or the consolidated display of repeated events function, consolidated events are displayed in the events list.

Figure 5–2: Example of consolidated display of consolidated events



Summary Status

Summary Status shows the number of repetitions. The number of repetitions is the sum total of the number of consolidated events plus the number of repeated events. No data is displayed for non-consolidated events.

- Consolidation completion events

The number of repetitions is displayed.

If suppression of repeated event monitoring is set, the number of repetitions to be displayed is from 1 to 1,000,000.

If repeated event consolidated display is set, the number of repetitions to be displayed is from 1 to 100.

Summary status	Event level
16	Warning

- Events being consolidated

The number of repetitions is displayed, together with a plus sign (+) indicating that consolidation is in progress.

For example, if the number of repetitions is 1 (only the consolidation start event), 1+ is displayed. If the number of repetitions is 2 (the consolidation start event and a repeated event), 2+ is displayed. On the **Severe Events** page, if the consolidation start event has already been deleted and there is no repeated event, 0+ is displayed.

Summary status	Event level
12+	Warning

The following is displayed when a consolidated event is deleted.

- When the consolidation start event is deleted

In the Event Console window, if you delete the consolidation start event on the **Severe Events** page, that event is displayed as deleted and Del is displayed to the right of the number of repetitions.

Summary status	Event level
11+ Del	Emergency

Subsequently, if event consolidation is completed and the event becomes a deleted non-consolidated event, it is no longer displayed on the **Severe Events** page of the Event Console window.

- When a repeated event is deleted

If you are using the consolidated display of repeated events function and you delete a repeated event from **Related Events** in the Related Events (Summary) window, the number of repetitions for consolidated events is reduced by the number of deleted events.

If the number of repetitions of consolidation completion events reaches 1 as a result of deletion of repeated events, that one event becomes a non-consolidated event. Furthermore, if that non-consolidated event has already been deleted, it is no longer displayed on the **Severe Events** page of the Event Console window.

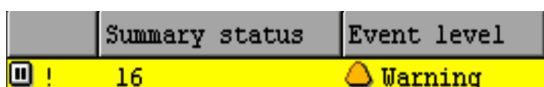
If you are using the repeated event monitoring suppression function, deleting a repeated event does not reduce the number of repetitions of consolidated events.

Response status display

A response status icon indicating the response status of a JP1 event is displayed in the far-left column.

The response status icon types and contents are the same as those displayed on the **Monitor Events** page and the **Severe Events** page of the Event Console window.

When you use the repeated event monitoring suppression function, an exclamation mark (!) is displayed if the 1st (the consolidation event) to 100th repeated events do not all have the same response status. If more than 100 events are consolidated, a different status among the 101st and subsequent events does not cause the exclamation mark (!) to appear.



Action

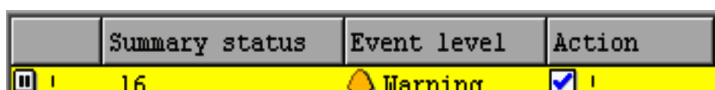
When the function for suppressing automated actions is being used, an icon indicating the action suppression status is displayed in the Event Console window.

Table 5–2: Action suppression status

Action suppression status	Explanation
	Action that was not suppressed
	Action that was suppressed
	Action that was partially suppressed

If a large number of events occur while the corresponding action is suppressed by the repeated event monitoring suppression function, the icon appears in the Event Console window.

When the action status of a consolidated event is different from the action status of a repeated event, an exclamation mark (!) is displayed as the action suppression status.



Type

If a large number of events occur while events are being suppressed by the repeated event monitoring suppression function, the icon appears in the Event Console window.



Pages in the Event Console window

If a large number of events occur while events are being suppressed by the repeated event monitoring suppression function, the icon appears on each page of the Event Console window.

(2) Displaying correlation events in the events list

Correlation events are displayed on the **Monitor Events** page, **Severe Events** page, and **Search Events** page of the Event Console window.

For a correlation event, an icon is displayed in **Type**.

Either the correlation succeeded icon  or the correlation failed  icon is displayed.

Note that **Type** is not a default display item. To display it, you must specify **Type** as a display item in the Preferences window. For details, see *2.24 Preferences window* in the manual *JP1/Integrated Management - Manager GUI Reference*.

5.1.3 Applying a filter

By applying a pre-set filter, you can restrict the JP1 events that are displayed in the Event Console window. The following four filters are available:

View filter

If a view filter is set, only those JP1 events that match the filtering condition are displayed.

For details about how to switch the view filter that needs to be applied when multiple view filters are set, see *5.5.1 Enabling a view filter to display only certain JP1 events*.

On the **Monitor Events** or **Severe Events** page (selected in the Event Console window), you can choose to save which view filter is applied, and whether the **View Filter** check box is selected. If you choose to save the applied status, it is saved when you log out of JP1/IM - View, and then restored at the next login. (Events are displayed according to status.) For details, see *4.16 Setting JP1/IM - View for each login user* in the *JP1/Integrated Management - Manager Configuration Guide*.

User filter

If a user filter is set, the JP1 events that are displayed are restricted according to which user is logged in.

Severe event filter

If a severe event filter is set, severe events are displayed on the **Severe Events** page of the Event Console window. For details about the **Severe Events** page, see *5.5.2 Displaying only severe events*.

When JP1/IM - View receives a severe event, the color of the light in the top area of the screen changes to red. If you change all severe events to Processed or delete them all on the **Severe Events** page, or if you cancel the severe events, the color of the light returns to green.

Event acquisition filter

If an event acquisition filter is set, JP1 events that JP1/IM - Manager acquires from JP1/Base are restricted.

For details about how to switch the event acquisition filter that is applied when multiple event acquisition filters are set, see *5.5.3 Switching the event acquisition filter to be applied*.

For details about how to set a common exclusion-condition based on JP1 events that have occurred during operation and then apply this condition, see *5.5.4 Setting an additional common exclusion-condition to exclude a JP1 event from the monitoring target or action execution*.

For details about how to preset each filter, see *4.2 Setting JP1 event filtering* in the *JP1/Integrated Management - Manager Configuration Guide*.

5.2 Displaying detailed JP1 event information

You can display the detailed attribute information of JP1 events that are displayed in the events list.

To display detailed information, in the events list in the Event Console window, double-click the JP1 event whose attributes you want to display. The Event Details window opens.

If you double-click a consolidated event displayed by the repeated event monitoring suppression function or the consolidated display of repeated events function, the detailed information about the consolidation start event is displayed. For details about how to check detailed information about repeated events that are consolidated into a consolidated event, see [5.4.1\(1\) Checking detailed information about repeated events that are consolidated into a consolidated event](#).

The Event Details window displays event attributes, a message, event guide information, and a memo.

Event attributes displays the event attribute name and attribute value registered for that JP1 event. The registered attributes differ depending on the JP1 event.

To display detailed information for the previous or next JP1 event in the events list, click the **Previous** or **Next** button.

You can also use one of the following methods to display details about a JP1 event:

- In the Event Console window, select a JP1 event, and then from the **View** menu, choose **Event Details**.
- In the Event Console window, select a JP1 event, and then from the pop-up menu, choose **Event Details**.
- In the Event Console window, select a JP1 event, and then click the **Event Details** button in the toolbar.

The table below shows the items that are displayed as detailed information.

Table 5–3: Detailed JP1 event information

Display name#1	Description
Serial number	Order in which the JP1 event arrived at this event server, regardless of the source.
Event ID	Value that indicates the source program of the event that occurred.
Source process ID	Process ID of the source application program.
Registered time	Time at which the JP1 event was registered in the source event server.
Arrival time	Time at which the JP1 event was registered in the local event server.
Source user ID	Source process user ID. The ID is -1 if the event comes from Windows.
Source group ID	Source process group ID. The ID is -1 if the event comes from Windows.
Source user name	Source process user name.
Source group name	Source process group name. The name is left blank if the event comes from Windows.
Source event server name	Source event server name (displayed as the registered host name in the events list). Even when the event is forwarded from JP1/Base (agent) to JP1/IM - Manager (site manager) to JP1/IM - Manager (integrated manager), for example, the event server name of the first JP1/Base is used.
Source IP address	IP address corresponding to the source event server.
Source serial number	Serial number at the source host (the value does not change through forwarding).
Severity	This attribute indicates the urgency of a JP1 event, in the following descending order: Emergency, Alert, Critical, Error, Warning, Notice, Information, and Debug. When you are using the integrated monitoring database, if you use the severity changing function to change a severity level, this attribute indicates the urgency of the JP1 event after the change.

Display name#1	Description
User name	Name of the user that is executing the job.
Product name	Name of the program that issued the JP1 event.
Object type	Name that indicates the type of object that triggered event generation.
Object name	Name of the object (job, jobnet, etc.) that triggered event generation.
Root object type	Object type. The root object type is normally the same as the object type, but the highest-order object type is used for multi-level objects, such as jobnets. The value range is the same as for the object type.
Root object name	Name that becomes the unit for specifying execution during user operations. The root object name is normally the same as the object name, but the highest-order object name is used for multi-level objects, such as jobnets.
Object ID	Serial number of the event that triggered an action.
Occurrence	Event that occurred for the object indicated by the object name.
Start time	Execution start time or re-execution start time.
End time	Execution end time.
Result code	Command execution result.
Source host name	Name of the host on which an event generating a JP1 event occurs. A name is displayed when the integrated monitoring database is used and when source host mapping is enabled.
Item name of program-specific information of extended attribute#2	Attribute value of the program-specific extended attribute defined in the definition file for extended event attributes (extended file).
Relation Event serial number	Serial numbers of correlation source events, delimited by spaces and displayed in the following format: <i>serial-numberΔserial-numberΔserial-number . . .</i>
Correlation event generation condition name	Approved correlation event generation condition name.
Severity (before change)	When the integrated monitoring database is used and when a severity level is changed using the severity changing function, the urgency of the JP1 event before the change is displayed. The urgency level can take one of the following values (listed in descending order): Emergency, Alert, Critical, Error, Warning, Notice, Information, and Debug.
Display message change definition name	Definition name of display message change. This item can be displayed when the integrated monitoring database is used and the detailed information whose message was changed by using the display message change function is selected.
Suppressed event ID	Serial number (unique number in the event database) of a repeated event that occurs more frequently than the threshold. When the repeated event monitoring suppression function is used, the value for this item is displayed in character string format.
Repeated event condition name	Condition name of a repeated event that is determined to be a repeated event. When the repeated event monitoring suppression function is used, the value for this item is displayed in character string format.
Monitoring ID	Log file trap ID.
Monitoring name	Log file trap name.
Common exclude conditions group ID	ID of the common exclusion-conditions group that caused the exclusion.
Common exclude conditions group name	Name of the common exclusion-conditions group that caused the exclusion.

Display name#1	Description
Common exclude conditions group target-for-exclusion	Exclusion target of the common exclusion-conditions. <code>action</code> appears when the JP1 event is excluded from automated-action execution.
Message	Character string describing the event. If the integrated monitoring database is used, both the original message and changed message can be displayed when the detailed information whose message was changed by using the display message change function is selected.
Guide	Event guide information corresponding to the JP1 event. This information is displayed when event guide display is enabled. If there is no event guide information for a JP1 event, the message <code>KAVB1588-I</code> is displayed.
Memo	When the integrated monitoring database is used and the function for setting memo entries is enabled, memo entries are displayed.

#1: For an event that matches a definition in the definition file for the extended event attributes, the item names specified in the definition file for the extended event attributes are displayed.

#2: This is the item name defined in the definition file for extended event attributes (extended file).

Note that items beginning with *Severity* may not be displayed in some cases, depending on the event.


5.2.1 Editing JP1 memo entries

When you are using the integrated monitoring database, by enabling the memo entry setup function, you can add memo entries to JP1 events saved in the integrated monitoring database. This subsection explains how to edit memo entries and apply them to JP1 events in the integrated monitoring database.

For details about how to set up the integrated monitoring database, see *1.4.2 Setting up the integrated monitoring database (for Windows)* or *2.4.2 Setting up the integrated monitoring database (for UNIX)* in the *JP1/Integrated Management - Manager Configuration Guide*.

For details about how to enable the memo entry startup function, see *4.7 Setting memo entries* in the *JP1/Integrated Management - Manager Configuration Guide*.

Note that the following operations require `JP1_Console_Admin` permission or `JP1_Console_Operator` permission:

1. Open the Edit Event Details window.
You can open the Edit Event Details window by clicking the **Edit** button in the Event Details window or by selecting a single event from the events list and selecting the **Edit Event Details** menu.
2. Describe a memo entry in the Edit Event Details window.
3. Click the **Apply** button in the Edit Event Details window.
The memo entry is displayed in **Memo**, which is a display item in the events list, and in the Event Details window. The memo icon  is also displayed for events that have memo entries.

5.3 Setting JP1 event response statuses




This subsection provides an overview on how to set JP1 event response statuses and explains the operation procedure. It also explains how to delete severe events that are displayed on the **Severe Events** page.

5.3.1 Settings for JP1 event response statuses

You can set a response status for any JP1 event listed on each page of the Event Console window. When you set a response status for an event, a response status icon is displayed in the far-left column of the events list.

The following table shows the response status types and the corresponding response status icons. Choose the response status to set for each situation based on the operation.

Table 5–4: Response status types and response status icons

Response status	Response status icon
Processed	
Processing	
Held	
Unprocessed	(No icon)
Different response status #	!

#

When you use the repeated event monitoring suppression function or the consolidated display of repeated events function, this symbol indicates a situation in which JP1 events with different response statuses set are consolidated and coexist in a single consolidated event.

When you use the repeated event monitoring suppression function, an exclamation mark (!) is displayed if the 1st (the consolidation event) to 100th repeated events do not all have the same response status. If more than 100 events are consolidated, a different status among the 101st and subsequent events does not cause the exclamation mark (!) to appear.

The response status that is set is registered in the logged-in manager's integrated monitoring database or event database. (For a JP1 event has been forwarded from another host, the information in the integrated monitoring database or event database of the forwarding source host is not changed.) Consequently, the response status is applied to the **Monitor Events** and **Severe Events** pages of instances of JP1/IM - View that are logged in to the same manager.

The **Search Events** page displays the content of JP1 events at the time of the search, and therefore the displayed content does not change even if the response status is set in another page. To refresh the display, perform the search again.

Setting a response status for a consolidated event

When you set a response status for a consolidated event, the response statuses of all repeated events that have been consolidated into the consolidated event by the setting time are also changed to the same response status. However, if you are using the repeated event monitoring suppression function and more than 100 events are consolidated, the response status for the 101st and subsequent events is not changed.

The response status of repeated events is not set if they are consolidated after the response status is changed. Since repeated events with different response statuses coexist within the consolidated event, an exclamation mark (!) is displayed as the response status.

5.3.2 Setting a response status for JP1 events from the events list

This subsection explains how to set a response status for JP1 events. This operation assumes the following:

- The JP1 user who logs in to JP1/IM - Manager has `JP1_Console_Admin` permissions or `JP1_Console_Operator` permissions.
 - If the response status is being set on the **Search Events** page, the search results must be from a logged-in manager.
1. In the Event Console window, from the events list in each page, select the JP1 event for which you wish to set a response status.
 2. Perform one of the following operations (which can be performed regardless of the response status of the selected event):
 - From the menu bar, choose **View**, and then from the submenu, select the response status you wish to set.
 - From the popup menu that opens when you right-click the mouse, select the response status you wish to set.
 - Among the buttons on the **Severe Events** page (if you are setting a response status from the **Severe Events** page), click the button for the response status you wish to set.



Note

To set a response status for a severe event, you can use the `jcochstat` command. For details about the `jcochstat` command, see *jcochstat* in *Chapter 1. Commands of the JP1/Integrated Management - Manager Command and Definition File Reference*.

5.3.3 Deleting severe events from the Severe Events page

This subsection explains how to delete severe events from the **Severe Events** page. This operation assumes the following:

- The JP1 user who logs in to JP1/IM - Manager has `JP1_Console_Admin` permissions or `JP1_Console_Operator` permissions.
1. In the Event Console window, from the events list in each page, select the JP1 event you wish to delete.
 2. Perform one of the following operations (which can be performed regardless of the response status of the selected event):
 - From the menu bar, choose **View**, and then **Delete**.
 - Right-click the mouse, and from the popup menu that opens, choose **Delete**.
 - Out of the buttons on the **Severe Events** page, click the **Delete** button.

The deletion operation here merely deletes the JP1 event from the window, but does not delete it from the event database or the integrated monitoring database. Likewise, the deletion information is not applied to other pages of the Event Console window.

5.4 Operating JP1 events from the Related Events window

This subsection explains how to operate JP1 events from the Related Events window. For details about the Related Events window, see the following locations in the manual *JP1/Integrated Management - Manager GUI Reference*:

- *2.8 Related Events (Summary) window*
- *2.9 Related Events (Correlation) window*

5.4.1 Checking detailed information about repeated events and changing the response status

When you use the repeated event monitoring suppression function or the consolidated display of repeated events function, and wish to check detailed information about repeated events that are consolidated into a consolidated event or set a response status for them, operate JP1 events from the Related Events (Summary) window.

(1) Checking detailed information about repeated events that are consolidated into a consolidated event

To check detailed information about repeated events that are consolidated into a consolidated event:

1. On the **Monitor Events** page or **Severe Events** page of the Event Console window, select one consolidated event.
2. In the Event Console window, from the View menu, choose **Display Related Event List**.[#]

The Related Events (Summary) window opens.

#

You cannot select this menu command if:

- Multiple events are selected on the **Monitor Events** page or **Severe Events** page
 - A non-consolidated event is selected
3. From **Related Events** in the Related Events (Summary) window, double-click the repeated event whose detailed information you wish to check.

The Event Details window opens.

If the repeated event monitoring suppression function is enabled, the 101st and subsequent repeated events do not appear in the Related Events (Summary) window. In this case, the **Events that cannot be displayed** area of the Related Events (Summary) window displays the arrival time of the 101st repeated event, and the arrival time of the last repeated event. If you want to view detailed information about the 101st and subsequent repeated events, specify the arrival times of repeated events (displayed in the **Events that cannot be displayed** area) as search conditions.

Note that you can also search for repeated events consolidated in a consolidation event. To do this, specify the suppressed event ID, which is assigned to each consolidation event, as a search condition.

For details about how to search for events, see [5.8 Searching for JP1 events](#).

(2) Setting a response status for repeated events that are consolidated into a consolidated event

To set a response status for repeated events that are consolidated into a consolidated event:

1. On the **Monitor Events** page or **Severe Events** page of the Event Console window, select one consolidated event.

2. In the Event Console window, from the View menu, choose **Display Related Event List**.#

The Related Events (Summary) window opens.

#

You cannot select this menu command if:

- Multiple events are selected on the **Monitor Events** page or **Severe Events** page.
- A non-consolidated event is selected.

3. In the Related Events (Summary) window, under **Related Events**, double-click the repeated event for which you wish to set a response status.

You can also select multiple repeated events.

4. Right-click the selected repeated event, and from the popup menu that opens, select the response status you wish to set.

The response status is set for the repeated event.

The response status of the consolidated event into which repeated events are consolidated does not change. Since repeated events with different response statuses coexist within the consolidated event, an exclamation mark (!) is displayed as the response status.

For details about the response status types and their corresponding icons, see [5.3.1 Settings for JP1 event response statuses](#).

5.4.2 Checking detailed information about a correlation event and changing the response status

You can perform the same kinds of operations on correlation events as on JP1 events. For example, you can display event details and change the response status.

In the case of a correlation approval event, from the correlation event, you can display the correlation source event that became the trigger for its generation. If the host that generated the correlation event is different from the host you logged in to using JP1/IM - View, the correlation source event is acquired from the host that generated the correlation event.

In the case of a correlation failure event, you can display the correlation source events that were associated according to the event-correlating condition until the time when the correlation failure occurred.

If you are using the repeated event monitoring suppression function or the consolidated display of repeated events function, correlation events may be consolidated and displayed as shown below.

Table 5–5: Example of consolidated display of correlation events

Display example	Explanation						
<table border="1"> <thead> <tr> <th>Summary status</th> <th>Type</th> <th>Event level</th> </tr> </thead> <tbody> <tr> <td>24</td> <td></td> <td> Error</td> </tr> </tbody> </table>	Summary status	Type	Event level	24		Error	Correlation events have been consolidated.
Summary status	Type	Event level					
24		Error					
<table border="1"> <thead> <tr> <th>Summary status</th> <th>Type</th> <th>Event level</th> </tr> </thead> <tbody> <tr> <td>18+</td> <td></td> <td> Error</td> </tr> </tbody> </table>	Summary status	Type	Event level	18+		Error	Correlation events are being consolidated.
Summary status	Type	Event level					
18+		Error					
<table border="1"> <thead> <tr> <th>Summary status</th> <th>Type</th> <th>Event level</th> </tr> </thead> <tbody> <tr> <td>15 Del</td> <td></td> <td> Alert</td> </tr> </tbody> </table>	Summary status	Type	Event level	15 Del		Alert	Correlation events that have been consolidated are deleted.
Summary status	Type	Event level					
15 Del		Alert					
<table border="1"> <thead> <tr> <th>Summary status</th> <th>Type</th> <th>Event level</th> </tr> </thead> <tbody> <tr> <td> 24</td> <td></td> <td> Error</td> </tr> </tbody> </table>	Summary status	Type	Event level	24		Error	The response status of the correlation event's consolidation start event is different from the response status of the repeated events.
Summary status	Type	Event level					
24		Error					

In this case, to display the correlation source event, first open the Related Events (Summary) window and then open the Related Events (Correlation) or Related Events (Correlation fails) window.

(1) Displaying correlation source events

This subsection explains how to display correlation source events. For details about how to view events that are consolidated and displayed, see [5.1.2\(1\) Displaying consolidated events in the events list](#).

1. On each page of the Event Console window, select one correlation event from the events list.
2. In the Event Console window, from the View menu, choose **Display Related Event List**.
 - If the correlation event that you selected in the previous step is a non-consolidated event:
The Related Events (Correlation) or Related Events (Correlation fails) window opens and lists correlation events. The next step is not necessary.
 - If the correlation event that you selected in the previous step is a consolidated event:
The Related Events (Summary) window opens. Proceed to the next step.

#

You cannot select this menu command when multiple JP1 events are selected from the events list.

3. If the Related Events (Summary) window opens in the previous step, select one correlation event from **Related Events**, and from the popup menu that opens when you right-click the mouse, select **Display Related Event List**. The Related Events (Correlation) or Related Events (Correlation fails) window opens and lists correlation source events.

(2) Setting a response status for a correlation source event from the Related Events (Correlation) or Related Events (Correlation fails) window

This subsection explains how to set a response status for a correlation source event from the Related Events (Correlation) or Related Events (Correlation fails) window. This operation assumes the following:

- The JP1 user who logs in to JP1/IM - Manager has `JP1_Console_Admin` permissions or `JP1_Console_Operator` permissions.
- If the response status is being set from the **Search Events** page, the search results must be from a logged-in manager.

1. Follow the procedure in [5.4.2\(1\) Displaying correlation source events](#) and display the correlation source event for which you wish to set a response status.
2. From **Related Events**, select the correlation source event for which you wish to set a response status.



Note

You can also set a response status for a correlation event by selecting a correlation event from **Display Items**.

3. Right-click the selected correlation source event, and from the popup menu that opens, select the response status you wish to set.
The response status is set for the correlation source event.



Note

Even if you change the response status of the correlation event to be displayed in the Related Events (Correlation) or Related Events (Correlation fails) window, the response status of the correlation source events displayed in the list does not change. Likewise, even if you change the response status of the correlation source events displayed in the list, the response status of the correlation event to be displayed does not change. This is because correlation source events and correlation events express different phenomena.

(3) Deleting correlation source events from the Related Events (Correlation) or Related Events (Correlation fails) window

This subsection explains how to delete correlation source events from the Related Events (Correlation) or Related Events (Correlation fails) window. This operation assumes the following:

- The JP1 user who logs in to JP1/IM - Manager has `JP1_Console_Admin` permissions or `JP1_Console_Operator` permissions.
1. Follow the procedure in [5.4.2\(1\) Displaying correlation source events](#), and from the **Severe Events** page, display the correlation source event you wish to delete.
 2. Make sure that the content displayed in **Display window:** of the Related Events (Correlation) or Related Events (Correlation fails) window is either of the following:
 - **Severe Events**
 - **Severe Events - Related Events (Summary)**
 3. From **Related Events**, select the correlation source event you wish to delete.



Note

You can also delete a correlation event by selecting a correlation event from **Display Items**.

4. Right-click the selected correlation source event, and from the popup menu that opens, choose **Delete**.
The correlation source event is deleted.
The deletion operation here merely deletes the correlation source event from the window, but does not delete it from the event database or the integrated monitoring database. Likewise, the deletion information is not applied to other pages of the Event Console window.

5.5 Applying a JP1/IM filter

This subsection explains how to apply a JP1/IM filter from JP1/IM - View.

5.5.1 Enabling a view filter to display only certain JP1 events

To switch the view filter that is applied to JP1 events displayed on the **Monitor Events** and **Severe Events** pages of the Event Console window, perform the following operation. Filters must already be set up before a view filter can be switched.

For details about setting up view filters, see the following section:

See *4.2.1 Settings for view filters* in the *JP1/Integrated Management - Manager Configuration Guide*.

1. From the **Filter name** list box, select the view filter you want to enable.
2. Check the **View filter** check box, or from the menu, choose **View**, and then **Apply Filter Settings**.
JP1 events that match the condition set by the filter are displayed on the **Monitor Events** and **Severe Events** pages of the Event Console window.

5.5.2 Displaying only severe events

To display only severe events on the screen, from the Event Console window, choose the **Severe Events** page. The events list on the **Severe Events** page displays only the severe events from among the JP1 events that are displayed on the **Monitor Events** page.

The administrator can define which JP1 events are considered severe events. The default is that JP1 events whose severity level is **Emergency**, **Alert**, **Critical**, or **Error** are defined as severe events.

If the number of severe events displayed on the **Severe Events** page exceeds the maximum number of events that can be displayed on the screen, the oldest severe events are erased. The first severe event to be erased is a **Processed** severe event. If there are no **Processed** severe events, the oldest event among the **Unprocessed**, **Held**, and **Processing** severe events is deleted. In this case, the oldest severe event is deleted regardless of its status. For details about how to set a response status for JP1 events, see *5.3.2 Setting a response status for JP1 events from the events list*.

By enabling the integrated monitoring database, you can display all events stored in it. To display specific events, use the slider to adjust the event display start-time. For details about how to set up the integrated monitoring database, see *1.4.2 Setting up the integrated monitoring database (for Windows)* or *2.4.2 Setting up the integrated monitoring database (for UNIX)* in the *JP1/Integrated Management - Manager Configuration Guide*.

When you use the repeated event monitoring suppression function, deleting a consolidated event from the events list deletes any of the oldest 100 repeated events that have not already been deleted. It does not delete the 101st and subsequent repeated events. Note that deleting a repeated event does not reduce the number of consolidated events.

If a view filter is set, you can further filter the JP1 events that are displayed. Select the filter you want to apply from the **Filter name** list box, and then select the **View Filter** check box. Only JP1 events that satisfy the set filtering conditions will be displayed.

If, in the Preferences window, you select the **Display** check box of the **Coloring** field, and you then click the **Include the Severe Events** page radio button, the background of a line in an event list is highlighted in the color for that event level.

You can change the background color in the system color definition file (`systemColor.conf`). For details, see *System color definition file (systemColor.conf)* in *Chapter 2. Definition Files* of the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

5.5.3 Switching the event acquisition filter to be applied

From the multiple event acquisition filters that have been saved, you can select the filtering condition that JP1/IM uses when it acquires JP1 events from JP1/Base, and you can switch to this condition.

In an event acquisition filter, you can switch between enabling and disabling a common exclusion-condition, which is defined to temporarily exclude certain JP1 events from being acquired.

You switch the common exclusion-condition when it is necessary to exclude a host on which maintenance work is being performed from the monitoring object, so that the JP1 events generated on the host undergoing maintenance are temporarily filtered out and not acquired.

The following three methods are available for switching event acquisition filters and common exclusion-conditions:

- Making the switch from the System Environment Settings window
If you know the name of the event acquisition filter you want to switch to, select that event acquisition filter from the System Environment Settings window and make the switch.
- Making the switch from the Event Acquisition Conditions List window
If you cannot identify the name of the event acquisition filter from the System Environment Settings window, check the setting content of event acquisition filters in the Event Acquisition Conditions List window and make the switch.
- Using the `jcochfilter` command to make the switch
Use the job scheduler function of JP1/AJS and execute the `jcochfilter` command at the specified time to create a jobnet that starts a maintenance job. In this way, you can automate the process of changing the maintenance job and monitoring state.

Note, however, that if an event acquisition filter is running for a compatibility reason, you cannot switch it.

To start the System Environment Settings window or Event Acquisition Conditions List window, you need JP1_Console_Admin permissions. In addition, when reference and operation permissions are set for a business group, operations in these windows might not be possible, depending on the combination of the JP1 resource group and JP1 permissions level. For details, see *3.1.4(2) Assigning a JP1 resource group and permission level to a JP1 user* in the *JP1/Integrated Management - Manager Overview and System Design Guide*.

For details about the events that are generated when an event acquisition filter is switched, see *3.2.2 Event acquisition filter* in the *JP1/Integrated Management - Manager Overview and System Design Guide*.

(1) Switching an event acquisition filter from the System Environment Settings window

To switch an event acquisition filter:

1. In the Event Console window, choose **Options** and then **System Environment Settings**.
The System Environment Settings window opens.
2. From the **A filter is being applied** drop-down list, select an event acquisition filter.
3. Click **Apply**.

The setting is enabled.

(2) Switching between enabling and disabling a common exclusion-condition from the System Environment Settings window

To switch between enabling and disabling a common exclusion-condition:

1. In the Event Console window, choose **Options** and then **System Environment Settings**.
The System Environment Settings window opens.
2. In **Common exclusion-conditions groups**, select the condition group you want to apply.
3. Click **Apply**.
The setting is enabled.

(3) Switching the event acquisition filter from the Event Acquisition Conditions List window

To switch an event acquisition filter:

1. In the Event Console window, choose **Options** and then **System Environment Settings**.
The System Environment Settings window opens.
2. In **Event acquisition conditions**, click the **Editing list** button.
The Event Acquisition Conditions List window opens.
3. From **Filter list**, select an event acquisition filter.
Select an event acquisition filter based on the filter ID or filter name. To check the content, select an event acquisition filter and click the **Edit** button. The Event Acquisition Settings window opens and you can check the content of the filter you selected.
4. Click **OK**.
The display returns to the System Environment Settings window.
5. Click **Apply**.
The setting is enabled.

In the Event Acquisition Conditions List window, you can add, edit, copy, and delete filtering conditions. For details, see *4.2.4 Settings for event acquisition filters* in the *JPI/Integrated Management - Manager Configuration Guide*.

(4) Switching between enabling and disabling a common exclusion-condition from the Event Acquisition Conditions List window

To switch between enabling and disabling a common exclusion-condition:

1. In the Event Console window, choose **Options** and then **System Environment Settings**.
The System Environment Settings window opens.
2. Click the **Editing list** button in **Event acquisition conditions**.
The Event Acquisition Conditions List window opens.
3. In **Common exclusion-conditions groups**, check the condition group you want to apply.

To check the content, select a common exclusion-condition and click the **Edit** button. The Common Exclusion-Conditions Settings window opens and you can check the content of the common exclusion-condition you selected.

4. Click **OK**.

The display returns to the System Environment Settings window.

5. Click **Apply**.

The setting is enabled.

(5) Using the `jcochfilter` command to switch an event acquisition filter

Each event acquisition filter is assigned a unique filter ID. By using this filter ID and the `jcochfilter` command, you can switch an event acquisition filter.

For details about the `jcochfilter` command, see *jcochfilter* (in *Chapter 1. Commands*) in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

To switch an event acquisition filter:

1. Enter the `jcochfilter` command and display an event acquisition conditions list.

Examples follow of displaying an event acquisition conditions list on a physical host and a logical host.

- Displaying an event acquisition conditions list on a physical host

Enter the command as follows.

```
jcochfilter
```

- Displaying an event acquisition conditions list on logical host `hostA`

Enter the command as follows.

```
jcochfilter -h hostA
```

A display example follows of an event acquisition conditions list on logical host `hostA`.

Figure 5–3: Using the `jcochfilter` command to display an event acquisition conditions list

```
> jcochfilter
KAVB1005-I The command (jcochfilter) has started.
KAVB0856-I The list of event acquisition filters will now be displayed.
(host name: hostA)
KAVB0857-I A connection to JP1/IM - Manager has been established.
Filter ID currently being used: 3
  Filter name: Normal operation filter
Common exclusion-conditions group ID currently being applied: 0
  Common exclusion-conditions group name: Application server maintenance
Common exclusion-conditions group ID currently being applied: 2
  Common exclusion-conditions group name: Database server maintenance

Defined filter list:
ID Filter name
0 Existing filtering condition
3 Normal operation filter
Defined common exclusion-conditions group list:
ID Condition group name
0 Application server maintenance
1 Web server maintenance
2 Database server maintenance
KAVB1002-I The command (jcochfilter) terminates normally.
```

If JP1/IM - Manager on the specified host has not started, you cannot use the command to switch an event acquisition filter.

2. Select an event acquisition filter based on the filter ID and filter name.

3. Enter the `jcochfilter -i` command and switch the event acquisition filter.

Examples of switching an event acquisition filter on a physical host and a logical host are described below.

- Switching an event acquisition filter on a physical host to a filter that has a filter ID of 3

Enter the command as follows.

```
jcochfilter -i 3
```

- Switching an event acquisition filter on logical host `hostA` to a filter that has a filter ID of 3

Enter the command as follows.

```
jcochfilter -i 3 -h hostA
```

(6) Using the `jcochfilter` command to switch between enabling and disabling a common exclusion-condition

Each common exclusion-condition is assigned a unique common exclusion-condition group ID. Using this common exclusion-condition group ID and the `jcochfilter` command, you can switch between enabling and disabling a common exclusion-condition.

For details about the `jcochfilter` command, see *jcochfilter* (in *Chapter 1. Commands*) in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

To switch between enabling and disabling a common exclusion-condition:

1. Enter the `jcochfilter` command and display an event acquisition conditions list.

Examples of displaying an event acquisition conditions list on a physical host and a logical host are described below.

- Displaying an event acquisition conditions list on a physical host

Enter the command as follows.

```
jcochfilter
```

- Displaying an event acquisition conditions list on logical host `hostA`

Enter the command as follows.

```
jcochfilter -h hostA
```

If JP1/IM - Manager on the specified host has not started, you cannot use the command to switch an event acquisition filter.

2. Select a common exclusion-conditions group based on the common exclusion-conditions group ID and the common exclusion-conditions group name.

3. Switch between enabling and disabling the common exclusion-conditions group.

Use one of the following options to switch between enabling and disabling the common exclusion-conditions group.

- `-e` option

Specify the common exclusion-conditions group ID you want to enable.

Unspecified common exclusion-conditions groups are disabled.

- `-on` or `-off` option

Specify the common exclusion-conditions group ID you want to enable.

The enabling and disabling settings of unspecified common exclusion-conditions groups are not changed.

These options can be used when the operating mode of the common exclusion-condition is extended mode.

The following describes an example of switching between enabling and disabling common exclusion-conditions on the physical host and a logical host.

- On the physical host, the common exclusion-conditions with common exclusion-conditions group ID 3 are enabled, and the common exclusion-conditions with common exclusion-conditions group IDs 1 and 2 are disabled (only the specified common exclusion-conditions groups are changed).
This specification can be used when the operating mode of the common exclusion-condition is extended mode.

```
jcochfilter -on 3 -off 1,2
```
- On the physical host, the common exclusion-conditions with common exclusion-conditions group ID 3 are enabled, and the other common exclusion-conditions are disabled.

```
jcochfilter -e 3
```
- On logical host `hostA`, the common exclusion-conditions with common exclusion-conditions group ID 3 are enabled, and the other common exclusion-conditions are disabled.

```
jcochfilter -e 3 -h hostA
```

5.5.4 Setting an additional common exclusion-condition to exclude a JP1 event from the monitoring target or action execution

If the common exclusion-condition is in extended mode, you can select a JP1 event that you do not want to monitor or one that you want to monitor but exclude from action execution in the Event Console window, and then right-click the JP1 event to display a popup menu. From the popup menu, choose **Exclude by Common Exclusion-Conditions** to register the JP1 event as a common exclusion-condition.

The registered common exclusion-condition is displayed as an additional common exclusion-condition in the System Environment Settings window.

(1) Setting additional common exclusion-conditions by using JP1 events that have occurred

1. If the common exclusion-condition is in basic mode, switch it to extended mode.
For details about how to change the mode, see 4.2.4(3)(a) *Switching between common exclusion-conditions basic mode and extended mode* in the *JP1/Integrated Management - Manager Configuration Guide*.
2. Select a JP1 event you want to exclude from the event list in the Event Console window.
3. Do either of the following to display the Common Exclusion-Condition Settings (Extended) window: In the Event Console window, choose **Display** and then **Exclude by Common Exclusion-Conditions**, or from the popup menu which appears on right clicking, choose **Exclude by Common Exclusion-Conditions**.

The Common Exclusion-Condition Settings (Extended) window opens because the attribute of the JP1 event selected in step 2 has been automatically set as an event condition.


The items that are automatically set can be changed by using the common-exclusion-conditions auto-input definition file (`common_exclude_filter_auto_list.conf`). For details about the common-exclusion-conditions auto-input definition file (`common_exclude_filter_auto_list.conf`), see *Common-exclusion-conditions auto-input definition file (common_exclude_filter_auto_list.conf)* in Chapter 2. *Definition Files* of the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

Nothing is displayed in **Common exclusion-conditions group ID** in the Common Exclusion-Condition Settings (Extended) window, and nothing can be set. The common exclusion-conditions group ID of an additional common exclusion-conditions group is assigned on registration.

4. Edit the necessary items in the Common Exclusion-Condition Settings (Extended) window.
5. Click the **OK** button.
6. A message asking whether the settings should be applied is displayed. If there is no problem, click the **OK** button.
A JP1 event indicating that an additional common exclusion-condition is set is displayed in the Event Console window, and the condition is applied to the event acquisition filter.

(2) Changing an additional common exclusion-condition to a common exclusion-condition

An additional common exclusion-condition can be changed to a common exclusion-condition.

1. In the System Environment Settings window, click the **Editing list** button to display the Event Acquisition Conditions List window.
2. In the **Common exclusion-conditions groups** field of the Event Acquisition Conditions List window, select the additional common exclusion-condition (**Type** is a  icon) you want to change to a common exclusion-condition.
3. Click the **Type** button.
4. A message asking whether the type should be changed is displayed. If there is no problem, click the **OK** button.
5. In the System Environment Settings window, click the **Apply** button.

The selected additional common exclusion-condition is changed to a common exclusion-condition.

At this point, the common exclusion-conditions group ID changes. The new group ID is created by adding 1 to the highest number of the already defined common exclusion-conditions group IDs. If the new common exclusion-conditions group ID exceeds the maximum value, an unused ID is assigned in order starting from 0.

Important

If you change an additional common exclusion-condition to a common exclusion-condition by mistake, click the **Close** button in the System Environment Settings window to cancel the change before clicking the **Apply** button.

5.6 Displaying an event by specifying an event display start-time

If a large number of JP1 events occur within a short time period, and they exceed the maximum number of events that can be displayed on the **Monitor Events** page, older events might not be visible. By specifying an event display start-time, you can display these hidden events on the **Monitor Events** page. Before you can specify an event display start-time, you must enable the integrated monitoring database. For details about how to enable the integrated monitoring database, see *1.4.2 Setting up the integrated monitoring database (for Windows)* or *2.4.2 Setting up the integrated monitoring database (for UNIX)* in the *JP1/Integrated Management - Manager Configuration Guide*. For details about the display range when specifying an event display start-time, see *2.2 Monitor Events page* in the manual *JP1/Integrated Management - Manager GUI Reference*.

You can specify the event display start-time on the following pages:

- **Monitor Events** page
- **Severe Events** page

To specify an event display start-time to display JP1 events that are no longer visible:

1. In the Event Console window, click the **Expand/Shrink** button to open the event display start-time specification area.

The event display start-time specification area is not displayed when you first log in.

For details about the event display start-time specification area, see *Figure 2-4 Monitor Events page with the event display start-time specification area displayed* in *2.2 Monitor Events page* in the manual *JP1/Integrated Management - Manager GUI Reference*.

2. Move the slider to the time at which to start displaying events.

Based on the specified event display start-time, events that pass the user filter and view filter currently being applied are collected from the integrated monitoring database and displayed. The default for the maximum number of events that can be displayed (scroll buffer size) is 500. You can halt the collection of events beginning at the event display start-time by specifying a new event display start-time or by clicking the **Cancel** button.

You can specify a precise event display start-time using the **Event display start-time** text box. The default for the **Event display start-time** text box differs depending on the time you log in to JP1/IM - Manager. If the login time is later than the base time, the base time of the day you are logging in to JP1/IM - Manager is displayed by default.

Example: You log in to JP1/IM - Manager on 2008-07-08 at 10:00, when the base time is 09:00.

The default value displayed in the **Event display start-time** text box is 2008-07-08 09:00.

If the time at which you log in to JP1/IM - Manager is earlier than the base time, the previous day's base time is displayed by default.

Example: You log in to JP1/IM - Manager on 2008-07-08 at 08:00, when the base time is 09:00.

The default value displayed in the **Event display start-time** text box is 2008-07-07 09:00.

Clicking the **Most Recent Event** button returns the event display start-time to the previous setting. If the automatic scrolling function is enabled, the latest event is displayed when a new event is received. To keep displaying the events for the time specified in the event display start-time specification area even when new events are received, disable the automatic scrolling function.

5.7 Narrowing the JP1 events to be displayed by specifying a time period

You can display a list of JP1 events by enabling the display of events for a specified time period. You can also use the Web version of the function for displaying events for a specified time period

You can display events for a specified time period on the following pages:

- **Monitor Events** page
- **Severe Events** page

Event display for a specified period displays JP1 events that have passed all filters (event acquisition filter, user filter, severe events filter, and view filter) and whose repeated events have been consolidated.

This subsection explains how to enable the function for displaying events for a specified period of time, and how to specify the desired time period.

Whether a JP1 event falls within the specified time period is determined by comparing the time at which the JP1 event arrived at JP1/IM - Manager and the current time of the host on which JP1/IM - View is running. If the time set in JP1/IM - Manager is different from the time set in JP1/IM - View, JP1 events outside the specified period might be displayed. Therefore, we recommend that you synchronize the times of JP1/IM - Manager and JP1/IM - View before displaying events.

1. From the menu in the Event Console window, choose **Options** and then **Preferences**.

The Preferences window opens.

2. On the **Event Attributes** page, select the **Enable** check box in the **Specified display event period** area. **Base time** and **Display period** become enabled.

3. Specify **Base time** and **Display period**.

For **Base time**, you can specify a time from 00:00 to 23:59 as the base time for a day. The default is 09:00.

The event display range varies according to the difference between the base time and the current time. The following explains the display range for JP1 events in each case.

- If the current time of the host on which JP1/IM - View is running is later than the base time:
The range starts at the base time (*display period* - 1) days earlier and ends at the base time on the following day.
- If the current time of the host on which JP1/IM - View is running is earlier the base time:
The range starts at the base time prior to the display period and ends at the base time on the current day.

The base time at the end is not included in the range.

For example, if the current time is 09:15, and if the display period is set to 2 days and the base time is set to 09:30, a list of JP1 events that occurred from 09:30 2 days ago to 09:29 today is displayed.

For **Display period**, you can specify a range from 1 to 31 days to indicate how many days' worth of JP1 events in the immediate past you want to display. The default is 1 day.

4. Click **OK**.

The specified content (event display for the specified period) is enabled, and the Preferences window closes. The Event Console window displays JP1 events for the specified period.

If the function for displaying events for a specified period is enabled, you can switch between displaying events for the specified period and not displaying those events, by selecting the **Specified display event period** check box in the Event Console window or by selecting **View - Specified display event period** from the menu in the Event Console window.

If the function for displaying events for a specified period in the Preferences window is enabled when you log in again, you can select both the **Specified display event period** check box and the **Specified display event period** menu, and you can display the events list of each page by applying event display for the specified period. If the function is disabled, you can hide both the **Specified display event period** check box and the **Specified display event period** menu, and you can display the events list of each page without applying event display for the specified period.

For details about the specified display event period, see *3.18 Specifying the event display period* in the *JP1/Integrated Management - Manager Overview and System Design Guide*.

5.8 Searching for JP1 events

You can use various conditions to search for JP1 events and display those JP1 events that satisfy the search condition.

This section explains how to search for JP1 events and how to display the search results.

For details about the search function, see *3.6 Searching for events* in the *JPI/Integrated Management - Manager Overview and System Design Guide*. For details about the window used to search for events, see *2.25 Event Search Conditions window* in the manual *JPI/Integrated Management - Manager GUI Reference*.

5.8.1 Search method

This subsection explains the method for searching for JP1 events.

When you enable the integrated monitoring database, you can select the search object from the event database and the integrated monitoring database. For details about how to set up the integrated monitoring database, see *1.4.2 Setting up the integrated monitoring database (for Windows)* or *2.4.2 Setting up the integrated monitoring database (for UNIX)* in the *JPI/Integrated Management - Manager Configuration Guide*.

(1) Search procedure

To search for JP1 events:

1. To use the attribute value of a JP1 event displayed in the events list as the search condition, select a JP1 event from the events list in the Event Console window.
2. In the Event Console window, choose **View** and then **Search Events**. Alternatively, on the **Search Events** page of the Event Console window, click the **Search Events** button.
The Event Search Conditions window opens.
3. In the Event Search Conditions window, specify search conditions.

In the Event Search Conditions window, specify the following items:

- Specify the search object

When you use the integrated monitoring database, **Search object** is displayed in the Event Search Conditions window, and you can select either the integrated monitoring database or the event database. If you are not using the integrated monitoring database, the item **Search object** is not displayed. JP1 events in the event database are searched.

- Enter the search host

Enter the search object host name (event server name) in **Search host**.

By default, the name of the connected host is specified.

If you are using the integrated monitoring database and you select the integrated monitoring database in **Search object**, the item **Search host** becomes inactive.

The address of the specified host name is resolved inside the manager. Therefore, specify a host name that can be resolved inside the manager.

In an environment protected by a firewall, exercise special care when searching for events using a viewer that is outside the firewall, since a single host IP address might appear differently when seen from outside or inside the firewall. If you use a viewer that is outside the firewall and you specify an IP address to search for events, specify an IP address that can be resolved inside the manager.

Specify an IP address also when you are connecting to an agent that is connected to multiple LANs via an NIC of a host other than the representative host.

- Specify a search direction

Specify the direction in which to search the integrated monitoring database or the event database.

Specify either **Past direction** or **Future direction** as the event search direction. The default is **Past direction**.

For details, see *5.8.1(2) Event search direction*.

- Specify a condition group

To differentiate between various event search conditions, names are assigned to condition groups.

You can specify multiple condition groups, and condition groups are *ORed*.

To specify condition groups, you must first click the **Show List** button to show the **List** area.

Adding a condition group: Clicking the **Add** button adds undefined name *conditions-group-n* (where *n* is a number).

Copying a condition group: Selecting a condition group and clicking the **Copy** button adds *condition-group-name-selected-for-copying*.

Deleting a condition group: Selecting a condition group and clicking the **Delete** button deletes the selected condition group.

Renaming a condition group: Selecting a condition group displays the name of the selected condition group in **Condition group name**. Editing this name and moving the focus changes the name of the condition group.

- Set up a condition (detailed settings of each condition group)

Set up a pass condition or exclusion-condition for the JP1 events to be searched for.

You can set up a condition by combining multiple conditions, and the conditions are *ANDed*.

The items you can specify differ depending on the specified search item.

If the search object is the event database, the items you can specify are as follows: Event source host name^{#1}, registered host name, event level, object type, object name, root object type, root object name, occurrence, user name, message, product name, event ID, start time, end time, registered time, arrival time, response status, action^{#2}, and program-specific extended attribute.

If the search object is the integrated monitoring database, the items you can specify are as follows: Event source host name^{#1}, registered host name, event level, object type, object name, root object type, root object name, occurrence, user name, message, product name, event ID, start time, end time, registered time, arrival time, response status, action^{#2}, program-specific extended attribute, memo^{#3}, new severity level^{#4}, original severity level^{#4}, new display message^{#5}, changed display message^{#5}, repeated events^{#6}, and suppressed event ID^{#6}.

#1: You can specify this item if source host mapping is enabled.

#2: If linkage with JP1/IM - Rule Operation is enabled, you can specify the action type as a search condition.

#3: You can specify this item if the memo function is enabled.

#4: You can specify this item if the severity changing function is enabled.

#5: You can specify this item if the display message change function is enabled.

#6: You can specify this item if the repeated event monitoring suppression function is enabled.

To commit the attribute value of the JP1 event selected in the Event Console window to the condition list, click the **Read From Selected Event** button.

If the repeated event monitoring suppression function is enabled, the **Read Suppressed Event ID From Selected Event** button appears. To apply the suppressed event ID of the repeated event selected in the Event Console window, click the **Read Suppressed Event ID From Selected Event** button. Because all repeated events consolidated in a single consolidation event have the same suppressed event ID, use this button to filter those repeated events, which have the same suppressed event ID as the selected repeated event.

You can use a regular expression to specify the following: Event source host name, registered host name, object type, object name, root object type, root object name, occurrence, user name, message, product name, program-

specific extended attribute, memo, suppressed event ID, and changed display message. For details about using a regular expression to specify search conditions, see [5.8.1\(3\) Using regular expressions to specify search conditions](#).

4. Click **OK**.

When the **Search Events** page opens and the search begins, **Searching** is displayed on the page tab. Events matching the search condition are sequentially displayed on the **Search Events** page of the Event Console window as search results.

To cancel the event search, click the **Cancel Search** button. You can halt the search if you executed an event search with an incorrect search condition, or if you have found the event you wanted to acquire.

(2) Event search direction

By specifying a search direction, you can search a range that satisfies a condition. In the Preferences window, you can change the number of events that can be acquired from a single search. By clicking the **Search for Next Event** button on the **Search Events** page of the Event Console window, you can acquire and display the events that could not be acquired in a single search.

When you specify **Past direction** for the event search direction, a search is executed beginning with the latest JP1 event registered in the integrated monitoring database or the event database (events are acquired from the latest event toward earlier events). When you specify **Past direction** and execute a search, events are acquired starting with the latest one, and these events are then displayed chronologically (in order of earliest to latest). Clicking the **Search for Next Event** button displays the next set of events, acquired with the **Search for Next Event** button, above the events that have already been displayed. Note that events are always displayed chronologically starting with the earlier ones (that is, events acquired earlier are displayed above events acquired later).

When you specify **Future direction** for the event search direction, a search is executed beginning with the earliest JP1 event registered in the integrated monitoring database or the event database (events are acquired from the earliest event towards later events). When you specify **Future direction** and execute a search, events are acquired starting with the earliest one. Clicking the **Search for Next Event** button displays the next set of events, acquired with the **Search for Next Event** button, below the events that have already been displayed.

See the examples in [5.8.2 Displaying the search results](#) to confirm the behavior of the event search operation.

(3) Using regular expressions to specify search conditions

You can specify a regular expression in the search conditions specified in the Event Search Conditions window. You can specify a regular expression for the following: Event source host name, registered host name, object type, object name, root object type, root object name, occurrence, user name, message, product name, program-specific extended attribute, memo, suppressed event ID, and changed display message.

To specify a regular expression as a search condition in the Event Search Conditions window, specify a regular expression as a search condition in the **Conditions** text box, and then select **Regular expression** from the list box on the right side. To specify a regular expression for a program-specific extended attribute, use the Event Search Detailed Conditions (Program-Specific Information in Extended Attribute) window.

The types of regular expressions that can be used depend on the settings of JP1/Base at the search target host. For details, see the description about regular expressions in the chapter on installation and setup in the *JP1/Base User's Guide*.

5.8.2 Displaying the search results

Event search results are displayed on the **Search Events** page in the Event Console window.

In the Preferences window, you can specify the number of events that can be acquired in a single event search. For details about how to specify the event acquisition count in the Preferences window, see 2.24 *Preferences window* in the manual *JP1/Integrated Management - Manager GUI Reference*.

To display the events that could not be acquired in a single event search, click the **Search for Next Event** button. The content that is displayed differs depending on the search direction and the range specified by each condition.

Display examples of event search results are shown below.

Assumptions:

- The number of events that can be acquired from a single event search is 20.
- Only the following events are stored in the event database.

Figure 5–4: Events stored in the event database

```
2000 07/01 00:01:00 Event 01
2000 07/01 00:02:00 Event 02
2000 07/01 00:03:00 Event 03
2000 07/01 00:04:00 Event 04
2000 07/01 00:05:00 Event 05
(Omitted)
2000 07/01 00:56:00 Event 56
2000 07/01 00:57:00 Event 57
2000 07/01 00:58:00 Event 58
2000 07/01 00:59:00 Event 59
2000 07/01 01:00:00 Event 60
```

Example 1:

In the Event Search Conditions window, in **Search direction**, clicking the **Past direction** radio button displays in an event list the last 20 JP1 event entries registered in the event database.

Figure 5–5: Last 20 JP1 event entries

```
2000 07/01 00:41:00 Event 41
2000 07/01 00:42:00 Event 42
(Omitted)
2000 07/01 00:59:00 Event 59
2000 07/01 01:00:00 Event 60
```

Clicking the **Search for Next Event** button adds the next set of 20 events and displays them above the events that are already displayed.

Figure 5–6: Display after the Search for Next Event button is clicked

```
2000 07/01 00:21:00 Event 21
2000 07/01 00:22:00 Event 22
(Omitted)
2000 07/01 00:39:00 Event 39
2000 07/01 01:40:00 Event 40
2000 07/01 00:41:00 Event 41
2000 07/01 00:42:00 Event 42
(Omitted)
2000 07/01 00:59:00 Event 59
2000 07/01 01:00:00 Event 60
```

} Added

Example 2:

In the Event Search Conditions window, in **Search direction**, clicking the **Future direction** radio button displays in an event list the first 20 JP1 event entries registered in the event database.

Figure 5–7: First 20 JP1 event entries

2000	07/01	00:01:00	Event 01
2000	07/01	00:02:00	Event 02
			(Omitted)
2000	07/01	00:19:00	Event 19
2000	07/01	00:20:00	Event 20

Clicking the **Search for Next Event** button adds the next set of 20 events and displays them below the events that are already displayed.

Figure 5–8: Display after the Search for Next Event button is clicked

2000	07/01	00:01:00	Event 01
2000	07/01	00:02:00	Event 02
			(Omitted)
2000	07/01	00:19:00	Event 19
2000	07/01	00:20:00	Event 20
2000	07/01	00:21:00	Event 21
2000	07/01	00:22:00	Event 22
			(Omitted)
2000	07/01	00:39:00	Event 39
2000	07/01	00:40:00	Event 40

} Added

5.9 Customizing JP1 event information by operation

You can customize JP1 event information according to different operations.

5.9.1 Displaying program-specific extended attributes of JP1 events (displaying program-specific extended attributes)

When you set up the definition file for extended event attributes (extended file), you can display program-specific extended attributes in the events list of the Event Console window using desired item names.

For details about how to set up the definition file for extended event attributes (extended file), see *4.11 Setting the display and specification of program-specific extended attributes* in the *JP1/Integrated Management - Manager Configuration Guide*.

To add the program-specific extended attributes defined in the definition file for extended event attributes (extended file) to display items in the Preferences window, and then display these attributes in the events list of the Event Console window:

Note that the Web-based JP1/IM - View cannot display in the events list the item names defined in the definition file for extended event attributes (extended file).

1. From the menu in the Event Console window, choose **Options** and then **Preferences**.
The Preferences window opens.
2. Choose **Event Attributes**, and then **Display items & order**. Then, from the **Available items** box, select a program-specific extended attribute defined in the definition file for extended event attributes (extended file).
In the **Available items** box, program-specific extended attributes defined in the definition file for extended event attributes (extended file) are displayed using item names.
3. Click the -> button to move the selected item to the **Display items & order** box.
The display order in the **Display items & order** box indicates the display order in the events list. To change the display order, select an item and click the **Up** or **Down** button to move the item name.
4. Click **OK**.
The Preferences window closes. Program-specific extended attributes are displayed in the events list of the Event Console window.

5.9.2 Displaying extended attributes of JP1 events (mapping of event information)

By mapping a program-specific extended attribute to an item with a basic attribute or common extended attribute, you can display the content of a program-specific extended attribute in the display item (basic attribute or common extended attribute) column of the events list.

An example follows.

Mapping definition settings

The following mapping definitions are set:

Event information mapping definition 1

Mapping program-specific extended attribute LOGHOST to the registered host name.

Mapping-target event ID: 12E0

Event information mapping definition 2

Mapping program-specific extended attribute LOGTIME to the arrival time.

Mapping-target event ID: 12E0

Events generated:

Events with the following content are generated.

Table 5–6: Event generation content

No.	Attribute	Content
1	Severity	Error
2	Registration time	2001/10/30 17:47:31
3	Arrival time	2001/10/30 17:47:39
4	Registered host name	host_A
5	User name	jp1nps
6	Event ID	000012E0
7	Message	KAJC391-E ...
8	LOGHOST	loghost_1
9	LOGTIME	1003976997#

#: In the time format, the value becomes 2001/10/25 11:29:57.

Display in the Event Console window:

Normally, the events list in the Event Console window displays the contents of Nos. 1 to 7 in the above table, but because No. 8 is mapped to No. 4 and No. 9 is mapped to No. 3, the following is displayed:

Table 5–7: Event Console window display

Severity	Registration time	Arrival time	Registered host name	User name	Event ID	Message
Error	10/25 17:47:31	# 10/25 11:29:57	# loghost_1	jp1nps	000012E0	KAJC391- E ...

To display a program-specific extended attribute, in the Event-Information Mapping Definitions window, map a display item to the program-specific extended attribute. To start the Event-Information Mapping Definitions window, you need JP1_Console_Admin permissions. In addition, when reference and operation permissions are set for a business group, operations in the Event-Information Mapping Definitions window might not be possible depending on the combination of JP1 resource group and JP1 permission level. For details, see *3.1.4(2) Assigning a JP1 resource group and permission level to a JP1 user in the JP1/Integrated Management - Manager Overview and System Design Guide*.

Note

Difference between event information mapping and source host mapping

The event information mapping functionality maps the value of an extended attribute of a JP1 event to the attribute of a display item in an event list, and displays it. This functionality can display another attribute

value in the registered host name field of an event list. Note, however, that the functionality can be used only for changing the display of an event list. It cannot be used for event conditions, such as actions and event correlation.

The source host mapping functionality, however, registers the host name and source host name of a JP1 event acquired by JP1/IM - Manager in order to monitor and manage JP1 events. This functionality can display information in the source host name field of an event list and can also be used for event conditions, such as actions and event correlation. Note, however, that you must use the integrated monitoring database and enable source host mapping.

To map a program-specific extended attribute:

1. In the Event Console window, from the **Options** menu, choose **Event-Information Mapping Definitions**.
The Event-Information Mapping Definitions window opens.
List of definitions shows the list of mapping definition information that is currently set.
You can create a maximum of 16 mapping definitions.
2. To enable event information mapping, from the **Mapping** menu, choose **Map**.
3. To create a new mapping definition, click the **Add** button. To modify defined mapping information, choose an item from **List of definitions** and then click the **Edit** button, or double-click the item in **List of definitions**.
The Event-Information Mapping Detailed Definitions window opens.
4. From **Display items & order**, select the display item in the events list to which you want to map the program-specific extended attribute.
You can select (in the Preferences window) the following items:
Source process ID, arrival time, source user ID, source group ID, source user name, source group name, registered host name, source serial number, severity, user name, product name, object type, object name, root object type, root object name, occurrence, start time, and end time.
 - Specification example: *registered-host-name*
5. In **Attribute name**, specify the name of the program-specific extended attribute you want to map.
You can specify a maximum of 32 characters consisting of uppercase letters, numbers, and underscores. You need not specify E to indicate a program-specific extended attribute.
Each display item can be mapped to a single program-specific extended attribute.
To map a program-specific extended attribute to arrival time, start time, or end time, specify an attribute name whose attribute value is a numeric value (from 0 to 2,147,483,647 seconds from January 1, 1970 UTC). If you specify a value other than a numeric value or an attribute with a numeric value that is outside the range, the original attribute is displayed.
 - Specification example: LOGHOST
6. In **Event ID**, specify the event ID of the JP1 event you want to map.
You can specify a maximum of 1,000 characters, consisting of letters A-F or a-f, numbers, and commas. Specify the value in hexadecimal format. The range of values that can be specified is 00000000 to 7FFFFFFF.
You can specify a maximum of 100 event IDs, delimited by commas.
 - Specification example 1: 3FFF
 - Specification example 2: 12345B, 7FFFFFFF
7. Click the **OK** button.

The Event-Information Mapping Detailed Definitions window closes, and the specified content is committed to the Event-Information Mapping Definitions window.

8. In the Event-Information Mapping Definitions window, click the **Apply** button.

For events that arrive after the **Apply** button has been clicked, the program-specific extended attribute is displayed along with this mapping definition.

You can specify the mapped program-specific extended attribute to filter JP1 events when using the view filter, severe event filter, and user filter.

When a program-specific extended attribute is displayed, it is preceded by the hash mark and a space (#).

To specify a displayed program-specific extended attribute as the filtering condition, you need not enter a hash mark and a space (#).

In the Preferences window, if you select the **Display** check box of the **Coloring** field, the background of a line in an event list is highlighted in the color for that event level.

If you changed the settings in the Event-Information Mapping Definitions window, the change is applied to the events list of all JP1/IM - Views connected to the same JP1/IM - Manager.

To view the information prior to mapping, select the mapped event and open the Event Details window. The Event Details window displays the information prior to mapping. Note that you can use the definition file for extended event attributes to display program-specific extended attributes in the Event Details window. For details, see the following explanations:

Using the definition file for extended event attributes to display program-specific extended attributes

See *3.14 Displaying user-defined event attributes* in the *JP1/Integrated Management - Manager Overview and System Design Guide*.

About the definition file for extended event attributes

See *Definition file for extended event attributes* in *Chapter 2. Definition Files* of the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

Note the following points when you are mapping program-specific extended attributes:

- In an event search, because the integrated monitoring database or the event database of Event Service is searched, events before mapping are not searched. Therefore, the mapping information is not reflected in the search results. To search for mapping-target events, use **Extended attribute** in the Event Search Conditions window to specify the information of the program-specific extended attribute you want to map.
- The related events displayed in the Related Events window are the result of an event search, and therefore do not reflect the mapping information.
- If you select an event to which a program-specific extended attribute is mapped and then click the **Read From Selected Event** button in the Event Search Conditions window, for example, the attribute of the display item at the mapping destination and the value of the program-specific extended attribute are not input into the condition list.

5.9.3 Adding a user-defined extended attribute to JP1 events that match a condition

This subsection explains how to add user-defined information as an extended attribute to JP1 events by using the additional extended attribute settings file of JP1/Base.

For details about the function, see *3.12 Adding program-specific attributes* in the *JP1/Integrated Management - Manager Overview and System Design Guide*.

1. Define the event attribute to be added to the additional extended attribute settings file of JP1/Base.

In the additional extended attribute settings file, define the condition for adding the attribute and the extended attribute to be added when the condition is satisfied.

In the event filter of JP1/Base, specify the specification format for attribute addition conditions.

For the first seven bytes of an extended attribute name, specify a name that begins with JP1ADD_.

For details about the additional extended attribute settings file, see the *JP1/Base User's Guide*.

Example of content to be specified in the additional extended attribute settings file:

```
# Event : Extended attribute adding setting
add
filter
# input Event-filter
B.ID IN 111
end-filter
# input Extended-attribute
E.JP1ADD_SYSTEMNAME SystemA
end-add
```

2. Start JP1/Base or execute the `jevextreload` command.

```
jevextreload [-h event-server-name] {-recv | -send}
```

For details about the additional extended attribute settings file and the `jevextreload` command, see the *JP1/Base User's Guide*.

5.9.4 Changing the severity level of JP1 events

When you are using the integrated monitoring database, you can change the severity level of an event by setting up the severity changing function.

For details about how to set up the integrated monitoring database, see *1.4.2 Setting up the integrated monitoring database (for Windows)* or *2.4.2 Setting up the integrated monitoring database (for UNIX)* in the *JP1/Integrated Management - Manager Configuration Guide*.

For details about how to set up the severity changing function, see *4.13 Setting the severity changing function* in the *JP1/Integrated Management - Manager Configuration Guide*.

The following shows how to change the severity level of an event.

(1) Setting a severity change definition in the Severity Change Definition Settings window

To set a severity change definition in the Severity Change Definition Settings window:

1. Make sure that the severity changing function is enabled for the event.

Check whether the function is enabled by executing the `jcoimdef` command with the `-chsev` option specified.

If it is not enabled, use the `jcoimdef` command to enable it. By default, the function is not enabled. After enabling

the severity changing function, restart JP1/IM - Manager. For details about the `jcoimdef` command, see *jcoimdef Chapter 1. Commands* of the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

2. In the Event Console window, select **Options**, and then **Severity Change Definitions**.

The View Severity Change Definitions window opens.

3. Click the **Add**, **Edit**, or **Delete** button according to your needs.

If you click the **Add** button:

The Severity Change Definition Settings window opens. You can set a new severity change definition.

If you click the **Edit** button:

The Severity Change Definition Settings window opens. You can edit the selected severity change definition.

If you click the **Copy** button:

The selected severity change definition is copied and added to the View Severity Change Definitions window. `Copy` is added to the beginning of the copied severity change definition.

If you click the **Delete** button:

The selected severity change definition is deleted.

In this case, skip step 4.

4. In the Severity Change Definition Settings window, set the severity.

Set an event condition for which you want to change the severity. Then, select a new severity level from **New severity level**, and then click the **OK** button.

5. In the View Severity Change Definitions window, click the **Apply** button to enable the severity change definition.

In the View Severity Change Definitions window, select the severity change definition that was set in the Severity Change Definition Settings window, and then select the **Apply** check box to enable the severity change definition. If you want to set multiple events, repeat steps 3 through 5.

6. A confirmation message appears. To apply the settings, click **Yes**.

The severity change definition you have set takes effect.

(2) Setting a severity change definition in the severity changing definition file

To set a severity change definition in the severity changing definition file:

1. Make sure that the severity changing function is enabled for the event.

Check whether the function is enabled by executing the `jcoimdef` command with the `-chsev` option specified. If it is not enabled, use the `jcoimdef` command to enable it. By default, the function is not enabled. After enabling the severity changing function, restart JP1/IM - Manager. For details about the `jcoimdef` command, see *jcoimdef Chapter 1. Commands* of the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

2. Define the severity level change for the event in the severity changing definition file.

Create a severity change definition for each system. You can change the severity level to any of the following: Emergency, Alert, Critical, Error, Warning, Notice, Information, and Debug.

For details about the severity changing definition file, see *Severity changing definition file (jcochsev.conf)* in *Chapter 2. Definition Files* of the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

Specification example for the severity changing definition file

```
DESC_VERSION=2
def severity-change-1
  cmt comment
  define enable
  cnd
  B.ID IN 100 200
  E.SEVERITY IN Warning
  B.SOURCESERVER IN hostA hostB hostC
end-cnd
sev Emergency
end-def
```

3. Execute the `jco_spmc_reload` command or restart JP1/IM - Manager.

If you changed the severity changing function from Disabled to Enabled in step 1, you need to restart JP1/IM - Manager.

For details about the `jco_spmc_reload` command, see *jco_spmc_reload* in *Chapter 1. Commands* of the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

The severity of the JP1 event after the change has been applied is displayed under **Severity** in the events list. The severity of the JP1 event before the change is displayed under **Original severity level** in the events list. Additionally, for the JP1 event whose severity was changed, an icon is displayed under **New severity level** in the events list.

Event Base Service changes the severity of the JP1 events received from the Event Service instance on the manager, and registers the new severity level in the integrated monitoring database. During this process, the content of Event Service's event database is not changed.

A mapping definition is sometimes used to change severity. By using a mapping definition, you can display a different attribute under **Severity** in the events list.

(3) Adding a severity change definition by using events that occur during operations

During system operations, you can select an event you want to change, and add conditions for the severity change definition in the Add Severity Change Definition Settings window.

If you select an event and then add a definition, the definition is registered at the top of the definitions displayed in the View Severity Change Definitions window, and that definition takes priority.

To set the severity level of events in the Add Severity Change Definition Settings window:

1. In the Event Console window, select an event whose severity you want to change, right-click the mouse, and from the popup menu that opens, choose **Add Severity Change Definition Settings**.

The Add Severity Change Definition Settings window opens.

2. In the Add Severity Change Definition Settings window, change the severity.

Set the event conditions for which the severity is to be changed, and from **New severity level**, select a new severity level.

3. Click the **OK** button.

The added severity change definition is applied to the View Severity Change Definitions window. An icon is displayed in the **Type** column of the severity change definition that was added during operations.

(4) Converting an added severity change definition to a regular severity change definition

To convert a severity change definition that was added during system operations to a regular severity change definition:

1. From the menu in the Event Console window, select **Options** and then **Severity Change Definitions** to display the View Severity Change Definitions window.
2. In the View Severity Change Definitions window, from **View Severity Change Definitions**, select the added severity change definition (for which an icon is displayed in the **Type** column) that you want to convert to a regular severity change definition.
3. Click the **Type** button.
4. A confirmation message appears. To apply the settings, click **Yes**.
The added severity change definition that you selected is converted to a regular severity change definition.
5. In the View Severity Change Definitions window, click the **Apply** button.
6. A confirmation message appears. To apply the settings, click **Yes**.
The severity change definition that you added takes effect.

5.9.5 Changing the message displayed for a JP1 event

When you use the integrated monitoring database, you can change the messages to be displayed for events by setting the display message change function.

You can configure the display message change function by using the GUI, or you can define the function in the display message change definition file and execute the `jco_spmd_reload` command to apply the settings.

Important

Do not set a severity change definition in the GUI and in the definition file at the same time. If you modify the definition file by using a text editor or another method while the definition is being modified in the GUI, data in the definition file might become different from that in memory.

For details about how to set up the integrated monitoring database, see *1.4.2 Setting up the integrated monitoring database (for Windows)* or *2.4.2 Setting up the integrated monitoring database (for UNIX)* in the *JP1/Integrated Management - Manager Configuration Guide*.

For details about how to configure the display message change function, see *4.14 Setting the display message change function* in the *JP1/Integrated Management - Manager Configuration Guide*.

The following shows how to change the messages to be displayed for events.

(1) Setting a display message change definition in the Display Message Change Definition Settings window

To set a display message change definition in the Display Message Change Definition Settings window:

1. Make sure that the display message change function is enabled for the event.

In the Event Console window, under **Options**, check whether **Display Message Change Definitions** is displayed. If it is not displayed, enabling the integrated monitoring database will enable the display message change function. When you enable the display message change function, restart JP1/IM - Manager.

In addition, if the IM database was not updated using the `jimdbupdate` command after an upgrade of JP1/IM - Manager from version 10-50 or earlier, update the IM database. For details about the `jimdbupdate` command, see `jimdbupdate` in *Chapter 1. Commands* of the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

2. In the Event Console window, choose **Options** and then **Display Message Change Definitions**.

The Display Message Change Definitions window opens.

3. Click the **Add**, **Edit**, **Copy**, or **Delete** button according to your needs.

- If you click the **Add** button:

The Display Message Change Definition Settings window opens. You can set a new display message change definition.

- If you click the **Edit** button:

The Display Message Change Definition Settings window opens. You can edit the selected display message change definition.

- If you click the **Copy** button:

The selected display message change definition is copied and added to the Display Message Change Definitions window. `Copy` is added to the beginning of the copied display message change definition.

- If you click the **Delete** button:

The selected display message change definition is deleted.

In this case, step 4 is skipped.

4. In the Display Message Change Definition Settings window, set the message.

Set an event condition for which you want to change the message. Then, set a new message format in **Message after the change**. If you specify the facility for converting the event information to inherit, you can standardize the message character count and the number display format so that they are easy to read. For details about the facility for converting the event information to inherit, see *Display message change definition file (jcochmsg.conf)* in *Chapter 2. Definition Files* of the manual *JP1/Integrated Management - Manager Command and Definition File Reference*. After setting, click the **OK** button.

5. In the Display Message Change Definitions window, click the **Apply** button to enable the setting.

In the Display Message Change Definition Settings window, select the display message change definition that was set in the Display Message Change Definitions window, and then select the **Apply** check box to enable it. If you want to set multiple events, repeat steps 3 through 5.

6. A confirmation message appears. To apply the settings, click **Yes**.

The display message change definition that you set takes effect.

(2) Setting a display message change definition in the display message change definition file

To set a display message change definition from the display message change definition file:

1. Make sure that the display message change function is enabled for the event.

In the Event Console window, under **Options**, check whether **Display Message Change Definitions** is displayed. If it is not displayed, enabling the integrated monitoring database will enable the display message change function. When you enable the display message change function, restart JP1/IM - Manager.

In addition, if the IM database was not updated using the `jimdbupdate` command after an upgrade of JP1/IM - Manager from version 10-50 or earlier, update the IM database. For details about the `jimdbupdate` command, see `jimdbupdate` in *Chapter 1. Commands* of the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

2. Define the display message change for the event in the display message change definition file.

Define a display message change definition for each system.

In the display message change definition, specify the event condition for the JP1 event whose display message you want to change, and a new message format.

If you use the facility for converting the event information to inherit, you can standardize the message character count and the number display format so that they can be displayed in an easy-to-read manner in the events list.


For details about the display message change definition file, see *Display message change definition file (jcochmsg.conf)* in *Chapter 2. Definition Files* of the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

Specification example for the display message change definition file

```
DESC_VERSION=1
def display-message-change-1
  cmt comment-1
  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 An error occurred in the database server
  end-def
```

3. Execute the `jco_spmc_reload` command or restart JP1/IM - Manager.

For details about the `jco_spmc_reload` command, see `jco_spmc_reload` in *Chapter 1. Commands* of the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

The message for the JP1 event after the change has been applied is displayed under **Changed display message** in the events list. The message for the JP1 event before the change was applied is displayed under **Message** in the events list. Additionally, for the JP1 event whose message was changed, the icon  is displayed under **New display message**.

Event Base Service changes the messages for the JP1 events received from the Event Service instance on the manager, stores the new messages in **Changed display message**, and registers them in the integrated monitoring database. During this process, the original messages are not changed.

(3) Adding a display message change definition by using events that occur during operations

During system operations, you can select an event you wish to change, and add a condition for a display message change definition from the Add Display Message Change Definitions window.

If you select an event and then add a definition, the definition is registered at the top of the definitions displayed in the Display Message Change Definitions window, and that definition takes priority.

To add a display message change definition in the Add Display Message Change Definitions window:

1. In the Event Console window, select an event whose display message you want to change, right-click the mouse, and from the popup menu that opens, choose **Display Message Change Definitions**.
The Add Display Message Change Definitions window opens.
2. In the Add Display Message Change Definitions window, change the display message.
Set the event conditions for changing the message. Then, set a new message format in **Message after the change**. If you specify the facility for converting the event information to inherit, you can standardize the message character count and the number display format so that they are easy to read. For details about the facility for converting the event information to inherit, see *Display message change definition file (jcochmsg.conf)* in *Chapter 2. Definition Files* of the manual *JP1/Integrated Management - Manager Command and Definition File Reference*. After setting, click the **OK** button.
3. Click the **OK** button.
The added display message change definition is applied to the Display Message Change Definitions window. An icon is displayed in the **Type** column of the display message change definition that was added during operations.

(4) Converting an added display message change definition to a regular display message change definition

To convert a display message change definition that was added during system operations to a regular display message change definition:

1. From the menu in the Event Console window, select **Options** and then **Display message change definitions** to display the Display Message Change Definitions window.
2. In the Display Message Change Definitions window, from **Display Message Change Definitions**, select the added display message change definition (for which an icon is displayed in the **Type** column) that you want to convert to a regular display message change definition.
3. Click the **Type** button.
4. A confirmation message appears. To change the type, click **Yes**.
The added display message change definition that you selected is converted to a regular display message change definition.
5. In the Display Message Change Definitions window, click the **Apply** button.
6. A confirmation message appears. To apply the settings, click **Yes**.
The display message change definition that you added takes effect.

5.10 Taking actions for the generation of a large number of events

The following two methods are available for handling the occurrence of a large number of JP1 events.

Suppressing event forwarding from an agent (JP1/Base function for suppressing event forwarding)

You can suppress event forwarding from an agent on which a large number of JP1 events have occurred and stop monitoring of the agent.

Consolidating the events on the manager (JP1/IM - Manager's repeated event monitoring suppression function)

By setting a repeated event condition, you can consolidate and display JP1 events that satisfy a condition in the events list, and you can suppress execution of automatic actions.

The next subsection explains the general procedures for handling a large number of events by using each of these methods.

We recommend that you establish an operational procedure to determine beforehand the method to use for handling the occurrence of a large number of JP1 events.

For an overview of suppressing monitoring of a large number of events, see *3.5.1 Mechanism of the suppression of monitoring of a large number of events* in the *JP1/Integrated Management - Manager Overview and System Design Guide*.

Also review the settings for JP1 events to be forwarded from JP1/Base to the manager, as well as the settings for JP1 event filtering on the manager. For details about the settings for JP1 events forwarded from JP1/Base, see *11.1.2 Considerations for forwarding JP1 events to managers* in the *JP1/Integrated Management - Manager Overview and System Design Guide*. For details about the settings for event filtering on the manager, see *11.1.3 Considerations for filtering JP1 events* in the *JP1/Integrated Management - Manager Overview and System Design Guide*.

Before you can handle a large number of events by using the method that consolidates events on the manager, you need to build the integrated monitoring database, enable it, and enable suppression of repeated event monitoring on the manager. For details, see *4.3 Setting monitoring of repeated events to be prevented* in the *JP1/Integrated Management - Manager Configuration Guide*.

5.10.1 General procedures and preparation for handling occurrence a large number of events

When a large number of events are detected, you can suppress event forwarding by the applicable agent, or you can set a repeated event condition to consolidate the events, based on the events displayed in the events list of the Event Console window. If a large number of events have occurred in the past or are expected to occur again, you can prepare for the large number of events by setting a threshold in advance for automatically suppressing event forwarding or for setting a repeated event condition.

The following figures show the general procedure for each of these processes.

Figure 5–9: General procedure for handling detection of a large number of events

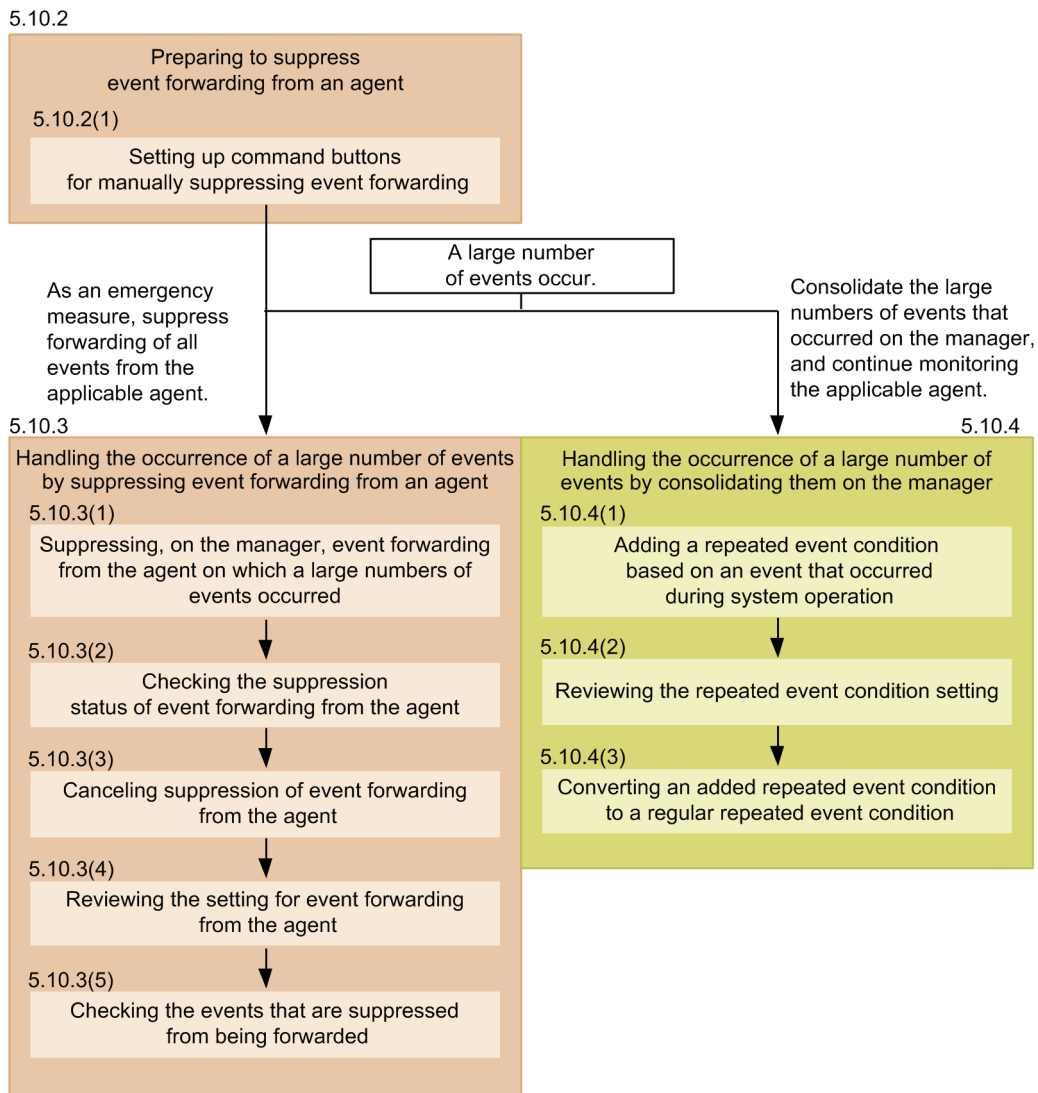
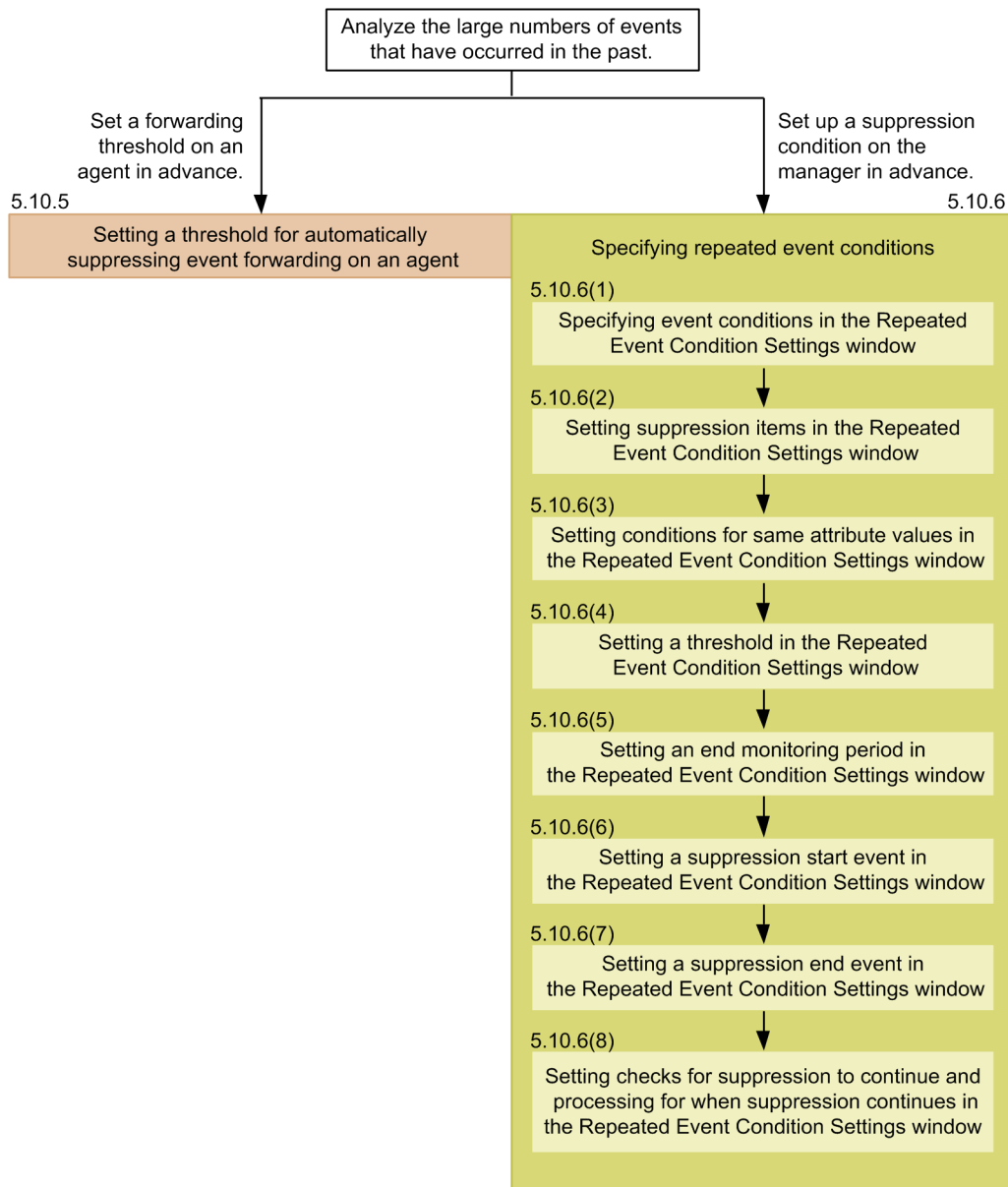


Figure 5–10: General procedure when a large number of events have occurred in the past or are expected to occur again



5.10.2 Preparing to suppress event forwarding from an agent

As part of the preparation to suppress event forwarding from an agent, set up command buttons to suppress event forwarding or cancel suppression. By setting up command buttons, you can reduce the number of command inputs required of the administrator when a large number of events need to be handled, thereby preventing operational mistakes.

The following describes the command buttons that can be set up and what each one does.

All supp button

- This is used when a large number of events occur on an agent.
- Before the command can be executed, a confirmation message appears, and the administrator must confirm execution.

- With regard to selecting an agent, the administrator selects a single event in the Console window of JP1/IM - View, and the host name is automatically extracted from it.

Cns supp button

- Operation is based on a trigger such as completion of a corrective action following an error, after which monitoring (forwarding) of events from the applicable agent resumes.
- Before the command can be executed, a confirmation message appears, and the administrator must confirm execution.
- With regard to selecting an agent, the administrator selects a single event in the Console window of JP1/IM - View, and the host name is automatically extracted from it.

Chk supp button

- This displays for confirmation the forwarding suppression status of a large number of events.

The following conditions are required for command execution:

- The JP1 user who executes the command from JP1/IM - View is registered in the authentication server.
 - The JP1 user who executes the command from JP1/IM - View has either of the following JP1 permissions:
 - JP1_Console_Admin
 - JP1_Console_Operator
 - The system configuration is defined using JP1/Base configuration management.
 - JP1 users and OS users are mapped on the manager host.
 - OS users mapped with JP1 users have execute permissions for the `jevagtfw` command on the manager host.
- For details about the `jevagtfw` command, see the chapter on commands in the *JP1/Base User's Guide*.

For details about how to set up a command execution environment, see *1.15 Setting up a command execution environment (for Windows)* or *2.14 Setting up a command execution environment (for UNIX)* in the *JP1/Integrated Management - Manager Configuration Guide*.

(1) Setting up command buttons for manually suppressing event forwarding

1. Terminate all instances of JP1/IM - View that are connected to JP1/IM - Manager.
2. Execute the `jcoimdef` command to enable the command buttons.

Command specification example

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

In the command execution result, confirm that `S_CMDBTN` is ON. Since the `-i` option is specified, command buttons are enabled immediately after command execution.

3. Set up the commands to be used as command buttons.

Create a command button definition file.

Definition example (for Windows)

```
def
  usr name-of-JP1-user-who-uses-the-command-button

  btn All supp
```

```

cmt Suppresses forwarding of all events from the applicable agent
cmdtype agent
inev true
hst manager-host-name
cmd "Base-path\bin\jevagtfw.exe" -s -o all $EVHOST
qui false
preview true
end-btn

btn Cns supp
cmt Cancels suppression of forwarding of all events from the applicable
agent
cmdtype agent
inev true
hst manager-host-name
cmd "Base-path\bin\jevagtfw.exe" -r -f $EVHOST
qui false
preview true
end-btn

btn Chk supp
cmt Confirms event forwarding suppression status
cmdtype agent
inev false
hst manager-host-name
cmd "Base-path\bin\jevagtfw.exe" -l
qui false
preview true
end-btn

end-def

```

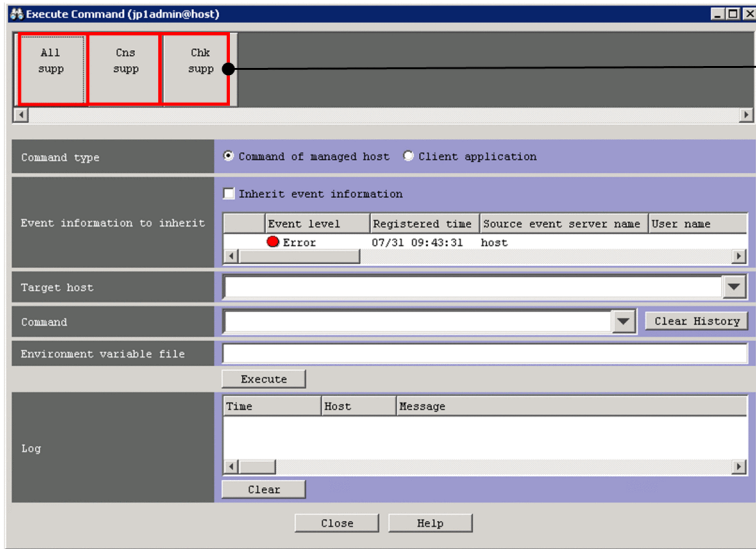
For \$EVHOST in the definition example, the event-issuing host name of the event selected in the Console window of JP1/IM - View is assigned.

For UNIX, replace *Base-path*\bin\jevagtfw.exe with /opt/jp1cons/bin/jevagtfw.exe.

4. Start the Console window of JP1/IM - View.

5. Confirm that the command buttons that were set in the Execute Command window are displayed.

To display the Execute Command window, click the **Execute Command** button in the Event Console window.



Make sure that the command buttons are displayed.

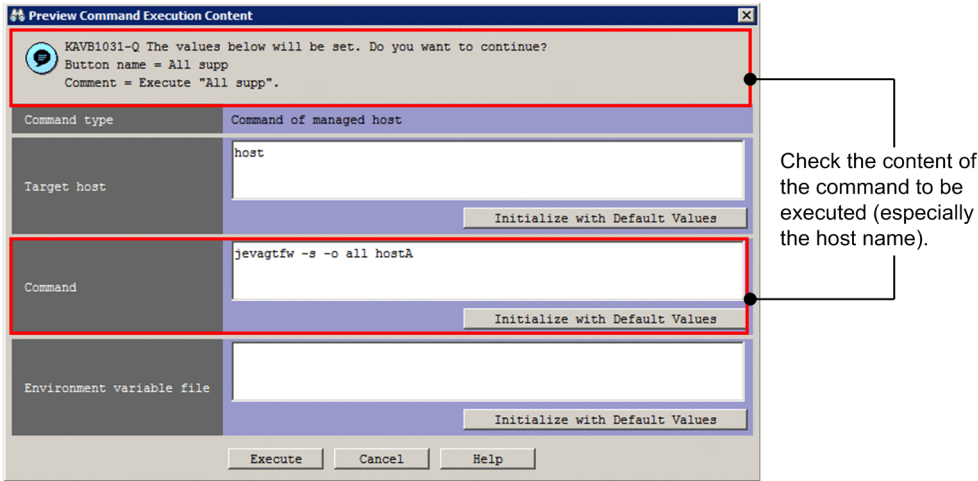
5.10.3 Handling the occurrence of a large number of events by suppressing event forwarding from an agent

This subsection explains how to use the command buttons that you set up in [5.10.2 Preparing to suppress event forwarding from an agent](#) to handle the occurrence of a large number of events by suppressing event forwarding from an agent.

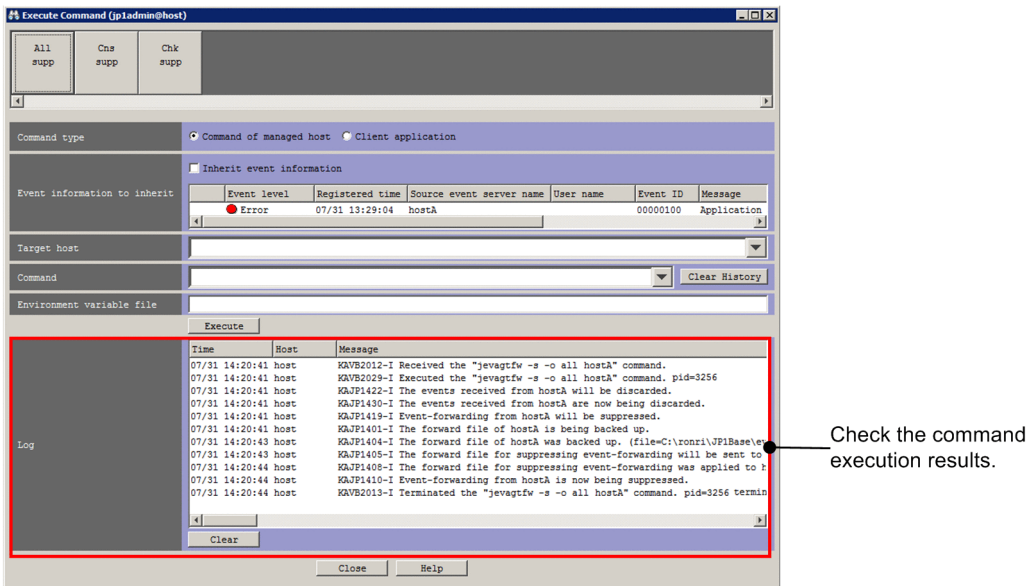
(1) Suppressing, on the manager, event forwarding from the agent on which a large numbers of events occurred

Using a command button that was set up, you can suppress, on the manager, event forwarding from an agent.

1. In the events list in the Event Console window, make sure that a large number of JP1 events are being output from a specific agent.
2. Select the JP1 events being forwarded from the agent that you wish to suppress.
3. Click the **Execute Command** button to display the Execute Command window.
4. Click the **All supp** command button that was set up in [5.10.2 Preparing to suppress event forwarding from an agent](#). The Preview Command Execution Content window opens. Check the content of the command to be executed (especially the name of the host to be suppressed).



5. In the Preview Command Execution Content window, click the **Execute** button to execute the `jevagtfw` command. Event forwarding from the specified agent is suppressed. In the **Log** area of the Execute Command window, you can check the execution result of the command.

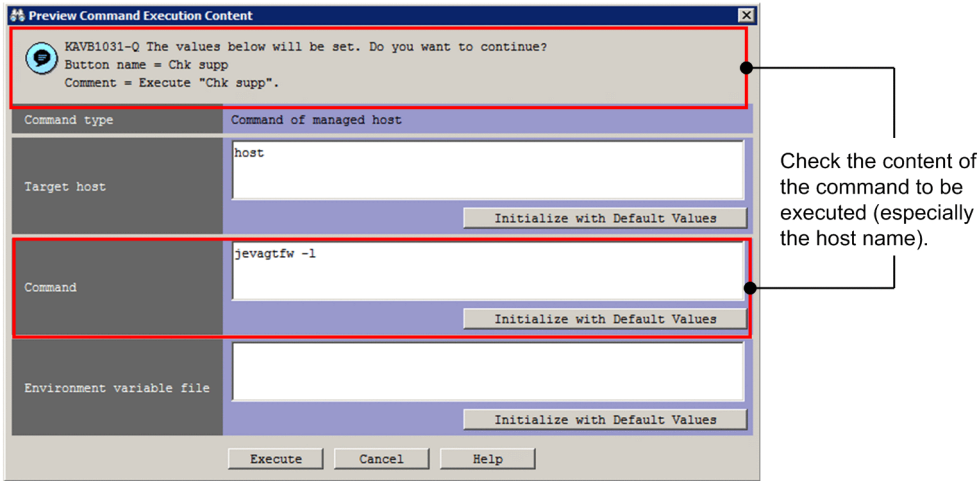


6. Identify the reason why a large number of events are occurring, and then solve the problem. While event forwarding is suppressed, investigate the agent that is outputting the events, and then solve the problem.

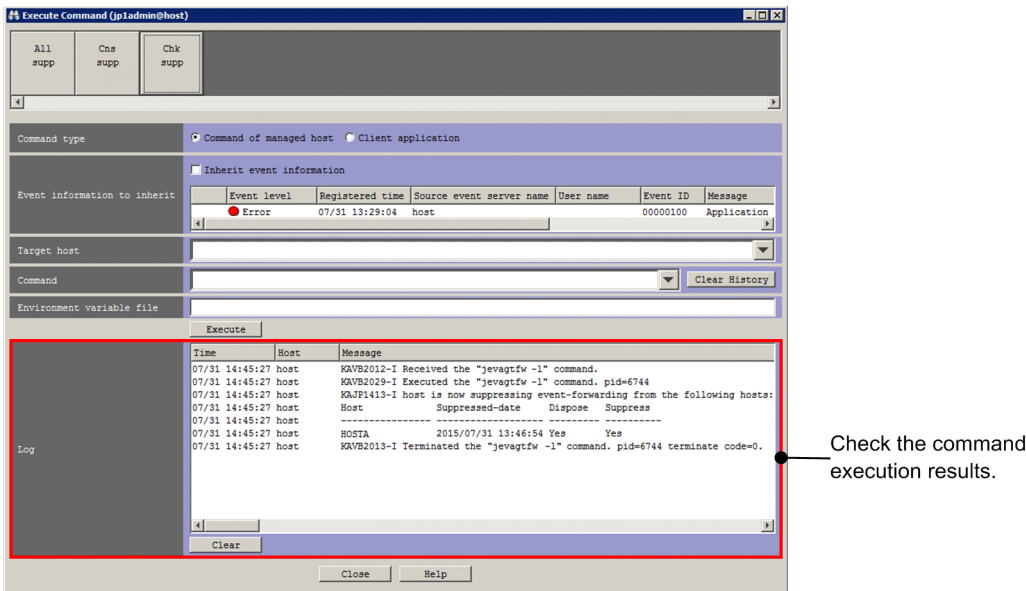
(2) Checking the suppression status of event forwarding from the agent

Using a command button that was set up, you can, on the manager, check the suppression status of event forwarding from an agent.

1. In the Event Console window, click the command button.
The Execute Command window opens.
2. Click the **Chk supp** command button that was set up in *5.10.2 Preparing to suppress event forwarding from an agent*.
The Preview Command Execution Content window opens. Check the content of the command to be executed.



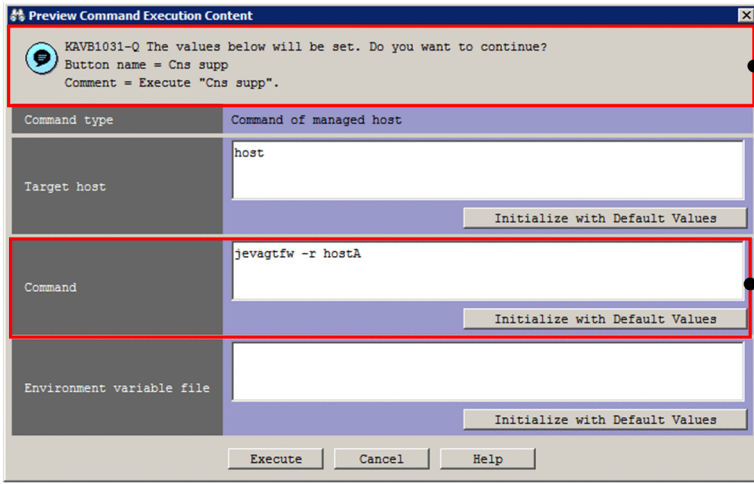
3. In the Preview Command Execution Content window, click the **Execute** button to execute the `jevagt fw` command. In the **Log** area of the Execute Command window, check the suppression status. You can check the execution result of the command in the **Log** area of the Execute Command window.



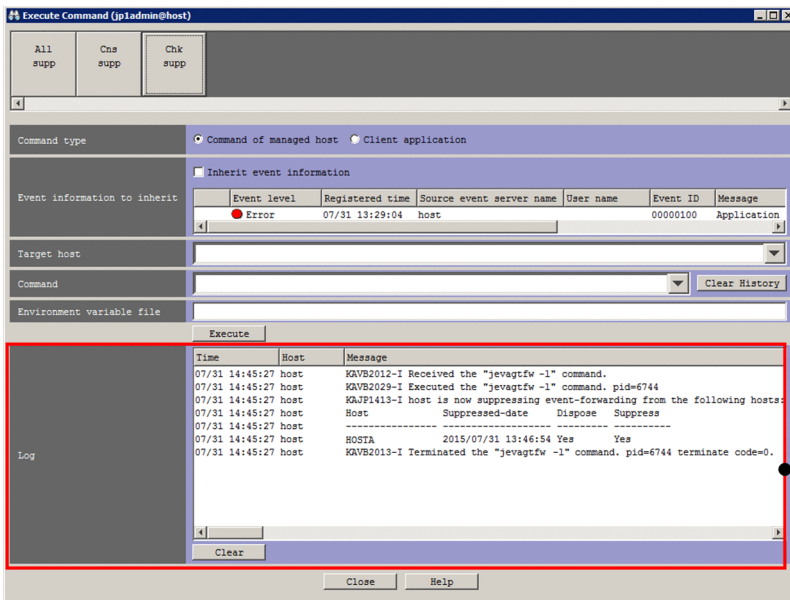
(3) Canceling suppression of event forwarding from the agent

Using a command button that was set up, you can, on the manager, cancel suppression of event forwarding from an agent.

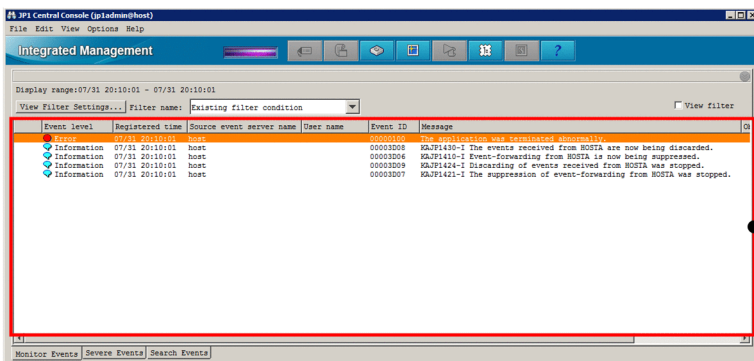
1. In the Event Console window, among the JP1 events whose forwarding from the agent was suppressed, select those for which you want to cancel suppression.
2. Click the **Execute Command** button to display the Execute Command window.
3. Click the **Cns supp** command button that was set up in *5.10.2 Preparing to suppress event forwarding from an agent*. The Preview Command Execution Content window opens. Check the content of the command to be executed (especially the name of the host to be released from suppression).



4. In the Preview Command Execution Content window, click the **Execute** button to execute the `jevagt fw` command. Suppression of event forwarding from the specified agent is canceled. In the **Log** area of the Execute Command window, you can check the execution result of the command.



5. Also in the Event Console window, confirm that suppression has been canceled and that events are being forwarded from the specified agent.



(4) Reviewing the setting for event forwarding from the agent

As a measure to prevent a large number of events from recurring, you can analyze the situation under which the recent large number of events occurred and set a threshold for suppressing automatic forwarding of events.

Analyze the situation under which the events occurred from the following viewpoints:

- If, the next time there is a large number of events, they need to be filtered, what kind of filtering condition is appropriate?
- How many events occurred within a set time period (for example, 60 seconds)?
- Are large numbers of events occurring continuously?

Based on the results of analyses carried out from these viewpoints, set the event forwarding condition (which is equivalent to the threshold for frequently occurring events) in the forwarding settings file of JP1/Base on the agent. For details about the setting procedure, see [5.10.5 Setting a threshold for automatically suppressing event forwarding on an agent](#).

(5) Checking the events that are suppressed from being forwarded

When you suppress event forwarding from an agent on which a large number of events have occurred, important events that need to be forwarded from the agent to the manager might not be forwarded. Therefore, search the relevant agent's event database from JP1/IM - View and check the events that occurred while forwarding was suppressed. For details about how to search for JP1 events, see [5.8 Searching for JP1 events](#).

5.10.4 Handling the occurrence of a large number of events by consolidating them on the manager

By setting a repeated event condition based on events that occur during system operation, you can consolidate and display JP1 events that satisfy a condition in the events list, and you can suppress execution of automatic actions. This subsection explains how to use this method for handling the occurrence of a large number of events.

Note that changing the response status requires `JP1_Console_Admin` permissions or `JP1_Console_Operator` permissions.

(1) Adding a repeated event condition based on an event that occurred during system operation

In the Repeated Event Condition Settings window, you can suppress repeated event monitoring using the conditions of a repeated event that has occurred during system operation. Conditions added in this manner are called *added repeated event conditions*.

1. In the events list in the Event Console window, select the JP1 event whose monitoring you want to suppress.
2. From the View menu in the Event Console window, choose Suppress by Repeated Event Conditions to display the Repeated Event Condition Settings window. Alternatively, right-click and from the popup menu that appears, choose Suppress by Repeated Event Conditions.


The Repeated Event Condition Settings window appears, with the attributes of the JP1 event you selected in step 1 already filled in as the repeated event conditions.

You can change what attributes are automatically filled in by editing the auto-input definition file for the repeated event condition (`event_storm_auto_list.conf`). For details about the auto-input display item definition

file for the repeated event condition, see *Auto-input definition file for the repeated event condition (event_storm_auto_list.conf)* in *Chapter 2. Definition Files* of the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

3. Edit the items in the Repeated Event Condition Settings window as needed.

4. Click the **OK** button.

The repeated event condition that you added appears in the List of Repeated Event Conditions window. The  icon appears in the **Type** column for repeated event conditions added during system operation.


Events that satisfy the set condition are excluded from repeated event monitoring. For details about how to start suppression of monitoring, see *3.5.4 When the suppression of monitoring of a large number of events starts* in the *JP1/Integrated Management - Manager Overview and System Design Guide*.

(2) Reviewing the repeated event condition setting

Review the repeated event condition that is specified. For details, see *5.10.6 Specifying repeated event conditions*.

(3) Converting an added repeated event condition to a regular repeated event condition

To convert a repeated event condition that was added during system operations to a regular repeated event condition:

1. In the Event Console window, from the **Options** menu, choose **Repeated Event Condition Settings** to display the Repeated Event Condition Settings window.
2. In the List of repeated event conditions area in the List of Repeated Event Conditions window, select the added repeated event condition (a condition with the  icon in the **Type** column) that you want to convert to a regular repeated event condition.
3. Click **Type**.
4. A confirmation message appears. To apply the settings, click **Yes**.
The selected repeated event condition that you added is converted to a regular repeated event condition.
5. In the List of Repeated Event Conditions window, click **Apply**.
6. A confirmation message appears. To apply the change, click **Yes**.
The repeated event condition that you added takes effect.

5.10.5 Setting a threshold for automatically suppressing event forwarding on an agent

To automatically suppress event forwarding by setting a threshold in advance, in case a large number of events occur on an agent:

1. Edit the forwarding setting file on the agent on which you want to automatically suppress event forwarding.
In the forwarding setting file of JP1/Base on the agent, set the conditions for suppressing event forwarding (which are equivalent to the threshold of frequently occurring events).
The format of the condition for suppressing event forwarding is as follows:


```
suppress ID unit-of-time threshold-value confirmation-count
[destination(optional)]
event-filter
end-suppress
```

For details about the conditions for suppressing event forwarding, see the description about the forwarding settings file (`forward`) in the *JP1/Base User's Guide*.

2. Enable the changes in the forwarding setting file.

Reload the forwarding setting file or restart the event service to enable the new settings.

If the event occurrence status matches the set conditions for suppressing event forwarding, event forwarding is suppressed.

While event forwarding is suppressed, investigate the agent that is outputting the large number of events, and resolve the problem.

5.10.6 Specifying repeated event conditions

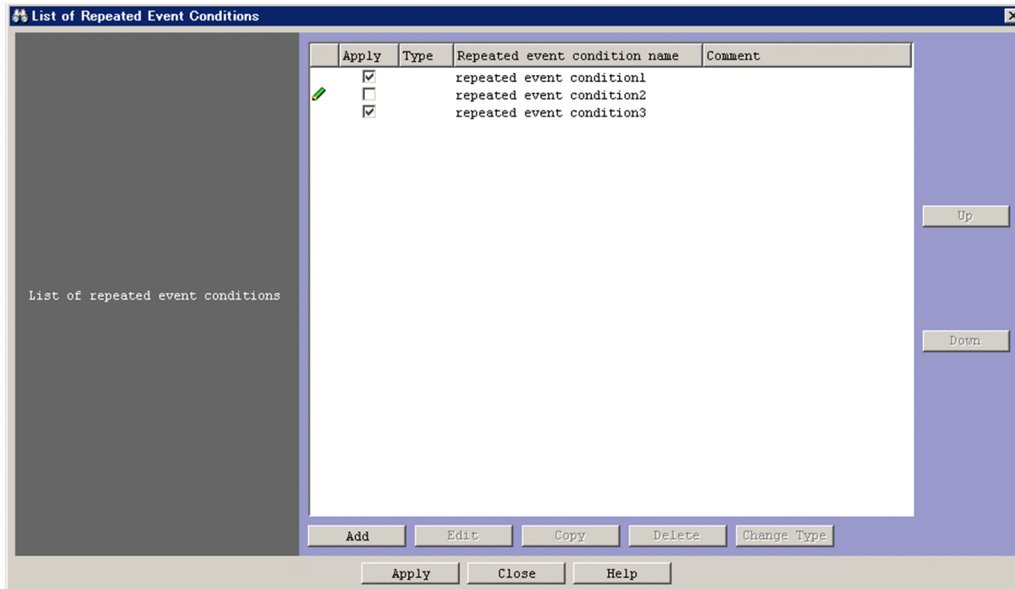
By specifying repeated event conditions, you can consolidate events that meet the specified conditions on the manager, display them in the events list, and suppress automatic action execution.

You can specify repeated event conditions in the Repeated Event Condition Settings window or List of Repeated Event Conditions window. For details about each window, see *2.17 Repeated Event Condition Settings window* and *2.19 List of Repeated Event Conditions window* in the manual *JP1/Integrated Management - Manager GUI Reference*.

To specify repeated event conditions, the JP1 user who performs operations from JP1/IM - View must have `JP1_Console_Admin` permissions.

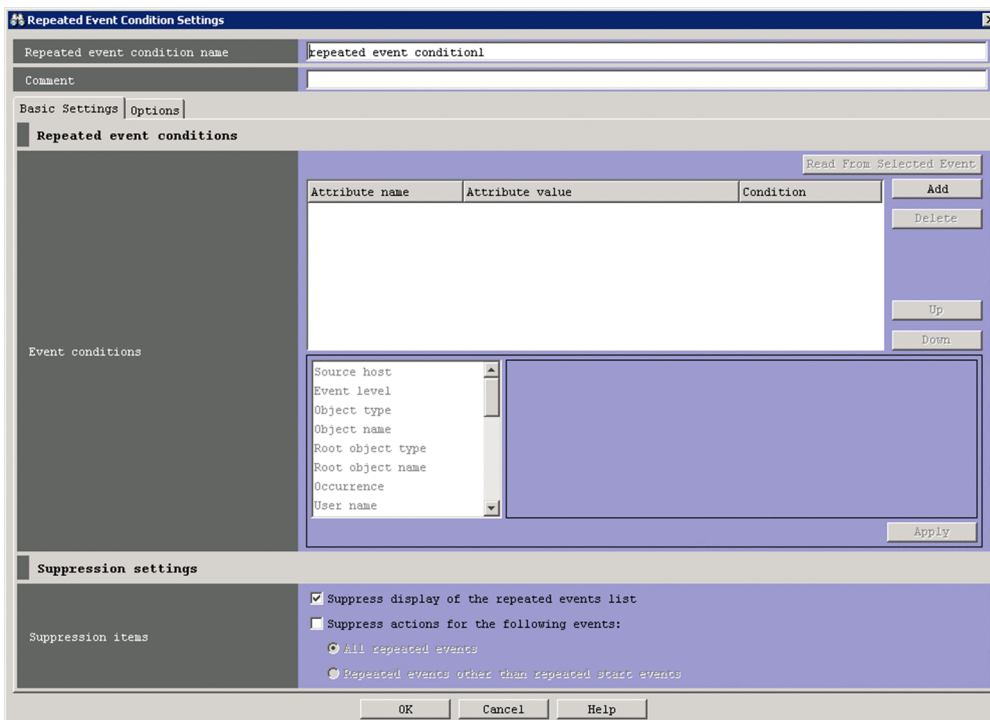
To specify repeated event conditions:

1. In the Event Console window, from the **Options** menu, choose **Repeated Event Condition Settings**.
The List of Repeated Event Conditions window opens.
2. Use one of the following methods to display the Repeated Event Condition Settings window:
 - To specify a new repeated event condition, in the List of Repeated Event Conditions window, click the **Add** button.
 - To edit an existing repeated event condition, in the List of Repeated Event Conditions window, select a displayed repeated event condition and click the **Edit** button.



The Repeated Event Condition Settings window opens.

3. On the **Basic Settings** page of the Repeated Event Condition Settings window, set **Event conditions**. (Optional) Specify the attribute value with which to compare events subject to monitoring that are acquired by the manager.



For details about the specification procedure, see [5.10.6\(1\) Specifying event conditions in the Repeated Event Condition Settings window](#).

4. On the **Basic Settings** page of the Repeated Event Condition Settings window, set **Suppression items**. (Required) Set the items to be suppressed for JP1 events that match the condition.
For details about the specification procedure, see [5.10.6\(2\) Setting suppression items in the Repeated Event Condition Settings window](#).
5. On the **Options** page of the Repeated Event Condition Settings window, specify **Conditions for same attribute values**. (Optional)

Specify attribute values when you want to group all repeated events that match the repeated event condition by attribute and suppress them. For example, you can group all events whose severity level is `Warning` or lower by each attribute of the registered host name (B . SOURCE SERVER).

The screenshot shows the 'Repeated Event Condition Settings' dialog box. The 'Options' tab is selected. The 'Suppression start/end' section is expanded, showing the following settings:

- Threshold:** Enable, [] events / [] seconds
- End monitoring period:** 300 seconds
- Suppression start event:** Issue
- Suppression end event:** Issue

The 'Notifications for when suppression continues' section is also expanded, showing:

- Checks for suppression to continue:** Enable. Timing of checks to decide whether suppression will continue:
 - Time: [] seconds
 - Number of events: [] events
- Processing for when suppression continues:**
 - Issue an event to notify that suppression will continue
 - Terminate suppression
 - Issue an event to notify that suppression will be terminated

For details about the specification procedure, see [5.10.6\(3\) Setting conditions for same attribute values in the Repeated Event Condition Settings window](#).

6. On the **Options** page of the Repeated Event Condition Settings window, specify **Threshold**. (Optional)
Specify the threshold for starting to suppress the display of repeated events and the execution of automatic actions. If no threshold is specified, suppression starts when an event is acquired that matches the repeated event condition is acquired.
For details about the specification procedure, see [5.10.6\(4\) Setting a threshold in the Repeated Event Condition Settings window](#).
7. On the **Options** page of the Repeated Event Condition Settings window, specify **End monitoring period**. (Required)
Specify the period (end monitoring period) for determining when a large number of events is no longer occurring.
For details about the specification procedure, see [5.10.6\(5\) Setting an end monitoring period in the Repeated Event Condition Settings window](#).
8. On the **Options** page of the Repeated Event Condition Settings window, specify **Suppression start event**. (Optional)
Specify a suppression start event if you want to issue an event that indicates that suppression of a large number of events has started.
For details about the specification procedure, see [5.10.6\(6\) Setting a suppression start event in the Repeated Event Condition Settings window](#).
9. On the **Options** page of the Repeated Event Condition Settings window, specify **Suppression end event**. (Optional)
Specify a suppression end event when you want to issue an event that indicates that suppression of a large number of events has ended.
For details about the specification procedure, see [5.10.6\(7\) Setting a suppression end event in the Repeated Event Condition Settings window](#).

10. On the **Options** page of the Repeated Event Condition Settings window, specify **Checks for suppression to continue** and **Processing for when suppression continues**. (Optional)
Specify these values if you want to determine whether suppression of repeated event monitoring is continuing at a specified time interval (seconds) or after a specified number of events, if you want to issue a JP1 event for notification if suppression is continuing, or if you want to terminate suppression.
For details about the specification procedure, see *5.10.6(8) Setting checks for suppression to continue and processing for when suppression continues in the Repeated Event Condition Settings window*.
11. In the Repeated Event Condition Settings window, click the **OK** button.
The repeated event condition is applied to the List of Repeated Event Conditions window.
12. In the List of Repeated Event Conditions window, select the **Apply** check box for the repeated event condition that was set.
13. In the List of Repeated Event Conditions window, click the **Apply** button.
14. A confirmation message appears. To apply the settings, click **Yes**.
The repeated event condition takes effect.

(1) Specifying event conditions in the Repeated Event Condition Settings window

The specification procedure is as follows:

1. Display the **Basic Settings** page of the Repeated Event Condition Settings window.
2. Specify event conditions by performing the necessary operations from among the following:
 - To add a new event condition, click the **Add** button.
An event condition whose **Attribute name**, **Attribute value**, and **Condition** are blank is added to the list of event conditions.
 - To edit an event condition, select the event condition you want to edit from the list of event conditions. Then, select **Attribute name**, **Attribute value**, and **Condition** from the event condition editing area and click the **Apply** button.
 - To delete an event condition, select the event condition you want to delete from the list of event conditions and then click the **Delete** button.
 - To set as a condition an attribute value that is the same as the event selected in the Event Console window, click the **Read From Selected Event** button.
The condition that was set before the **Read From Selected Event** button was clicked is deleted and overwritten with the attribute value that is the same as the event selected in the Event Console window.

(2) Setting suppression items in the Repeated Event Condition Settings window

The specification procedure is as follows:

1. Display the **Basic Settings** page of the Repeated Event Condition Settings window.
2. Select one or both of the following check boxes:
 - **Suppress display of the repeated events list**
 - **Suppress actions of the repeated events**

3. If you selected **Suppress actions of the repeated events** in step 2, specify the range of events for which you want to suppress actions.

Select one of the following:

- **All repeated events**

Actions are suppressed for all repeated events that match the repeated event conditions.

- **Repeated events other than repeated start events**

Actions are suppressed for all repeated events that match the repeated event conditions, except for repeated start events (which triggered suppression).

(3) Setting conditions for same attribute values in the Repeated Event Condition Settings window

The specification procedure is as follows:

1. Display the **Options** page of the Repeated Event Condition Settings window.
2. Specify conditions for same attribute values by performing whichever of the following operations is necessary:
 - To add a condition for same attribute values, from the **Conditions for same attribute values** drop-down list, select an attribute name and click the **Add** button.
 - To delete a condition for same attribute values, from the **Attribute name** list in **Conditions for same attribute values**, select an attribute name and click the **Delete** button.

(4) Setting a threshold in the Repeated Event Condition Settings window

The specification procedure is as follows:

1. Display the **Options** page of the Repeated Event Condition Settings window.
2. For **Threshold**, select the **Enable** check box.
3. Set a threshold.

For example, if the threshold is set to 10 events in 3 seconds (**10 events / 3 seconds**), suppression starts if ten or more events were acquired during the three seconds prior to the arrival time of the last event acquired by JP1/IM - Manager.

(5) Setting an end monitoring period in the Repeated Event Condition Settings window

The specification procedure is as follows:

1. Display the **Options** page of the Repeated Event Condition Settings window.
2. Specify the end monitoring period.

The concept of end monitoring period differs depending on whether a threshold is set in [5.10.6\(4\) Setting a threshold in the Repeated Event Condition Settings window](#). The following describes the difference between setting and not setting a threshold when the end monitoring period is set to 300 seconds.

If a threshold is set:

A large number of events is judged to no longer be occurring when the threshold that was set is not exceeded for 300 seconds prior to the arrival time of the last event acquired by JP1/IM - Manager.

If a threshold is not set:

A large number of events is judged to no longer be occurring when no repeated event matching the repeated event condition is acquired during the 300 seconds prior to the arrival time of the last event acquired by JP1/IM - Manager.

(6) Setting a suppression start event in the Repeated Event Condition Settings window

The specification procedure is as follows:

1. Display the **Options** page of the Repeated Event Condition Settings window.
2. For **Suppression start event**, select the **Issue** check box.

(7) Setting a suppression end event in the Repeated Event Condition Settings window

The specification procedure is as follows:

1. Display the **Options** page of the Repeated Event Condition Settings window.
2. For **Suppression end event**, select the **Issue** check box.

(8) Setting checks for suppression to continue and processing for when suppression continues in the Repeated Event Condition Settings window

Checks for suppression to continue and **Processing for when suppression continues** must be specified together. The specification procedure is as follows:

1. Display the **Options** page of the Repeated Event Condition Settings window.
2. In **Checks for suppression to continue**, select the **Enable** check box.
3. In **Checks for suppression to continue**, specify the trigger for determining whether suppression is continuing. Select either **Time** or **Number of events**. For details about the differences between these settings, see *3.4.7 Issuing notifications when the suppression of repeated-event display continues* in the *JP1/Integrated Management - Manager Overview and System Design Guide*.
4. In **Processing for when suppression continues**, select the processing that is to take place when suppression continues. Select either **Issue an event to notify that suppression will continue** or **Terminate suppression**. If you selected **Terminate suppression**, you can select the **Issue an event to notify that suppression will be terminated** check box to issue a JP1 event that indicates that suppression has been terminated.

5.10.7 Stopping, on the manager, a log file trap that issues a large numbers of events

The procedure described in this subsection shows how to stop a specific log file trap, by using IM Configuration Management on the manager, as an action to take when a large numbers of events are issued by the log file trap. For

details about how to stop a specific log file trap without using IM Configuration Management, see the description about suppressing forwarding of large numbers of events in the *JP1/Base User's Guide*.

Before you can perform the procedure described in this subsection, IM Configuration Management must be used to manage the profile of the agent. For a general description of profile management using IM Configuration Management, see *6.5 Profile management* in the *JP1/Integrated Management - Manager Overview and System Design Guide*. For details about how to set an agent's profile using IM Configuration Management, see *3.5 Setting the profiles* in the *JP1/Integrated Management - Manager Configuration Guide*.

Also, mapping of the event source host must be enabled before you can perform the procedure described below. For details about how to enable mapping of the event source host, see *4.15 Setting event source host mapping* in the *JP1/Integrated Management - Manager Configuration Guide*.

1. In the events list in the Event Console window, make sure that a large number of JP1 events issued by a log file trap are being output.
2. Display the Event Details window for the relevant JP1 event.
3. In the Event Details window, make sure that the event source host name and monitoring name[#] are displayed for **Event attributes**.

#

In the Event Details window, to display the monitoring name of a log file trap for **Event attributes**, JP1/IM - Manager must be version 10-50 or later, and JP1/Base on the agent must be version 10-50 or later.

4. Log in to the IM configuration management viewer (IM Configuration Management), and display the IM Configuration Management window.
5. Click the **IM Configuration** tab to display the **IM Configuration** page.
6. In the tree area, select the event source host name of the log file trap, and then from the **View** menu, select **Display Profiles**.
The Display/Edit Profiles window for the relevant host appears.
7. In the tree area, select **JP1/Base**, and then from the **Edit** menu, select **Exclusive Editing Settings**.
Exclusive editing of the profile is permitted.
8. From **Log File Trapping** in the tree area, select the monitoring name of the log file trap you want to suppress, and then from the **Operation** menu, select **Stop Process**.
A confirmation message is output, asking you whether to stop the log file trap.

9. Click the **Yes** button.

The log file trap stops.

While the log file trap is stopped, investigate the source application that output the logs, and resolve the problem that caused the log output.

5.10.8 Consolidated display when events with the same attributes occur consecutively

When you consolidate the display of repeated events, JP1 events that have the same content and that occur consecutively over a short period of time can be displayed as a single event on the **Monitor Events** page or **Severe Events** page of

the Event Console window. You can configure the consolidated display of repeated events function in the Preferences window.

You cannot use the consolidated display of repeated events function concurrently with the event monitoring suppression function.

You can view detailed information about repeated events and consolidated events. You can also change response statuses similarly to the case in which repeated events are not being monitored. To change a response status, you need `JP1_Console_Admin` permissions or `JP1_Console_Operator` permissions.

For a general description of the consolidated display of repeated events function, see *3.4.10 Suppressing repeated-event display by the consolidated display of repeated events* in the *JP1/Integrated Management - Manager Overview and System Design Guide*.

If you want to consolidate JP1 events that do not occur consecutively, or if you want to specify event conditions or certain criteria under which consolidation starts, use repeated event monitoring suppression instead of the consolidated display of repeated events. For details about repeated event monitoring suppression, see *5.10.4 Handling the occurrence of a large number of events by consolidating them on the manager*.

(1) Setting up the consolidated display of repeated events function

1. From the menu in the Event Console window, choose **Options** and then **Preferences**.

The Preferences window opens.

2. In the **Event Attribute** area, click the **Enable** check box beside **Display most significant status**.

The **Timeout time** field becomes available.

3. Specify the timeout time.

Specify the timeout period for consolidating repeated events.

Event consolidation ends when more than time the specified timeout period has elapsed between the consolidation start event and the arrival of received events.

4. Click **OK**.

The settings take effect.

Events that have been consolidated into a single event appear as a consolidated event on the **Monitor Events** page and **Severe Events** page of the Event Console window.

Supplementary note:

The consolidated display of repeated events applies to events received after you have configured the feature. Events received before this time are not subject to consolidated display. Event consolidation ends when more than a specified length of time has elapsed between the consolidation start event and the arrival of received events. A maximum of 100 events can be consolidated into a single event.

5.11 Handling JP1 events by linking with other products

This subsection explains the operational procedure in JP1/IM - View for handling JP1 events by linking with other products.

5.11.1 Registering JP1 events as incidents in JP1/IM - Service Support (linking with JP1/IM - Service Support)

By linking JP1/IM - Manager with JP1/IM - Service Support, you can register JP1 events displayed in JP1/IM - View as incidents in JP1/Service Support. For details about how to link JP1/IM - Manager with JP1/Service Support, see *9.1.1 Enabling calling the JP1/Service Support window in the JP1/Integrated Management - Manager Configuration Guide*.

You can register incidents in JP1/Service Support by displaying the Select the process work board as the registration target window of JP1/Service Support from the following windows:

- Any page in the Event Console window
- Related Events window
- Event Details window

The following describes how to display the Select the process work board as the registration target window of JP1/Service Support from each of these windows. The procedure for registering an incident in JP1/Service Support from the Select the process work board as the registration target window is described in the *JP1/Service Support Operator's Guide*.

Note that registering JP1 events as incidents requires `JP1_Console_Admin` permission or `JP1_Console_Operator` permission.

(1) Displaying JP1/Service Support from pages of the Event Console window

To display JP1/Service Support from pages of the Event Console window:

1. In the Event Console window, from the list of JP1 events displayed in the events list, select a JP1 event that you want to register as an incident.
Note that although JP1 events registered in other event databases can be displayed in the **Search Events** page, you cannot register these JP1 events as incidents. Only JP1 events registered in the event database of the manager can be registered as incidents.
2. Right-click the event and choose **Register Incident**, or from the **View** menu, choose **Register Incident**.
Your Web browser (Internet Explorer) opens and displays the Select the process work board as the registration target window of JP1/Service Support.

(2) Displaying JP1/Service Support from the Related Events window

To display JP1/Service Support from the Related Events window:

1. From the JP1 events displayed in the Related Events window, select a JP1 event that you want to register as an incident.

2. Right-click the event and choose **Register Incident**.

Your Web browser (Internet Explorer) opens and displays the Select the process work board as the registration target window of JP1/Service Support.

(3) Displaying JP1/Service Support from the Event Details window

To display JP1/Service Support from the Event Details window:

1. In the Event Details window, click the **Register Incident** button.

Your Web browser (Internet Explorer) opens and displays the Select the process work board as the registration target window of JP1/Service Support.

5.11.2 Displaying operating procedures for JP1 events (linking with JP1/Navigation Platform)

By linking JP1/IM - Manager with JP1/Navigation Platform, you can access the descriptions of operating procedures provided by JP1/Navigation Platform directly from a JP1 event in JP1/IM - View. This process uses single sign-on. For details about how to link JP1/IM - Manager with JP1/Navigation Platform, see *9.2 Linking to JP1/Navigation Platform* in the *JP1/Integrated Management - Manager Configuration Guide*.

To display the window of JP1/Navigation Platform where work tasks are executed from the Event Details window using single sign-on:

1. In the Event Details window, click a link in the **Guide** area.

Your Web browser (Internet Explorer) opens and displays the operating procedure that corresponds to the selected JP1 event in the window of JP1/Navigation Platform where work tasks are executed.

5.11.3 Checking the rule startup request status and making a rule startup request (linking with JP1/IM - Rule Operation)

This subsection explains how to check whether a rule startup request was correctly reported to JP1/IM - Rule Operation when JP1/IM is linked to JP1/IM - Rule Operation. It also explains how to open the Rule Log Details window of JP1/IM - Rule Operation.

(1) Checking whether a rule startup request was reported to JP1/IM - Rule Operation

With a rule startup request, you can use the function for monitoring automated action status to monitor action status and delay. By setting up these items, you can detect the following types of problems at an early stage in their occurrence:


- Reporting of a rule startup request did not finish within the expected time frame, or took a long time to finish.
- Reporting of a rule startup request failed (with the `Fail`, `Error`, or `Error (Miss)` status).

When a problem is detected, you can generate a JP1 event (event ID=2010 or 2011) or execute a notification command.

For details about setup, see *4.5.3 Settings for monitoring the automated action execution status* in the *JP1/Integrated Management - Manager Configuration Guide*.

To check whether a rule startup request was reported:

1. In the Event Console window, monitor rule startup events.

Rule startup events are those JP1 events that show  in **Action Type**.

2. Open the Action Log window or List of Action Results window, and check the execution results for rule startup requests.

Check the execution status of the rule startup requests.

3. Cancel or re-execute rule startup requests as needed.

If a rule startup request is stuck in **Running** status or is in **Error** status, it cannot be reported to JP1/IM - Rule Operation. Therefore, cancel or re-execute rule startup requests as needed.

When the function for monitoring automated action status is set for rule startup requests:

When reporting using the delay monitoring function or status monitoring function is executed once, reporting is suppressed until the user cancels reporting suppression. When an error in a rule startup request is detected by the delay monitoring function or status monitoring function, after you have finished re-executing or have canceled the rule startup request, follow the procedure described below.

1. In the Event Console window, from the **Options** menu, display **Function-Status Notification Return**, and then **Action Delay Monitoring** and **Action Status Monitoring**, and then select a function name that is enabled.

A suppressed function is displayed in gray letters. When you select a function name that is enabled, a dialog box asking whether to cancel reporting suppression opens.

2. Click **Yes** in the dialog box.

Reporting suppression is canceled, thus enabling monitoring again.



Note

You can determine whether a rule startup request has matched the rule startup condition on the JP1/IM - Rule Operation side by checking the return code displayed in the following three windows:

- Action Log window
- List of Action Results window
- Action Log Details window

For details about the Action Log, List of Action Results, and Action Log Details windows, see *Chapter 1. Window Transitions and Login Window* in the manual *JP1/Integrated Management - Manager GUI Reference*.

For details about operations such as checking automated action status and re-execution, also see [7.2.2 Checking the execution results of automated actions](#).

(2) Displaying the Rule Log Details window of JP1/IM - Rule Operation

When a rule startup request is reported to JP1/IM - Rule Operation and satisfies the rule startup condition of JP1/IM - Rule Operation, you can display the Rule Log Details window of JP1/IM - Rule Operation from the following three windows:

- Action Log window
- List of Action Results window
- Action Log Details window

The procedure for each of these windows follows.

- Opening the Rule Log Details window of JP1/IM - Rule Operation from the Action Log window

To open the Rule Log Details window of JP1/IM - Rule Operation from the Action Log window:

1. Select a single rule startup event from the events list in the Event Console window.
2. Use one of the following methods to open the Action Log window:
 - From the menu bar, choose **View** and then **Action Log**.
 - From the popup menu, choose **Action Log**.
 - Click the **Action Log** button.

The Action Log window opens.

3. Select a single rule startup request execution result.

Rule startup events are those events that show  in **Type**. Additionally, make sure that **Return Code** in **Log** is 0.

4. Click the **Rule Log Details** button.

The Rule Log Details window of JP1/IM - Rule Operation opens.

- Opening the Rule Log Details window of JP1/IM - Rule Operation from the List of Action Results window

To open the Rule Log Details window of JP1/IM - Rule Operation from the List of Action Results window:

1. In the Event Console window, choose **View** and then **List of Action Results**.

The List of Action Results window opens. This window lists the results of both rule startup requests and automated actions.

2. Select a single rule startup request execution result.

Rule startup events are those events that show  in **Type**. Additionally, make sure that **Return Code** in **Log** is 0.

3. Click the **Rule Log Details** button.

The Rule Log Details window of JP1/IM - Rule Operation opens.

- Opening the Rule Log Details window of JP1/IM - Rule Operation from the Action Log Details window

You can also open the Rule Log Details window of JP1/IM - Rule Operation from the Action Log Details window, which can be opened from the Action Log window and List of Action Results window that are explained above.

To open the Rule Log Details window of JP1/IM - Rule Operation from the Action Log Details window:

1. From **Log** in the Action Log window or the List of Action Results window, select a single rule startup request and click the **Details** button.

The Action Log Details window opens. Make sure that **Return Code** (attribute name) in **Log** is 0.

2. Click the **Rule Log Details** button.

The Rule Log Details window of JP1/IM - Rule Operation opens.

For details about the Action Log window, List of Action Results window, and Action Log Details window, see *Chapter 1. Window Transitions and Login Window* in the manual *JP1/Integrated Management - Manager GUI Reference*.

For details about the Rule Log Details window, see the manual *Job Management Partner 1/Integrated Management - Rule Operation GUI Reference*.

5.11.4 Opening a monitor window of the application that issued JP1 events

You can open the monitor window of the program that is related to the received JP1 event to view the information or perform other operations. You cannot use this function in the Web version of JP1/IM - View.

To open a monitor window from the Event Console window:

1. From the events list in the Event Console window, select a JP1 event and choose **View** and then **Monitor**.

Alternatively, click the  icon on the toolbar, or choose **Monitor** from the popup menu.

The monitor window (Web page or application program) of the corresponding program opens.

You can also open a monitor window by clicking the **Monitor** button in the Event Details window.

If there is no program that corresponds to the selected JP1 event or if the settings necessary for opening a monitor window have not been made, you cannot choose the menu or button. For details about how to open a monitor window, see 4.17 *Setting monitor startup for linked products* in the *JP1/Integrated Management - Manager Configuration Guide*.

(1) List of applications that can open a monitor window

The following table lists programs that can open a monitor window. For details about the OSs that support the applications, see the documentation for the applicable application.

Program name	Window type	Monitor start definition file name
JP1/NETM/Asset Information Manager	Web page	hitachi_jp1_aim_mon.conf
JP1/PFM	Web page	hitachi_jp1_pfmmgr_mon.conf
JP1/IM - Rule Operation	Application window	hitachi_jp1_im_rm_mon.conf
JP1/IM - Event Gateway for Network Node Manager i	Web page	hitachi_jp1_im_egn_mon.conf
JP1/Base (SNMP trap)	Web page	hitachi_jp1_imevtgw_mon.conf
JP1/AJS2 - Scenario Operation	Application window	hitachi_jp1_ajs2so_mon.conf
JP1/AJS3 (version 9 or later) or JP1/AJS2 (version 8 or earlier)	Application window	hitachi_jp1_ajs2_mon.conf
JP1/AJS2 mainframe	Application window	hitachi_jp1_ajs2_mainframe_mon.conf
Cosminexus Application Server	Application window	hitachi_cosminexus_manager_mon.conf

5.11.5 Displaying performance reports for JP1 events when linking with JP1/PFM

If you specify settings for linking with JP1/PFM, you can use single sign-on to access the JP1/PFM - Web Console report window from JP1 events displayed in JP1/IM - View. For details about the settings for linking with JP1/PFM, see the JP1/PFM documentation.

(1) Displaying the JP1/PFM - Web Console report window from any page in the Event Console window

The procedure is as follows:

1. In the Event Console window, check the list of events and select the JP1 event for which you want to view a report.
2. In the Event Console window, select the **View** menu, and then select **Display Performance**. Alternatively, select **Display Performance** from the pop-up menu.
JP1/PFM - Web Console starts, and the report window is displayed.

(2) Displaying the JP1/PFM - Web Console report window from the Event Details window

The procedure is as follows:

1. In the Event Details window, click the **Display Performance** button.
JP1/PFM - Web Console starts, and the report window is displayed.

6

System Monitoring from Central Scope

This chapter explains how to use JP1/IM - View to monitor monitored objects.

6.1 Monitoring from the Monitoring Tree window

You can monitor the statuses of monitored objects from the Monitoring Tree window. You can also perform various types of operations, such as changing the statuses and monitoring statuses for the monitoring nodes (monitoring groups and monitored objects) displayed in the Monitoring Tree window.

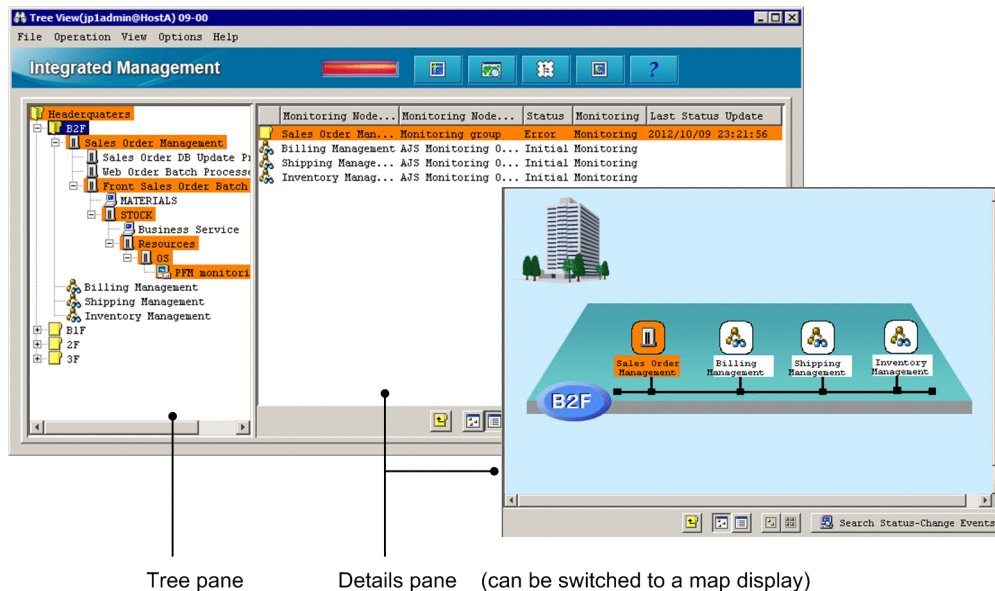
When the monitoring range settings of the monitoring tree are enabled, the monitoring tree displays only the monitoring nodes that are set for the JP1 resource group of the logged-in JP1 user. In this case, a virtual root node is displayed as the highest-order node. If there is no monitoring node that can be displayed, only the virtual root node is displayed. However, if the JP1 resource group is JP1_Console and if the user has logged in as a JP1 user with JP1_Console_Admin permission, all monitoring nodes are displayed.

You can use one of the following three methods to open the Monitoring Tree window:

- Log in to JP1/IM - Manager (Central Scope).
- Click the **Central Scope** button in the Event Console window.
- From the menu bar in the Event Console window, choose **File** and then **Central Scope**.

A Monitoring Tree window display example follows.

Figure 6–1: Monitoring Tree window display example



6.1.1 Changing the status of monitoring nodes

This subsection explains how to change the status of a monitoring node displayed in the Monitoring Tree window. The status that can be changed and the action that occurs at the time of the change differ depending on the monitoring node type (monitoring group or monitored object). For details, see 4.2.2 *Statuses of monitoring nodes* in the *JP1/Integrated Management - Manager Overview and System Design Guide*.

Changing the status of a monitoring node requires at least JP1_Console_Operator permission. When the monitoring range settings of the monitoring tree are enabled, you can change the status of only those monitoring nodes that can be accessed with at least JP1_Console_Operator permission from among the monitoring nodes being displayed.

To change the status of a monitoring node:

1. Select a monitoring node displayed in the tree pane or details pane.
2. Use either of the following methods to change the status of the monitoring node:
 - From the menu bar, choose **Operation** and then **Change Status**, and then change the status to the desired one.
 - From the popup menu that opens when you right-click the mouse, choose **Change Status** and then change the status to the desired one.

A confirmation dialog box opens.

3. In the configuration dialog box, click **Yes**.

6.1.2 Changing the monitoring status of monitoring nodes

This subsection explains how to change the monitoring status of a monitoring node. The action that occurs at the time of the change differs depending on the monitoring node type (monitoring group or monitored object). For details, see *4.2.2 Statuses of monitoring nodes* in the *JP1/Integrated Management - Manager Overview and System Design Guide*.

Changing the monitoring status of a monitoring node requires at least `JP1_Console_Operator` permission. When the monitoring range settings of the monitoring tree are enabled, you can change the status of only those monitoring nodes that can be accessed with at least `JP1_Console_Operator` permission from among the monitoring nodes being displayed.

To change the monitoring status of a monitoring node:

1. Select a monitoring node displayed in the tree pane or details pane.
2. Use one of the following methods to change the status of the monitoring node:
 - From the menu bar, choose **Operation** and then **Change Monitoring Status**, and then change the monitoring status to the desired one.
 - From the popup menu that opens when you right-click the mouse, choose **Change Monitoring Status**, and then change the monitoring status to the desired one.
 - From the popup menu that opens when you right-click the mouse, choose **Properties** and select either **Monitoring** or **Not Monitoring** from the **General** page, and then click **OK** or **Apply**.
 - Open the Properties window by double-clicking the selected monitoring node, select either **Monitoring** or **Not Monitoring** from the **General** page, and then click **OK** or **Apply** (limited to monitored objects only).

Important

- If the monitoring status of a higher-order monitoring group is set to **Not Monitoring**, you cannot set a lower-order monitoring node alone to **Monitoring**.
- When the monitoring status of a monitoring node is set to **Not Monitoring**, the status returns to the initial status.

6.1.3 Searching for monitoring nodes

This subsection explains how to search for monitoring nodes. When the monitoring range settings of the monitoring tree are enabled, you cannot execute a search using the virtual root node as the starting point. Furthermore, the virtual root node cannot be a search target.

To search for monitoring nodes:

1. Select a monitoring group displayed in the tree pane or details pane.
You can restrict the monitoring nodes that can be searched to the selected monitoring group and the monitoring nodes that are in that monitoring group.
2. Use either of the following methods to open the Search window:
 - From the menu bar, choose **View** and then **Search**.
 - From the popup menu that opens when you right-click the mouse, choose **Search**.
3. Enter a condition into the Search window and click the **Search** button.
Monitoring nodes that match the search condition are displayed in a list.

You can perform the following operations on the monitoring nodes that are displayed in the list:

- Change the status or monitoring status of a monitoring node.
To change the status or monitoring status of a monitoring node, right-click to open the popup menu.
- With the target monitoring node selected, open the Monitoring Tree window.
To do so in this case, double-click the mouse.

6.1.4 Searching for status-change events

This subsection explains how to search for status-change events.

1. Select a monitoring node whose status has changed.
2. Use one of the following methods to search for status-change events:
 - From the menu bar, choose **View** and then **Search Status-Change Events**.
 - From the popup menu that opens when you right-click the mouse, choose **Search Status-Change Events**.
 - Click the **Search Status-Change Events** button located in the lower portion of the details pane.

When you execute a status-change event search on a monitored object, up to 100 JP1 events matching the status change condition of that monitored object are displayed sequentially, starting with the earliest event, on the **Search Events** page of the Event Console window (the 101st and subsequent events are not displayed). Therefore, if the number of JP1 events displayed as search results has increased, we recommend that you manually change the status of the monitored object as needed.

If the number of JP1 events matching the status change condition of the monitored object exceeds 100, a warning JP1 event (event ID = 00003FB1) is generated. When this JP1 event is generated, check how JP1 events matching the status change condition are handled, and manually change the status of the monitored object.

When you execute a status-change event search on a monitoring group, up to 100 JP1 events matching the status change condition of the monitored objects in that monitored group are displayed sequentially on the **Search Events** page of the Event Console window, starting with the earliest event (the 101st and subsequent events are not displayed). Note that if

a status change condition has been defined for a monitoring group, only up to 100 status-change events requiring action are sequentially displayed, starting with the earliest event, even if there are events that changed the status of lower-order monitoring nodes.

Important

- When you manually change the status of a monitoring node, you clear the status-change event history. Consequently, you will not be able to search for (display) the status-change events that have occurred in the past. Therefore, before you manually change the status of a monitoring node, check how JP1 events matching the status-change condition are handled.
- The JP1 events that can be searched using a status-change event search are restricted by a user filter (if the user is subject to restriction by a user filter).
- We recommend that you open the Event Console window before searching for status-change events.
- If the number of JP1 events matching the status-change condition of the monitored object exceeds 100, the completed-action linkage function becomes inactive. Therefore, if the number of JP1 events displayed as search results has increased, we recommend that you manually change the status of the monitored object as needed.

6.1.5 Displaying the attributes of monitoring nodes

To display the attributes of a monitoring node:

1. Select a monitoring node.
2. Use one of the following methods to open the Properties window:
 - From the menu bar, choose **View** and then **Properties**.
 - From the menu bar, choose **Options** and then **Basic Information**.
 - From the menu bar, choose **Options** and then **Status-Change Condition**.
 - From the menu bar, choose **Options** and then **Event-Issue Conditions**.
 - From the popup menu that opens when you right-click the mouse, choose **Properties**.
 - Double-click (limited to a monitored object).

A JP1 user having at least `JP1_Console_Operator` permission can change several of the attributes displayed in the Properties window. To change the attributes of a monitoring node, log in as a user with at least the operating permission of `JP1_Console_Operator`.

6.1.6 Displaying guide information

To display guide information:

1. Select a monitored object.
2. Use either of the following methods to open the Guide window.
 - From the menu bar, choose **View** and then **Guide**.
 - From the popup menu that opens when you right-click the mouse, choose **Guide**.


You must define in advance, in a guide information file, the conditions for displaying guide information according to various situations and the guide information content.

About the guide information function, definition file, and settings:

- About the details to set in the guide information and the guide function:
See *4.8 Guide function* in the *JPI/Integrated Management - Manager Overview and System Design Guide*.
- About editing the guide information file:
See *5.6 Editing guide information* in the *JPI/Integrated Management - Manager Configuration Guide*.
- About the format of the guide information file:
See *Guide information file (jcs_guide.txt)* (in *Chapter 2. Definition Files*) in the manual *JPI/Integrated Management - Manager Command and Definition File Reference*.

6.1.7 Opening the Visual Monitoring window

To open the Visual Monitoring window:

1. Use either of the following methods to display the Open Visual Monitoring Window window.
 - From the menu bar, choose **View** and then **Visual Monitoring**.
 - Click the  icon in the toolbar.
2. Select a Visual Monitoring window name displayed in the Open Visual Monitoring Window window and click **OK**.

6.1.8 Displaying a login user list

To display a list of JPI users that have logged in to JPI/IM - Manager (Central Scope):

1. In the menu bar, choose **Options** and then **Login User List**.

6.1.9 Saving the information in the Monitoring Tree window on the local host

To save the information on the local host:

1. From the menu bar, choose **File** and then **Save Monitoring-Tree Status**.
The file selection window opens.
2. Save the information in the desired folder under a desired name on the local host.
The monitoring tree information is saved in a CSV file.


When the monitoring range settings of the monitoring tree are enabled, you cannot save the information in the Monitoring Tree window on the local host. To save the information, save it on the local host from the Monitoring Tree (Editing) window.

6.2 Monitoring from the Visual Monitoring window

You can monitor the statuses of monitored objects from the Visual Monitoring window.

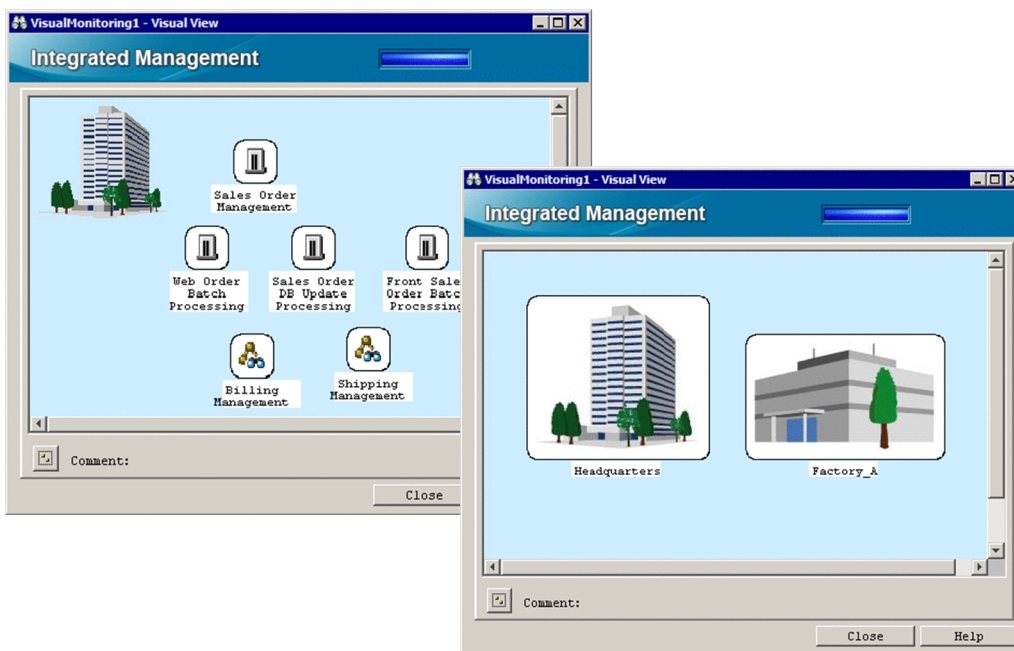
When the monitoring range settings of the monitoring tree are enabled, the Visual Monitoring window displays only the monitoring nodes that are set for the JP1 resource group of the logged-in JP1 user. However, if the JP1 resource group is JP1_Console and if the user has logged in as a JP1 user with JP1_Console_Admin permission, all monitoring nodes are displayed.

To open the Visual Monitoring window:

1. Use either of the following methods to open the Open Visual Monitoring Window window.
 - From the menu bar in the Monitoring Tree window, choose **View** and then **Visual Monitoring**.
 - Click the  icon in the toolbar of the Monitoring Tree window.
2. Select a Visual Monitoring window name displayed in the Open Visual Monitoring Window window and click **OK**.
When the monitoring range settings of the monitoring tree are enabled, if a visual monitoring window does not contain any monitoring node that can be displayed, it is not displayed in the list in the Open Visual Monitoring Window window.

A Visual Monitoring window display example follows.

Figure 6–2: Visual Monitoring window display example



6.2.1 Opening the Monitoring Tree window from the Visual Monitoring window

To open the Monitoring Tree window from the Visual Monitoring window:

1. Select a monitoring node and double-click it.

The Monitoring Tree window opens with the monitoring node selected that you double-clicked in the Visual Monitoring window.

6.2.2 Changing the status of monitoring nodes

This subsection explains how to change the status of a monitoring node displayed in the Visual Monitoring window. The status that can be changed and the action that occurs at the time of the change differ depending on the monitoring node type (monitoring group or monitored object). For details, see *4.2.2 Statuses of monitoring nodes* in the *JP1/Integrated Management - Manager Overview and System Design Guide*.

Changing the status of a monitoring node requires at least `JP1_Console_Operator` permission. When the monitoring range settings of the monitoring tree are enabled, you can change the status of only those monitoring nodes that can be accessed with at least `JP1_Console_Operator` permission from among the monitoring nodes being displayed.

To change the status of a monitoring node:

1. Select a monitoring node.
2. From the popup menu that opens when you right-click the mouse, choose **Change Status** and change the status to the desired one.
A confirmation dialog box opens.
3. In the configuration dialog box, click **Yes**.

6.2.3 Changing the monitoring status of monitoring nodes

This subsection explains how to change the monitoring status of a monitoring node. The action that occurs at the time of the change differs depending on the monitoring node type (monitoring group or monitored object). For details, see *4.2.2 Statuses of monitoring nodes* in the *JP1/Integrated Management - Manager Overview and System Design Guide*.

Changing the monitoring status of a monitoring node requires at least `JP1_Console_Operator` permission. When the monitoring range settings of the monitoring tree are enabled, you can change the status of only those monitoring nodes that can be accessed with at least `JP1_Console_Operator` permission from among the monitoring nodes being displayed.

To change the monitoring status of a monitoring node:

1. Select a monitoring node.
2. Use either of the following methods to change the status of the monitoring node:
 - From the popup menu that opens when you right-click the mouse, choose **Change Monitoring Status**, and then change the monitoring status to the desired one.
 - From the popup menu that opens when you right-click the mouse, choose **Properties** and select either **Monitoring** or **Not Monitoring** from the **General** page, and then click **OK** or **Apply**.

Important

- If the monitoring status of a higher-order monitoring group is set to **Not Monitoring**, you cannot set a lower-order monitoring node alone to **Monitoring**. Check the monitoring status of the higher-order monitoring group in the Monitoring Tree window.
- When the monitoring status of a monitoring node is set to **Not Monitoring**, the status returns to the initial status.

6.2.4 Searching for monitoring nodes

To search for monitoring nodes:

1. Select a monitoring group.

You can restrict the monitoring nodes that can be searched to the selected monitoring group and the monitoring nodes that are in that monitoring group.

2. From the popup menu that opens when you right-click the mouse, choose **Search**.

3. Enter a condition into the Search window and click the **Search** button.

Monitoring nodes that match the search condition are displayed in a list.

You can perform the following operations on the monitoring nodes that are displayed in the list:

- Change the status or monitoring status of a monitoring node.
To change the status or monitoring status of a monitoring node, right-click to open the popup menu.
- With the target monitoring node selected, open the Monitoring Tree window.
To do so in this case, double-click the mouse.

6.2.5 Searching for status-change events

To search for status-change events:

1. Select a monitoring node whose status has changed.
2. From the popup menu that opens when you right-click the mouse, choose **Search Status-Change Events**.

When you execute a status-change event search on a monitored object, up to 100 JP1 events matching the status-change condition of that monitored object are displayed sequentially, starting with the earliest event, on the **Search Events** page of the Event Console window (the 101st and subsequent events are not displayed). Therefore, if the number of JP1 events displayed as search results has increased, we recommend that you manually change the status of the monitored object as needed.

If the number of JP1 events matching the status-change condition of the monitored object exceeds 100, a warning JP1 event (event ID = 00003FB1) is generated. When this JP1 event is generated, check how JP1 events matching the status-change condition are handled, and manually change the status of the monitored object.

When you execute a status-change event search on a monitoring group, up to 100 JP1 events matching the status-change condition of the monitored objects in that monitored group are displayed sequentially on the **Search Events** page of the

Event Console window, starting with the earliest event (the 101st and subsequent events are not displayed). Note that if a status change condition has been defined for a monitoring group, only up to 100 status-change events requiring action are sequentially displayed, starting with the earliest event, even if there are events that changed the status of lower-order monitoring nodes.

Important

- When you manually change the status of a monitoring node, you clear the status-change event history. Consequently, you will not be able to search for (display) the status-change events that have occurred in the past. Therefore, before you manually change the status of a monitoring node, check how JP1 events matching the status-change condition are handled.
- The JP1 events that can be searched using a status-change event search are restricted by a user filter (if the user is subject to restriction by a user filter).
- We recommend that you open the Event Console window before searching for status-change events.
- If the number of JP1 events matching the status change condition of the monitored object exceeds 100, the completed-action linkage function becomes inactive. Therefore, if the number of JP1 events displayed as search results has increased, we recommend that you manually change the status of the monitored object as needed.

6.2.6 Displaying the attributes of monitoring nodes

To display the attributes of a monitoring node:

1. Select a monitoring node.
2. From the popup menu that opens when you right-click the mouse, choose **Properties**.
The Properties window opens.

A JP1 user having at least `JP1_Console_Operator` permission can change several of the attributes displayed in the Properties window. To change the attributes of a monitoring node, log in as a user with at least the operating permission of `JP1_Console_Operator`.

6.2.7 Displaying guide information

To display guide information:

1. Select a monitored object.
2. From the popup menu that opens when you right-click the mouse, choose **Guide**.

You must define in advance, in a guide information file, the conditions for displaying guide information according to various situations and the guide information content.

About the guide information function, definition file, and settings:

- About the details to set in the guide information and the guide function:
See *4.8 Guide function* in the *JP1/Integrated Management - Manager Overview and System Design Guide*.
- About editing the guide information file:

See 5.6 *Editing guide information* in the *JPI/Integrated Management - Manager Configuration Guide*.

- About the format of the guide information file:

See *Guide information file (jcs_guide.txt)* (in *Chapter 2. Definition Files*) in the manual *JPI/Integrated Management - Manager Command and Definition File Reference*.

7

System Operation Using JP1/IM

This chapter explains the use of JP1/IM - View for system operations. For details about the windows explained in this chapter, see *Chapter 2. Event Console Window* and *Chapter 3. Monitoring Tree Window* in the manual *JP1/Integrated Management - Manager GUI Reference*.

7.1 Executing a command

You can execute commands on an agent host or a manager host. You can also execute the commands (client application) of a client host (viewer host). You can use this function when you are connected to JP1/IM - Manager (Central Scope) from JP1/IM - View.

If JP1/Base on the host stops while a command is being executed, `CMD . EXE` and the executing command (in Windows) or a shell and the executing command (in UNIX) might remain. In such cases, either manually stop the command or restart the host.

In addition, commands in the queue are discarded if JP1/Base on the host that stops while a command is being executed.


7.1.1 Executing a command by using Command Execution

The following operations require `JP1_Console_Admin` permission or `JP1_Console_Operator` permission.

- Executing a command on an agent host
- Executing a command on a manager host
- Executing a client application

To execute a command that inherits event information, select the JP1 event, and then execute the command.

The following describes the method of operation.

1. In the Event Console window, choose **Options** and then **Execute Command**, or from the toolbar, click the  icon.

The Execute Command window opens.

2. Select **Command type**.

If you are executing a command on a managed host (agent host or manager host), select the **Command of managed host** radio button.

If you are executing a client application, select the **Client application** radio button.

3. If necessary, select **Event Information to inherit**.

If you want to inherit event information, select the **Inherit event information** check box.

4. For **Target host**, specify the host on which the command is to be executed.

For the target host, specify the host name that is specified as the managed host in the system configuration definition.

You can also select from the list box a host name that was specified in the past. A maximum of five host names specified in the past are saved in the list box.

If you selected the **Inherit event information** check box in step 3, event information is inherited and automatically entered.

You can also specify a host group name for the command target host. When you specify a host group name, the command will be executed on all hosts that comprise the host group. Host group names that can be specified are those that are defined by the login manager.

For details about the procedure for defining host groups, see *1.15 Setting up a command execution environment (for Windows)* or *2.14 Setting up a command execution environment (for UNIX)* in the *JP1/Integrated Management - Manager Configuration Guide*.

When you set a business group or monitoring group, you can specify a business group or a monitoring group for the target host name. The specification method follows.

Example: When business group management system is specified for the target host name

/Management system

For details about the specification method, see *3.1.4(3) How to specify business groups* in the *JPI/Integrated Management - Manager Overview and System Design Guide*.

5. In **Command**, specify the command to be executed. Also specify an **Environment variable file** as needed.

Enter the command line to be executed in **Command**.

You can also select from the list box a command that was specified in the past. To erase the history of commands specified in the past, click the **Clear History** button.

For **Environment variable file**, specify the absolute path to the environment variable file located at the command target host.

The following commands can be executed:

When the command target host is running under Windows

- Executable files (.com and .exe)
- Batch files (.bat)
- JPI/Script script files (.spt) (Association must be set up to allow .spt files to be executed.)
- Data files (.vbs) that have a file type (extension) associated with applications that can execute automatic actions

When the command target host is running under UNIX

- UNIX commands
- Shell scripts

The following types of commands cannot be executed:

- Commands that require interactive operations
- Commands that open a window
- Commands that come with an escape sequence or control code
- Commands that do not end, such as a daemon
- Commands that must interact with the desktop, such as Windows Messenger and DDE (in Windows)
- Commands that shut down the OS, such as shutdown and halt

6. Click the **Execute** button.

When the **Inherit event information** check box in **Event information to inherit** is not selected


The command whose command type was selected in **Command type** is executed on the host specified in **Target host**. After the command is executed, **Time**, **Host**, and **Message** appear in **Log**. There is no need to perform the following steps.

When the **Inherit event information** check box in **Event information to inherit** is selected

The Preview Command Execution Content window opens. Go to the next step.

7. Check the information in the Preview Command Execution Content window.

Check the information for **Target host**, **Command**, and **Environment variable file** after the variables are replaced.

An item for which  is displayed has a setting error. Review the settings.

For details about the Preview Command Execution Content window, see *2.41 Preview Command Execution Content window* in the manual *JPI/Integrated Management - Manager GUI Reference*.

8. Click the **Execute** button.

If there is no problem with the information in the Preview Command Execution Content window, the command is executed, and the Preview Command Execution Content window closes. After the command is executed, **Time**, **Host**, and **Message** appear in **Log** in the Execute Command window.

7.1.2 Executing a command by using the Command button

There are two ways to execute a command previously registered for a **Command** button, depending on the type of host on which the command is executed.

- Executing a command on an agent host or manager host
- Executing a command defined on the source host of the selected event

To execute a command, you need `JP1_Console_Admin` permission or `JP1_Console_Operator` permission. When you move the cursor to the **Command** button, the information set for the **Command** button is displayed in the Execute Command window. Before executing a command, make sure that you check the information for the command.

To execute a command that inherits event information, select the JP1 event, and then execute the command.

For details about how to set the **Command** button, refer to the following:

- For Windows
1.15 Setting up a command execution environment (for Windows) in the JP1/Integrated Management - Manager Configuration Guide
- For UNIX
2.14 Setting up a command execution environment (for UNIX) in the JP1/Integrated Management - Manager Configuration Guide

(1) Executing a command on an agent host or manager host

The following describes how to immediately execute a command on an agent host or manager host.

(a) Immediately executing a command

To immediately execute a command after the **Command** button is clicked, create the following settings.

Event information is not inherited when the command is executed:

Specify `true` for the `gui` parameter in the command button definition file. If you specify this parameter, when the **Command** button is clicked, a message asking whether the command is to be executed is not displayed, and the command is immediately executed on the agent host or manager host.

Event information is inherited when the command is executed:

Specify `false` for the `preview` parameter in the command button definition file. If you specify this parameter, when the **Command** button is clicked, the Preview Command Execution Content window does not open, and the command is immediately executed.

The following describes the procedure for immediately executing a command:

1. In the Event Console window, select **Option** and then **Execute Command**. Alternatively, on the toolbar, click



The Execute Command window opens.

2. Click the **Command** button to which the command you want to execute has been assigned.
The command is executed.

(b) Executing a command after changing the information registered for the command

The following describes how to execute a command after changing the information registered for it.

When you execute a command that inherits event information, the Preview Command Execution Content window opens, and you can change the information for the command. The following operation is effective when you execute the command on a managed host that does not inherit events.

1. In the Event Console window, choose **Option** and then **Execute Command**. Alternatively, on the toolbar, click



The Execute Command window opens.

2. Right-click the **Command** button to which the command you want to execute has been assigned to display a popup menu.
3. On the popup menu, click **Custom Execution**.

The setting information for the **Command** button is displayed in **Command type**, **Event information to inherit**, **Target host**, **Command**, and **Environment variable file** of the Execute Command window. You can now edit the setting information.

Edit **Target host**, **Command**, and **Environment variable file** as needed.

4. Click the **Execute** button.
The command is executed on the agent host or manager host.

(2) Executing a command defined on the source host of the selected event

The following applies to the source host of the event when the host is undergoing examination or when corrective action for an error is being performed for it. If you do not specify anything in **Target host**, but define a **Command** button, and then click the **Command** button, you can execute a command defined on the source host of the selected event. Note that even if the attribute of another JP1 event is mapped, the source host before the mapping is set in **Target host**.

The following describes the procedure for executing a command defined on the source host of the selected event.

1. In the Event Details window, choose the **Execute Command** button.
The Event Details window opens.
2. Click the **Command** button to which the command you want to execute is assigned.

Event information is not inherited when the command is executed:

A message asking whether the command is to be executed is displayed. If there is no problem, you can click the **OK** button.

The command defined on the source host of the selected event is executed. Note that when `true` is specified for the `qui` parameter in the command button definition file, the command is executed immediately without displaying any message. There is no need to perform the following steps.


Event information is inherited when the command is executed:

When `false` is specified for the `preview` parameter in the command button definition file, the command is executed immediately without displaying the Preview Command Execution Content window. There is no need to perform the following steps.

When `true` is specified, the Preview Command Execution Content window opens. Go to the next step.

3. Check the information in the Preview Command Execution Content window.

Check the information for **Target host**, **Command**, and **Environment variable file** after the variables are replaced.

An item for which  is displayed has a setting error. Review the settings.

For details about the Preview Command Execution Content window, see 2.41 *Preview Command Execution Content window* in the manual *JP1/Integrated Management - Manager GUI Reference*.

4. Click the **Execute** button.

If there is no problem in the information in the Preview Command Execution Content window, the command is executed, and the Preview Command Execution Content window closes. After the command is executed, **Time**, **Host**, and **Message** appear in **Log** in Execute Command window.

7.1.3 User that executes commands

Commands are executed by mapping the JP1 user who logged in to JP1/IM - Manager (Central Scope) to the user name under the OS, according to the user mapping definition at the command execution host. Commands cannot be executed if user mapping is not defined or if the login JP1 user name is not registered in the user mapping definition.

In UNIX, commands are executed using the shell environment of the OS user that is mapped. If you want to execute a command that uses two-byte characters, you will need change the shell environment of the OS user to support two-byte characters.

For details about user mapping definitions, see the *JP1/Base User's Guide*.

7.1.4 Checking command execution status and deleting a command

After a command is executed from the Execute Command window of JP1/IM - View, if the message reporting execution termination (KAVB2013-I) is not displayed in **Log**, a problem may have occurred at the command execution host.

In this case, follow the procedure described below to check the command execution status, and if necessary, delete the command.

Important

The procedure described here can be used only when the version of JP1/Base on the command execution host is 07-51 or later. This procedure cannot be used if the JP1/Base version is 07-00 or earlier.

To check the command execution status and delete a command:

1. Using the `jcocmdshow` command, check the command status.

Execute the `jcocmdshow` command on the command execution host, and based on the returned information, investigate whether a problem has occurred. Based on the investigation, if it is determined that the command needs to be stopped, proceed to the next step.

2. Using the `jcocmddel` command, delete the command.

Execute the `jcocmddel` command on the command execution host to delete the command.

3. Using the `jcocmdshow` command, check the command status.

Execute the `jcocmdshow` command to determine whether the command has been correctly deleted.

For the command syntax:

See the chapter that explains commands in the *JPI/Base User's Guide*.

7.2 Executing automated actions and taking necessary steps

You can automatically execute an action (command) when a certain JP1 event is received. This function is called the *automated action function*. You can execute an action not only on the host on which the definition of automated actions is stored, but also on an agent host or manager host.

For details about how to define automated actions, see the following sections:

- For setting up automated actions (using the GUI)
See *2.32 Action Parameter Definitions window* in the manual *JP1/Integrated Management - Manager GUI Reference*.
- For setting up automated actions (using a definition file)
See *Automated action definition file (actdef.conf)* (in *Chapter 2. Definition Files*) in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

The following three types of status checks can be executed on automated actions:

- Checking the execution status of an automated action
Checks whether a problem has occurred during execution of the automated action.
- Checking the execution result of the automated action and the operation needed (cancellation or re-execution of the automated action)
Checks the execution result of the automated action that was executed. Additionally, checks detailed information or initiates manual re-execution of the automated action as needed.
- Checking the operating status of the automated action function
Checks whether the automated action function is working. If not, automated actions cannot be executed.

The following subsections explain how to perform these checks and automated actions.

7.2.1 Checking the execution status of an automated action

When you enable the automated action execution monitoring (delay monitoring and status monitoring) function, you can quickly detect the occurrence of even the following problems.

- The automated action did not terminate within the expected time. Alternatively, it took a long time to terminate.
- Execution of the automated action failed (the status transitioned to `Fail`, `Error`, or `Error (Miss)`).

You must specify in advance, when you are defining the automated action, whether to enable the execution monitoring (delay monitoring and status monitoring) function. You must also set up a JP1 event to be generated or a notification command to be executed when a problem is detected.

For details about settings, see the following sections:

For setting up automated actions (using the GUI)

See *2.32 Action Parameter Definitions window* in the manual *JP1/Integrated Management - Manager GUI Reference*.

See *2.33.1 Action Parameter Detailed Definitions window* in the manual *JP1/Integrated Management - Manager GUI Reference*.

For setting up automated actions (using a definition file)

See *Automated action definition file (actdef.conf)* (in *Chapter 2. Definition Files*) in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

For setting up JP1 event generation and notification commands

See *Automatic action notification definition file (actnotice.conf)* (in *Chapter 2. Definition Files*) in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

The checking procedure is described below. To enable the execution monitoring (delay monitoring and status monitoring) function again after an error has been detected, you need `JP1_Console_Admin` permission or `JP1_Console_Operator` permission. In addition, when the reference and operation permissions are set for a business group, operations in the Event-Information Mapping Definitions window might not be possible depending on the combination of JP1 resource group and JP1 permission level. For details, see *3.1.4(2) Assigning a JP1 resource group and permission level to a JP1 user* in the *JP1/Integrated Management - Manager Overview and System Design Guide*.

To check the execution status of an automated action:

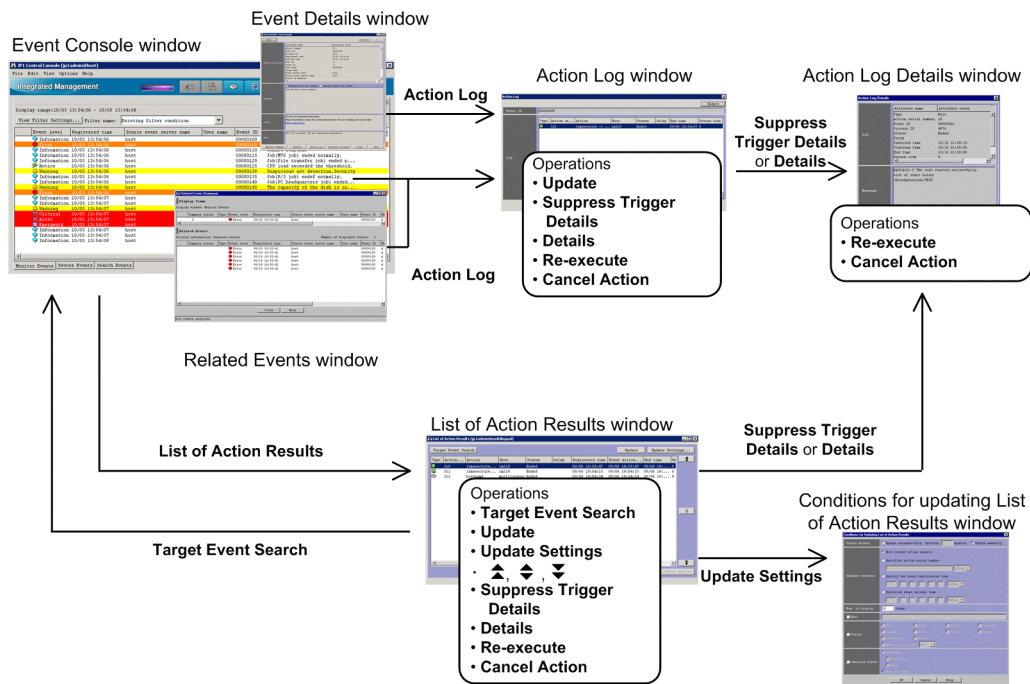
1. In the Event Console window, check the execution status of the automated action. Alternatively, check whether a notification command has reported that an error occurred.
If generation of a JP1 event was set, a JP1 event with event ID 2010 or 2011 is displayed in the events list. If execution of a notification command was set, the notification command reports the error.
When you find out that an error has occurred based on the JP1 event or via notification by a notification command, proceed to the next step.
2. Using the Action Log window and the List of Action Results window, check the execution status of the automated action and then take the necessary steps.
As needed, use the Action Log window and the List of Action Results window to check details or to cancel/re-execute the action. For details, see *7.2.2 Checking the execution results of automated actions*.
Note that once notification by the delay monitoring function or status monitoring function is executed, further notification is suppressed until the user releases the notification suppression. Therefore, release the notification suppression as needed. To release a suppressed function, proceed to the next step.
3. From the menu in the Event Console window, choose **Options** and then **Function-Status Notification Return**, and then from **Action Delay Monitoring**, choose **Action Status Monitoring** and select the function name that is enabled.
A suppressed function is displayed in gray letters (to indicate that it is disabled). When you select an enabled function name, a dialog box opens, asking you whether to release the notification suppression.
4. In the dialog box, click **Yes**.
Clicking **Yes** releases the notification suppression, enabling the monitoring function again.

7.2.2 Checking the execution results of automated actions

You can check the execution results of automated actions in the Action Log window or List of Action Results window of JP1/IM - View. You can also check the execution results by using the `jcashowa` command.

In the Action Log window and List of Action Results window, you can also perform operations such as displaying action details and re-executing actions, in addition to checking execution results. The figure below shows the window transitions and operations related to automated actions.

Figure 7–1: Window transitions and operations related to automated actions



Operations are divided into those that display detailed information about action execution results and those for repeating an operation (re-execution or cancellation) on action execution results.

The procedures for checking the execution results and for repeating an operation (re-execution or cancellation) follow.

(1) Checking the execution results of automated actions

You can check the execution results of automated actions in the Action Log window or List of Action Results window, or by using the `jcashowa` command.

(a) Checking the execution results in the Action Log window

In the Action Log window, you can display the execution results of automated actions that were set for the events selected from the events list in the Event Console window.

To check the execution results in the Action Log window:

1. From the events list in the Event Console window, select an event for which the action icon is displayed in the **Action** column.
2. Using one of the following methods, open the Action Log window:
 - From the menu bar, choose **View** and then **Action Log**.
 - From the popup menu, choose **Action Log**.
 - Click the **Action Log** button.

The Action Log window opens.

The Action Log window displays the selected event IDs and the execution results of the automated actions that are specified for those event IDs.

3. To view the details of the execution result of each automated action, or to view the details about the automated action that became a trigger for suppressing an action, open the Action Log Details window.

To view the execution results of an automated action:

- From **Log**, select an automated action and click the **Details** button.
- Double-click an automated action displayed in **Log**.

To view the automated action that became a suppression trigger:

- From **Log**, select an automated action that is suppressed, and click the **Suppress Trigger Details** button.

The Action Log Details window opens.

This window displays the execution results and the message that was issued. For details about the execution results that are displayed, see *2.37 Action Log Details window* in the manual *JP1/Integrated Management - Manager GUI Reference*.

If the Related Events window is open, you can open the Action Log window by selecting an event that has the action icon attached and then choosing **Action Log** from the popup menu. If the Event Details window is open, you can open the Action Log window by clicking the **Action Log** button.

(b) Checking the execution results in the List of Action Results window

In the List of Action Results window, you can display the execution results of automated actions that were set by the logged-in manager. Set the condition for the automated actions to be displayed in the Conditions for Updating List of Action Results window.

To check the execution results in the List of Action Results window:

1. From the Event Console window, choose **View** and then **List of Action Results**.

The List of Action Results window opens.

From among the automated actions that were set by the logged-in manager, the List of Action Results window displays a list of those execution results for automated actions that satisfy the condition specified in the Conditions for Updating List of Action Results window.




2. To change the condition for displaying the execution results of automated actions, click the **Update Settings** button.

The Conditions for Updating List of Action Results window opens.

In this window, you can specify an updating method (automatic update or manual update) and an action result acquisition range, as well as a display item count and display condition to be used during updating. For details, see *2.39 Conditions for Updating List of Action Results window* in the manual *JP1/Integrated Management - Manager GUI Reference*.

3. To update the display content of the execution results of automated actions according to an updated condition, click the **Update** button.

The display content is updated according to the content that is specified in the Conditions for Updating List of Action Results window.

4. To display the execution results of automated actions that occurred before the automated actions currently listed, click the  icon. To display the execution results of automated actions that occurred after the automated actions currently listed, click the  icon. To re-display execution results according to the updating condition that is specified in the Conditions for Updating List of Action Results window, click the  icon.

5. To view the details of the execution result of each automated action, or to view the details about the automated action that became a trigger for suppressing an action, use one of the following methods to open the Action Log Details window:

To view the details of the execution result of each automated action:

- From **Log**, select an automated action and then click the **Details** button.

- Double-click an automated action displayed in **Log**.

To view the automated action that became a suppression trigger:

- From **Log**, select an automated action that is suppressed, and then click the **Suppress Trigger Details** button.

The Action Log Details window opens.

This window displays the execution result and the message that has been issued. For details about the execution results to be displayed, see *2.37 Action Log Details window* in the manual *JP1/Integrated Management - Manager GUI Reference*.

6. To display the JP1 event that triggered execution of the automated action, from **Log**, select an automated action, and then click the **Target Event Search** button.

An event search is executed and the **Search Events** page of the Event Console window displays the JP1 event that triggered execution of the automated action.

(c) Using the `jcashowa` command to check execution results

You can use the `jcashowa` command to display the execution results of automated actions. When executed, the `jcashowa` command displays the results of executed automated actions that are stored in the action information file. Use the `jcashowa` command in an environment in which JP1/IM - View is not used, or when you want to output the execution results of automated actions to a file.

A command execution example follows. To display the execution results of automated actions that were taken for JP1 events received between 16:00 and 17:00 on July 1, enter the following from the manager:

```
jcashowa -d 07/01/16:00,07/01/17:00
```

For details about the `jcashowa` command syntax and the execution result display method, see *jcashowa* (in *Chapter 1. Commands*) in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

(2) Canceling automated actions

When an automated action is in one of the following statuses, you can cancel that automated action:

- Wait, Queue, or Running
- Send (Miss), Wait (Miss), Queue (Miss), or Running (Miss)

You can cancel an automated action in the Action Log window, List of Action Results window, Action Log Details window, or by using the `jcacancel` command. To use one of these windows to cancel an automated action, you need `JP1_Console_Admin` permission or `JP1_Console_Operator` permission. In addition, when the reference and operation permissions are set for a business group, operations in the Event-Information Mapping Definitions window might not be possible depending on the combination of JP1 resource group and JP1 permission level. For details, see *3.1.4(2) Assigning a JP1 resource group and permission level to a JP1 user* in the *JP1/Integrated Management - Manager Overview and System Design Guide*.

(a) Canceling an automated action from the Action Log window or List of Action Results window

To cancel an automated action from the Action Log window or List of Action Results window:

1. Open the Action Log window or List of Action Results window.
For details about how to open windows, see *7.2.2(1) Checking the execution results of automated actions*.
2. Select the automated action you want to cancel.

3. Click the **Cancel Action** button.

The cancellation confirmation dialog box opens.

4. Click **OK**.

The request to cancel the selected automated action is accepted.

5. To check the status following the cancellation, click the **Update** button.

(b) Canceling an automated action from the Action Log Details window

To cancel an automated action from the Action Log Details window:

1. Open the Action Log Details window.

For details about how to open windows, see [7.2.2\(1\) Checking the execution results of automated actions](#).

2. Click the **Cancel Action** button.

The cancellation confirmation dialog box opens.

3. Click **OK**.

The request to cancel the selected automated action is accepted.

4. To check the status following the cancellation, click the **Close** button and return to the Action Log window or List of Action Results window, and then click the **Update** button.

(c) Using the `jcacancel` command to cancel automated actions

You can use the `jcacancel` command to cancel automated actions. Use this command when you want to cancel automated actions in batches by host or system. Before executing the `jcacancel` command to cancel automated actions, confirm which automated actions will be canceled. For details about the confirmation method, see [7.2.2\(1\) Checking the execution results of automated actions](#).

A command execution example follows. To cancel all automated actions that are queued or running on `host01` in a single batch, enter the following from the manager:

```
jcacancel -s host01
```

For details about the `jcacancel` command syntax and the execution result display method, see `jcacancel` (in *Chapter 1. Commands*) in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

(3) Re-executing an automated action

When an automated action is in one of the following statuses listed, you can re-execute that automated action:

- Deterrent, Ended, Error, Cancel, or Kill
- Ended (Miss) or Error (Miss)

You can re-execute an automated action from the Action Log window, List of Action Results window, or Action Log Details window. To use one of these windows to re-execute an automated action, you need `JP1_Console_Admin` permission or `JP1_Console_Operator` permission.

In addition, when the reference and operation permissions are set for a business group, operations in the Event-Information Mapping Definitions window might not be possible depending on the combination of JP1 resource group and JP1 permission level. For details, see [3.1.4\(2\) Assigning a JP1 resource group and permission level to a JP1 user](#) in the *JP1/Integrated Management - Manager Overview and System Design Guide*.

(a) Re-executing an automated action from the Action Log window or List of Action Results window

To re-execute an automated action from the Action Log window or List of Action Results window:

1. Open the Action Log window or List of Action Results window.
For details about how to open windows, see *7.2.2(1) Checking the execution results of automated actions*.
2. Select the automated action you want to re-execute.
3. Click the **Re-execute** button.
The re-execution request confirmation dialog box opens.
4. Click **OK**.
The request to re-execute the selected automated action has been accepted.
5. To check the status following the re-execution, click the **Update** button to update the List of Action Results window.

(b) Re-executing an automated action from the Action Log Details window

To re-execute an automated action from the Action Log Details window:

1. Open the Action Log Details window.
For details about how to open windows, see *7.2.2(1) Checking the execution results of automated actions*.
2. Click the **Re-execute** button.
The re-execution request confirmation dialog box opens.
3. Click **OK**.
The request to re-execute the selected automated action has been accepted.
4. To check the status following the re-execution, click the **Close** button to return to the Action Log window or the List of Action Results window, and then click the **Update** button.

7.2.3 Checking the operating status of the automated action function

If the automated action function is not running, no automated action is executed even if an event that triggers automated action is registered in the JP1/Base of the manager. You can use the `jcstatus` command to check the operating status of the automated action function.

When the `jcstatus` command is executed, information indicating a status (`RUNNING`, `STANDBY`, or `STOP`) is output to standard output according to the operating status (`running`, `standby`, or `stopped`). If the operating status is `RUNNING`, the automated action function is running. If the operating status is `STANDBY`, the automated action function is not running and therefore the automated action is not executed. To change the status to `RUNNING`, you need to execute the `jcchange` command. If the operating status is `STOP`, JP1/IM - Manager may have stopped. In this case, you need to restart JP1/IM - Manager.

For details, see the following sections:

For the `jcstatus` command and the display format

See *jcstatus* (in *Chapter 1. Commands*) in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

For the `jcachange` command and the display format

See *jcachange* (in *Chapter 1. Commands*) in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

For details about how to start and stop JP1/IM - Manager:

See *Chapter 3. Starting and Stopping JP1/IM - Manager*.

7.3 Opening other application windows from the Tool Launcher

The Tool Launcher window displays a list of programs linked to JP1/IM, and you can start a program from this window. You can start the following two types of programs:

Application programs in the viewer

These are application programs that are installed on the same host as JP1/IM - View. When you select a program from the Tool Launcher, an executable file is started.

Web page

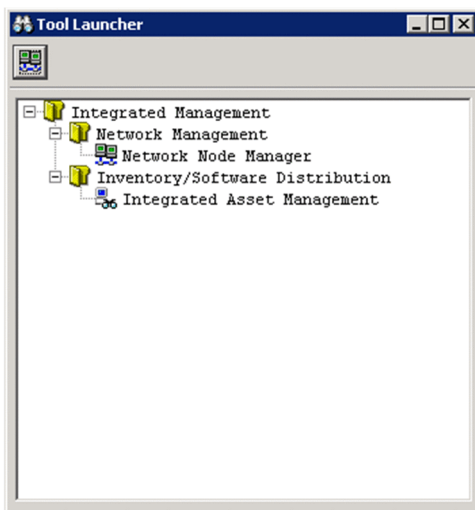
When an application on the system provides a Web page, you can display that Web page. When you select a program from the Tool Launcher, a Web browser starts and displays the Web page.

To use these functions, you must set the URL of the Web page in advance. For details about the setting, see *Web page call definition file (hitachi_jp1_product-name.html)* (in *Chapter 2. Definition Files*) in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

Furthermore, before using the Tool Launcher to link to another product, check the operating environment (supported OS and browsers, for example) of that product.

An example of the Tool Launcher window follows.

Figure 7–2: Tool Launcher window example



The above figure shows the Tool Launcher window when no application program linked to JP1/IM has been installed in the viewer. When an application program is installed in the viewer, that installed application program is added to the tree in the display.

For details about the programs to be linked, see [7.3.2 Functions that can be operated from the Tool Launcher window](#).

7.3.1 Operations in the Tool Launcher window

The Tool Launcher window displays the functions of the programs linked to JP1/IM in a tree format. A folder expresses a function category. By double-clicking the end of the tree, you can open a Web page or application program window.

To display a Web page or open an application program window:

1. In the Event Console window, from the **Monitoring Tree** page, choose **Options** and then **Start Integrated Function Menu**. Alternatively, from the toolbar, click the  icon.

The Tool Launcher window opens.

If `MENU_AUTO_START=ON` is specified in the `tuning.conf` file of JP1/IM - View, the Tool Launcher window automatically opens when you log in. For details about the `tuning.conf` file of JP1/IM - View, see *IM-View settings file (tuning.conf)* in *Chapter 2. Definition Files* of the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

2. Expand the tree in the Tool Launcher and double-click the item you want to display.

The window for the selected function opens.




Note:

When an application program is invoked from the Tool Launcher, the application program cannot start if the OS user that started JP1/IM - View does not have the necessary permissions to execute the application program being invoked.

You must also start JP1/IM - View using the permissions that can execute the application program being invoked.

The functions listed in the table below can also be invoked from toolbar icons.

Table 7–1: Functions that can be invoked from toolbar icons

Function name	Icon
Network node manager	
Windows Remote Controller	
Inventory/Software Distribution	

#: The Windows edition of JP1/IM - View cannot link to the Web page of JP1/Software Distribution Manager; therefore, the **Inventory/Software Distribution** icon is not displayed.

7.3.2 Functions that can be operated from the Tool Launcher window

The table below shows the functions that are displayed in the Tool Launcher window.

If the window type is an application window and the applicable program is not installed in the viewer, the function name is not displayed in the viewer.

For details about the supported versions of linkage products and the supported OSs, see the documentation of the applicable linkage product.

Table 7–2: Functions displayed in the Tool Launcher window

Menu item			Description of the function that starts		
Folder name	Subfolder name	Function name	Window type	Program name	Installation destination
Network Management	--	Network Node Manager	Web page	JP1/Cm2/NNM	Host within the system
				HP NNM	

Menu item			Description of the function that starts		
Folder name	Subfolder name	Function name	Window type	Program name	Installation destination
	--	Internet Gateway	Application window	JP1/Cm2/Internet Gateway Server	Host on which JP1/IM - View is installed
Job Management	--	Job Scheduler	Application window	JP1/AJS - View	Host on which JP1/IM - View is installed
	--	Scenario Operation	Application window	JP1/AJS2 - Scenario Operation View	Host on which JP1/IM - View is installed
	--	Print Service	Application window	JP1/NPS	Host on which JP1/IM - View is installed
	File Transmission	Transmission Regist. & Exe.	Application window	JP1/FTP	Host on which JP1/IM - View is installed
		Log Information	Application window		
Auto-Start Program Registration		Application window			
Inventory/Software Distribution	--	Integrated Asset Management	Web page	JP1/Asset Information Manager	Host within the system
	--	Inventory/Software Distribution	Web page	JP1/Software Distribution Manager	Host within the system
	--	Facilities Asset Management	Application window	JP1/NetInsight II - Facility Manager	Host on which JP1/IM - View is installed
	--	Windows Remote Controller	Application window	JP1/NETM/Remote Control Manager	Host on which JP1/IM - View is installed
	--	Distribution /Asset Management	Application window	JP1/Software Distribution Manager	Host on which JP1/IM - View is installed
Storage Management	Storage Area Management	Storage System Operation Management	Web page	Hitachi Tuning Manager software	Host within the system
		Storage Hardware Management	Web page	Hitachi Device Manager software	
		Storage Resource Management	Web page	Hitachi Provisioning Manager	
		Storage Replication Management	Web page	Hitachi Replication Manager software	
		Tiered Storage	Web page	Hitachi Tiered Storage Manager software	

Menu item			Description of the function that starts		
Folder name	Subfolder name	Function name	Window type	Program name	Installation destination
		Resource Management			
		Global I/O Path Operation Management	Web page	Hitachi Global Link Manager software	
Server Management	--	Management Console	Application window	JP1/Server Conductor	Host on which JP1/IM - View is installed
	--	Web Console	Web page		Host within the system
Hardware Management	--	SANRISE2000 Remote Console	Application window	SANRISE	Host on which JP1/IM - View is installed
	-	SANRISE H512/H48 Remote Control XP	Application window		
Automated Notification	--	Notification Rule Setting	Application window	TELstaff or JP1/TELstaff	Host on which JP1/IM - View is installed
Mainframe Linkage	--	VOS3 Console Operation	Application window	VOS3 AOMPLUS(AOMPLUS CIF)	Host on which JP1/IM - View is installed
Cosminexus Operation Management	--	Cosminexus Operation Management Portal	Application window	Cosminexus Application Server	Host on which JP1/IM - View is installed

Legend:

--: None

8

Managing the System Hierarchy Using IM Configuration Management

This chapter explains how to use IM Configuration Management to manage the system hierarchy (IM configuration). For details about the windows described in this chapter, see *Chapter 4. IM Configuration Management Window* in the manual *JP1/Integrated Management - Manager GUI Reference*.

8.1 Managing hosts

If you change the JP1/IM system configuration or the host information, such as the name or IP address of a managed host, you must review the information related to the hosts managed in the IM Configuration Management database.

Perform the following tasks from the IM Configuration Management - View to manage host information.

Registering hosts

To register a new host in the IM Configuration Management database, use the Register Host window, which you can open from the IM Configuration Management window.

For details about the method, see *3.1.1 Registering hosts* in the *JP1/Integrated Management - Manager Configuration Guide*.

Deleting a host

You can delete a host registered in the IM Configuration Management database on the **Host List** page of the IM Configuration Management window.

For details about the method, see *3.1.6 Deleting hosts* in the *JP1/Integrated Management - Manager Configuration Guide*.

Collecting information from hosts

You can collect host information from the **Host List** page or **IM Configuration** page of the IM Configuration Management window.

For details about when host information is collected or the collection method, see *3.1.3 Collecting information from hosts* in the *JP1/Integrated Management - Manager Configuration Guide*.

Changing the host information

To change the host information registered in the IM Configuration Management database, use the Edit Host Properties window, which you can open from the IM Configuration Management window.

For details about the method, see *3.1.5 Changing the attributes of host information* in the *JP1/Integrated Management - Manager Configuration Guide*.

If you edit the host name registered in the system hierarchy (IM configuration), you must re-apply the system hierarchy. For details about the procedure for applying the system hierarchy, see *3.2.4(3) Applying a system hierarchy to a system managed by IM Configuration Management* in the *JP1/Integrated Management - Manager Configuration Guide*.

Displaying a host list

To display a list of the hosts registered in the IM Configuration Management database, use the **Host List** page of the IM Configuration Management window.

For details about the method, see *3.1.4 Displaying host information* in the *JP1/Integrated Management - Manager Configuration Guide*.

8.2 Managing the system hierarchy

If you change the system hierarchy (IM configuration), you must review the system configuration definition information registered in the IM Configuration Management database.

Perform the following tasks from the IM Configuration Management - View to manage the system hierarchy.

Collecting system hierarchy information

To collect the system configuration definition information, use the **Host List** page or **IM Configuration** page of the IM Configuration Management window. You can collect system configuration definition information from all hosts that constitute a system.

For details about the method, see *3.2.1 Collecting the system hierarchy* in the *JP1/Integrated Management - Manager Configuration Guide*.

Displaying the system hierarchy

To display the system hierarchy, use the **IM Configuration** page of the IM Configuration Management window.

For details about the method, see *3.2.2 Displaying the system hierarchy* in the *JP1/Integrated Management - Manager Configuration Guide*.

Verifying the system hierarchy

You can verify whether the collected configuration definition information matches the configuration definition information maintained by IM Configuration Management. To verify the configuration definition information, use the **Host List** page or **IM Configuration** page of the IM Configuration Management window.

For details about the method, see *3.2.3 Verifying the system hierarchy* in the *JP1/Integrated Management - Manager Configuration Guide*.

Editing the system hierarchy

You can edit the configuration definition information to add, move, and delete hosts. To edit the configuration definition information, use the Edit Agent Configuration window or the Edit Remote Monitoring Configuration window, which you can open from the IM Configuration Management window.

For details about the method, see *3.2.4 Editing the system hierarchy* in the *JP1/Integrated Management - Manager Configuration Guide*.

Applying the system hierarchy

You can apply the configuration definition information edited in the Edit Agent Configuration window or the Edit Remote Monitoring Configuration window to all the hosts constituting a system. To apply the configuration definition information, use the Edit Agent Configuration window or the Edit Remote Monitoring Configuration window.

For details about the method, see *3.2.4(3) Applying a system hierarchy to a system managed by IM Configuration Management* in the *JP1/Integrated Management - Manager Configuration Guide*.

Synchronizing system hierarchies

When the system hierarchy is defined separately by the integrated manager and the site managers, you must synchronize the system hierarchies used by the integrated manager and the site managers. To synchronize the system hierarchies, use the **IM Configuration** page of the IM Configuration Management window.

For details about the method, see *3.2.5 Synchronizing the system hierarchy* in the *JP1/Integrated Management - Manager Configuration Guide*.

8.3 Managing the configuration of a virtual system

This section explains how to manage a system hierarchy that contains a virtual host (virtual system configuration) by operating IM Configuration Management - View or by executing a command.

The management of a virtual configuration requires virtualization software and virtual environment management software. For details about the software you can use, see 6.3 *Virtualization configuration management* in the *JP1/Integrated Management - Manager Overview and System Design Guide*.

8.3.1 Registering a virtual system host

To register a virtual host into IM Configuration Management, open the Register Host window from the IM Configuration Management window.

For details about the method, see 3.3.1(2) *Setting virtualization configuration information* in the *JP1/Integrated Management - Manager Configuration Guide*.

8.3.2 Displaying host information in a virtual system

This subsection explains how to display information about a host that is registered as a virtual host in the system hierarchy. To display host information, invoke the **Host List** page of the IM Configuration Management window.

1. In the IM Configuration Management window, click the **Host List** tab.
The **Host List** page opens.
2. From the tree pane, select a virtual host.
3. Use either of the following methods to collect host information:
 - From the menu bar, choose **Operation** and then **Collect Host Information**.
 - From the popup menu that opens when you right-click the mouse, choose **Collect Host Information**.

If you want to collect host information, JP1/Base must be running on the virtual host.

Note that, because JP1/Base cannot be installed on VMware ESX and Hitachi Compute Blade logical partitioning feature, executing **Collect Host Information** causes an error.

4. Click the **Basic Information** button, **Product Information** button, or **Service Information** button.
Depending on the button you clicked, the node information display area displays different host information. You cannot click the **Lower Host Information** button.

8.3.3 Applying the management information to the Central Scope monitoring tree

To use Central Scope to monitor a virtual host registered in the system hierarchy, you need to export the management information of IM Configuration Management and import it into the monitoring tree information of Central Scope. The procedure follows:

1. Execute the `jclexport` command.

Export the configuration information of IM Configuration Management.

2. Execute the `jcsdbexport` command.

Export the monitoring tree information of Central Scope.

3. Using the output files of both the `jcfexport` and `jcsdbexport` commands as arguments, execute the `jcfmkcsdata` command.

Merge the configuration information of IM Configuration Management with the monitoring tree information.

4. Execute the `jcsdbimport` command.

Import the merged management information of IM Configuration Management and the monitoring tree information.

Using Central Scope - View, make sure that the merged virtual host is displayed.

8.4 Managing business groups

When monitoring targets are set as business groups, you must create, edit, and delete the business groups at the same time you review the configuration of business groups.

Creating a new business group

For details about the procedure for creating a new business group, see *3.4.1(1)(a) Creating a business group* in the *JP1/Integrated Management - Manager Configuration Guide*.

Editing the registration information of a business group

For details about the procedure for editing the registration information of a business group, see *3.4.1(1)(b) Editing the properties of a business group* in the *JP1/Integrated Management - Manager Configuration Guide*.

Deleting unnecessary business groups

For details about the procedure for deleting unnecessary business groups, see *3.4.1(1)(c) Deleting a business group* in the *JP1/Integrated Management - Manager Configuration Guide*.

After creating, editing, or deleting business groups, you need to apply the hierarchy of the business groups and the monitoring groups to the monitoring tree. For details about the procedure for applying the management hierarchy, see *3.4.4(2) Applying business group information and monitoring group information to the Central Scope monitoring tree* in the *JP1/Integrated Management - Manager Configuration Guide*.

8.5 Managing profiles

If you change the content of a profile during system update or maintenance or apply the content of a profile to the profile of another host, you must review the profile registered in the IM Configuration Management database.

Perform the following tasks from the IM Configuration Management - View to manage profiles.

There are two types of profiles: one for valid configuration information and the other for the content of the configuration file.

Obtaining profiles

You can obtain the following profiles:

- Valid JP1/Base configuration information on an agent host
- The JP1/Base configuration file on an agent host (event forwarding settings file, log file trap action-definition file, log-file trap startup definition file, event log trap action-definition file, and local action definition file)
- Valid configuration information for a monitored remote host

For details about the method, see *3.5.1(2) Collecting profiles* in the *JP1/Integrated Management - Manager Configuration Guide*.

Obtaining a list of profiles

You can obtain a list of profiles managed by JP1/Base on an agent host. This information is displayed in the tree pane of the Display/Edit Profiles window.

For details about the method, see *3.5.1(1) Collecting profile lists* in the *JP1/Integrated Management - Manager Configuration Guide*.

Displaying profiles

You can display the profiles for JP/Base on an agent host and a monitored remote host in the Display/Edit Profiles window.

For details about the method, see *3.5.1(3) Displaying profiles* in the *JP1/Integrated Management - Manager Configuration Guide*.

Editing settings files

You can edit settings files in the Display/Edit Profiles window. The following types of profiles can be edited by using a settings file:

- **Event Forwarding**
- **Log File Trapping**
- **Event Log Trapping**
- **Local Action**
- **Log File Trapping** under **Remote Monitoring**
- **Event Log Trapping** under **Remote Monitoring**

For details about the method, see *3.5.1(5) Editing configuration files* in the *JP1/Integrated Management - Manager Configuration Guide*.

Applying edited settings file information

You can apply edited settings file information.

For details about the method, see *3.5.1(6) Applying edited information in configuration files* in the *JP1/Integrated Management - Manager Configuration Guide*.

8.6 Managing service operation status

This chapter explains how to use IM Configuration Management - View to manage the status of service operations on each host.

8.6.1 Collecting service operation information

In an agent configuration, you can collect information about the operation of services that are running on each host from the system hierarchy.

Note that in a remote monitoring configuration, you cannot collect service operation information.

To collect service operation information, use the **Host List** page or **IM Configuration** page of the IM Configuration Management window. The procedure differs according to the page you select.

(1) Collecting service operation information from the Host List page

To collect service operation information from the **Host List** page of the IM Configuration Management window:

1. In the IM Configuration Management window, click the **Host List** tab.

The **Host List** page opens.

2. From the tree pane, select a host.

You cannot collect service operation information by selecting **Host List**. Furthermore, the range of hosts from which operation information can be collected varies depending on the manager on which IM Configuration Management is running. For details about the range of hosts that can be selected, see *6.7.2 Collecting service activity information* in the *JP1/Integrated Management - Manager Overview and System Design Guide*.

3. Click the **Service Information** button.

The collected service operation information is displayed in the node information display area.

4. From the menu bar, choose **Display** and then **Refresh**.

The latest service option information is collected from the host, and the display in the node information display area is refreshed.

(2) Collecting service operation information from the IM Configuration page

To collect service operation information from the **IM Configuration** page of the IM Configuration Management window:

1. In the IM Configuration Management window, click the **IM Configuration** tab.

The **IM Configuration** page opens.

2. From the tree pane, select a host.

The range of hosts from which operation information can be collected varies depending on the manager on which IM Configuration Management is running. For details about the range of hosts that can be selected, see *6.7.2 Collecting service activity information* in the *JP1/Integrated Management - Manager Overview and System Design Guide*.

3. Use either of the following methods to collect host information.

- From the menu bar, choose **Operation** and then **Collect Host Information**.
- From the popup menu that opens when you right-click the mouse, click **Collect Host Information**.

4. Click the **Service Information** button.

The collected service operation information is displayed in the node information display area.

5. From the menu bar, choose **Display** and then **Refresh**.

The latest service option information is collected from the host, and the display in the node information display area is refreshed.

8.6.2 Service operation information display

For details about how to display the operation information of services that are running on each host from the system hierarchy (IM configuration), see [8.6.1 Collecting service operation information](#).

The information on services in the IM Configuration Management window displays the following types of operation information:

Table 8–1: Operation information that is displayed for each service

Product name	Service name	Operating status
JP1/Base	JP1/Base	The operating status of the service is displayed as one of the following: <ul style="list-style-type: none"> • Running • Stopped • Partially running • Collection failed
	Event Service	
	Log file trap	
JP1/IM - Manager	JP1/IM - Manager	

Detailed Information in the IM Configuration Management window displays the execution results of the commands that collect information from individual services as follows.

Table 8–2: Commands that collect information about individual services

Service name	Collection command
JP1/Base	<code>jbs_spm�_status</code>
Event Service	<code>jevstat</code>
Log file trap	<code>jevlogstat ALL</code>
JP1/IM - Manager	<code>jco_spm�_status</code>
Log file trap (remote)	<code>jcfallogstat#</code>
Event log trap (remote)	<code>jcfaleltstat#</code>

#: Information corresponding to the collection command is output.

8.7 Exporting and importing management information of IM Configuration Management

This section explains how to execute commands to export and import the management information of IM Configuration Management.

8.7.1 Exporting management information of IM Configuration Management

By outputting (exporting) management information managed by IM Configuration Management and then inputting (importing) it, you can copy management information from one host to another. In addition, by editing the system configuration information that has been exported, you can easily modify it. This subsection explains the management information that is exported by the `jcfexport` command. For details about the `jcfexport` command, see *jcfexport* in *Chapter 1. Commands* of the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

(1) Host information

Information related to the host managed by IM Configuration Management is exported to the host input information file and the collected host information file.

For details about the host input information file, see *Host input information file (host_input_data.csv)* in *Chapter 2. Definition Files* of the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

For details about the collected host information file, see *Collected host information file (host_collect_data.csv)* in *Chapter 2. Definition Files* of the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

(2) System hierarchy information

The system hierarchy information is exported to a file. You can edit the exported file and import it.

The information that is output differs according to the system monitoring method:

- Agent monitoring
- Remote monitoring

(a) Configuration information for agent monitoring

The name of the file that is exported is `system_tree_information.txt`.

The following table describes the configuration information for agent monitoring that is output to the file.

Table 8–3: JP1/IM's system hierarchy information that is exported

Output item	Description of output value
[<i>managing-host</i>]	<ul style="list-style-type: none">• Indicates the integrated manager, a site manager, or a relay manager that manages JP1/Base hosts.• The first managing host that is defined is the integrated manager, and the managing hosts subsequently defined are either site managers or relay managers.• Hosts are treated as managed hosts until the next host in square brackets [] appears.• If the system hierarchy is divided and defined, the host name is preceded by an asterisk (*).

Output item	Description of output value
<i>managed-host</i>	<ul style="list-style-type: none"> • A JP1/Base host that is managed by a managing host. • A site manager or relay manager is defined as a host managed by the integrated manager. • If the system hierarchy is divided and defined, the host name is preceded by an asterisk (*).

(b) Configuration information for remote monitoring

The configuration information for remote monitoring is exported to a file. The name of the file to be exported is `system_remote_tree_information.txt`.

The following table describes the configuration information for remote monitoring that is output to the file.

Table 8–4: Configuration information for remote monitoring that is exported

Output item	Description of output value
[<i>managing-host</i>]	<ul style="list-style-type: none"> • Indicates the integrated manager or site manager that manages the remote monitoring configuration. • For a site manager, the host name is preceded by an asterisk (*).
<i>managed-host</i>	A host that is managed remotely in IM Configuration Management

(3) Profile information

The profile information that is running on the host is exported. The files that are exported differ according to the system monitoring method:

- Agent monitoring
- Remote monitoring

(a) Profile information for agent monitoring

The profile information of the JP1/Base that is running on the host is exported. The file is exported to the first-level directory (*host-name*) and the second-level directory (*JP1Base*) under the `definition_files` directory. The log file trap action definition file is exported to the third-level directory (`cf_log_file_trap`). The following table describes the profile information that is exported.

Table 8–5: Name of the files for exporting profile information for agent monitoring

Profile information	Export file name
Event forwarding settings file	<code>forward</code>
Log-file trap action definition file	Any name
Log-file trap startup definition file	<code>jevlog_start.conf</code>
Event log-trap action definition file	<code>ntevent.conf</code>
Local action execution definition file	<code>jbslcact.conf</code>

Note: There is no data to be exported for a host for which profile settings files are not collected (in such a case, the directories are not created).

(b) Profile information for remote monitoring

The profile information of JP1/IM - Manager is exported to a file, and cannot be edited.

The file is exported to the first-level directory (*host-name*) and the second-level directory (*a1*) under the *definition_files* directory. The log file trap action-definition file is exported to the third-level directory (*cf_log_file_trap*), and the event log trap action definition file is exported to the third-level directory (*cf_event_log_trap*). The following table describes the profile information that is exported.

Table 8–6: Names of the files for exporting profile information for remote monitoring

Profile information	Export file name
Remote-monitoring log file trap action-definition file	Any name
Remote monitoring startup definition file	<code>jevlog_start.conf</code>
Remote-monitoring event log trap action-definition file	<code>nthevent.conf</code>

(4) Remote authentication information

When remote monitoring is used, remote authentication information is exported. The name of the file to be exported is `wmi.ini` or `ssh.ini`.

(5) Business group information

When business groups are used, information about the business groups is exported to a file named `monitoring_system_data.csv`. The following table describes the business group information output to `monitoring_system_data.csv`.

Table 8–7: Exported business group information

Line	Output item	Output value
First line (header information)	Product name	<code>JP1/IM-CF</code>
	File format version	File format version For example, if the version of JP1/IM - Manager is 09-50, 095000 is output.
	Character code	Character code This depends on the setting of the <code>LANG</code> environment variable on the manager. For details, see <i>Table 2-80 Character encoding of files in Host input information file (host_input_data.csv) in Chapter 2. Definition Files of the manual JP1/Integrated Management - Manager Command and Definition File Reference.</i>
Second line (header information)	Business group name	<code>Monitoring_system_name</code>
	Assigned JP1 resource group name	<code>JP1_resource_group_name</code>
	Comment	<code>Comment</code>
	Host name	<code>Host_name_list</code>
Third and subsequent lines	Business group name	Name of the business group
	Assigned JP1 resource group name	Name of the JP1 resource group assigned to the business group
	Comment	<code>Comment</code>
	Host name	Name of the host registered in the business group (If there are multiple hosts, hosts are delimited with a comma (,) and the entire string of hosts is enclosed in double quotation marks (""))

Note: Business group information is sorted in ascending order of business group name before being output.

The following shows an example of outputting business group information:

```
JP1/IM-CF;095000;UTF-8,, ,
Monitoring_system_name,JP1_resource_group_name,Comment,Host_name_list
System1,,This is the empty system,
System2,Resource_A,This is System2,"host21,host22,host23,host24"
System3,Resource_A,This is System3,"host31,host32"
```

(6) Monitoring group information

When business groups are used, the monitoring group information of IM Configuration Management is exported to a file named `monitoring_group_data.csv`. The following table describes the monitoring group information that is output to `monitoring_group_data.csv`.

Table 8–8: Exported monitoring group information

Line	Output item	Output value
First line (header information)	Product name	JP1/IM-CF
	File format version	File format version For example, if the version of JP1/IM - Manager is 10-50, 101000 is output.
	Character code	Character code This depends on the setting of the LANG environment variable of the manager. For details, see <i>Table 2-76 Character encoding of files in Host input information file (host_input_data.csv) in Chapter 2. Definition Files of the manual JP1/Integrated Management - Manager Command and Definition File Reference.</i>
Second line (header information)	Monitoring group path	Monitoring_group_path
	Comment	Comment
	Host name	Host_name_list
Third and subsequent lines	Monitoring group path	Monitoring group path
	Comment	Comment
	Host name	Name of the host registered in the monitoring group (If there are multiple hosts, hosts are delimited with a comma (,) and the entire string of hosts is enclosed in double quotation marks (""))

Note: Monitoring group information is sorted in ascending order of monitoring group path and before being output.

The following shows an example of outputting monitoring group information:

```
JP1/IM-CF;101000;UTF-8,, ,
Monitoring_group_path,Comment,Host_name_list
/System1/Group1,This is the empty group,
/System1/Group2,This is Group2,host2
/System2/Group1,This is Group1,"host11,host12,host13,host14"
```

8.7.2 Importing management information of IM Configuration Management

If necessary, you can edit the management information of IM Configuration Management that has been output (exported) from a host, and you can input (import) the edited information onto a different host. You use the `jcimport` command for the import operation, but you cannot import collected host information.

Since importing will change the data held by IM Configuration Management, we recommend that you back up the data before executing the import operation.

This subsection explains the system configuration information that is imported by the `jcimport` command. For details about how to apply the imported management information of IM Configuration Management to a system, see [8.7.3 Applying the imported management information of IM Configuration Management to a system](#).

For details about the `jcimport` command, see `jcimport` in *Chapter 1. Commands* of the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

(1) Host information

In the case of manually-entered information, the content of the export file (`host_input_data.csv`) is imported.

The table below shows the items that are imported from the export file (`host_input_data.csv`) for manually-entered information, and the input range for each item.

Table 8–9: Host information that is imported (manually-entered information)

Item	Input range	Required/Optional	Default
Host	A character string of up to 255 bytes may be input. Permitted characters are alphanumeric characters, periods (.) and the hyphen (-), excluding control codes.	Required ^{#1}	--
IP address	Permitted characters are alphanumeric characters, periods (.), and colons (;). Control codes are not permitted.	Optional	Blank
Host name list	Host names can be input. Permitted characters are alphanumeric characters periods (.) and the hyphen (-), excluding control codes.	Optional	Blank
Comment	A character string of up to 80 bytes may be input.	Optional	Blank
Host type	You can input one of the following: <ul style="list-style-type: none"> • physical • logical • virtual • unknown 	Optional	physical
Active host	A character string of up to 255 bytes may be input. Permitted characters are alphanumeric characters periods (.) and the hyphen (-), excluding control codes.	Optional	Blank
Standby host	Host names can be input. For each host name, a character string of up to 255 bytes may be input. Permitted characters are alphanumeric characters periods (.) and the hyphen (-), excluding control codes.	Optional	Blank

Item	Input range	Required/Optional	Default
VMM host	A character string of up to 255 bytes can be input. Permitted characters are alphanumeric characters periods (.) and the hyphen (-), excluding control codes.	Optional	Blank
Virtual manager type	One of the following can be input. This item is not case sensitive. For a virtualization system management host: - vCenter - JP1/SC/CM - SCVMM - HCSM For a VMM host: - ESX#2 - Hyper-V - KVM - Virtage#3	Optional	Blank
User name	A character string of up to 255 bytes can be input. Permitted characters are alphanumeric characters other than control codes.	Optional	Blank
Password#4	A character string of up to 255 bytes can be input. Permitted characters are alphanumeric characters other than control codes.	Optional	Blank
Domain name#5	A character string of up to 255 bytes can be input. Permitted characters are alphanumeric characters other than control codes.	Optional	Blank
Communication type#6	Either http, https, or ssh can be input. This item is not case sensitive. Which communication types you can specify depends on the virtual manager type: When the virtual manager type is vCenter: https or http can be input. When the virtual manager type is HCSM: http can be input. When the virtual manager type is KVM: ssh can be input.	Optional	When the virtual manager type is vCenter: https When the virtual manager type is HCSM: http When the virtual manager type is KVM: ssh
Port number#7	A numeric value from 1 to 65535 can be entered.	Optional	When the virtual manager type is HCSM: 23015 When the virtual manager type is KVM: 22
Private key file name#8	A character string of up to 256 bytes can be input. This item is case sensitive. Permitted characters are alphanumeric characters other than control codes.	Optional	Blank
Virtualization management former host name	A character string of up to 255 bytes can be input. Permitted characters are alphanumeric characters, periods (.) and hyphens (-). Control codes are not permitted.	Optional	Blank
Remote communication type	This item can be used for remote monitoring. You can input one of the following:	Optional	disable

Item	Input range	Required/Optional	Default
	<ul style="list-style-type: none"> • disable • ssh • wmi 		
Authentication information category ^{#9}	<p>This item can be used for remote monitoring. You can input one of the following:</p> <ul style="list-style-type: none"> • common • host • Blank 	Optional	Blank

Legend:

--: There is no default value.

Note: The length (in bytes) of the character string is in UTF-8.

#1: If the required item is not specified, an error occurs. If an optional item is not specified, the default value is imported.

#2: ESX indicates VMware ESX.

#3: Virtage indicates the Hitachi Compute Blade logical partitioning feature.

#4: This item must be input when the virtual manager type is vCenter, SCVMM, or HCSM.

#5: This item must be input when the virtual manager type is SCVMM.

#6: This item must be input when the virtual manager type is vCenter, HCSM, or KVM.

#7: This item must be input when the virtual manager type is HCSM or KVM.

#8: This item must be input when the virtual manager type is KVM.

#9: When you change the host name of the host whose authentication information category is set to host, the authentication information used for remote monitoring is not inherited. In such cases, reset the remote communication settings in the IM Configuration Management window after the import is complete.

If characters that do not have code compatibility or model-dependent characters are used in the host information, these characters may become garbled when they are imported.

If any of the conditions listed below applies to the export file (`host_input_data.csv`) for manually-entered information, an error occurs and the file is not imported.

- A host name is duplicated.
- A host name is longer than 255 bytes.
- The number of hosts exceeds the number supported (1,024 if the IM database size is S or M, and 10,000 if the size is L).
- A value outside the permitted input range is specified.
- The number of input data columns is insufficient (the number of commas is insufficient).
- The host name described for the active host, standby host, or VMM host does not exist in the host information file.
- A value other than `physical` or `virtual` is specified as the host type for the active host or standby host.
- A value other than `physical` is specified as the host type for the VMM host.
- A value other than `physical`, `logical`, `virtual`, or `unknown` is specified as a host type.
- A value other than `ESX`, `Hyper-V`, `KVM`, `Virtage`, `vCenter`, `JP1/SC/CM`, `SCVMM`, `vCenter`, or `Virtage` is specified as the virtual manager type.
- The virtual manager type is specified as a host with type `logical` or `unknown`.
- The host name described for the virtualization management former source host name does not exist in the host information file.

- A value other than `physical` or `virtual` is specified as the host type described for the virtualization management former source host name.
- A value other than `SCVMM` is specified as the virtual manager type of a host for which a domain name is set.
- A value other than `vCenter`, `HCSM`, or `KVM` is specified as the virtual manager type of a host for which a communication type is specified.
- A character string other than `https` or `http` is specified as the communication type of a host whose virtual manager type is `vCenter`.
- A character string other than `http` is specified as the communication type of a host whose virtual manager type is `HCSM`.
- A character string other than `ssh` is specified as the communication type of a host whose virtual manager type is `KVM`.
- The virtual system configuration information does not correspond to the information in the following table.

Host type	Virtual manager type	Configuration information corresponding to virtual manager type	Required/Optional	Remarks
Physical host	--	N	--	--
	vCenter	Virtual management former host name	Optional	SCVMM is specified as the virtual management former host name.
		User name	Optional	
		Password	Optional	
		Communication type	Optional	
	JP1/SC/CM	N	--	--
	SCVMM	User name	Optional	--
		Password	Optional	
		Domain name	Optional	
	HCSM	User name	Optional	--
		Password	Optional	
		Port number	Optional	
		Communication type	Optional	
	ESX	Virtual management former host name	Optional	vCenter is specified as the virtual management former host name.
	Hyper-V	Virtual management former host name	Optional	SCVMM is specified as the virtual management former host name.
KVM	User name	Optional	--	
	Port number	Optional		
	Private key file name	Required		
	Communication type	Optional		
Virtage	Virtual management former host name	Optional	JP1/SC/CM or HCSM is specified as	

Host type	Virtual manager type	Configuration information corresponding to virtual manager type	Required/Optional	Remarks
				the virtual management former host name.
Virtual host	--	VMM host name	Required	A value other than vCenter, JP1/SC/CM, SCVMM, or HCSM is specified as the VMM host name.
	vCenter	VMM host name	Required	A value other than vCenter, JP1/SC/CM, SCVMM, or HCSM is specified as the VMM host name. SCVMM is specified as the virtual management former host name.
		Virtual management former host name	Optional	
		User name	Optional	
		Password	Optional	
		Communication type	Optional	
	JP1/SC/CM	VMM host name	Required	A value other than vCenter, JP1/SC/CM, SCVMM, or HCSM is specified as the VMM host name.
	SCVMM	VMM host name	Required	A value other than vCenter, JP1/SC/CM, SCVMM, or HCSM is specified as the VMM host name.
		User name	Optional	
		Password	Optional	
		Domain name	Optional	
	HCSM	VMM host name	Required	A value other than vCenter, JP1/SC/CM, SCVMM, or HCSM is specified as the VMM host name.
		User name	Optional	
		Password	Optional	
		Port number	Optional	
		Communication type	Optional	
	KVM	VMM host name	Required	A value other than vCenter, JP1/SC/CM, SCVMM, or HCSM is specified as the VMM host name.
		User name	Optional	
		Port number	Optional	
		Private key file name	Optional	
Communication type		Optional		
Logical host	--	N	--	--
Unknown	--	N	--	--

Legend:

--: Not applicable

N: Cannot be input (Input of the item causes an error)

- A value other than `disable`, `ssh`, or `wmi` is specified as the remote communication type.
- A value other than `common`, `host`, or a blank is specified as the authentication information category.
- When `ssh` or `wmi` is specified as the remote communication type, a blank is specified for the authentication information category.

If a host has the same host name as the import destination host, that host is not registered in IM Configuration Management as a managed host after the export file (`host_input_data.csv`) for manually-entered information has been imported.

(2) System hierarchy information

The content of the export file for the system hierarchy information is imported. The export file differs according to the system monitoring method:

- Agent monitoring
- Remote monitoring

(a) Configuration information for agent monitoring

The name of the file to which the configuration information for agent monitoring is exported is `system_tree_information.txt`.

If any of the conditions listed below applies to the content of the export file for the configuration information for agent monitoring, an error occurs and the file is not imported.

- The same host is described on multiple lines (the managed host has multiple higher hosts).
- The host configuration is looped.
- The host name specified for the managing host is not enclosed in square brackets [] (] is missing).
- No host name is specified for the managing host.
- More than 10,000 hosts are defined.
- The local host is defined as the managed host.

After the export file (`host_input_data.csv`) for host information (manually-entered information) or the export file for the configuration information for agent monitoring is edited, the host name specified in the export file for the configuration information for agent monitoring might not be specified in the export file for the host information (manually-entered information) in some cases. In those cases, after the export file for the configuration information for agent monitoring is imported, an import warning message is displayed and the undefined host is automatically registered in IM Configuration Management as a managed host.

When you are trying to import the configuration information for agent monitoring, if the export file for the configuration information for agent monitoring is not found in the specified directory, an error message is displayed and the import operation is halted.

(b) Configuration information for remote monitoring

The name of the file to which the configuration information for remote monitoring is exported is `system_remote_tree_information.txt`.

If any of the conditions listed below applies to the content of the export file for the configuration information for remote monitoring, an error occurs and the file is not imported.

- The same host is specified on multiple lines. (The managed host has multiple higher hosts.)
- The host configuration is looped.
- The host name specified for the managing host is not enclosed in square brackets [] (] is missing).
- No host name is specified for the managing host.
- More than 1,024 hosts are defined.
- The local host is defined as the managed host.

After the export file (`host_input_data.csv`) for host information (manually-entered information) or the export file for the configuration information for remote monitoring is edited, the host name specified in the export file for the configuration information for remote monitoring might not be specified in the export file for the host information (manually-entered information) in some cases. In those cases, after the export file for the configuration information for remote monitoring is imported, an import warning message is displayed and the undefined host is automatically registered in IM Configuration Management as a managed host.

When you are trying to import the configuration information for remote monitoring, if the export file for the configuration information for remote monitoring is not found in the specified directory, an error message is displayed and the import operation is halted.

(3) Profile information

The content of the export files for the profile information is imported. The file that is imported differs according to the system monitoring method:

- Agent monitoring
- Remote monitoring

Table 8–10: Export file for agent monitoring profile information to be imported

Profile information	Export file name
Event Forwarding Settings File	<code>forward</code>
Log-file trap action definition file	Any name
Log-file trap startup definition file	<code>jevlog_start.conf</code>
Event Log-Trap Action Definition File	<code>ntevent.conf</code>
Local Action Execution Definition File	<code>jbslcact.conf</code>

When agent monitoring profile information is imported, the destination is determined using the directory name under `definition_files` directory. The directory name on the hierarchy one step below the `definition_files` directory is read as a host name, and the directory name on the hierarchy two steps below the `definition_files` directory is read as a product name. The file stored in each directory is registered on the applicable host as settings information. Consequently, if you change the host name in the export file (`host_input_data.csv`) for host information (manually-entered information), you must also change the directory name. If you do not change it, the profile information cannot be imported.

The profile information file is loaded as a character code described in `encode` of the export file (`data_information.txt`) for the export data information. For this character code, the environment variable `LANG` of the OS of the server that executed the export operation is set. When you import profile information, make sure that the character code described in the export file (`data_information.txt`) matches the character code of the profile information file.

If characters that do not have code compatibility or model-dependent characters are used in the host information, these characters may become garbled when they are imported.

If more than 10,000 hosts are defined, an error occurs and no file is imported.

If the export file for the profile (configuration file) contains an unsupported product or unsupported profile, these are ignored and processing continues.

(a) Remote monitoring profile information

When remote monitoring is used, the content of the export file for the remote monitoring profile information is imported. The remote monitoring profile information cannot be edited.

The following table describes the export files for remote monitoring profile information to be imported.

Table 8–11: Remote monitoring profile information to be imported and the export file names

Profile information	Export file name
Remote-monitoring log file trap action-definition file	Any name
Remote monitoring startup definition file	jevlog_start.conf
Remote-monitoring event log trap action-definition file	nthevent.conf

When remote monitoring profile information is imported, the destination is determined using the directory name under `definition_files` directory.

The directory name on the hierarchy one step below the `definition_files` directory is read as a host name, and the directory name on the hierarchy two steps below the `definition_files` directory is read as a product name. The file stored in each directory is registered on the applicable host as settings information. Consequently, if you change the host name in the export file (`host_input_data.csv`) for host information (manually-entered information), you must also change the directory name. If you do not change it, the profile information cannot be imported.

The profile information file is loaded in the encoding described in `encode` of the export file (`data_information.txt`) for the export data information. For this encoding, the value of the `LANG` environment variable of the OS of the server that executed the export operation is set. When you import profile information, make sure that the character encoding described in the export file (`data_information.txt`) matches the character encoding of the profile information file. If characters without code compatibility or model-dependent characters are used in the host information, these characters might be unreadable when they are imported.

(4) Remote authentication information

When remote monitoring is used, the content of the export file for the remote authentication information is imported. The name of the file to be imported is `wmi.ini` or `ssh.ini`.

When you use remote monitoring, after the remote authentication information is imported, invoke the System Common Settings window from the IM Configuration Management - View, check the settings, and then click the **OK** button.

(5) Business group information

When business groups are used, the content of the export file for the monitoring group information of IM Configuration Management is imported. If any of the conditions listed below applies to the content of the export file (`monitoring_system_data.csv`) for the business group information, an error occurs and the file is not imported.

- Business groups that have the same name exist at the same level.

- A value outside the permitted input range is specified.
- The number of input data columns is insufficient (the number of commas does not match).

Save the export file for business group information (`monitoring_system_data.csv`) with the character encoding specified in line 1 (header information). If you save this file in UTF-8, make sure that no BOM (byte order mark) is included.

The following table describes items that are imported and the input range of each item.

Table 8–12: Imported items (business group information)

Item	Input range	Required/Optional	Default
Business group name	A maximum of 255 bytes of characters can be entered in UTF-8. All characters are permitted except control characters, forward slashes (/), and single-byte commas (,). The first and the last characters cannot be a single-byte space. The characters are case sensitive. To specify a double quotation mark ("), specify two double quotation marks in succession and then enclose the entire string in double quotation marks. Do not use environment-dependent characters for business group names. Such characters can cause character corruption in the definition.	Required	--
Assigned JP1 resource group name	A character string of up to 64 bytes can be input. Permitted characters are ASCII codes other than symbols (" / [] ; : , = + ? < >), a tab, or a space.	Optional	Blank
Comment	A maximum of 80 bytes of characters can be entered in UTF-8. All characters are permitted except control characters. To specify a double quotation mark ("), specify two double quotation marks in succession and then enclose the entire string in double quotation marks. If you specify a comma (,), enclose the	Optional	Blank

Item	Input range	Required/Optional	Default
	entire string in double quotation marks.		
Host name	A maximum of 2,500 host names can be specified delimited by a comma (,). When you specify multiple host names, enclose the entire string in double quotation marks ("). For an input range consisting of a single host name, see <i>Table 8-9 Host information that is imported (manually-entered information)</i> .	Optional	Blank

Legend:

--: There is no default value.

(6) Monitoring group information

When business groups are used, the content of the export file for the business group information is imported. If any of the conditions listed below applies to the content of the export file (`monitoring_group_data.csv`) for the monitoring group information, an error occurs and the file is not imported.

- Monitoring groups or hosts that have the same name exist at the same level.
- A value outside the permitted input range is specified.
- The number of input data columns is insufficient (the number of commas does not match).
- A higher-level monitoring group is not defined on a line whose line number is younger than that of lower-level monitoring groups.

Save the export file for business group information (`monitoring_group_data.csv`) with the character encoding specified in line 1 (header information). If you save this file in UTF-8, make sure that no BOM (byte order mark) is included.

The following table describes items that are imported and the input range of each item.

Table 8–13: Imported items (monitoring group information)

Item	Input range	Required/Optional	Default
Monitoring group path	A maximum of 2,048 bytes of characters can be entered in UTF-8. All characters are permitted except control characters. The characters are case sensitive. To specify a double quotation mark ("), specify two double quotation marks in succession and then enclose the entire string	Required	--

Item	Input range	Required/Optional	Default
	in double quotation marks. Do not use environment-dependent characters for monitoring group names. Such characters can cause character corruption in the definition.		
Comment	A maximum of 80 bytes of characters can be entered in UTF-8. All characters are permitted except control characters. To specify a double quotation mark ("), specify two double quotation marks in succession and then enclose the entire string in double quotation marks. If you specify a comma (,), enclose the entire string in double quotation marks.	Optional	Blank
Host name	A maximum of 2,500 host names can be specified delimited by a comma (,). If you specify multiple host names, enclose the entire string in double quotation marks ("). For an input range consisting of a single host name, see <i>Table 8-9 Host information that is imported (manually-entered information)</i> .	Optional	Blank

Legend:

--: There is no default value.

8.7.3 Applying the imported management information of IM Configuration Management to a system

After you have imported the management information of IM Configuration Management by executing the `jcfimport` command, perform the procedures described below to apply the imported management information.

(1) Collecting host information

To collect host information:

1. In the IM Configuration Management window, click the **Host List** or **IM Configuration** tab.
The **Host List** page or **IM Configuration** page opens.

2. From the tree pane, select a host.

If the selected host has lower-order hosts, you can also select a host from the **Lower Host Information** list that is displayed when you click the **Lower Host Information** button. In this case, you can select multiple hosts at the same time.

3. Use either of the following methods to collect host information:

- From the menu bar, choose **Operation** and then **Collect Host Information**.
- From the popup menu that opens when you right-click the mouse, choose **Collect Host Information**.

When a message confirming collection of information from the selected host is issued, click **Yes**. Information is collected from the selected host.

(2) Applying the system hierarchy information

To apply the system hierarchy information:

(a) In an agent configuration

When the system hierarchy information is not applied, the tree in the **IM Configuration** tab in the IM Configuration Management window is displayed in gray.

Perform the following procedure to apply the system hierarchy information.

1. From the menu bar in the IM Configuration Management window, choose **Edit** and then **Edit Agent Configuration**. The Edit Agent Configuration window opens.
2. In the Edit IM Configuration window, check the **Acquire update right** check box. You can now edit the JP1/IM system configuration.
3. Select the highest node in the tree (integrated manager) and use either of the following methods to change the integrated manager:
 - From the menu bar, choose **Operation** and then **Exchange Hosts**.
 - From the popup menu that opens when you right-click the mouse, choose **Exchange Hosts**.

This step is not necessary if the exporting host is the same as the importing host.

4. From the menu bar in the Edit Agent Configuration window, choose **Operation** and then **Apply Agent Configuration**.

The system hierarchy information is applied to the actual system.

5. Clear the **Acquire update right** check box.

If you are acquiring the current system hierarchy, this operation is not necessary. From the menu bar in the IM Configuration Management window, choose **Edit** and then **Collect IM Configuration** to acquire the current system hierarchy.

(b) In a remote configuration

Perform the following procedure to apply the system hierarchy information.

1. From the menu bar in the IM Configuration Management window, choose **Edit** and then **Edit Remote Monitoring Configuration**.

The Edit Remote Monitoring Configuration window opens.

2. In the Edit IM Configuration window, check the **Acquire update right** check box.

You can now edit the JP1/IM system configuration.

3. Select the highest node in the tree (integrated manager) and use either of the following methods to change the integrated manager:

- From the menu bar, choose **Operation** and then **Exchange Hosts**.
- From the popup menu that opens when you right-click the mouse, choose **Exchange Hosts**.

This step is not necessary if the exporting host is the same as the importing host.

4. From the menu bar in the Edit Remote Monitoring Configuration window, choose **Operation** and then **Apply Remote Monitoring Configuration**.

The system hierarchy information is applied to the actual system.

5. Clear the **Acquire update right** check box.

If you are acquiring the current system hierarchy, this operation is not necessary. From the menu bar in the IM Configuration Management window, choose **Edit** and then **Collect IM Configuration** to acquire the current system hierarchy.

(3) Applying the profile information

Merely importing the management information of IM Configuration Management does not apply the configuration file to the system. Use either of the following methods to apply the configuration file:

- Batch-apply the configuration file
- Apply the configuration file to hosts individually

For details about how to apply the configuration file, see *3.5.1(6) Applying edited information in configuration files* in the *JP1/Integrated Management - Manager Configuration Guide*.

If you are acquiring a system's current profile information, there is no need to apply the profile information. You can simply batch-collect profiles. For details about how to collect profile lists, see *3.5.1(1) Collecting profile lists* in the *JP1/Integrated Management - Manager Configuration Guide*.

9

Linking with BJEX or JP1/AS

JP1/IM can monitor the response-request messages issued by BJEX or JP1/AS as JP1 events, allowing operators to respond to these messages from JP1/IM - View. This chapter describes the functionality of JP1/IM that allows this to take place, and explains the process of linking JP1/IM with BJEX or JP1/AS. It also describes the command options you can use when linking with BJEX or JP1/AS.

9.1 Overview of BJEX and JP1/AS linkage

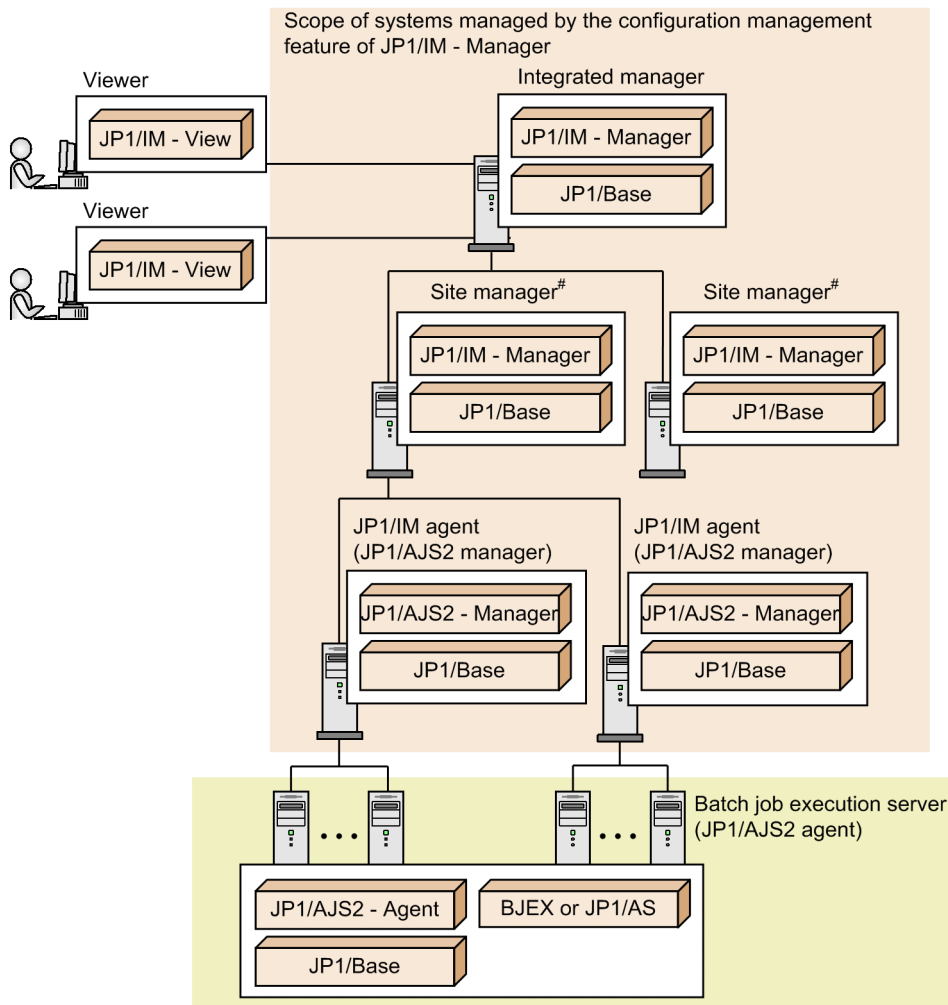
BJEX is a product that realizes mainframe-like job management in an open system. JP1/AS is a system used to create and execute shell scripts that serve as batch jobs. A job management system that links with JP1/AJS to control batch jobs (jobs that execute batch processing) is called a *batch job execution system*. By deploying JP1/IM in a batch job execution system, you can monitor the execution status and results of batch jobs in JP1/IM - View based on the JP1 events issued by BJEX or JP1/AS.

The messages output by BJEX and JP1/AS include response-request messages that require the operator to respond to them while a batch job is executing. BJEX and JP1/AS issue response-request messages as JP1 events. JP1/IM allows you to monitor these JP1 events and respond to the messages as needed. The JP1 events that correspond to response-request messages are called *response-waiting events*. The functionality of JP1/IM that manages and responds to response-waiting events is called the *response-waiting event management function*. JP1/IM uses this function when linking with BJEX or JP1/AS. It is disabled by default. Enable the response-waiting event management function when linking with BJEX or JP1/AS.

9.1.1 System configuration when linking JP1/IM with a batch job execution system

This section describes the configuration of a system in which JP1/IM links with a batch job execution system.

Figure 9–1: Configuration example of batch job execution system with JP1/IM



#: Can be a site manager or relay manager.

In the example in the figure, JP1/IM is configured as a hierarchical system that incorporates site managers. The JP1/IM system in the figure monitors a batch job execution system.

The role and prerequisite products of each server are described below. For a list of supported operating systems, see the documentation for the product concerned. For details about version requirements, see the JP1/IM - Manager release notes.

Viewer

Connects to JP1/IM - Manager from JP1/IM - View to monitor and work with events. The prerequisite products for a viewer are:

- JP1/IM - View#
#: In the Web-based JP1/IM - View, you can monitor response-waiting events in the same manner as ordinary JP1 events. However, only a limited range of functions are available. For details, see [9.4 Working with response-waiting events](#).

Integrated manager

A server that manages systems from an integrated perspective. The prerequisite products for an integrated manager are:

- JP1/IM - Manager
- JP1/Base

Site manager or relay manager

A server subordinate to an integrated manager. You can use site managers and relay managers when you want to manage large-scale systems in a hierarchy. The prerequisite products for a site manager or relay manager are:

- JP1/IM - Manager
- JP1/Base

JP1/IM agent (JP1/AJS manager)

A server monitored by JP1/IM. In the example in the figure, JP1/IM agents also function as JP1/AJS managers. The prerequisite products for a JP1/IM agent are:

- JP1/AJS - Manager
- JP1/Base

Batch job execution server (JP1/AJS agent)

A server that executes processing, such as batch jobs, in response to requests from JP1/AJS - Manager. A batch job execution server can link with JP1/IM even if it is not part of the system whose configuration is being managed by JP1/IM. JP1/IM - Manager links with BJEX or JP1/AS on the batch job execution server in a 1:*n* ratio (where *n* is an integer of 1 or higher). For details about how to configure linkage with BJEX or JP1/AS, see [9.3 Configuring JP1/IM to link with BJEX and JP1/AS](#).

The prerequisite products for a batch job execution server are:

- JP1/AJS - Agent
- JP1/Base
- BJEX or JP1/AS

9.2 JP1/IM functionality for BJEX and JP1/AS linkage

This section describes the JP1/IM functionality that is used when linking with BJEX or JP1/AS.

9.2.1 Handling response-waiting events in JP1/IM

The following response-waiting events are issued when a batch job enters a status where it is waiting for a response from an operator:

- In BJEX
Event ID: 00005C21
- In JP1/AS
Event ID: 00007121

To monitor response-waiting events in JP1/IM, you need to configure BJEX or JP1/AS to issue the response-waiting event directly to the JP1/IM - Manager host (the integrated manager). You also need to enable the response-waiting event management function in JP1/IM - Manager.

For details about the response-waiting event (event ID: 00007121), see the *JP1/Advanced Shell Description, User's Guide, Reference, and Operator's Guide*.

(1) Paths through which response-waiting events are issued

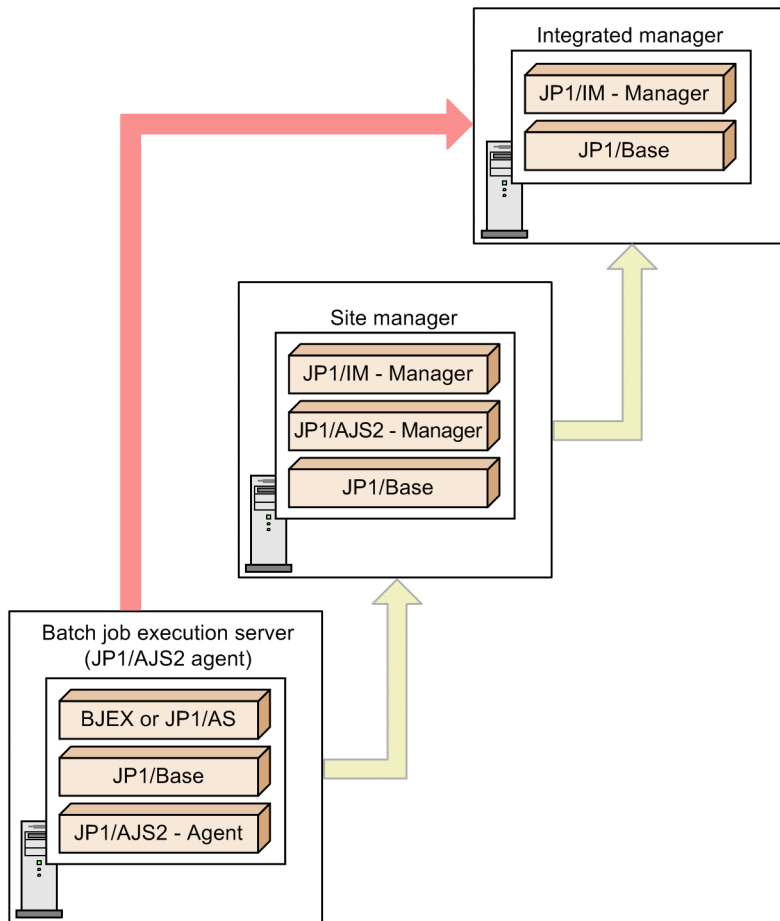
BJEX and JP1/AS issue response-waiting events directly to the integrated manager, not by the usual forwarding paths provided by JP1/Base. To have BJEX issue all response-waiting events directly to the integrated manager, specify the JP1/IM - Manager host name in the `JP1IM_MANAGER_HOST` parameter of the BJEX configuration file (`bjex.conf`). When JP1/IM is linked with JP1/AS, specify the JP1/IM - Manager host name in the `HOSTNAME_JP1IM_MANAGER` parameter in the JP1/AS environment file.

Order in which response-waiting events from BJEX or JP1/AS and JP1 events from other products arrive on the same host



Products like JP1/AJS and JP1/Base that reside on the BJEX or JP1/AS host use the paths provided by JP1/Base to forward JP1 events to the integrated manager via site managers. For this reason, response-waiting events issued by BJEX or JP1/AS, and JP1 events issued by other products, might not arrive at the integrated manager in the order in which they were issued. You can identify which message belongs to which job by viewing the job ID in the message of the response-waiting event.

The following figure shows the paths through which response-waiting events are forwarded from BJEX and JP1/AS hosts:

Figure 9–2: Forwarding paths of response-waiting events issued by BJEX or JP1/AS



Legend:

-  : Path through which BJEX or JP1/AS issues a response-waiting event
-  : Path through which JP1/AJS2 and JP1/Base issue JP1 events (using the forwarding path of JP1/Base)

Important

When BJEX or JP1/AS forwards a waiting-response event to an instance of JP1/IM - Manager that is not on the specified host, it is not handled as a response-waiting event at the destination. In this case, you will be unable to respond to the message at the destination host.

(2) Response-waiting event management function

The response-waiting event management function lets you respond to response-waiting events from JP1/IM - View. You can enable this function in the configuration of the instance of JP1/IM - Manager that links with BJEX or JP1/AS.

After you enable the response-waiting event management function, you must enable the setting that allows individual users to respond to and work with response-waiting events. You can do so in the Preferences window of JP1/IM - View.

For details about how to enable this setting, see [9.3 Configuring JP1/IM to link with BJEX and JP1/AS](#).

Note that you can still monitor waiting-response events as ordinary JP1 events if you do not enable the response-waiting event management function and the setting that allows users to respond to and work with these events.

Important

Response-waiting events are handled as such if they are received by JP1/IM - Manager after the response-waiting event management function is enabled. Response-waiting events received before the function is enabled are handled as ordinary JP1 events.

9.2.2 Monitoring response-waiting events

Because JP1/IM handles response-waiting events in the same manner as ordinary JP1 events, you can use automated action notification and other JP1/IM features with these events.

The following describes how each of the following features works with waiting-response events. Features that are not described here work the same way as with ordinary JP1 events.

- Monitoring in the Event Console window
- JP1 event filtering
- Monitoring repeated events
- Searching for events
- Outputting information from JP1/IM - View in CSV format

(1) Monitoring in the Event Console window

Waiting-response events appear in the lists of events on the Monitor Events page, Severe Events page, and Search Events page, like ordinary JP1 events. The Response-Waiting Events page only shows response-waiting events. This page is displayed only when the response-waiting event management function and the setting that allows users to respond to and work with response-waiting events is enabled. Note that the Response-Waiting Events page does not appear in the Web-based JP1/IM - View.

From the list of events in the Event Console window, you can perform the following operations and configuration with respect to response-waiting events in the same manner as ordinary JP1 events:

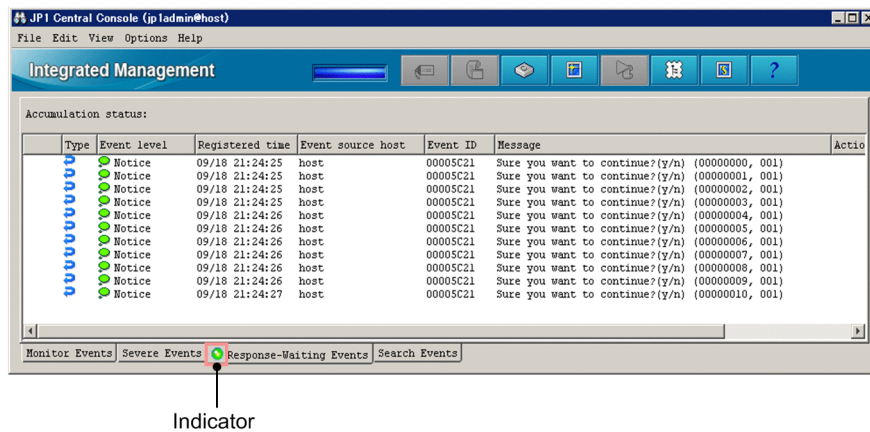
- Display detailed information about a response-waiting event
- Open the monitors of linked products
- Display execution results of automated actions
- Change display items for JP1 events
- Set the background color for JP1 events
- Set the response status for response-waiting events
- Specify the event display period

For details about these features, see *3.1 Centralized monitoring using JP1 events* in the *JP1/Integrated Management - Manager Overview and System Design Guide*.

(a) Monitoring on the Response-Waiting Events page

The Response-Waiting Events page displays a list of response-waiting events for which a response is not yet provided. This page is shown below.

Figure 9–3: Response-Waiting Events page



An indicator on the tab of the Response-Waiting Events page lets the operator know whether there are events that require a response. When there are response-waiting events listed on the Response-Waiting Events page, the indicator on the tab is lit green.


In addition to the event database, response-waiting events are stored in a *file for accumulated response-waiting events* in a process called *response-waiting event accumulation*. The Response-Waiting Event page displays information about the events recorded in the file for accumulated response-waiting events.

Response-waiting events are removed from the Response-Waiting Events page when:

- An operator responds to the response-waiting event
- The response-waiting event is released from the hold-and-accumulate state
- The response-waiting event is canceled

For details about what causes response-waiting events to be released from the hold-and-accumulate state, see [9.2.3 Accumulation of response-waiting events](#).

The indicator on the tab becomes unlit after all response-waiting events have disappeared from the Response-Waiting Events page.

To allow the operator to distinguish response-waiting events, the  icon appears in the **Type** column for these events on each page of the Event Console window.

Note that the Response-Waiting Events page does not display the background colors that have been assigned to JP1 events.

(2) Filtering response-waiting events

You can use the following filters to filter response-waiting events:

- Event receiver filter
- Severe events filter
- View filter

When you enable the response-waiting event management function, items that allow the operator to select whether to display response-waiting events appear in the condition definition windows for the event receiver filter and severe events filter. To filter response-waiting events using the view filter, the response-waiting event management function and the setting that allows users to respond to and work with response-waiting events must be enabled.

For details about the windows in which filter conditions are defined, see [2.44.8 Filter condition definition windows](#) in the manual *JP1/Integrated Management - Manager GUI Reference*.

Note that event acquisition filters do not allow you to specify conditions that specifically identify response-waiting events. Configure event acquisition filters so that they filter events at the product level for products that issue response-waiting events.

(3) Consolidated display of response-waiting events

If a network problem or some other issue causes the same batch job to issue the same response-waiting event several times in succession, the events are displayed as a single *consolidated event*. Events are only consolidated on the Monitor Events page and Severe Events page.

If identical response-waiting events are issued as a result of an error of some kind, the operator does not need to respond to each and every event. If you respond to one of these waiting-response events, you do not need to respond to the others. However, response-waiting events that no longer require a response remain on the Response-Waiting Events page until they are released from the hold-and-accumulate state. For details about how to release these events, see [9.2.3 Accumulation of response-waiting events](#).

(4) Searching for response-waiting events

When searching for JP1 events, you can specify a response-waiting event as a search condition. Conditions that apply to response-waiting events only appear in the Event Search Conditions window if you enable the response-waiting event management function and the setting that allows users to respond to and work with response-waiting events.

For details about the Event Search Conditions window, see [2.44.7 Event Search Conditions window](#) in the manual *JP1/Integrated Management - Manager GUI Reference*.

You can only respond to response-waiting events from the search results if you search the logged-in JP1/IM manager host for response-waiting events. If you do not specify the logged-in manager host, you cannot respond to the response-waiting events that appear in the search results.

(5) Outputting information from JP1/IM - View in CSV format

You can output information about response-waiting events displayed in the list of events in CSV format. You can output CSV information in two ways:

- Save the information in the list of events to a file
You can save a snapshot of the event information displayed in JP1/IM - View to a CSV file. A snapshot means information extracted at a specific time.
- Copy JP1 event information, action execution results, or other information to the clipboard
If the feature that allows you to copy information to the clipboard is enabled, you can copy selected parts of response-waiting event information, action execution results, and other information to the clipboard in CSV format. This feature is enabled by default.

The following table shows the events lists whose response-waiting events can be saved to a CSV file or copied to the clipboard in CSV format.

Table 9–1: Events lists that can be output to a CSV file or copied to the clipboard

Operation	Monitor Events page	Severe Events page	Related Events window	Response-Waiting Events page	Search Events page
CSV output	Y	Y	N	Y	Y

Operation	Monitor Events page	Severe Events page	Related Events window	Response-Waiting Events page	Search Events page
Copy to clipboard	Y	Y	Y	Y	Y

Legend:

Y: Can be saved or copied.

N: Cannot be saved or copied.

When you save information about response-waiting events to a CSV file or copy it to the clipboard, the icon in the **Type** column is replaced with the text `Response-waiting event` in the CSV data. If icons indicating a repeated event and a response-waiting event are output for an event, the icons are replaced with the text `Repeated event, Response-waiting event` in the CSV data. When you output the information on the Response-Waiting Events page in CSV format, **Response-Waiting Events** appears as the name of the source window in the header information.

For details about how to enable the copy to clipboard feature, see *1.19.2 Customizing operation of JP1/IM - View (Central Console viewer and Central Scope viewer) (for Windows)* in the *JP1/Integrated Management - Manager Configuration Guide*.

9.2.3 Accumulation of response-waiting events

When you enable the response-waiting event management function, response-waiting events that arrive in the event database on the manager host are recorded in a *file for accumulated response-waiting events* in addition to the event database. A maximum of 2,000 response-waiting events are stored in this file. This process is called *accumulation of response-waiting events*.

The Response-Waiting Events page displays information about the response-waiting events in the file for accumulated response-waiting events.

(1) When response-waiting events are released from the hold-and-accumulate state

Response-waiting events are deleted from the file for accumulated response-waiting events and released from the hold-and-accumulate state when:

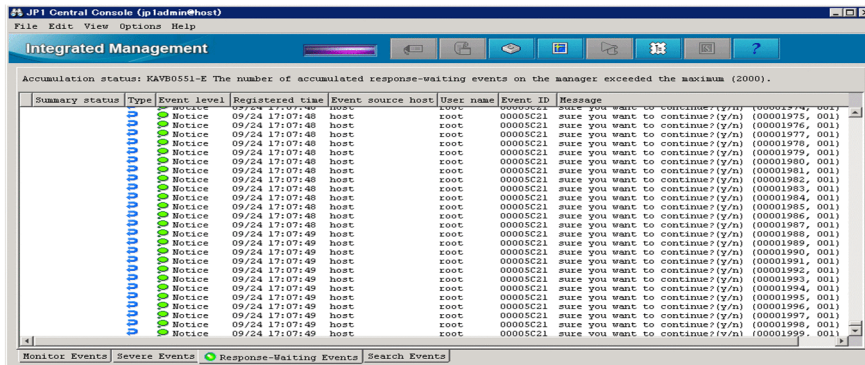
- An operator successfully responds to a response-waiting event
- The response-waiting event is canceled in BJEX or JP1/AS
- An operator manually releases the event from the hold-and-accumulate state
- There are more than 2,000 response-waiting events
In this case, accumulated response-waiting events are released in order from the oldest.
- You disable the response-waiting event management function and restart JP1/IM - Manager

A response-waiting event that is released from the hold-and-accumulate state disappears from the Response-Waiting Events page when you next refresh the list of events in JP1/IM - View. Note that such events, while no longer appearing in the Response-Waiting Events page, still appear in search results in the Search Events page as long as they remain in the event database.

(2) Notification when the number of response-waiting events exceeds 2,000

JP1/IM - Manager monitors the number of response-waiting events in the hold-and-accumulate state, and notifies the operator when the number exceeds 2,000 by issuing a JP1 event (event ID: 00003F41). The message KAVB0551-E also appears on the Response-Waiting Events page.

Figure 9–4: Response-Waiting Events page when the number of response-waiting events exceeds 2,000



The JP1 event reporting that the number of response-waiting events in the hold-and-accumulate state has exceeded the maximum is issued only once. The message KAVB0551-E remains on the Response-Waiting Events page. When the number of events in the hold-and-accumulate state exceeds the limit, take action as described in the message to resume monitoring events in the hold-and-accumulate state in the usual way. Then the message KAVB0551-E disappears from the Response-Waiting Events page. The JP1 event is issued again when the number of events next exceeds 2,000.

For details about how to resume monitoring of events in the hold-and-accumulate state, see [9.4.4 Resuming monitoring of events in the hold-and-accumulate state](#).

Responding to response-waiting events that have been released from the hold-and-accumulate state

You can respond to a response-waiting event that was removed from the Response Waiting Events page after exceeding the maximum number of events by searching for the event from the Search Events page. You can identify an event that was released from the hold-and-accumulate state by viewing the KAVB1801-E message in the integrated trace log on the manager host.

If the response-waiting event was also deleted from the event database, you can respond to the event by executing the response command (`bjexchmsg` or `adshchmsg`) on the host that issued the event. For details about how to respond using the response command (`adshchmsg`) of JP1/AS, see *JP1/Advanced Shell Description, User's Guide, Reference, and Operator's Guide*.

9.2.4 Responding to response-waiting events

You can respond to response-waiting events from JP1/IM - View. For example, a message might ask the operator if he or she wants to continue batch processing, to which the operator can respond `y`es in text format. You can enter responses in the Enter Response window displayed from a response-waiting event.

You can display the Enter Response window by clicking a response-waiting event in the list of events in the following pages:

- Response-Waiting Events page
- Search Events page

You can only respond to events from this page if the events in the search results are found on the logged-in manager host.

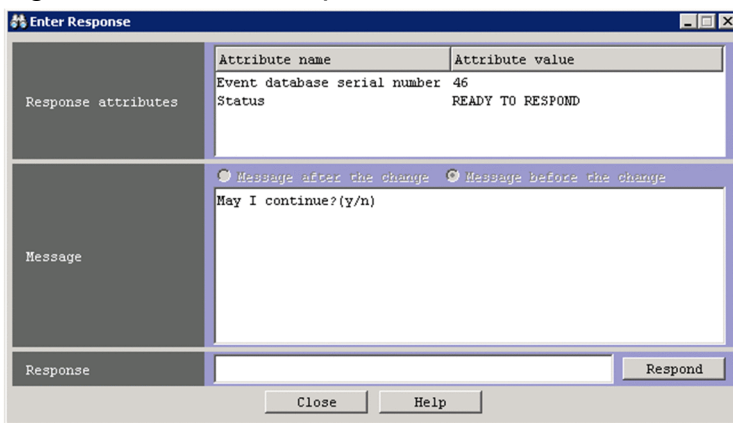
- Related Events window

You can respond to events in this window if the window was displayed from the Response-Waiting Events page. If you displayed the Related Events window from the Search Events page, you can only respond if the events in the search results are on the logged-in manager host.

(1) Framework in which responses are made to response-waiting events

You can only respond to response-waiting events if the process that issued the event still exists and is in a status that allows it to accept the response. You can view the status of the source process as the value of the **Status** attribute in the **Response attributes** area of the Enter Response window. JP1/IM - Manager checks the status of the source process when you open the Enter Response window. If a communication error prevents it from contacting the process and identifying its status, the message KAVB0555-E appears and the Enter Response window does not open.

Figure 9–5: Enter Response window



The following table lists the statuses that appear as the value of the **Status** attribute in the **Response attributes** area:

Table 9–2: Statuses of source processes for response-waiting events

Source process status	Description	Can response be entered
READY TO RESPOND	The job that issued the event is waiting for a response.	Y
NO LONGER MANAGED BY BJEX or NO LONGER MANAGED BY JP1/AS	One of the following applies: <ul style="list-style-type: none"> • The job that issued the event was canceled by JP1/AJS • The job that issued the event was terminated by a KILL command • When you displayed or refreshed the Enter Response window for an event for which a response had been issued, BJEX was no longer monitoring the status of the event 	N
RESPONDED SUCCESSFULLY	You have successfully responded to the response-waiting event in the Enter Response window. This status appears only in the Enter Response window when you have just entered a response.	N
ALREADY RESPONDED	An operator has already responded to the event. This status appears when you display or refresh an Enter Response window for an event for which a response has already been entered.	N

Legend:

Y: A response can be entered.

N: A response cannot be entered.

You can enter a response if the status of the source process is `READY TO RESPOND`. You cannot respond to response-waiting events in any other status, because the event has either already been responded to or the source process no longer exists.

When you respond to a response-waiting event, the response you entered is sent to the process that issued the event. If the response reaches the source process and is successful, the status of the response-waiting event changes to *Processed*. The response-waiting event is then released from the hold-and-accumulate state and disappears from the Response-Waiting Events page.

A timeout occurs if JP1/IM - Manager has not successfully communicated with the source process after 60 seconds when attempting to check its status or provide a response. You can change the timeout time. Consider extending the timeout time if you frequently encounter an error message (KAVB0554-E or KAVB0555-E) due to heavy loads on the source server or network congestion. For details about how to set the timeout time, see [9.3.4\(1\) Setting the timeout time for connections](#).

(2) Conditions for responding to response-waiting events

You can respond to response-waiting events under the following conditions:

- The operating permission of the responding JP1 user is `JP1_Console_Operator` or higher.
- You have not yet responded to the event.
You can only respond once to a response-waiting event, even if you acquire the event again by changing the event acquisition start location of the event acquisition filter.
- The response-waiting event was received after you enabled the response-waiting event management function.
You cannot respond to response-waiting events received while the response-waiting event management function is disabled.
- When searching for events, the logged-in manager host is specified as the search target.

Note that you cannot respond to response-waiting events from the Web-based JP1/IM - View.

(3) Using the response command of BJEX or JP1/AS

If a communication error between the source process and JP1/IM - Manager prevents you from responding to an event from JP1/IM - View, you can use the response command (`bjexchmsg` or `adshchmsg`) provided by the source process on the source host. You can also use this approach to respond to events that were released from the hold-and-accumulate state and removed from the event database. For details about how to respond using the response command (`adshchmsg`) of JP1/AS, see *JP1/Advanced Shell Description, User's Guide, Reference, and Operator's Guide*.

9.2.5 Canceling response-waiting events

In some circumstances, such as after canceling a BJEX or JP1/AS job from JP1/AJS or deleting a job in BJEX or JP1/AS, a response-waiting event might remain in the system despite no longer requiring a response. In this scenario, BJEX issues a cancellation event (event ID: 00005C22, 00005C23, or 00005C24) to JP1/IM - Manager as soon as the job is canceled. JP1/AS also sends a cancellation event (event ID: 00007122, 00007123, or 00007124) to JP1/IM - Manager. When JP1/IM - Manager receives this cancellation event, it releases the response-waiting event from the hold-and-accumulate state and the event disappears from the Response-Waiting Events page. The response status of the response-waiting event then changes to *Processed*.

For details about cancellation events of JP1/AS, see *JP1/Advanced Shell Description, User's Guide, Reference, and Operator's Guide*.

You can also cancel response-waiting events manually from JP1/IM - View. To cancel a response-waiting event that is no longer required, release the event from the hold-and-accumulate state in JP1/IM - View.

9.3 Configuring JP1/IM to link with BJEX and JP1/AS

This section describes how to configure JP1/IM - Manager to link with BJEX or JP1/AS. The descriptions in this section assume that JP1/IM - Manager is already set up.

We recommend the following configuration for JP1/Base and JP1/IM - Manager:

- JP1/Base and JP1/IM - Manager are in a cluster configuration on the manager host.
- The health check function is enabled for JP1/Base and JP1/IM - Manager.

9.3.1 Configuring JP1/IM - Manager

The following describes how to configure JP1/IM - Manager.

(1) Enabling the response-waiting event management function

Enable the response-waiting event management function in JP1/IM - Manager. After enabling the response-waiting event management function, you can:

- Accumulate response-waiting events
- Cancel response-waiting events
- Enable the settings that allow users to respond to and work with response-waiting events
The relevant settings appear in the Preferences window.
- Filter response-waiting events
Items that allow you to select whether to filter response-waiting events appear in the Detailed Settings for Event Receiver Filter window and the Severe Event Definitions window.

To enable the response-waiting event management function:

1. Execute the `jcoimdef` command.
Execute `jcoimdef -resevent ON`.
2. Restart JP1/IM - Manager.
Note: The feature is not enabled if you use the `jco_spmd_reload` command.

For details about the `-resevent` option of the `jcoimdef` command, see [9.5.1 jcoimdef](#).

(2) Configuring the event acquisition filter

Configure the event acquisition start location so that processing continues from where it last stopped.

To set the start location of the event acquisition filter:

1. Execute the `jcoimdef` command.
Execute `jcoimdef -b -1`.
2. Execute the `jco_spmd_reload` command or restart JP1/IM - Manager.

For details about the `jcoimdef` command, see `jcoimdef` in *Chapter 1. Commands of the JP1/Integrated Management - Manager Command and Definition File Reference*.

For details about the `jco_spm�_reload` command, see `jco_spm�_reload` in *Chapter 1. Commands of the JP1/Integrated Management - Manager Command and Definition File Reference*.

9.3.2 Configuring JP1/IM - View

The following describes how to configure JP1/IM - View.

(1) Enabling the setting that allow users to respond to and work with response-waiting events

In the Preferences window of JP1/IM - View, you can enable the setting that allows individual users to respond to and work with response-waiting events. After you enable this setting, users can:

- Monitor response-waiting events
The Response-Waiting Events page appears in the Event Console window.
- Respond to response-waiting events
Users can respond to these events in the Enter Response window.
- Search for response-waiting events
Items that relate to response-waiting events can now be specified as search conditions in the Search Events window.
- Filter response-waiting events
Items that allow the operator to select whether to display response-waiting events appear in the Settings for View Filter window.

To allow users to respond to and work with response-waiting events:

1. Display the Preferences window.
In the Event Console window, from the **Options** menu, choose **User Preferences**.
2. In the **Response-waiting event** area, select the **Enable** check box.
3. Click **OK**.

For details about the Preferences window, see 2.44.6 *Preferences window* in the manual *JP1/Integrated Management - Manager GUI Reference*.

(2) Configuring the event receiver filter

You can use an event receiver filter to limit which JP1 events each user can monitor. If you do not wish for a particular user to view response-waiting events, configure the event receiver filter to hide those events. By default, response-waiting events are displayed.

For details about how to create and modify an event receiver filter, see 4.2.2 *Settings for event receiver filters* in the *JP1/Integrated Management - Manager Configuration Guide*.

For details about the Detailed Settings for Event Receiver Filter window, see 2.44.8 *Filter condition definition windows* in the manual *JP1/Integrated Management - Manager GUI Reference*.

9.3.3 Configuring JP1/Base

In JP1/Base on the authentication server, assign the appropriate operating permissions to JP1 users who will work with response-waiting events.

The following operations require `JP1_Console_Operator` permission or higher:

- Responding to waiting-response events
- Manually releasing response-waiting events from the hold-and-accumulate state

The following operations require `JP1_Console_Admin` permission or higher:

- Resuming monitoring of response-waiting events in the hold-and-accumulate state

For details about how to assign permissions, see the chapter describing user management setup in the *JP1/Base User's Guide*.

9.3.4 Communication settings between BJEX or JP1/AS and JP1/IM - Manager

This section describes the settings that govern communication between BJEX or JP1/AS and JP1/IM - Manager.

(1) Setting the timeout time for connections

You can change the length of time after which a timeout occurs for connections established for purposes such as checking the status of the source process or entering a response. Under most circumstances, you do not need to change this setting. If you frequently encounter error messages (KAVB0554-E or KAVB0555-E) due to network congestion or heavy loads on the source server, set a longer timeout time. You can set the timeout time in JP1/IM - Manager.

To change the timeout time for connections:

1. Define the following parameter in a file you create on the manager.

```
[logical-host-name\JP1CONSOLEMANAGER]
"RESEV_TIMEOUT_MAX"=dword:hexadecimal-value
```

Replace *logical-host-name* with `JP1_DEFAULT` if the host is a physical host, and the logical host name if the host is a logical host.

Specify the timeout time as a hexadecimal value within a range from 60 to 3,600 seconds. The default is `dword:0000003c` (60 seconds).

2. Execute the `jbssetcnf` command.

Execute the `jbssetcnf` command with the definition file you created specified in a command argument. When you execute the `jbssetcnf` command, the setting in the definition file is applied to the common definition information. For details about the `jbssetcnf` command, see the *JP1/Base User's Guide*.

3. Execute the `jco_spmc_reload` command or restart JP1/IM - Manager.

The new definition takes effect.

For details about the `jco_spmc_reload` command, see `jco_spmc_reload` in *Chapter 1. Commands of the JP1/Integrated Management - Manager Command and Definition File Reference*.

(2) Configuring packet filtering in firewall environments

In an environment that uses a firewall, configure packet filtering so that BJEX or JP1/AS can communicate with JP1/IM - Manager through the firewall. The following table shows the port numbers used for communication between BJEX or JP1/AS and JP1/IM - Manager, and the direction in which packets pass through the firewall:

Table 9–3: Port numbers used for communication between BJEX or JP1/AS and JP1/IM - Manager

Service	Port	Traffic direction
jp1bsplugin	20306/tcp	JP1/IM - Manager -> BJEX or JP1/AS
jp1imevt	20098/tcp	BJEX or JP1/AS -> JP1/IM - Manager

Legend:

->: Direction of established connection

For details about the other port numbers used by JP1/IM and JP1/Base, see the following references:

- Port numbers used by JP1/Base: Description of port numbers in the *JP1/Base User's Guide*
- Port numbers used by JP1/IM: *Appendix C. Port Numbers* in the *JP1/Integrated Management - Manager Overview and System Design Guide*

9.3.5 Configuring BJEX or JP1/AS

This section describes how to configure BJEX or JP1/AS when linking with JP1/IM - Manager.

(1) Specifying the link-target JP1/IM - Manager

BJEX and JP1/AS can link with one JP1/IM - Manager host, which you must specify in the appropriate configuration file. To specify the link-target JP1/IM - Manager host for BJEX, specify the JP1/IM - Manager host name in the BJEX configuration file (`bjex.conf`). To specify the link-target host for JP1/AS, specify the host name in the JP1/AS environment file.

For details about the environment file of JP1/AS, see *JP1/Advanced Shell Description, User's Guide, Reference, and Operator's Guide*.

(2) Setting the maximum number of response-waiting events

You can set the maximum number of response-waiting events that BJEX or JP1/AS can issue. Because the maximum number of events that can be in the hold-and-accumulate state is 2,000, estimate the number of response-waiting events so that the result of the following equation is 2,000 or less:

Total value of USERREPLY_WAIT_MAXCOUNT parameter across all hosts that output response-waiting events + Maximum number of response-waiting events output by all other products

You can set the maximum number of response-waiting events that BJEX can issue in the BJEX configuration file (`bjex.conf`). For JP1/AS, you can set this value in the JP1/AS environment file. For details about the number of response-waiting events that JP1/AS issues, see *JP1/Advanced Shell Description, User's Guide, Reference, and Operator's Guide*.

9.4 Working with response-waiting events

This section describes the operations you can perform on response-waiting events.

Important

Restrictions affecting the Web-based JP1/IM - View

From the Web-based JP1/IM - View, you cannot respond to response-waiting events, release an event from the hold-and-accumulate state, or resume monitoring of events in the hold-and-accumulate state. The Response-Waiting Events page does not appear in the Event Console window in the Web-based JP1/IM - View. However, you can change the response status of response-waiting events and register incidents manually.

9.4.1 Flow of tasks for responding to response-waiting events

This section describes the flow of tasks for monitoring and responding to response-waiting events in Central Console and Central Scope.

(1) Monitoring response-waiting events in Central Console

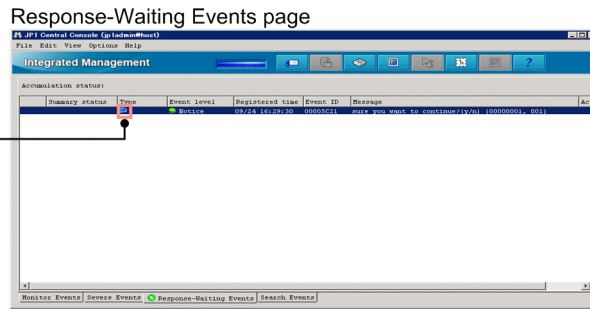
The following figure shows an overview of how to monitor and respond to response-waiting events in Central Console:

Figure 9–6: Monitoring and responding to response-waiting events in Central Console

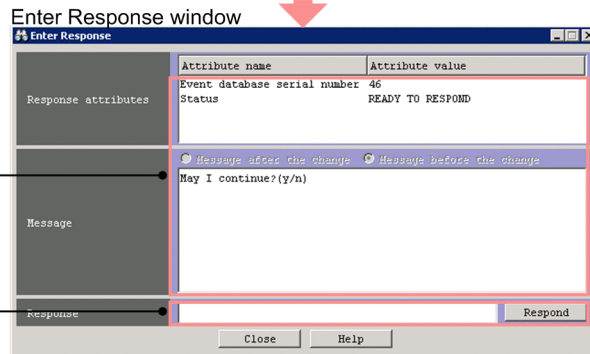
1. A response-waiting event appears on the Response-Waiting Events page.



Icon indicating a response-waiting event



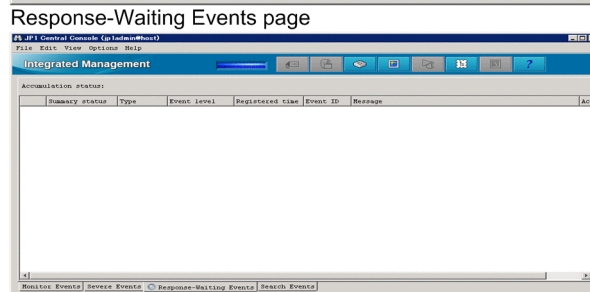
2. Display the Enter Response window.



3. Check the status of the source process of the response-waiting event, and the message contents.

4. Enter a response and then click **Respond**.

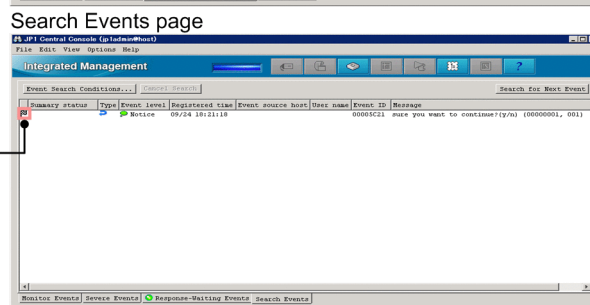
5. If the response is successful, the response-waiting event disappears from the Response-Waiting Events page.



6. When you search for the response-waiting event in the Search Events page, the event appears in *Processed* status in the search results.



Icon indicating *Processed* status



Legend:

: Operation performed by user

The numbers in the figures correspond to the steps below:

1. When JP1/IM - Manager receives a response-waiting event, the event appears on the Response-Waiting Events page of the Event Console window.
2. Display the Enter Response window for the response-waiting event.
3. Check the status of the source process and the message contents.
Make sure that the status of the source process is **READY TO RESPOND**.
4. Enter a response in the **Response** area and then click **Respond**.
5. If the response is successful, the response-waiting event disappears from the Response-Waiting Events page.
6. When you search for a response-waiting event from the Search Events window, the event appears in the search results with the status *Processed*.

(2) Monitoring response-waiting events in Central Scope

The following figure shows an overview of how to monitor and respond to response-waiting events in Central Scope:

Figure 9–7: Monitoring and responding to response-waiting events in Central Scope

1. A response-waiting event matches a status change condition of a monitored object, causing the status of the object to change.
2. Display the response-waiting event by searching for the status-change event.
3. Display the Enter Response window.
4. Check the status of the source process of the response-waiting event, and the message contents.
5. Enter a response and then click **Respond**.
6. When you search for the response-waiting event in the Search Events page of central console, the event appears in Processed status in the search results.
7. The response-waiting event transitioning to Processed status causes the status of the monitored object to automatically return to Normal.

Monitoring Tree window of central scope

Monitoring Node Name	Monitoring Node Type	Status
node6	User Monitoring Object	Error

Search Events page of central console

Summary status	Type	Event level	Registered time	Event ID	Message
Processed	Status-Change	Notice	09/24 18:21:18	00003C21	use you want to continue?(y/n) (00000001, 001)

Enter Response window

Attribute name	Attribute value
Event database serial number	46
Status	READY TO RESPOND

Message: use you want to continue?(y/n)

Buttons: Close, Help, Respond

Search Events page of central console

Summary status	Type	Event level	Registered time	Event source host	User name	Event ID	Message
Processed	Status-Change	Notice	09/24 18:21:18			00003C21	use you want to continue?(y/n) (00000001, 001)

Monitoring Tree window of central scope

Monitoring Node Name	Monitoring Node Type	Status
node6	User Monitoring Object	Initial

Legend:

: Operation performed by user

The numbers in the figures correspond to the steps below:

1. When JP1/IM - Manager receives a response-waiting event that matches the status change condition for a monitored object, the status of the monitored object changes.
2. Search for the status change event from the monitored object and display response-waiting events in the Search Events page.
3. Display the Enter Response window for the response-waiting event.
4. Check the status of the source process and the message contents.
Make sure that the status of the source process is READY TO RESPOND.

5. Enter a response in the **Response** area and then click **Respond**.
6. If the response is successful, the response-waiting event appears in the search results with the status *Processed* when you search from the Search Events window again.
7. With the response to the response-waiting event now complete, the status of the monitored object in the Monitoring Tree window returns to normal.

9.4.2 Responding to response-waiting events

The conditions under which you can respond to a response-waiting event are described in [9.2.4\(2\) Conditions for responding to response-waiting events](#). You must have `JP1_Console_Operator` permission or higher to perform this operation.

To respond to a response-waiting event:

1. Use one of the following methods to display the Enter Response window:
 - On the Response-Waiting Events page or Search Events page, select a response-waiting event, and from the **View** menu, choose **Enter Response**.
 - On the Response-Waiting Events page, Search Events page, or Related Events window, right-click a response-waiting event and choose **Enter Response** from the popup menu.
 - In the Event Details window, click **Enter Response**.

2. Enter a response in the **Response** area of the Enter Response window.

Check the message contents and enter an appropriate response.

- You can enter a maximum of 512 bytes.
- You can enter characters in the 0x20 to 0x7E range of the ASCII character set.

3. Click **Respond**.

A confirmation dialog box appears. Click **Yes** to submit the response to the response-waiting event. Click **No** to return to the Enter Response window without submitting the response.

If the response is successful, the response-waiting event disappears from the Response-Waiting Events page, and the response status of the event changes to *Processed*.

9.4.3 Manually releasing response-waiting events from the hold-and-accumulate state

If an event no longer requires a response, or the event was not released from the hold-and-accumulate state despite a successful response, you can manually release the event from the hold-and-accumulate state. Note that this operation requires `JP1_Console_Operator` permission or higher.

To release a response-waiting event from the hold-and-accumulate state:

1. Display the Response-Waiting Events page of the Event Console window.
2. Check the status of the source process of the response-waiting event you want to release.

Display the Enter Response window by selecting the response-waiting event you want to release. Make sure that the status of the source process is `NO LONGER MANAGED BY BJEX` or `ALREADY RESPONDED`.

3. Change the response status of the response-waiting event to *Processed*.

If the event can be released, change the status of the event to *Processed* by choosing **Processed** from the **View** menu.

4. Select the response-waiting event that you want to release from the hold-and-accumulate state, and from the **View** menu, choose **Remove Accumulated Events**. Alternatively, right-click the event and choose **Remove Accumulated Events** from the popup menu.

You can select multiple response-waiting events. When you click **Remove Accumulated Events**, the selected events are removed from the hold-and-accumulate state.

The response-waiting events disappear from the Response-Waiting Events page when you refresh the list of events.

You cannot accumulate an event again after releasing it. If you inadvertently release a response-waiting event, you can respond to the event by searching for it from the Search Events page.

9.4.4 Resuming monitoring of events in the hold-and-accumulate state

When normal monitoring of events in hold-and-accumulate state is resumed after the number of accumulated response-waiting events has exceeded 2,000, you can be notified by a JP1 event when the number of accumulated events once again exceeds 2,000. This operation requires `JP1_Console_Admin` permission.

Before you resume monitoring accumulated events, identify and respond to the overflowed response-waiting events by reviewing the integrated trace log on the manager. For details about how to respond to response-waiting events that have been released from the hold-and-accumulate state, see [9.2.3\(2\) Notification when the number of response-waiting events exceeds 2,000](#).

To resume monitoring of events in the hold-and-accumulate state:

1. In the Event Console window, from the **Options** menu, choose **Function-Status Notification Return** and then **Monitor Accumulation Status**.

The system resumes monitoring the events in the hold-and-accumulate state. The message KAVB0551-E disappears from the **Accumulation status** area of the Response-Waiting Events page when you next refresh the Event Console window.

9.5 Command usage when linking with BJEX or JP1/AS

This section describes the command options you need to use when linking with BJEX or JP1/AS. For information about other options and details of the commands themselves, see *Chapter 1. Commands* in the *JP1/Integrated Management - Manager Command and Definition File Reference*. Note that the *JP1/Integrated Management - Manager Command and Definition File Reference* does not describe the options for linking with BJEX.

9.5.1 jcoimdef

The `jcoimdef` command is used to set up the system environment for JP1/IM - Manager, and to reference settings. When you execute this command, the settings are output to standard output.

You can specify the following option when linking with BJEX or JP1/AS:

`-resevent {ON | OFF}`

Specify the `-resevent ON` option to enable the response-waiting event management function. To disable the function, specify `-resevent OFF`.

If you execute the `jcoimdef` command with the `-resevent` option to enable or disable the response-waiting event management function while JP1/IM - Manager is running, you will need to restart JP1/IM - Manager. You will also need to restart any instances of JP1/IM - View that are connected to JP1/IM - Manager.

For details about the `jcoimdef` command, see `jcoimdef` in *Chapter 1. Commands* of the *JP1/Integrated Management - Manager Command and Definition File Reference*.

9.5.2 jim_log.bat (Windows only)

`jim_log.bat` is a tool for collecting data when an error occurs 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.

You can specify the following option when linking with BJEX or JP1/AS:

`-a`

Specify this option to prevent the tool from collecting the file for accumulated response-waiting events.

The file for accumulated response-waiting events collected by `jim_log.bat` is stored in the following folders as primary data:

Internal folder for primary data on physical hosts

`data-folder\jpl_default\imm_1st\cons\log\response`

Internal folder for primary data on logical hosts

`data-folder\logical-host-name\imm_1st\cons\log\response`

For details about the `jim_log.bat` tool, see `jim_log.bat (Windows only)` in *Chapter 1. Commands* of the *JP1/Integrated Management - Manager Command and Definition File Reference*.

9.5.3 jim_log.sh (UNIX only)

`jim_log.sh` is a tool for collecting data when an error occurs 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.

You can specify the following option when linking with BJEX or JP1/AS:

`-a`
Specify this option to prevent the tool from collecting the file for accumulated response-waiting events.

The file for accumulated response-waiting events collected by `jim_log.sh` is stored in the following directories as primary data:

Internal directory for primary data on physical hosts

`./var/opt/jp1cons/log/response`

Internal directory for primary data on logical hosts

`./shared-disk/jp1cons/log/response`

For details about the `jim_log.sh` tool, see *jim_log.sh (UNIX only)* in *Chapter 1. Commands of the JP1/Integrated Management - Manager Command and Definition File Reference*.

10

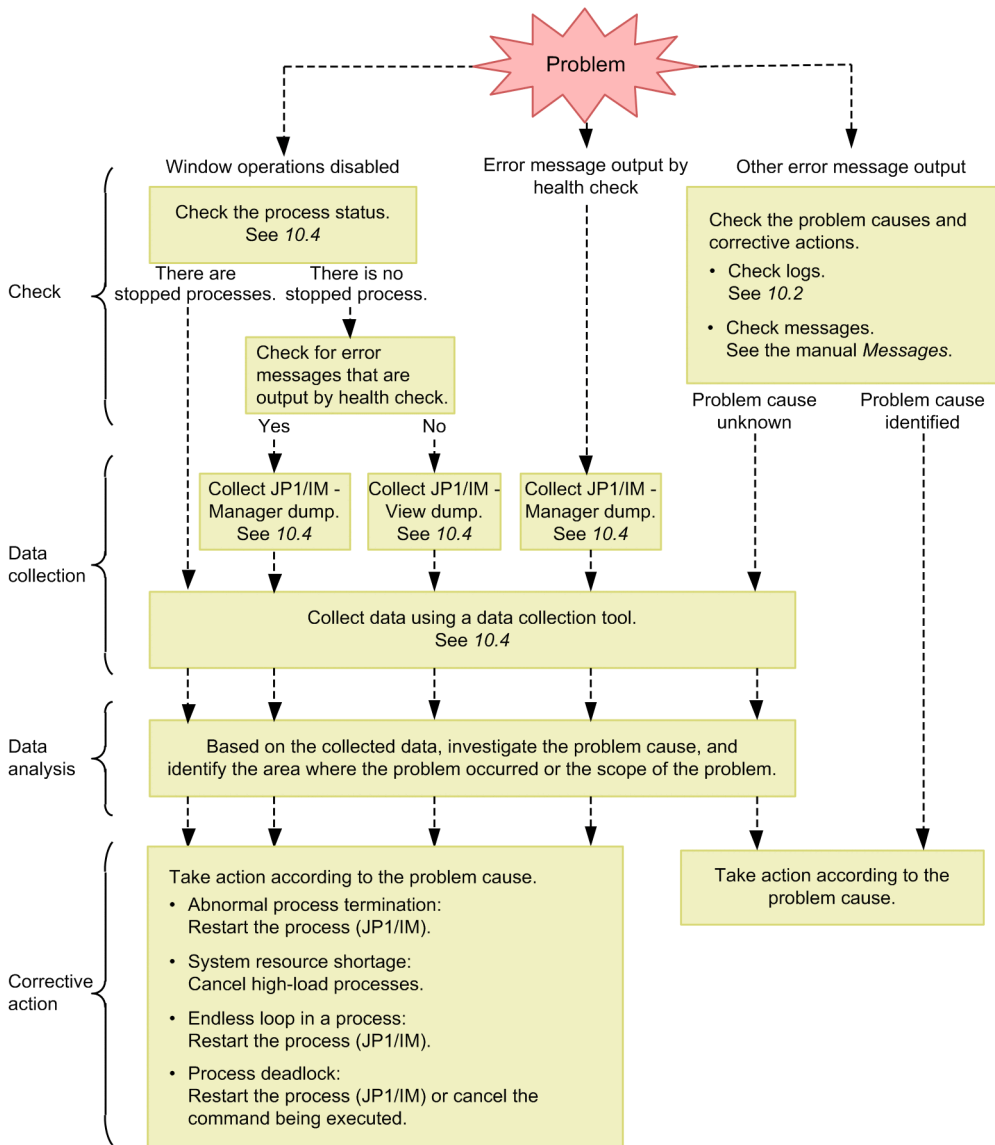
Troubleshooting

This chapter explains how to handle problems if they occur in JP1/IM. It also explains items that tend to cause problems.

10.1 Troubleshooting procedure

The figure below shows the procedure to follow when a problem occurs in JP1/IM.

Figure 10–1: Troubleshooting procedure



10.2 Log information types

The following three types of logs are output by JP1/IM:

- Common message log
- Integrated trace log
- Operation log

This section explains these three types of log information.

10.2.1 Common message log

The common message log contains log information for the system administrator and reports system problems. The common message log reports a minimal amount of necessary problem information.

The common message log is output to the syslog file in UNIX, and to the Windows Event Log in Windows.

In UNIX, the common message log is output to the following files:

- Files under `/var/adm/syslog/` (in AIX)
- `/var/log/messages` (in Linux)

Important

In UNIX, a message whose output destination is the syslog file might not actually be output, depending on the behavior of the syslog file.

10.2.2 Integrated trace log

The integrated trace log contains log information that is obtained by using the Hitachi Network Objectplaza Trace Library (HNTRLib2) to integrate the trace information that is output by individual programs into a single output file. The integrated trace log outputs more detailed messages than the common message log.

The default output destination of the integrated trace log is as follows:

In Windows:

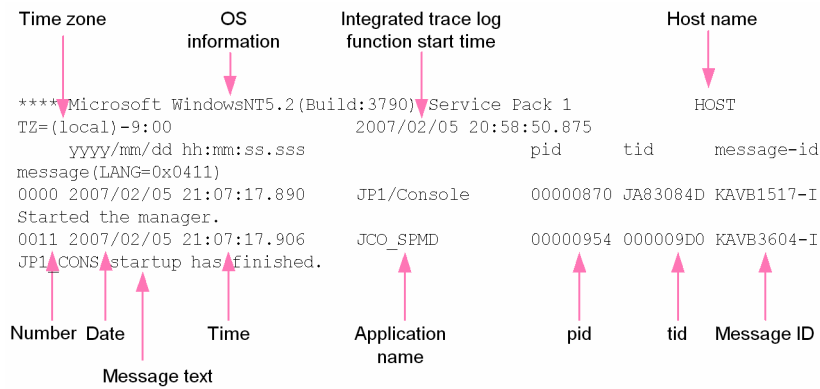
```
system-drive\Program Files\Hitachi\HNTRLib2\spool\hntr2{1|2|3|4}.log
```

In UNIX:

```
/var/opt/hitachi/HNTRLib2/spool/hntr2{1|2|3|4}.log
```

You can view the integrated trace log file from a text editor of your choice. The figure below shows an output example of the integrated trace log.

Figure 10–2: Integrated trace log file output example



The header information that is output to the integrated trace log file and the output items are explained below.

Table 10–1: Integrated trace log file header information

Header information	Explanation
OS information	Information on the OS under which the Hitachi Network Objectplaza Trace Library (HNTRLib2) started.
Host name	The name of the host on which the Hitachi Network Objectplaza Trace Library (HNTRLib2) started.
Time zone	In Windows: OS's time zone In UNIX: Environment variable TZ of the integrated trace process. If the environment variable TZ is not set up, Unknown is output.
Integrated trace log function start time	Time at which the Hitachi Network Objectplaza Trace Library (HNTRLib2) started.

Table 10–2: Integrated trace log file output items

Output items	Explanation
Number (4 digits)	Trace code serial number A number is assigned to each process that outputs a log.
Date (10 bytes)	Trace collection date: <i>yyyy/mm/dd</i> (year/month/day)
Time (12 bytes)	Trace collection time (local time): <i>hh:mm:ss.sss</i> (hour:minutes:seconds.milliseconds)
AP name (16 bytes or shorter)	Name that identifies an application (application identifier) The following AP names are output by JP1/IM - Manager: <ul style="list-style-type: none"> • JP1/IM-Manager Service JP1/IM-Manager • Event Base Service evflow • Automatic Action Service jcamain • Event Generation Service evgen • Central Scope Service jcsmain • IM Configuration Management Service jcfmain

Output items	Explanation
	<ul style="list-style-type: none"> • Process management JCO_SPMD • jcochstat command jcochngstat • Other commands <i>command-name</i> <p>The following AP names are output by JP1/IM - View:</p> <ul style="list-style-type: none"> • Central Console - View JP1/IM-View • Central Scope - View JP1/IM-View • IM Configuration Management - View JP1/IM-View • Edit Tree window JP1/IM-Edit
pid	Process ID assigned by the OS
tid	Thread ID for identifying a thread
Message ID	Message ID explained in the message output format. Message ID used by this product.
Message text	Message text that is output to the integrated trace log. Message text that is output from this product.

The log time that is output to the integrated trace log is formatted according to the time zone of the process that output the log.

Consequently, if a user who has changed the environment variable *TZ* starts a service or executes a command, a time that is different from the time zone that is set in the OS may be output.

10.2.3 Operation log

The operation log of JP1/IM - Manager contains log information about the login and logout history, including who attempted login or logout when and where, and whether the attempt was successful or failed. The operation log is used to find the cause of security problems such as unauthorized access, and to collect information necessary to ensure secure system operation. For details about the operation log, see *Appendix K. Operation Log Output in the JP1/Integrated Management - Manager Overview and System Design Guide*.

10.2.4 Log files and directory list

This subsection explains the types of log information that are output by JP1/IM, default file names, and directory names.

Note that the files explained here are output for product maintenance purposes. Therefore, there is no need for the user to view or modify these files. If a problem such as a system error occurs, the user may be asked to temporarily retain these files on site for the purpose of collecting data.

(1) In Windows

The tables below show the default log files and folders that are output by the Windows version of JP1/IM.

The *Log type* column lists the log types that are output by JP1/IM.

The *Default file name and folder name* column describes log file names as absolute paths when JP1/IM - Manager, JP1/IM - View, or JP1/Base is installed in the default mode. *Default file name and folder name* in a cluster operation system describes the log file names of shared folders as absolute paths.

The *Maximum disk usage* column shows the maximum disk space used by each log file. When there are multiple log files, the combined total is given.

The *File-switching timing* column shows how JP1/IM times output destination log file switching. When the file reaches the size shown in this column or when the event shown in this column occurs, the output destination is switched. If there are multiple log files and if the maximum disk usage is reached, files are overwritten, beginning with the ones that have the oldest update dates.

Table 10–3: JP1/IM - Manager (common to all components) log files and folders (Windows)

Log type	Default file name and folder name	Maximum disk usage	File-switching timing
Operation log	<i>Manager-path</i> \log\operationlog \imm_operation{none 1 2... 16}.log ^{#1}	55 MB ^{#1}	5 MB ^{#1#2}
jimnodecount command log	<i>Manager-path</i> \log\nodecount \jimnodecount_cmd{1 2}.log	20 MB	10 MB

#1: You can change the output destination, the number of files that can be saved, and the file size. For details, see *Operation log definition file (imm_operationlog.conf)* (Chapter 2. Definition Files) in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*. The number of bytes shown in the Maximum disk usage and File-switching timing columns are the values used when the number of files that can be saved and the file size are set to initial values.

#2: For details about the operation when switching the operation log file, see *K.2 Storage format of operation log output* in the *JP1/Integrated Management - Manager Overview and System Design Guide*.

Table 10–4: JP1/IM - Manager (Central Console) log files and folders (Windows)

Log type	Default file name and folder name	Maximum disk usage	File-switching timing
Process management log	<i>Console-path</i> \log\JCO_SPMD{1 2 3}.log	384 KB	128 KB
	<i>Console-path</i> \log\JCO_SPMD_COMMAND{1 2 3}.log	384 KB	128 KB
	<i>shared-folder</i> \jplcons\log\JCO_SPMD{1 2 3}.log	384 KB	128 KB
	<i>shared-folder</i> \jplcons\log \JCO_SPMD_COMMAND{1 2 3}.log	384 KB	128 KB
Stack trace log	<i>Console-path</i> \log\javalog0{1 2 3 4}.log	1 MB	At startup or 256 KB
	<i>shared-folder</i> \jplcons\log\javalog0{1 2 3 4}.log	1 MB	At startup or 256 KB
Logical host settings program log	<i>Console-path</i> \log\jplhassetup.{log log.old}	2,000 KB	1,000 KB
Setup log	<i>Console-path</i> \log\command \comdef[_old].log	512 KB	256 KB
Event console log	<i>Console-path</i> \log\console\EVCONS{1 2 3}.log	30,720 KB	10,240 KB
	<i>Console-path</i> \log\console\jplcons{1 2 3 4 5 6 7 8}.log	40,960 KB	5,120 KB ^{#1}

Log type	Default file name and folder name	Maximum disk usage	File-switching timing
	<i>Console-path</i> \log\console\evtcon_exe{1 2 3}.log	256 KB × 3	256 KB
	<i>Console-path</i> \log\console\JCOAPI{1 2 3}.log	96KB	32KB
	<i>Console-path</i> \log\console\jplconsM{1 2... 60}.log	300 MB	5 MB ^{#1}
	<i>Console-path</i> \log\console\jpleventStormDef{1 2 3 4 5}.log	100 MB	20 MB
	<i>Console-path</i> \log\console\jplfilterDef{1 2 3 4 5}.log	100 MB	20 MB
	<i>Console-path</i> \log\console\jplbizGroupDef{1 2}.log	10 MB	5 MB
	<i>Console-path</i> \log\console\jplcmdButtonDef{1 2 3 4 5}.log	25 MB	5 MB
	<i>Console-path</i> \log\console\jplexattrnameDef{1 2 3 4 5}.log	25 MB	5 MB
	<i>shared-folder</i> \jplcons\log\console\EVCONS{1 2 3}.log	30,720 KB	10,240 KB
	<i>shared-folder</i> \jplcons\log\console\jplcons{1 2 3 4 5 6 7 8}.log	40,960 KB	5,120 KB ^{#1}
	<i>shared-folder</i> \jplcons\log\console\evtcon_exe{1 2 3}.log	256 KB × 3	256 KB
	<i>shared-folder</i> \jplcons\log\console\JCOAPI{1 2 3}.log	96 KB	32 KB
	<i>shared-folder</i> \jplcons\log\console\jplconsM{1 2... 60}.log	300 MB	5 MB ^{#1}
	<i>shared-folder</i> \jplcons\log\console\jpleventStormDef{1 2 3 4 5}.log	100 MB	20 MB
	<i>shared-folder</i> \jplcons\log\console\jplfilterDef{1 2 3 4 5}.log	100 MB	20 MB
	<i>shared-folder</i> \jplcons\log\console\jplbizGroupDef{1 2}.log	10 MB	5 MB
	<i>shared-folder</i> \jplcons\log\console\jplcmdButtonDef{1 2 3 4 5}.log	25 MB	5 MB
	<i>shared-folder</i> \jplcons\log\console\jplexattrnameDef{1 2 3 4 5}.log	25 MB	5 MB
Automated action trace log	<i>Console-path</i> \log\action\JCAMAIN{1 2 3 4 5}.log	25,600 KB ^{#2}	5,120 KB
	<i>shared-folder</i> \jplcons\log\action\JCAMAIN{1 2 3 4 5}.log	25,600 KB ^{#2}	5,120 KB
Product information log	<i>Console-path</i> \log\hliclib\hliclibtrc{1 2 3 4 5}.log	5 MB	1 MB
	<i>Console-path</i> \log\hliclib\hlicliberr{1 2 3 4 5}.log	5 MB	1 MB

Log type	Default file name and folder name	Maximum disk usage	File-switching timing
	<i>Console-path</i> \log\hliclib \hliclibmgrtrc{1 2 3 4 5}.log	5 MB	1 MB
	<i>Console-path</i> \log\hliclib \hliclibmgrerr{1 2 3 4 5}.log	5 MB	1 MB
	<i>shared-folder</i> \jplcons\log\hliclib \hliclibtrc{1 2 3 4 5}.log	5 MB	1 MB
	<i>shared-folder</i> \jplcons\log\hliclib \hlicliberr{1 2 3 4 5}.log	5 MB	1 MB
	<i>shared-folder</i> \jplcons\log\hliclib \hliclibmgrtrc{1 2 3 4 5}.log	5 MB	1 MB
	<i>shared-folder</i> \jplcons\log\hliclib \hliclibmgrerr{1 2 3 4 5}.log	5 MB	1 MB
Action information file	<i>Console-path</i> \log\action\actinf.log	626 KB ^{#3}	No switching
	<i>shared-folder</i> \jplcons\log\action \actinf.log	626 KB ^{#3}	No switching
Action host name file	<i>Console-path</i> \log\action\acttxt{1 2}.log	48.9 MB ^{#4}	When the action information file wraps around
	<i>shared-folder</i> \jplcons\log\action \acttxt{1 2}.log	48.9 MB ^{#4}	When the action information file wraps around
Action re-execution file	<i>Console-path</i> \log\action\actreaction	300 MB	When system switching occurs
	<i>shared-folder</i> \jplcons\log\action \actreaction	300 MB	When system switching occurs
jcochstat, and jcoevtreport command trace logs ^{#5}	<i>Console-path</i> \log\command\CMD{1 2 3}.log	3,072 KB	1,024 KB
	<i>Console-path</i> \log\command\jplcons_cmd{1 2}.log	12,288 KB	6,144 KB
	<i>Console-path</i> \log\command\jplconsM_cmd{1 2}.log	12,288 KB	6,144 KB
	<i>Console-path</i> \log\command \jplexattrnameDef_cmd{1 2 3 4 5}.log	25 MB	5 MB
Plug-in log	<i>Console-path</i> \log\command\jcoplugin{1 2 3}.log	3 MB	1 MB
Reporting status storage file	<i>Console-path</i> \log\notice\notice_stat.dat	72B	No switching
	<i>shared-folder</i> \jplcons\log\notice \notice_stat.dat	72B	No switching
Action definition backup file	<i>Console-path</i> \log\action\actdefbk.conf	2,048 KB	No switching
	<i>shared-folder</i> \jplcons\log\action \actdefbk.conf	2,048 KB	No switching
Event base trace log	<i>Console-path</i> \log\evflow\EVFLOW{1 2 3 4 5 6 7 8 9 10}.log	100 MB	10 MB

Log type	Default file name and folder name	Maximum disk usage	File-switching timing
	<i>Console-path</i> \log\evflow\jpllevflowM{1 2... 60}.log	300 MB	5 MB
	<i>Console-path</i> \log\evflow\jplactDef{1 2 3 4 5}.log	25 MB	5 MB
	<i>Console-path</i> \log\evflow\jplchsevDef{1 2 3 4 5}.log	25 MB	5 MB
	<i>Console-path</i> \log\evflow\jplchmsgDef{1 2 3 4 5}.log	25 MB	5 MB
	<i>Console-path</i> \log\evflow\jplhostmapDef{1 2 3 4 5}.log	25 MB	5 MB
	<i>Console-path</i> \log\evflow\evflow_exe{1 2 3}.log	256 KB × 3	256 KB
	<i>shared-folder</i> \jplcons\log\evflow\EVFLOW{1 2 3 4 5 6 7 8 9 10}.log	100 MB	10 MB
	<i>shared-folder</i> \jplcons\log\evflow\jpllevflowM{1 2... 60}.log	300 MB	5 MB
	<i>shared-folder</i> \jplcons\log\evflow\jplactDef{1 2 3 4 5}.log	25 MB	5 MB
	<i>shared-folder</i> \jplcons\log\evflow\jplchsevDef{1 2 3 4 5}.log	25 MB	5 MB
	<i>shared-folder</i> \jplcons\log\evflow\jplchmsgDef{1 2 3 4 5}.log	25 MB	5 MB
	<i>shared-folder</i> \jplcons\log\evflow\jplhostmapDef{1 2 3 4 5}.log	25 MB	5 MB
	<i>shared-folder</i> \jplcons\log\evflow\evflow_exe{1 2 3}.log	256 KB × 3	256 KB
Matching information file	<i>Console-path</i> \log\evflow\evflowinf.log	12B	No switching
	<i>shared-folder</i> \jplcons\log\evflow\evflowinf.log	12B	No switching
Event base error log	<i>Console-path</i> \log\evflow\jpllevflow{1 2 3 4 5 6 7 8}.log	40,960 KB	5,120 KB
	<i>shared-folder</i> \jplcons\log\evflow\jpllevflow{1 2 3 4 5 6 7 8}.log	40,960 KB	5,120 KB
Event base stack trace	<i>Console-path</i> \log\evflow\javalog0{1 2 3 4}.log	1 MB	At startup or 256 KB
	<i>shared-folder</i> \jplcons\log\evflow\javalog0{1 2 3 4}.log	1 MB	At startup or 256 KB
Automated action error log	<i>Console-path</i> \log\action\jplact{1 2 3}.log	15,360 KB	5,120 KB
	<i>shared-folder</i> \jplcons\log\action\jplact{1 2 3}.log	15,360 KB	5,120 KB
Correlation event generation history file	<i>Console-path</i> \operation\evgen\egs_discrim{1 2 3}.log ^{#6}	30 MB ^{#6}	10 MB ^{#6}

Log type	Default file name and folder name	Maximum disk usage	File-switching timing
	<i>shared-folder</i> \jplcons\operation\evgen\egs_discrim{1 2 3}.log ^{#6}	30 MB ^{#6}	10 MB ^{#6}
Common exclusion history file	<i>Console-path</i> \operation\comexclude\comexclude{1 2 3 4 5}.log	100 MB	20 MB
	<i>shared-folder</i> \jplcons\operation\comexclude\comexclude{1 2 3 4 5}.log	100 MB	20 MB
Common exclusion-conditions definition history file	<i>Console-path</i> \operation\comexclude\comexcludeDef{1 2 3 4 5}.log	100 MB	20 MB
	<i>shared-folder</i> \jplcons\operation\comexclude\comexcludeDef{1 2 3 4 5}.log	100 MB	20 MB
Correlation event generation trace log	<i>Console-path</i> \log\evgen\EVGEN{1 2 3}.log	15 MB	5 MB
	<i>Console-path</i> \log\evgen\evgen_exe{1 2 3}.log	256 KB × 3	256 KB
	<i>shared-folder</i> \jplcons\log\evgen\EVGEN{1 2 3}.log	15 MB	5 MB
	<i>shared-folder</i> \jplcons\log\evgen\evgen_exe{1 2 3}.log	256 KB × 3	256 KB
Correlation event generation individual log	<i>Console-path</i> \log\evgen\jplegs{1 2}.log	20 MB	10 MB
	<i>Console-path</i> \log\evgen\jplegsM{1 2}.log	20 MB	10 MB
	<i>shared-folder</i> \jplcons\log\evgen\jplegs{1 2}.log	20 MB	10 MB
	<i>shared-folder</i> \jplcons\log\evgen\jplegsM{1 2}.log	20 MB	10 MB
Correlation event generation individual log (for commands)	<i>Console-path</i> \log\evgen\jplegs_cmd{1 2 3 4}.log	20 MB	5 MB
	<i>Console-path</i> \log\evgen\jplegsM_cmd{1 2 3 4}.log	20 MB	5 MB
Correlation event generation stack trace log	<i>Console-path</i> \log\evgen\javalog0{1 2 3 4}.log	1 MB	At startup or 256 KB
	<i>shared-folder</i> \jplcons\log\evgen\javalog0{1 2 3 4}.log	1 MB	At startup or 256 KB
Correlation event generation process inheriting definition file	<i>Console-path</i> \log\evgen\egs_discrim_info{1 2 3 4}.dat	312 MB ^{#7}	At termination
	<i>shared-folder</i> \jplcons\log\evgen\egs_discrim_info{1 2 3 4}.dat	312 MB ^{#7}	At termination
Correlation event generation definition application log	<i>Console-path</i> \log\evgen\jplegsDefine{1 2}.log	10 MB	5 MB
	<i>shared-folder</i> \jplcons\log\evgen\jplegsDefine{1 2}.log	10 MB	5 MB
File for accumulated response-waiting events ^{#8}	<i>Console-path</i> \log\response\resevent.dat	40 MB	No switching
	<i>shared-folder</i> \jplcons\log\response\resevent.dat	40 MB	No switching

Log type	Default file name and folder name	Maximum disk usage	File-switching timing
Backup file for accumulated response-waiting events	<i>Console-path</i> \log\response \resevent.dat.dump	40 MB	No switching
	<i>shared-folder</i> \jplcons\log\response \resevent.dat.dump	40 MB	No switching
Command execution history folder	<i>Base-path</i> \log\COMMAND\ <i>shared-folder</i> \jplbase\log\COMMAND\ 	See the <i>JP1/Base User's Guide</i> .	
Remote command log	<i>Base-path</i> \log\JCOCMD\jcocmd_result{1 2 3}.log <i>Base-path</i> \log\JCOCMD\jcocmdapi{1 2 3}.log <i>Base-path</i> \log\JCOCMD\jcocmdapi_trace{1 2 3}.log <i>Base-path</i> \log\JCOCMD\jcocmdcom{1 2 3}.log <i>Base-path</i> \log\JCOCMD\jcocmdcom_trace{1 2 3}.log <i>Base-path</i> \log\JCOCMD\jcocmdexe{1 2 3}.log <i>Base-path</i> \log\JCOCMD\jcocmdexe_trace{1 2 3}.log <i>Base-path</i> \log\JCOCMD\jcocmdrouter{1 2 3}.log <i>Base-path</i> \log\JCOCMD \jcocmdrouter_trace{1 2 3}.log <i>Base-path</i> \log\JCOCMD\JCOCMDCMD{1 2 3}.log <i>shared-folder</i> \jplbase\log\JCOCMD \jcocmd_result{1 2 3}.log <i>shared-folder</i> \jplbase\log\JCOCMD \jcocmdapi{1 2 3}.log <i>shared-folder</i> \jplbase\log\JCOCMD \jcocmdapi_trace{1 2 3}.log <i>shared-folder</i> \jplbase\log\JCOCMD \jcocmdcom{1 2 3}.log <i>shared-folder</i> \jplbase\log\JCOCMD \jcocmdcom_trace{1 2 3}.log <i>shared-folder</i> \jplbase\log\JCOCMD \jcocmdexe{1 2 3}.log <i>shared-folder</i> \jplbase\log\JCOCMD \jcocmdexe_trace{1 2 3}.log <i>shared-folder</i> \jplbase\log\JCOCMD \jcocmdrouter{1 2 3}.log		

Log type	Default file name and folder name	Maximum disk usage	File-switching timing
	<i>shared-folder</i> \jplbase\log\JCOCMD \jcocmdrouter_trace{1 2 3}.log		
	<i>shared-folder</i> \jplbase\log\JCOCMD \JCOCMDCMD{1 2 3}.log		
Configuration management log	<i>Base-path</i> \log\route\JBSRT{1 2 3}.log		
	<i>shared-folder</i> \jplbase\log\route\JBSRT{1 2 3}.log		
Trace log file	<i>Base-path</i> \sys\tmp\event\logtrap \jelallog\jelallog{1 2 3 4 5}.log		
	<i>Base-path</i> \sys\tmp\event\logtrap \jelalelt\jelalelt{1 2 3 4 5}.log		
Integrated monitoring database application log	<i>Console-path</i> \log\evflow\EVFLOW_DBAPI{1 2... 16}.log	200 MB	12.5 MB
	<i>Console-path</i> \log\console\EVCONS_DBAPI{1 2 3 4 5}.log	50 MB	10 MB
	<i>Console-path</i> \log\command\CMD_DBAPI{1 2 3 4 5}.log	50 MB	10 MB
	<i>shared-folder</i> \jplcons\log\evflow \EVFLOW_DBAPI{1 2... 16}.log	200 MB	12.5 MB
	<i>shared-folder</i> \jplcons\log\console \EVCONS_DBAPI{1 2 3 4 5}.log	50 MB	10 MB
API log for the IM Configuration Management database	<i>Console-path</i> \log\evflow \EVFLOW_CFDDBAPI{1 2 3}.log	30 MB	10 MB
	<i>Console-path</i> \log\console \EVCONS_CFDDBAPI{1 2 3}.log	30 MB	10 MB
	<i>Console-path</i> \log\command\CMD_CFDDBAPI{1 2 3}.log	30 MB	10 MB
	<i>shared-folder</i> \jplcons\log\evflow \EVFLOW_CFDDBAPI{1 2 3}.log	30 MB	10 MB
	<i>shared-folder</i> \jplcons\log\console \EVCONS_CFDDBAPI{1 2 3}.log	30 MB	10 MB
jcodbsetup command log	<i>Console-path</i> \log\imdb\jcodbsetup{1 2}.log	512 KB	256 KB
jcodbunsetup command log	<i>Console-path</i> \log\imdb\jcodbunsetup{1 2}.log	512 KB	256 KB
jimmail command log	<i>Console-path</i> \log\mail\jimmail_cmd{1 2 3}.log	15 MB	5 MB
	<i>Console-path</i> \log\mail\jimmail_cmdM{1 2 3}.log	15 MB	5 MB
	<i>Console-path</i> \log\mail\JIMMAIL{1 2 3}.log	15 MB	5 MB
	<i>Console-path</i> \log\mail\jimmail_exe{1 2 3}.log	15 MB	5 MB

Log type	Default file name and folder name	Maximum disk usage	File-switching timing
jimmelpasswd command log	<i>Console-path</i> \log\mail \jimmelpasswd_cmd{1 2 3}.log	768 KB	256 KB
	<i>Console-path</i> \log\mail \jimmelpasswd_cmdM{1 2 3}.log	768 KB	256 KB
	<i>Console-path</i> \log\mail\JIMMAILPASSWORD{1 2 3}.log	768 KB	256 KB
	<i>Console-path</i> \log\mail \jimmelpasswd_exe{1 2 3}.log	768 KB	256 KB

Note: The logs above are process-by-process trace logs. The process-by-process trace log is the log information that is output by each function of JP1/IM. It is output to a different log file depending on the function that is being used. Since the process-by-process trace log contains product information, its content is not made public.

#1: The file size may be dozens of kilobytes larger than this value.

#2: You can set this value to be from 65,536 bytes (64 kilobytes) to 104,857,600 bytes (100 megabytes), as described in *Automated action environment definition file (action.conf.update)* (in *Chapter 2. Definition Files*) in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

#3: You can set this value to be from 1 to 4,096 kilobytes, as described in *Automated action environment definition file (action.conf.update)* (in *Chapter 2. Definition Files*) in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

#4: This is the value when the size of the action information file is the default value (626 kilobytes). You can use the following estimation formula to estimate the maximum disk usage by this file. Each time an action is performed, the size increases by 5 kilobytes.

$((\text{action information file size} \div 64 \text{ bytes}) - 1) \times 5 \text{ kilobytes}$

#5: The files are output to the *jcochstat* and *jcoevtreport* command trace logs on the physical host in a cluster operation system as well.

#6: You can change the file count and file size as described in the *Correlation event generation environment definition file* (in *Chapter 2. Definition Files*) in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

#7: This file is used to output the memory information for inheriting data during correlation event generation, and therefore its size varies depending on the correlation event generation condition and the correlation-source event. For details about estimating the size of this file, see the JP1/IM - Manager release notes.

#8: This file is created when you start JP1/IM - Manager after enabling the response-waiting event management function.

Table 10–5: JP1/IM - Manager (Central Scope) log files and folders (Windows)

Log type	Default file name and folder name	Maximum disk usage	File-switching timing
Central Scope trace log	<i>Scope-path</i> \log\jcsmain{1 2 3}.log	6 MB	2 MB
	<i>Scope-path</i> \log\jcsmain_trace{1 2 3}.log	6 MB	2 MB
	<i>shared-folder</i> \JP1Scope\log\jcsmain{1 2 3}.log	6 MB	2 MB
	<i>shared-folder</i> \JP1Scope\log \jcsmain_trace{1 2 3}.log	6 MB	2 MB
Communication trace log	<i>Scope-path</i> \log\jcsmain_trace_com{1 2 3}.log	6 MB	2 MB
	<i>shared-folder</i> \JP1Scope\log \jcsmain_trace_com{1 2 3}.log	6 MB	2 MB
	<i>Scope-path</i> \log\jcsmain_trace_ping{1 2 3}.log	6 MB	2 MB
	<i>shared-folder</i> \JP1Scope\log \jcsmain_trace_ping{1 2 3}.log	6 MB	2 MB
Logical host settings program log	<i>Scope-path</i> \log\jplhasetup.{log log.old}	2,000 KB	1,000 KB

Log type	Default file name and folder name	Maximum disk usage	File-switching timing
Database operation API trace log	<i>Scope-path</i> \log\jcsmain_trace_db{1 2 3}.log	6 MB	2 MB
	<i>shared-folder</i> \JP1Scope\log\jcsmain_trace_db{1 2 3}.log	6 MB	2 MB
jcshostsexport command log	<i>Scope-path</i> \log\jcshostsexport{1 2 3}.log	6 MB	2 MB
	<i>shared-folder</i> \JP1Scope\log\jcshostsexport{1 2 3}.log	6 MB	2 MB
jcshostsimport command log	<i>Scope-path</i> \log\jcshostsimport{1 2 3}.log	6 MB	2 MB
	<i>shared-folder</i> \JP1Scope\log\jcshostsimport{1 2 3}.log	6 MB	2 MB
jcscdbsetup command log	<i>Scope-path</i> \log\jcscdbsetup{1 2 3}.log	6 MB	2 MB
	<i>shared-folder</i> \JP1Scope\log\jcscdbsetup{1 2 3}.log	6 MB	2 MB
jcschstat command log	<i>Scope-path</i> \log\jcschstat{1 2 3}.log	6 MB	2 MB
	<i>shared-folder</i> \JP1Scope\log\jcschstat{1 2 3}.log	6 MB	2 MB
jcscdbexport command log	<i>Scope-path</i> \log\jcscdbexport{1 2 3}.log	6 MB	2 MB
	<i>shared-folder</i> \JP1Scope\log\jcscdbexport{1 2 3}.log	6 MB	2 MB
jcscdbimport command log	<i>Scope-path</i> \log\jcscdbimport{1 2 3}.log	6 MB	2 MB
	<i>shared-folder</i> \JP1Scope\log\jcscdbimport{1 2 3}.log	6 MB	2 MB
jcscdbconvert command log	<i>Scope-path</i> \log\jcscdbconvert{1 2 3}.log	6 MB	2 MB
	<i>shared-folder</i> \JP1Scope\log\jcscdbconvert{1 2 3}.log	6 MB	2 MB
jplcsverup command log	<i>Scope-path</i> \log\jplcsverup_front{1 2 3}.log	6 MB	2 MB
jplcshaverup command log	<i>shared-folder</i> \JP1Scope\log\jplcshaverup_front{1 2 3}.log	6 MB	2 MB

Table 10–6: JP1/IM - Manager (IM Configuration Management) log files and folders (Windows)

Log type	Default file name and folder name	Maximum disk usage	File-switching timing
IM Configuration Management trace log	<i>Manager-path</i> \log\imcf\jcfallogtrap{1 2 3 4 5 6 7 8 9 10}.log	200 MB	10 MB
	<i>Manager-path</i> \log\imcf\jcfallogtrap_VM_trace{1 2 3}.log	3 MB	1 MB
	<i>Manager-path</i> \log\imcf\jcfallogtrap_trace_auth{1 2 3 4 5 6 7 8 9 10}.log	20 MB	2 MB
	<i>Manager-path</i> \log\imcf\jcfmain{1 2 3 4 5 6 7 8 9 10}.log	20 MB	2 MB

Log type	Default file name and folder name	Maximum disk usage	File-switching timing
	<i>Manager-path</i> \log\imcf\jcfmain_trace{1 2 3 4 5 6 7 8 9 10}.log	20 MB	2 MB
	<i>Manager-path</i> \log\imcf\jcfmain_VM_trace{1 2 3}.log	3 MB	1 MB
	<i>shared-folder</i> \JP1IMM\log\imcf\jcfallogtrap{1 2 3 4 5 6 7 8 9 10}.log	200 MB	10 MB
	<i>shared-folder</i> \JP1IMM\log\imcf\jcfallogtrap_VM_trace{1 2 3}.log	3 MB	1 MB
	<i>shared-folder</i> \JP1IMM\log\imcf\jcfallogtrap_trace_auth{1 2 3 4 5 6 7 8 9 10}.log	20 MB	2 MB
	<i>shared-folder</i> \JP1IMM\log\imcf\jcfmain{1 2 3 4 5 6 7 8 9 10}.log	20 MB	2 MB
	<i>shared-folder</i> \JP1IMM\log\imcf\jcfmain_trace{1 2 3 4 5 6 7 8 9 10}.log	20 MB	2 MB
	<i>shared-folder</i> \JP1IMM\log\imcf\jcfmain_VM_trace{1 2 3}.log	3 MB	1 MB
Communication trace log	<i>Manager-path</i> \log\imcf\jcfmain_trace_com{1 2 3 4 5 6 7 8 9 10}.log	20 MB	2 MB
	<i>Manager-path</i> \log\imcf\jcfmain_ping{1 2 3 4 5 6 7 8 9 10}.log	20 MB	2 MB
	<i>shared-folder</i> \JP1IMM\log\imcf\jcfmain_trace_com{1 2 3 4 5 6 7 8 9 10}.log	20 MB	2 MB
	<i>shared-folder</i> \JP1IMM\log\imcf\jcfmain_ping{1 2 3 4 5 6 7 8 9 10}.log	20 MB	2 MB
Authentication trace log	<i>Manager-path</i> \log\imcf\jcfmain_trace_auth{1 2 3 4 5 6 7 8 9 10}.log	20 MB	2 MB
	<i>shared-folder</i> \JP1IMM\log\imcf\jcfmain_trace_auth{1 2 3 4 5 6 7 8 9 10}.log	20 MB	2 MB
Logical host settings program log	<i>Manager-path</i> \log\imcf\jp1hasetup.{log log.old}	2,000 KB	1,000 KB
Database operation API trace log	<i>Manager-path</i> \log\imcf\jcfmain_trace_db{1 2 3 4 5 6 7 8 9 10}.log	20 MB	2 MB
	<i>shared-folder</i> \JP1IMM\log\imcf\jcfmain_trace_db{1 2 3 4 5 6 7 8 9 10}.log	20 MB	2 MB
Command common log	<i>Manager-path</i> \log\imcf\jcfcommand{1 2 3}.log	3 MB	1 MB

Log type	Default file name and folder name	Maximum disk usage	File-switching timing
	<i>shared-folder</i> \JP1IMM\log\imcf \jcfcommand{1 2 3}.log	3 MB	1 MB
jcfallogstart command log	<i>Manager-path</i> \log\imcf\jcfallogstart{1 2 3}.log	9 MB	3 MB
	<i>Manager-path</i> \log\imcf \jcfallogstart_VM_trace{1 2 3}.log	3 MB	1 MB
	<i>shared-folder</i> \JP1IMM\log\imcf \jcfallogstart{1 2 3}.log	9 MB	3 MB
	<i>shared-folder</i> \JP1IMM\log\imcf \jcfallogstart_VM_trace{1 2 3}.log	3 MB	1 MB
jcfallogstat command log	<i>Manager-path</i> \log\imcf\jcfallogstat{1 2 3}.log	9 MB	3 MB
	<i>Manager-path</i> \log\imcf \jcfallogstat_VM_trace{1 2 3}.log	3 MB	1 MB
	<i>shared-folder</i> \JP1IMM\log\imcf \jcfallogstat{1 2 3}.log	9 MB	3 MB
	<i>shared-folder</i> \JP1IMM\log\imcf \jcfallogstat_VM_trace{1 2 3}.log	3 MB	1 MB
jcfallogstop command log	<i>Manager-path</i> \log\imcf\jcfallogstop{1 2 3}.log	9 MB	3 MB
	<i>Manager-path</i> \log\imcf \jcfallogstop_VM_trace{1 2 3}.log	3 MB	1 MB
	<i>shared-folder</i> \JP1IMM\log\imcf \jcfallogstop{1 2 3}.log	9 MB	3 MB
	<i>shared-folder</i> \JP1IMM\log\imcf \jcfallogstop_VM_trace{1 2 3}.log	3 MB	1 MB
jcfallogreload command log	<i>Manager-path</i> \log\imcf\jcfallogreload{1 2 3}.log	9 MB	3 MB
	<i>Manager-path</i> \log\imcf \jcfallogreload_VM_trace{1 2 3}.log	3 MB	1 MB
	<i>shared-folder</i> \JP1IMM\log\imcf \jcfallogreload{1 2 3}.log	9 MB	3 MB
	<i>shared-folder</i> \JP1IMM\log\imcf \jcfallogreload_VM_trace{1 2 3}.log	3 MB	1 MB
jcfallogdef command log	<i>Manager-path</i> \log\imcf\jcfallogdef{1 2 3}.log	9 MB	3 MB
	<i>Manager-path</i> \log\imcf \jcfallogdef_VM_trace{1 2 3}.log	3 MB	1 MB
	<i>shared-folder</i> \JP1IMM\log\imcf \jcfallogdef{1 2 3}.log	9 MB	3 MB
	<i>shared-folder</i> \JP1IMM\log\imcf \jcfallogdef_VM_trace{1 2 3}.log	3 MB	1 MB
jcfaleltstart command log	<i>Manager-path</i> \log\imcf\jcfaleltstart{1 2 3}.log	6 MB	2 MB

Log type	Default file name and folder name	Maximum disk usage	File-switching timing
	<i>Manager-path</i> \log\imcf \jcfaleltstart_VM_trace{1 2 3}.log	3 MB	1 MB
	<i>shared-folder</i> \JP1IMM\log\imcf \jcfaleltstart{1 2 3}.log	6 MB	2 MB
	<i>shared-folder</i> \JP1IMM\log\imcf \jcfaleltstart_VM_trace{1 2 3}.log	3 MB	1 MB
jcfaleltstat command log	<i>Manager-path</i> \log\imcf\jcfaleltstat{1 2 3}.log	6 MB	2 MB
	<i>Manager-path</i> \log\imcf \jcfaleltstat_VM_trace{1 2 3}.log	3 MB	1 MB
	<i>shared-folder</i> \JP1IMM\log\imcf \jcfaleltstat{1 2 3}.log	6 MB	2 MB
	<i>shared-folder</i> \JP1IMM\log\imcf \jcfaleltstat_VM_trace{1 2 3}.log	3 MB	1 MB
jcfaleltstop command log	<i>Manager-path</i> \log\imcf\jcfaleltstop{1 2 3}.log	6 MB	2 MB
	<i>Manager-path</i> \log\imcf \jcfaleltstop_VM_trace{1 2 3}.log	3 MB	1 MB
	<i>shared-folder</i> \JP1IMM\log\imcf \jcfaleltstop{1 2 3}.log	6 MB	2 MB
	<i>shared-folder</i> \JP1IMM\log\imcf \jcfaleltstop_VM_trace{1 2 3}.log	3 MB	1 MB
jcfaleltreload command log	<i>Manager-path</i> \log\imcf\jcfaleltreload{1 2 3}.log	6 MB	2 MB
	<i>Manager-path</i> \log\imcf \jcfaleltreload_VM_trace{1 2 3}.log	3 MB	1 MB
	<i>shared-folder</i> \JP1IMM\log\imcf \jcfaleltreload{1 2 3}.log	6 MB	2 MB
	<i>shared-folder</i> \JP1IMM\log\imcf \jcfaleltreload_VM_trace{1 2 3}.log	3 MB	1 MB
jcfaleltdef command log	<i>Manager-path</i> \log\imcf\jcfaleltdef{1 2 3}.log	6 MB	2 MB
	<i>Manager-path</i> \log\imcf \jcfaleltdef_VM_trace{1 2 3}.log	3 MB	1 MB
	<i>shared-folder</i> \JP1IMM\log\imcf \jcfaleltdef{1 2 3}.log	6 MB	2 MB
	<i>shared-folder</i> \JP1IMM\log\imcf \jcfaleltdef_VM_trace{1 2 3}.log	3 MB	1 MB
jcfcolvmesx command log	<i>Manager-path</i> \log\imcf \jcfcolvmesx_trace{1 2 3}.log	3 MB	1 MB
jcfcolvmcvmm command log	<i>Manager-path</i> \log\imcf \jcfcolvmcvmm_trace{1 2 3}.log	3 MB	1 MB
jcfcolvmvirtage command log	<i>Manager-path</i> \log\imcf \jcfcolvmvirtage_trace{1 2 3}.log	3 MB	1 MB

Log type	Default file name and folder name	Maximum disk usage	File-switching timing
jcfcolumvc command log	<i>Manager-path</i> \log\imcf \jcfcolumvc_trace{1 2 3}.log	3 MB	1 MB
jcfcolumkvm command log	<i>Manager-path</i> \log\imcf \jcfcolumkvm_trace{1 2 3}.log	3 MB	1 MB
jcfcolumhcsn command log	<i>Manager-path</i> \log\imcf \jcfcolumhcsn_trace{1 2 3}.log	3 MB	1 MB
jcfexport command log	<i>Manager-path</i> \log\imcf \jcfexport_VM_trace{1 2 3}.log	3 MB	1 MB
	<i>shared-folder</i> \JP1IMM\log\imcf \jcfexport_VM_trace{1 2 3}.log	3 MB	1 MB
jcfimport command log	<i>Manager-path</i> \log\imcf \jcfimport_VM_trace{1 2 3}.log	3 MB	1 MB
	<i>shared-folder</i> \JP1IMM\log\imcf \jcfimport_VM_trace{1 2 3}.log	3 MB	1 MB
jcfmkhostsdata command log	<i>Manager-path</i> \log\imcf \jcfmkhostsdata_trace{1 2 3}.log	3 MB	1 MB
Stack trace log	<i>Manager-path</i> \log\imcf\javalog{1 2 3 4}.log	1 MB	At startup or 256 KB

Note: The logs above are process-by-process trace logs. The process-by-process trace log is the log information that is output by each function of JP1/IM. It is output to a different log file depending on the function that is being used. Since the process-by-process trace log contains product information, its content is not made public.

Table 10–7: JP1/IM - View log files and folders

Log type	Default file name and folder name	Maximum disk usage	File-switching timing
JP1/IM - View log ^{#1}	<i>View-path</i> \log\VIEW{1 2 3}.log	30,720 KB	10,240 KB
	<i>View-path</i> \log\jplconv{1 2 3 4}.log	20,480 KB	5,120 KB ^{#2}
	<i>View-path</i> \log\jplconvM{1 2... 60}.log	102,400 KB	5,120 KB ^{#2}
	<i>View-path</i> \log\jplcsov[_old].log	6,144 KB	3,072 KB ^{#2}
	<i>View-path</i> \log\jplcsovM[_old].log	6,144 KB	3,072 KB ^{#2}
	<i>View-path</i> \log\imrm\jplrmJP1-IM-RM View{1 2 3}.log ^{#3}	3,072 KB	1,024 KB
	<i>View-path</i> \log\imrm\jplrmJP1-IM-RM View_dbg{1 2 3}.log ^{#3}	3,072 KB	1,024 KB
	<i>View-path</i> \log\jrmview\view{1 2 3}.log ^{#3}	3,072 KB	1,024 KB
Stack trace log ^{#1}	<i>View-path</i> \log\javalog0{1 2}.log	512 KB	At startup or 256 KB
Integrated trace log	<i>system-drive</i> :\Program Files\Hitachi \HNTRLib2\spool\hntr2{1 2 3 4}.log	1,024 KB	256 KB
Product information log ^{#1}	<i>View-path</i> \log\hliclib\hliclibtrc{1 2 3 4 5}.log	5 MB	1 MB

Log type	Default file name and folder name	Maximum disk usage	File-switching timing
	<i>View-path</i> \log\hliclib\hlicliberr{1 2 3 4 5}.log	5 MB	1 MB
	<i>View-path</i> \log\hliclib\hliclibmgrtrc{1 2 3 4 5}.log	5 MB	1 MB
	<i>View-path</i> \log\hliclib\hliclibmgrerr{1 2 3 4 5}.log	5 MB	1 MB

Note: When you use Windows, replace *View-path*\log\ with *system-drive*:\ProgramData\Hitachi\jp1\jp1_default\JP1CoView\log\.

#1: This log is a process-by-process trace log. The process-by-process trace log is the log information that is output by each function of JP1/IM. It is output to a different log file depending on the function that is being used. Since the process-by-process trace log contains product information, its content is not made public.

#2: The file size may be dozens of kilobytes larger than this value.

#3: This log is output only when JP1/IM - Rule Operation is linked.

Table 10–8: JP1/IM - IM Configuration Management - View log files and folders

Log type	Default file name and folder name	Maximum disk usage	File-switching timing
IM Configuration Management trace log [#]	<i>View-path</i> \log\jcfview\VIEW{1 2 3}.log	30 MB	10 MB
Stack trace log [#]	<i>View-path</i> \log\jcfjavalog{1 2}.log	512 KB	At startup or 256 KB
Integrated trace log	<i>system-drive</i> :\Program Files\Hitachi\HNTRLib2\spool\hntr2{1 2 3 4}.log	1,024 KB	256 KB

Note: When you use Windows, replace *View-path*\log\ with *system-drive*:\ProgramData\Hitachi\jp1\jp1_default\JP1CoView\log\.

For Windows, the location represented by *system-drive*:\Program Files is determined at installation by an OS environment variable and might differ depending on the environment.

#: This log is a process-by-process trace log. The process-by-process trace log is the log information that is output by each function of JP1/IM. It is output to a different log file depending on the function that is being used. Since the process-by-process trace log contains product information, its content is not made public.

(2) In UNIX

The tables below show the default log files and folders that are output by the UNIX version of JP1/IM.

The *Log type* column lists the log types that are output by JP1/IM.

The *Default file name and folder name* column describes log file names as absolute paths when JP1/IM - Manager or JP1/Base is installed in the default mode. *Default file name and folder name* in a cluster operation system describes the log file names of shared folders as absolute paths.

The *Maximum disk usage* column shows the maximum disk space used by each log file. When there are multiple log files, the combined total is given.

The *File-switching timing* column shows how JP1/IM times output destination log file switching. When the file reaches the size shown in this column or when the event shown in this column occurs, the output destination is switched. If there are multiple log files and if the maximum disk usage is reached, files are overwritten, beginning with the ones that have the oldest update dates.

Table 10–9: JP1/IM - Manager (common to all components) log files and folders (UNIX)

Log type	Default file name and folder name	Maximum disk usage	File-switching timing
Operation log	/var/opt/jplimm/log/operationlog/ imm_operation{none 1 2... 16}.log ^{#1}	55 MB ^{#1}	5 MB ^{#1#2}
jimnodecount command log	/var/opt/jplimm/log/nodecount/ jimnodecount_cmd{1 2}.log	20 MB	10 MB

#1: You can change the output destination, the number of files that can be saved, and the file size. For details, see *Operation log definition file (imm_operationlog.conf)* (Chapter 2. Definition Files) in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*. The number of bytes shown in the Maximum disk usage and File-switching timing columns are the values used when the number of files that can be saved and the file size are set to initial values

#2: For details about the operation when switching the operation log file, see *K.2 Storage format of operation log output* in the *JP1/Integrated Management - Manager Overview and System Design Guide*.

Table 10–10: JP1/IM - Manager (Central Console) log files and directories (UNIX)

Log type	Default file name and directory name	Maximum disk usage	File-switching timing
Process management log ^{#1}	/var/opt/jplcons/log/JCO_SPMD{1 2 3}.log	384 KB	128 KB
	/var/opt/jplcons/log/ JCO_SPMD_COMMAND{1 2 3}.log	384 KB	128 KB
	<i>shared-directory</i> /jplcons/log/JCO_SPMD{1 2 3}.log	384 KB	128 KB
	<i>shared-directory</i> /jplcons/log/ JCO_SPMD_COMMAND{1 2 3}.log	384 KB	128 KB
Stack trace log ^{#1}	/var/opt/jplcons/log/javalog0{1 2 3 4}.log	1 MB	At startup or 256 KB
	<i>shared-directory</i> /jplcons/log/javalog0{1 2 3 4}.log	1 MB	At startup or 256 KB
JP1/IM startup log ^{#1}	/var/opt/jplcons/log/ jco_start.log[.old]	1 KB	At startup
	<i>shared-directory</i> /jplcons/log/ jco_start_logical-host-name.log[.old]	1 KB	At startup
JP1/IM kill log ^{#1, #2}	<i>shared-directory</i> /jplcons/log/ jco_killall.cluster{none 1 2 3 4}	2 KB	When the jco_killall.cluster command is executed
Setup log	/var/opt/jplcons/log/JCO_SETUP/ jco_setup.log	100 KB	During installation
	/var/opt/jplcons/log/JCO_SETUP/ jco_inst.log ^{#1}	100 KB	During installation
	/var/opt/jplcons/log/jco_setup/ <i>logical-host-name</i> / jco_setup.log ^{#1}	100 KB	During installation
	/var/opt/jplcons/log/jco_setup/ <i>logical-host-name</i> / reg.txt ^{#1}	100 KB	During installation
	/var/opt/jplcons/log/jco_setup/ <i>logical-host-name</i> / reg_def.txt ^{#1}	100 KB	During installation

Log type	Default file name and directory name	Maximum disk usage	File-switching timing
	/var/opt/jplcons/log/command/comdef[_old].log ^{#1}	512 KB	256 KB
Event console log ^{#1}	/var/opt/jplcons/log/console/EVCONS{1 2 3}.log	30,720 KB	10,240 KB
	/var/opt/jplcons/log/console/jplcons{1 2 3 4 5 6 7 8}.log	40,960 KB	5,120 KB ^{#3}
	/var/opt/jplcons/log/console/JCOAPI{1 2 3}.log	96 KB	32 KB
	/var/opt/jplcons/log/console/jplconsM{1 2... 60}.log	300 MB	5 MB ^{#3}
	/var/opt/jplcons/log/console/jpleventStormDef{1 2 3 4 5}.log	100 MB	20 MB
	/var/opt/jplcons/log/console/jplfilterDef{1 2 3 4 5}.log	100 MB	20 MB
	/var/opt/jplcons/log/console/jplbizGroupDef{1 2}.log	10 MB	5 MB
	/var/opt/jplcons/log/console/evtcon_exe{1 2 3}.log	256 KB × 3	256 KB
	/var/opt/jplcons/log/console/jplcmdButtonDef{1 2 3 4 5}.log	25 MB	5 MB
	/var/opt/jplcons/log/console/jplexattrnameDef{1 2 3 4 5}.log	25 MB	5 MB
	<i>shared-directory</i> /jplcons/log/console/EVCONS{1 2 3}.log	30,720 KB	10,240 KB
	<i>shared-directory</i> /jplcons/log/console/jplcons{1 2 3 4 5 6 7 8}.log	40,960 KB	5,120 KB ^{#3}
	<i>shared-directory</i> /jplcons/log/console/JCOAPI{1 2 3}.log	96 KB	32 KB
	<i>shared-directory</i> /jplcons/log/console/jplconsM{1 2... 60}.log	300 MB	5 MB ^{#3}
	<i>shared-directory</i> /jplcons/log/console/jpleventStormDef{1 2 3 4 5}.log	100 MB	20 MB
	<i>shared-directory</i> /jplcons/log/console/jplfilterDef{1 2 3 4 5}.log	100 MB	20 MB
	<i>shared-directory</i> /jplcons/log/console/jplbizGroupDef{1 2}.log	10 MB	5 MB
	<i>shared-directory</i> /jplcons/log/console/evtcon_exe{1 2 3}.log	256 KB × 3	256 KB
	<i>shared-directory</i> /jplcons/log/console/jplcmdButtonDef{1 2 3 4 5}.log	25 MB	5 MB
	<i>shared-directory</i> /jplcons/log/console/jplexattrnameDef{1 2 3 4 5}.log	25 MB	5 MB
Automated action trace log ^{#1}	/var/opt/jplcons/log/action/JCAMAIN{1 2 3 4 5}.log ^{#4}	25,600 KB	5,120 KB

Log type	Default file name and directory name	Maximum disk usage	File-switching timing
	<i>shared-directory</i> /jplcons/log/action/JCAMAIN{1 2 3 4 5}.log ^{#4}	25,600 KB	5,120 KB
Action information file ^{#1}	/var/opt/jplcons/log/action/actinf.log	626 KB ^{#5}	No switching
	<i>shared-directory</i> /jplcons/log/action/actinf.log	626 KB ^{#5}	No switching
Action host name file ^{#1}	/var/opt/jplcons/log/action/acttxt{1 2}.log	48.9 MB ^{#6}	When the action information file wraps around
	<i>shared-directory</i> /jplcons/log/action/acttxt{1 2}.log	48.9 MB ^{#6}	When the action information file wraps around
Action re-execution file ^{#1}	/var/opt/jplcons/log/action/actreaction	300 MB	When system switching occurs
	<i>shared-directory</i> /jplcons/log/action/actreaction	300 MB	When system switching occurs
jcochafmode, jcochstat, and jcoevtreport command trace logs ^{#1, #7}	/var/opt/jplcons/log/command/CMD{1 2 3}.log	3,072 KB	1,024 KB
	/var/opt/jplcons/log/command/jplcons_cmd{1 2}.log	12,288 KB	6,144 KB
	/var/opt/jplcons/log/command/jplconsM_cmd{1 2}.log	12,288 KB	6,144 KB
	/var/opt/jplcons/log/command/jplexattrnameDef_cmd{1 2 3 4 5}.log	25 MB	5 MB
Plug-in log ^{#1}	/var/opt/jplcons/log/command/jcoplugin{1 2 3}.log	3 MB	1 MB
Reporting status storage file ^{#1}	/var/opt/jplcons/log/notice/notice_stat.dat	72B	No switching
	<i>shared-directory</i> /jplcons/log/notice/notice_stat.dat	72B	No switching
Action definition backup file ^{#1}	/var/opt/jplcons/log/action/actdefbk.conf	2,048 KB	No switching
	<i>shared-directory</i> /jplcons/log/action/actdefbk.conf	2,048 KB	No switching
Event base trace log ^{#1}	/var/opt/jplcons/log/evflow/EVFLOW{1 2 3 4 5 6 7 8 9 10}.log	100 MB	10 MB
	/var/opt/jplcons/log/evflow/jplevflowM{1 2... 60}.log	300 MB	5 MB
	/var/opt/jplcons/log/evflow/jplactDef{1 2 3 4 5}.log	25 MB	5 MB
	/var/opt/jplcons/log/evflow/jplchsevDef{1 2 3 4 5}.log	25 MB	5 MB
	/var/opt/jplcons/log/evflow/jplchmsgDef{1 2 3 4 5}.log	25 MB	5 MB

Log type	Default file name and directory name	Maximum disk usage	File-switching timing
	/var/opt/jplcons/log/evflow/jplhostmapDef{1 2 3 4 5}.log	25 MB	5 MB
	/var/opt/jplcons/log/evflow/evflow_exe{1 2 3}.log	256 KB × 3	256 KB
	shared-directory/jplcons/log/evflow/EVFLOW{1 2 3 4 5 6 7 8 9 10}.log	100 MB	10 MB
	shared-directory/jplcons/log/evflow/jplevflowM{1 2... 60}.log	300 MB	5 MB
	shared-directory/jplcons/log/evflow/jplactDef{1 2 3 4 5}.log	25 MB	5 MB
	shared-directory/jplcons/log/evflow/jplchsevDef{1 2 3 4 5}.log	25 MB	5 MB
	shared-directory/jplcons/log/evflow/jplchmsgDef{1 2 3 4 5}.log	25 MB	5 MB
	shared-directory/jplcons/log/evflow/jplhostmapDef{1 2 3 4 5}.log	25 MB	5 MB
	shared-directory/jplcons/log/evflow/evflow_exe{1 2 3}.log	256 KB × 3	256 KB
Matching information file ^{#1}	/var/opt/jplcons/log/evflow/evflowinf.log	12B	No switching
	shared-directory/jplcons/log/evflow/evflowinf.log	12B	No switching
Event base error log ^{#1}	/var/opt/jplcons/log/evflow/jplevflow{1 2 3 4 5 6 7 8}.log	40,960 KB	5,120 KB
	shared-directory/jplcons/log/evflow/jplevflow{1 2 3 4 5 6 7 8}.log	40,960 KB	5,120 KB
Automated action error log ^{#1}	/var/opt/jplcons/log/action/jplact{1 2 3}.log	15,360 KB	5,120 KB
	shared-directory/jplcons/log/action/jplact{1 2 3}.log	15,360 KB	5,120 KB
Correlation event generation history file ^{#1}	/var/opt/jplcons/operation/evgen/egs_discrim{1 2 3}.log ^{#8}	30 MB ^{#8}	10 MB ^{#8}
	shared-directory/jplcons/operation/evgen/egs_discrim{1 2 3}.log ^{#8}	30 MB ^{#8}	10 MB ^{#8}
Common exclusion history file	/var/opt/jplcons/operation/comexclude/comexclude{1 2 3 4 5}.log	100 MB	20 MB
	shared-directory/jplcons/operation/comexclude/comexclude{1 2 3 4 5}.log	100 MB	20 MB
Common exclusion-conditions definition history file	/var/opt/jplcons/operation/comexclude/comexcludeDef{1 2 3 4 5}.log	100 MB	20 MB
	shared-directory/jplcons/operation/comexclude/comexcludeDef{1 2 3 4 5}.log	100 MB	20 MB

Log type	Default file name and directory name	Maximum disk usage	File-switching timing
Correlation event generation trace log #1	/var/opt/jplcons/log/evgen/EVGEN{1 2 3}.log	15 MB	5 MB
	/var/opt/jplcons/log/evgen/evgen_exe{1 2 3}.log	256 KB × 3	256 KB
	<i>shared-directory</i> /jplcons/log/evgen/EVGEN{1 2 3}.log	15 MB	5 MB
	<i>shared-directory</i> /jplcons/log/evgen/evgen_exe{1 2 3}.log	256 KB × 3	256 KB
Correlation event generation individual log (for Event Generation Service)#1	/var/opt/jplcons/log/evgen/jplegs{1 2}.log	20 MB	10 MB
	/var/opt/jplcons/log/evgen/jplegsM{1 2}.log	20 MB	10 MB
	<i>shared-directory</i> /jplcons/log/evgen/jplegs{1 2}.log	20 MB	10 MB
	<i>shared-directory</i> /jplcons/log/evgen/jplegsM{1 2}.log	20 MB	10 MB
Correlation event generation individual log (for commands)#1	/var/opt/jplcons/log/evgen/jplegs_cmd{1 2 3 4}.log	20 MB	5 MB
	/var/opt/jplcons/log/evgen/jplegsM_cmd{1 2 3 4}.log	20 MB	5 MB
Correlation event generation stack trace log#1	/var/opt/jplcons/log/evgen/javalog0{1 2 3 4}.log	1 MB	At startup or 256 KB
	<i>shared-directory</i> /jplcons/log/evgen/javalog0{1 2 3 4}.log	1 MB	At startup or 256 KB
Correlation event generation process inheriting definition file#1	/var/opt/jplcons/log/evgen/egs_discrim_info{1 2 3 4}.dat	312 MB#9	At termination
	<i>shared-directory</i> /jplcons/log/evgen/egs_discrim_info{1 2 3 4}.dat	312 MB#9	At termination
Correlation event generation definition application log#1	/var/opt/jplcons/log/evgen/jplegsDefine{1 2}.log	10 MB	5 MB
	<i>shared-directory</i> /jplcons/log/evgen/jplegsDefine{1 2}.log	10 MB	5 MB
File for accumulated response-waiting events#1, #10	/var/opt/jplcons/log/response/resevent.dat	40 MB	No switching
	<i>shared-directory</i> /jplcons/log/response/resevent.dat	40 MB	No switching
Backup file for accumulated response-waiting events#1, #10	/var/opt/jplcons/log/response/resevent.dat.dump	40 MB	No switching
	<i>shared-directory</i> /jplcons/log/response/resevent.dat.dump	40 MB	No switching
Integrated monitoring database application log#1	/var/opt/jplcons/log/evflow/EVFLOW_DBAPI{1 2... 16}.log	200 MB	12.5 MB
	/var/opt/jplcons/log/console/EVCONS_DBAPI{1 2 3 4 5}.log	50 MB	10 MB

Log type	Default file name and directory name	Maximum disk usage	File-switching timing
	/var/opt/jplcons/log/command/ CMD_DBAPI{1 2 3 4 5}.log	50 MB	10 MB
	<i>shared-directory</i> /jplcons/log/evflow/ EVFLOW_DBAPI{1 2... 16}.log	200 MB	12.5 MB
	<i>shared-directory</i> /jplcons/log/console/ EVCONS_DBAPI{1 2 3 4 5}.log	50 MB	10 MB
API log for the IM Configuration Management database ^{#1}	/var/opt/jplcons/log/evflow/ EVFLOW_CFDBAPI{1 2 3 4 5}.log	30 MB	10 MB
	/var/opt/jplcons/log/console/ EVCONS_CFDBAPI{1 2 3}.log	30 MB	10 MB
	/var/opt/jplcons/log/command/ CMD_CFDBAPI{1 2 3}.log	30 MB	10 MB
	<i>shared-directory</i> /jplcons/log/evflow/ EVFLOW_CFDBAPI{1 2 3 4 5}.log	30 MB	10 MB
	<i>shared-directory</i> /jplcons/log/console/ EVCONS_CFDBAPI{1 2 3}.log	30 MB	10 MB
jcodbsetup command log ^{#1}	/var/opt/jplcons/log/imdb/ jcodbsetup{1 2}.log	512 KB	256 KB
jcodbunsetup command log ^{#1}	/var/opt/jplcons/log/imdb/ jcodbunsetup{1 2}.log	512 KB	256 KB
Command execution history directory ^{#1}	/var/opt/jplbase/log/COMMAND/	See the <i>JPI/Base User's Guide</i> .	
	<i>shared-directory</i> /jplbase/log/COMMAND		
Remote command log ^{#1}	/var/opt/jplbase/log/JCOCMD/ jcocmd_result{1 2 3}.log		
	/var/opt/jplbase/log/JCOCMD/ jcocmdapi{1 2 3}.log		
	/var/opt/jplbase/log/JCOCMD/ jcocmdapi_trace{1 2 3}.log		
	/var/opt/jplbase/log/JCOCMD/ jcocmdcmc{1 2 3}.log		
	/var/opt/jplbase/log/JCOCMD/ jcocmdcmc_trace{1 2 3}.log		
	/var/opt/jplbase/log/JCOCMD/ jcocmdcom{1 2 3}.log		
	/var/opt/jplbase/log/JCOCMD/ jcocmdcom_trace{1 2 3}.log		
	/var/opt/jplbase/log/JCOCMD/ jcocmdexe{1 2 3}.log		
	/var/opt/jplbase/log/JCOCMD/ jcocmdexe_trace{1 2 3}.log		
/var/opt/jplbase/log/JCOCMD/ jcocmdrouter{1 2 3}.log			

Log type	Default file name and directory name	Maximum disk usage	File-switching timing
	<code>/var/opt/jp1base/log/JCOCMD/jcocmdrouter_trace{1 2 3}.log</code>		
	<code>/var/opt/jp1base/log/JCOCMD/JCOCMDCMD{1 2 3}.log</code>		
	<code>shared-directory/jp1base/log/JCOCMD/jcocmd_result{1 2 3}.log</code>		
	<code>shared-directory/jp1base/log/JCOCMD/jcocmdapi{1 2 3}.log</code>		
	<code>shared-directory/jp1base/log/JCOCMD/jcocmdapi_trace{1 2 3}.log</code>		
	<code>shared-directory/jp1base/log/JCOCMD/jcocmdcmc{1 2 3}.log</code>		
	<code>shared-directory/jp1base/log/JCOCMD/jcocmdcmc_trace{1 2 3}.log</code>		
	<code>shared-directory/jp1base/log/JCOCMD/jcocmdcom{1 2 3}.log</code>		
	<code>shared-directory/jp1base/log/JCOCMD/jcocmdcom_trace{1 2 3}.log</code>		
	<code>shared-directory/jp1base/log/JCOCMD/jcocmdexe{1 2 3}.log</code>		
	<code>shared-directory/jp1base/log/JCOCMD/jcocmdexe_trace{1 2 3}.log</code>		
	<code>shared-directory/jp1base/log/JCOCMD/jcocmdrouter{1 2 3}.log</code>		
	<code>shared-directory/jp1base/log/JCOCMD/jcocmdrouter_trace{1 2 3}.log</code>		
	<code>shared-directory/jp1base/log/JCOCMD/JCOCMDCMD{1 2 3}.log</code>		
Configuration management log ^{#1}	<code>/var/opt/jp1base/log/route/JBSRT{1 2 3}.log</code>		
	<code>shared-directory/jp1base/log/route/JBSRT{1 2 3}.log</code>		
Trace log file ^{#1}	<code>/var/opt/jp1base/sys/tmp/event/logtrap/jeallog/jeallog{1 2 3 4 5}.log</code>		

#1: This log is a process-by-process trace log. The process-by-process trace log is the log information that is output by each function of JP1/IM. It is output to a different log file depending on the function that is being used. Since the process-by-process trace log contains product information, its content is not made public.

#2: This log is created only in a cluster environment.

#3: The file size may be dozens of kilobytes larger than this value.

#4: You can set this value to be from 64 kilobytes to 100 megabytes, as described in *Automated action environment definition file (action.conf.update)* (in Chapter 2. Definition Files) in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

#5: You can set this value to be from 1 to 4,096 kilobytes as described in *Automated action environment definition file (action.conf.update)* (in Chapter 2. Definition Files) in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

#6: This is the value when the size of the action information file is the default value (626 kilobytes). You can use the following estimation formula to estimate the maximum disk usage by this file. Each time an action is performed, the size increases by 5 kilobytes.

((action information file size ÷ 64 bytes) - 1) × 5 kilobytes

#7: The files are output to the `jcchostat` and `jcchafmode` command trace logs on the physical host in a cluster operation system as well.

#8: You can change the file count and file size as described in *Correlation event generation environment definition file* (in Chapter 2. *Definition Files*) in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

#9: This file is used to output the memory information for inheriting data during correlation event generation, and therefore its size varies depending on the correlation event generation condition and the correlation-source event. For details about estimating the size of this file, see the JP1/IM - Manager release notes.

#10: This file is created when you start JP1/IM - Manager after enabling the response-waiting event management function.

Table 10–11: JP1/IM - Manager (Central Scope) log files and directories (UNIX)

Log type	Default file name and directory name	Maximum disk usage	File-switching timing
Central Scope trace log [#]	<code>/var/opt/jp1scope/log/jcsmain{1 2 3}.log</code>	6 MB	2 MB
	<code>/var/opt/jp1scope/log/jcsmain_trace{1 2 3}.log</code>	6 MB	2 MB
	<code>shared-directory/jp1scope/log/jcsmain{1 2 3}.log</code>	6 MB	2 MB
	<code>shared-directory/jp1scope/log/jcsmain_trace{1 2 3}.log</code>	6 MB	2 MB
Communication trace log	<code>/var/opt/jp1scope/log/jcsmain_trace_com{1 2 3}.log</code>	6 MB	2 MB
	<code>shared-directory/jp1scope/log/jcsmain_trace_com{1 2 3}.log</code>	6 MB	2 MB
	<code>/var/opt/jp1scope/log/jcsmain_trace_ping{1 2 3}.log</code>	6 MB	2 MB
	<code>shared-directory/jp1scope/log/jcsmain_trace_ping{1 2 3}.log</code>	6 MB	2 MB
Database operation API trace log	<code>/var/opt/jp1scope/log/jcsmain_trace_db{1 2 3}.log</code>	6 MB	2 MB
	<code>shared-directory/jp1scope/log/jcsmain_trace_db{1 2 3}.log</code>	6 MB	2 MB
jcshostsexport command log	<code>/var/opt/jp1scope/log/jcshostsexport{1 2 3}.log</code>	6 MB	2 MB
	<code>shared-directory/jp1scope/log/jcshostsexport{1 2 3}.log</code>	6 MB	2 MB
jcshostsimport command log	<code>/var/opt/jp1scope/log/jcshostsimport{1 2 3}.log</code>	6 MB	2 MB
	<code>shared-directory/jp1scope/log/jcshostsimport{1 2 3}.log</code>	6 MB	2 MB
jcscdbsetup command log	<code>/var/opt/jp1scope/log/jcscdbsetup{1 2 3}.log</code>	6 MB	2 MB
	<code>shared-directory/jp1scope/log/jcscdbsetup{1 2 3}.log</code>	6 MB	2 MB
jcschstat command log	<code>/var/opt/jp1scope/log/jcschstat{1 2 3}.log</code>	6 MB	2 MB
	<code>shared-directory/jp1scope/log/jcschstat{1 2 3}.log</code>	6 MB	2 MB

Log type	Default file name and directory name	Maximum disk usage	File-switching timing
jcsdbimport command log	/var/opt/jp1scope/log/jcsdbimport{1 2 3}.log	6 MB	2 MB
	<i>shared-directory</i> /jp1scope/log/jcsdbimport{1 2 3}.log	6 MB	2 MB
jcsdbexport command log	/var/opt/jp1scope/log/jcsdbexport{1 2 3}.log	6 MB	2 MB
	<i>shared-directory</i> /jp1scope/log/jcsdbexport{1 2 3}.log	6 MB	2 MB
Setup log	/var/opt/jp1scope/log/JCS_SETUP/jcs_setup.log	100 KB	During installation
	/var/opt/jp1scope/log/jcs_setup/logical-host-name/jcs_setup.log	100 KB	During installation
	/var/opt/jp1scope/log/jcs_setup/logical-host-name/reg.txt	100 KB	During installation
	/var/opt/jp1scope/log/jcs_setup/logical-host-name/reg_def.txt	100 KB	During installation

#: This log is a process-by-process trace log. The process-by-process trace log is the log information that is output by each function of JP1/IM. It is output to a different log file depending on the function that is being used. Since the process-by-process trace log contains product information, its content is not made public.

Table 10–12: JP1/IM - Manager (IM Configuration Management) log files and folders (UNIX)

Log type	Default file name and directory name	Maximum disk usage	File-switching timing
IM Configuration Management trace log	/var/opt/jp1imm/log/imcf/jcfallogtrap{1 2 3 4 5 6 7 8 9 10}.log	200 MB	10 MB
	/var/opt/jp1imm/log/imcf/jcfallogtrap_VM_trace{1 2 3}.log	3 MB	1 MB
	/var/opt/jp1imm/log/imcf/jcfallogtrap_trace_auth{1 2 3 4 5 6 7 8 9 10}.log	20 MB	2 MB
	/var/opt/jp1imm/log/imcf/jcfmain{1 2 3 4 5 6 7 8 9 10}.log	20 MB	2 MB
	/var/opt/jp1imm/log/imcf/jcfmain_trace{1 2 3 4 5 6 7 8 9 10}.log	20 MB	2 MB
	/var/opt/jp1imm/log/imcf/jcfmain_VM_trace{1 2 3}.log	3 MB	1 MB
	<i>shared-directory</i> /jp1imm/log/imcf/jcfallogtrap{1 2 3 4 5 6 7 8 9 10}.log	200 MB	10 MB
	<i>shared-directory</i> /jp1imm/log/imcf/jcfallogtrap_VM_trace{1 2 3}.log	3 MB	1 MB
	<i>shared-directory</i> /jp1imm/log/imcf/jcfallogtrap_trace_auth{1 2 3 4 5 6 7 8 9 10}.log	20 MB	2 MB

Log type	Default file name and directory name	Maximum disk usage	File-switching timing
	<i>shared-directory</i> /jplimm/log/imcf/ jcfmain{1 2 3 4 5 6 7 8 9 10}.log	20 MB	2 MB
	<i>shared-directory</i> /jplimm/log/imcf/ jcfmain_trace{1 2 3 4 5 6 7 8 9 10}.log	20 MB	2 MB
	<i>shared-directory</i> /jplimm/log/imcf/ jcfmain_VM_trace{1 2 3}.log	3 MB	1 MB
Communication trace log	/var/opt/jplimm/log/imcf/ jcfmain_trace_com{1 2 3 4 5 6 7 8 9 10}.log	20 MB	2 MB
	/var/opt/jplimm/log/imcf/ jcfmain_ping{1 2 3 4 5 6 7 8 9 10}.log	20 MB	2 MB
	<i>shared-directory</i> /jplimm/log/imcf/ jcfmain_trace_com{1 2 3 4 5 6 7 8 9 10}.log	20 MB	2 MB
	<i>shared-directory</i> /jplimm/log/imcf/ jcfmain_ping{1 2 3 4 5 6 7 8 9 10}.log	20 MB	2 MB
Authentication trace log	/var/opt/jplimm/log/imcf/ jcfmain_trace_auth{1 2 3 4 5 6 7 8 9 10}.log	20 MB	2 MB
	<i>shared-directory</i> /jplimm/log/imcf/ jcfmain_trace_auth{1 2 3 4 5 6 7 8 9 10}.log	20 MB	2 MB
Database operation API trace log	/var/opt/jplimm/log/imcf/ jcfmain_trace_db{1 2 3 4 5 6 7 8 9 10}.log	20 MB	2 MB
	<i>shared-directory</i> /jplimm/log/imcf/ jcfmain_trace_db{1 2 3 4 5 6 7 8 9 10}.log	20 MB	2 MB
Command common log	/var/opt/jplimm/log/imcf/ jcfcommand{1 2 3}.log	3 MB	1 MB
	<i>shared-directory</i> /jplimm/log/imcf/ jcfcommand{1 2 3}.log	3 MB	1 MB
jcfallogstart command log	/var/opt/jplimm/log/imcf/ jcfallogstart{1 2 3}.log	9 MB	3 MB
	/var/opt/jplimm/log/imcf/ jcfallogstart_VM_trace{1 2 3}.log	3 MB	1 MB
	<i>shared-directory</i> /jplimm/log/imcf/ jcfallogstart{1 2 3}.log	9 MB	3 MB
	<i>shared-directory</i> /jplimm/log/imcf/ jcfallogstart_VM_trace{1 2 3}.log	3 MB	1 MB
jcfallogstat command log	/var/opt/jplimm/log/imcf/ jcfallogstat{1 2 3}.log	9 MB	3 MB
	/var/opt/jplimm/log/imcf/ jcfallogstat_VM_trace{1 2 3}.log	3 MB	1 MB

Log type	Default file name and directory name	Maximum disk usage	File-switching timing
	<i>shared-directory</i> /jplimm/log/imcf/ jcfallogstat{1 2 3}.log	9 MB	3 MB
	<i>shared-directory</i> /jplimm/log/imcf/ jcfallogstat_VM_trace{1 2 3}.log	3 MB	1 MB
jcfallogstop command log	/var/opt/jplimm/log/imcf/ jcfallogstop{1 2 3}.log	9 MB	3 MB
	/var/opt/jplimm/log/imcf/ jcfallogstop_VM_trace{1 2 3}.log	3 MB	1 MB
	<i>shared-directory</i> /jplimm/log/imcf/ jcfallogstop{1 2 3}.log	9 MB	3 MB
	<i>shared-directory</i> /jplimm/log/imcf/ jcfallogstop_VM_trace{1 2 3}.log	3 MB	1 MB
jcfallogreload command log	/var/opt/jplimm/log/imcf/ jcfallogreload{1 2 3}.log	9 MB	3 MB
	/var/opt/jplimm/log/imcf/ jcfallogreload_VM_trace{1 2 3}.log	3 MB	1 MB
	<i>shared-directory</i> /jplimm/log/imcf/ jcfallogreload{1 2 3}.log	9 MB	3 MB
	<i>shared-directory</i> /jplimm/log/imcf/ jcfallogreload_VM_trace{1 2 3}.log	3 MB	1 MB
jcfallogdef command log	/var/opt/jplimm/log/imcf/ jcfallogdef{1 2 3}.log	9 MB	3 MB
	/var/opt/jplimm/log/imcf/ jcfallogdef_VM_trace{1 2 3}.log	3 MB	1 MB
	<i>shared-directory</i> /jplimm/log/imcf/ jcfallogdef{1 2 3}.log	9 MB	3 MB
	<i>shared-directory</i> /jplimm/log/imcf/ jcfallogdef_VM_trace{1 2 3}.log	3 MB	1 MB
jcfcolvmesx command log	<i>Manager-path</i> \log\imcf \jcfcolvmesx_trace{1 2 3}.log	3 MB	1 MB
jcfcolvmvirtage command log	<i>Manager-path</i> \log\imcf \jcfcolvmvirtage_trace{1 2 3}.log	3 MB	1 MB
jcfcolvmvc command log	<i>Manager-path</i> \log\imcf \jcfcolvmvc_trace{1 2 3}.log	3 MB	1 MB
jcfcolvmkvm command log	<i>Manager-path</i> \log\imcf \jcfcolvmkvm_trace{1 2 3}.log	3 MB	1 MB
jcfcolvmhscsm command log	<i>Manager-path</i> \log\imcf \jcfcolvmhscsm_trace{1 2 3}.log	3 MB	1 MB
jcfexport command log	/var/opt/jplimm/log/imcf/ jcfexport_VM_trace{1 2 3}.log	3 MB	1 MB
	<i>shared-directory</i> /jplimm/log/imcf/ jcfexport_VM_trace{1 2 3}.log	3 MB	1 MB
jcfimport command log	/var/opt/jplimm/log/imcf/ jcfimport_VM_trace{1 2 3}.log	3 MB	1 MB

Log type	Default file name and directory name	Maximum disk usage	File-switching timing
	<i>shared-directory</i> /jplimm/log/imcf/ jcfimport_VM_trace{1 2 3}.log	3 MB	1 MB
jcfmkhostsdata command log	/var/opt/jplimm/log/imcf/ jcfmkhostsdata_trace{1 2 3}.log	3 MB	1 MB
Stack trace log	/var/opt/jplimm/log/imcf/javalog0{1 2 3 4}.log	1 MB	At startup or 256 KB
Setup log	/var/opt/jplimm/log/imcf/JCF_SETUP/ jcf_setup.log	100 KB	During installation
	/var/opt/jplimm/log/imcf/JCF_SETUP/ <i>logical-host-name</i> /jcf_setup.log	100 KB	During installation

Note: The logs above are process-by-process trace logs. The process-by-process trace log is the log information that is output by each function of JP1/IM. It is output to a different log file depending on the function that is being used. Since the process-by-process trace log contains product information, its content is not made public.

10.3 Data that needs to be collected when a problem occurs

This section describes the data that needs to be collected when a problem occurs.

Note that JP1 provides *data collection tools* for batch-collecting the necessary data. The data that can be collected using a data collection tool is the OS system information and JP1 information. The following subsections explain data collection in Windows and UNIX.

10.3.1 In Windows

(1) OS system information

You need to collect the OS-related information listed in the table below. These types of information can be collected using data collection tools.

The two data collection tools (the `jim_log.bat` command and the `jcoview_log.bat` command) collect different types of data. When the `jim_log.bat` command is executed, all of the data listed in the table below is collected. The data that can be collected by executing the `jcoview_log.bat` command is indicated in the far-right column.

Table 10–13: OS system information (Windows)

Information type	Collected data	File name#1	View
Data collection date/time	<ul style="list-style-type: none"> date /t execution result time /t execution result 	date.log	Y
Hitachi integrated installer log file	Files under <i>Windows-installation-folder</i> \Temp\HCDINST\	Copies of the files indicated at left	Y
JP1/IM - Manager installation/uninstallation log file	<i>Windows-installation-folder</i> \Temp \HITACHI_JP1_INST_LOG \jplimm_inst{1 2 3 4 5}.log	jplimm_inst{1 2 3 4 5}.log	Δ
JP1/IM - View installation/uninstallation log file	<i>Windows-installation-folder</i> \Temp \HITACHI_JP1_INST_LOG \jplcoview_inst{1 2 3 4 5}.log	jplcoview_inst{1 2 3 4 5}.log	Y
JP1/Base installation/uninstallation log file	<i>Windows-installation-folder</i> \Temp \HITACHI_JP1_INST_LOG \jplbase_inst{1 2 3 4 5}.log	jplbase_inst{1 2 3 4 5}.log	Δ
Product information log file	Files under <i>Windows-installation-folder</i> \Temp\jplcommon\	Copies of the files indicated at left	Y
Host name settings that are set in the machine	<i>system-root-folder</i> \system32\drivers\etc\hosts	Hosts	Y
Service port settings that are set in the machine	<i>system-root-folder</i> \system32\drivers\etc \services	Services	Y
NIC installation status	ipconfig /all execution result	ipconfig.log	Y
Startup service list	net start execution result	netstart.log	Y
Network statistical information	netstat -nao execution result	netstat.log	Y

Information type	Collected data	File name#1	View
Machine's environment variable	set execution result	set.log	Y
Machine's system information	msinfo32 /report-file-name execution result	msinfo32.log	Y
Registry information	Content of the registry HKEY_LOCAL_MACHINE\SOFTWARE\HITACHI or HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\HITACHI collected by the reg command	hitachi_reg.txt	Y
Product information file	Files under <i>system-drive</i> :Program Files\jplcommon\	Copies of the files indicated at left	Y
JP1/IM - Manager installation information	<i>system-drive</i> :Program Files\InstallShield Installation Information\{BB5D25EC-537C-4794-BD7A-C7E22CC4AD30}\setup.ini	imm_setup.ini	Δ
JP1/IM - Manager installation log file	<i>system-drive</i> :Program Files\InstallShield Installation Information\{BB5D25EC-537C-4794-BD7A-C7E22CC4AD30}\setup.ilg	imm_setup.ilg	Δ
JP1/Base installation information	<i>system-drive</i> :Program Files\InstallShield Installation Information\{F8C71F7C-E5DE-11D3-A21E-006097C00EBC}\setup.ini	base_setup.ini	Δ
JP1/Base installation log file	<i>system-drive</i> :Program Files\InstallShield Installation Information\{F8C71F7C-E5DE-11D3-A21E-006097C00EBC}\setup.ilg	base_setup.ilg	Δ
JP1/IM - View installation information	<i>system-drive</i> :Program Files\InstallShield Installation Information\{6C01AA81-B45B-4AA6-ACE9-AC9A86B19F1F}\setup.ini	imv_setup.ini	Y
JP1/IM - View installation log file	<i>system-drive</i> :Program Files\InstallShield Installation Information\{6C01AA81-B45B-4AA6-ACE9-AC9A86B19F1F}\setup.ilg	imv_setup.ilg	Y
JP1/Base access permission information (installation folder)	cacls <i>Base-path</i> execution result	cacls_jplbase.log	Δ
	cacls <i>shared-folder</i> \JP1Base execution result#2	cacls_jplbase.log	--
JP1/Base access permission information (log folder)	cacls <i>Base-path</i> \log execution result	cacls_jplbase_log.log	Δ
	cacls <i>shared-folder</i> \JP1Base\log execution result#2	cacls_jplbase_log.log	--

Information type	Collected data	File name#1	View
JP1/Base access permission information (command execution history folder)	cacls <i>Base-path</i> \log\COMMAND execution result	cacls_jp1base_log_COMMAND.log	Δ
	cacls <i>shared-folder</i> \JP1Base\log\COMMAND execution result#2	cacls_jp1base_log_COMMAND.log	--
JP1/Base access permission information (event database folder)	cacls <i>Base-path</i> \sys execution result	cacls_jp1base_sys.log	Δ
JP1/Base access permission information (event database folder)	cacls <i>Base-path</i> \sys\event execution result	cacls_jp1base_sys_event.log	Δ
	cacls <i>shared-folder</i> \JP1Base\event execution result#2	cacls_jp1base_event.log	--
JP1/Base access permission information (event database folder)	cacls <i>Base-path</i> \sys\event\servers execution result	cacls_jp1base_sys_event_servers.log	Δ
JP1/Base access permission information (event database folder)	cacls <i>Base-path</i> \sys\event\servers\default execution result	cacls_jp1base_sys_event_servers_default.log	Δ
JP1/IM - Manager (Central Console) access permission information (installation folder)	cacls <i>Console-path</i> execution result	cacls_jp1cons.log	Δ
	cacls <i>shared-folder</i> \JP1Cons execution result#2	cacls_jp1cons.log	--
JP1/IM - Manager (Central Console) access permission information (log folder)	cacls <i>Console-path</i> \log execution result	cacls_jp1cons_log.log	Δ
	cacls <i>shared-folder</i> \JP1Cons\log execution result#2	cacls_jp1cons_log.log	--
JP1/IM - Manager (Central Console) access permission information (correlation history folder)	cacls <i>Console-path</i> \operation execution result	cacls_jp1cons_operation.log	Δ
	cacls <i>shared-folder</i> \JP1Cons\operation execution result#2	cacls_jp1cons_operation.log	--
JP1/IM - Manager (Central Console) access permission information (correlation event generation history folder)	cacls <i>Console-path</i> \operation\evgen execution result	cacls_jp1cons_operation_evgen.log	Δ
	cacls <i>shared-folder</i> \JP1Cons\operation\evgen execution result#2	cacls_jp1cons_operation_evgen.log	--
JP1/IM - Manager (Central Console) access permission information (common exclusion history folder)	cacls <i>Console-path</i> \operation\comexclude execution result	cacls_jp1cons_operation_comexclude.log	Δ
JP1/IM - View access permission information (installation folder)	cacls <i>View-path</i> execution result	cacls_jp1coview.log	Y
JP1/IM - View access permission information (log folder)	cacls <i>system-drive</i> :\ProgramData\Hitachi\jp1\jp1_default\JP1CoView\log execution result	cacls_programdata_jp1coview_log.log	Y
JP1/IM - Manager access permission information (installation folder)	cacls <i>Manager-path</i> execution result	cacls_jp1imm.log	Δ

Information type	Collected data	File name#1	View
JP1/IM - Manager access permission information (log folder)	cacls <i>Manager-path</i> \log execution result	cacls_jplimm_log.log	Δ
JP1/IM - Manager (Central Scope) access permission information (installation folder)	cacls <i>Scope-path</i> execution result	cacls_jplscope.log	Δ
	cacls <i>shared-folder</i> \JP1Scope execution result#2	cacls_jplscope.log	--
JP1/IM - Manager (Central Scope) access permission information (log folder)	cacls <i>Scope-path</i> \log execution result	cacls_jplscope_log.log	Δ
	cacls <i>shared-folder</i> \JP1Scope\log execution result#2	cacls_jplscope_log.log	--
JP1/IM - Manager (Central Scope) access permission information (database folder)	cacls <i>Scope-path</i> \database execution result	cacls_jplscope_database.log	Δ
	cacls <i>shared-folder</i> \JP1Scope\database execution result#2	cacls_jplscope_database.log	--
JP1/IM - Manager (Central Scope) access permission information (database folder)	cacls <i>Scope-path</i> \database\event execution result	cacls_jplscope_database_event.log	Δ
	cacls <i>shared-folder</i> \JP1Scope\database\event execution result#2	cacls_jplscope_database_event.log	--
JP1/IM - Manager (Central Scope) access permission information (database folder)	cacls <i>Scope-path</i> \database\jcsdb execution result	cacls_jplscope_database_jcsdb.log	Δ
	cacls <i>shared-folder</i> \JP1Scope\database\jcsdb execution result#2	cacls_jplscope_database_jcsdb.log	--
JP1/IM - Manager (Central Scope) access permission information (database folder)	cacls <i>Scope-path</i> \database\jcsdb\event execution result	cacls_jplscope_database_jcsdb_event.log	Δ
	cacls <i>shared-folder</i> \JP1Scope\database\jcsdb\event execution result#2	cacls_jplscope_database_jcsdb_event.log	--
JP1/IM - Manager (Central Scope) access permission information (database folder)	cacls <i>Scope-path</i> \database\jcsdb\pw execution result	cacls_jplscope_database_jcsdb_pw.log	Δ
	cacls <i>shared-folder</i> \JP1Scope\database\jcsdb\pw execution result#2	cacls_jplscope_database_jcsdb_pw.log	--
JP1/IM - Manager (Central Scope) access permission information (database folder)	cacls <i>Scope-path</i> \database\jcsdb\tree execution result	cacls_jplscope_database_jcsdb_tree.log	Δ
	cacls <i>shared-folder</i> \JP1Scope\database\jcsdb\tree execution result#2	cacls_jplscope_database_jcsdb_tree.log	--
JP1/IM - Manager (Central Scope) access permission information (database folder)	cacls <i>Scope-path</i> \database\jcsdbhosts execution result	cacls_jplscope_database_jcsdbhosts.log	Δ
	cacls <i>shared-folder</i> \JP1Scope\database\jcsdbhosts execution result#2	cacls_jplscope_database_jcsdbhosts.log	--
Access permission information for the operation log file output destination	cacls <i>operation-log-output-destination</i> execution result	cacls_jplimm_operationlog.log	Δ

Information type	Collected data	File name#1	View
	<p><i>operation-log-output-destination</i> indicates the folder specified in the following common definition: [JP1_DEFAULT\JP1IMM \OPERATION] "LOGFILEDIR"</p>		
	<p><i>cacls operation-log-output-destination</i> execution result <i>operation-log-output-destination</i> indicates the folder specified in the following common definition: [logical-host-name\JP1IMM \OPERATION] "LOGFILEDIR"</p>	cacls_jplimm_operationlog.log	--
JP1/Base file list	dir <i>Base-path</i> /s execution result	dir_jplbase.log	Δ
	dir <i>shared-folder</i> \JP1Base /s execution result#2	dir_logical-host-name_jplbase.log	--
JP1/IM - Manager (Central Console) file list	dir <i>Console-path</i> /s execution result	dir_jplcons.log	Δ
	dir <i>shared-folder</i> \JP1Cons /s execution result#2	dir_logical-host-name_jplcons.log	--
JP1/IM - View file list	dir <i>View-path</i> /s execution result	dir_jplcoview.log	Y
	Only for Windows dir <i>system-drive</i> :\ProgramData \Hitachi\jpl\jpl_default \JP1CoView /s execution result	dir_programdata_jplcoview.log	Y
JP1/IM - Manager file list	dir <i>Manager-path</i> /s execution result	dir_jplimm.log	Δ
JP1/IM - Manager (Central Scope) file list	dir <i>Scope-path</i> /s execution result	dir_jplscope.log	Δ
	dir <i>shared-folder</i> \JP1Scope /s execution result#2	dir_logical-host-name_jplscope.log	--
List of files at the operation log output destination	dir <i>operation-log-output-destination</i> /s execution result <i>operation-log-output-destination</i> indicates the folder specified in the following common definition: [JP1_DEFAULT\JP1IMM \OPERATION] "LOGFILEDIR"	dir_jplimm_operationlog.log	Δ
	dir <i>operation-log-output-destination</i> /s execution result <i>operation-log-output-destination</i> indicates the folder specified in the following common definition: [logical-host-name\JP1IMM \OPERATION] "LOGFILEDIR"	dir_jplimm_operationlog.log	--
Host name for resolving network address	jbsgethostbyname execution result	<ul style="list-style-type: none"> jbsgethostbyname.log (standard output) 	Δ

Information type	Collected data	File name ^{#1}	View
		<ul style="list-style-type: none"> • jbsgethostbyname_err.log (standard error) 	
	jbsgethostbyname <i>logical-host-name</i> execution result ^{#2}	<ul style="list-style-type: none"> • jbsgethostbyname.log (standard output) • jbsgethostbyname_err.log (standard error) 	--
Health check	jbshcstatus -debug -a execution result	<ul style="list-style-type: none"> • jbshcstatus.log (standard output) • jbshcstatus_err.log (standard error) 	Δ
	jbshcstatus -debug -a -h <i>logical-host-name</i> execution result ^{#2}	<ul style="list-style-type: none"> • jbshcstatus.log (standard output) • jbshcstatus_err.log (standard error) 	--
Process operation status of Event Service	jevstat execution result	<ul style="list-style-type: none"> • jevstat.log (standard output) • jevstat_err.log (standard error) 	Δ
	<ul style="list-style-type: none"> • jevstat <i>logical-host-name</i> execution result 	<ul style="list-style-type: none"> • jevstat.log (standard output) • jevstat_err.log (standard error) 	--
Process operation status of items other than Event Service	jbs_spm�_status execution result	<ul style="list-style-type: none"> • jbs_spm�_status.log (standard output) • jbs_spm�_status_err.log (standard error) 	Δ
	jbs_spm�_status -h <i>logical-host-name</i> execution result ^{#2}	<ul style="list-style-type: none"> • jbs_spm�_status.log (standard output) • jbs_spm�_status_err.log (standard error) 	--
Automated action execution result	jcashowa execution result ^{#5}	<ul style="list-style-type: none"> • jcashowa.log (standard output) • jcashowa_err.log (standard error) 	Δ
	jcashowa -h <i>logical-host-name</i> execution result ^{#2, #5}	<ul style="list-style-type: none"> • jcashowa.log (standard output) • jcashowa_err.log (standard error) 	--
Automated action status	jcastatus execution result	<ul style="list-style-type: none"> • jcastatus.log (standard output) • jcastatus_err.log (standard error) 	Δ
	jcastatus -h <i>logical-host-name</i> execution result ^{#2}	<ul style="list-style-type: none"> • jcastatus.log (standard output) • jcastatus_err.log (standard error) 	--
Automated action definition file content	jcastatus -d execution result	<ul style="list-style-type: none"> • jcastatus_d.log (standard output) • jcastatus_d_err.log (standard error) 	Δ
	jcastatus -d -h <i>logical-host-name</i> execution result ^{#2}	<ul style="list-style-type: none"> • jcastatus_d.log (standard output) • jcastatus_d_err.log (standard error) 	--
Event Generation Service status	jcoegsstatus execution result	<ul style="list-style-type: none"> • jcoegsstatus.log (standard output) • jcoegsstatus_err.log (standard error) 	Δ
	jcoegsstatus -h <i>logical-host-name</i> execution result ^{#2}	<ul style="list-style-type: none"> • jcoegsstatus.log (standard output) • jcoegsstatus_err.log (standard error) 	--
Process operation status	jco_spm�_status execution result	<ul style="list-style-type: none"> • jco_spm�_status.log (standard output) • jco_spm�_status_err.log (standard error) 	Δ
	jco_spm�_status -h <i>logical-host-name</i> execution result ^{#2}	<ul style="list-style-type: none"> • jco_spm�_status.log (standard output) • jco_spm�_status_err.log (standard error) 	--

Information type	Collected data	File name#1	View
Data collection command execution result	jim_log.bat command execution result	jim_log_result.log	Y
JP1/IM - Manager license information	Trace logs and error logs that are output by the license library (HLICLIB) at installation	<ul style="list-style-type: none"> hlicliberr{n}.log hliclibmgrerr{n}.log hliclibtrc{n}.log hliclibmgrtrc{n}.log 	--
JP1/IM - View license information	Trace logs and error logs that are output by the license library (HLICLIB) at installation	<ul style="list-style-type: none"> hlicliberr{n}.log hliclibmgrerr{n}.log hliclibtrc{n}.log hliclibmgrtrc{n}.log 	--
Windows event log	<ul style="list-style-type: none"> Application: <i>system-root-folder</i> \system32\config \AppEvent.Evt System: <i>system-root-folder</i> \system32\config \SysEvent.Evt 	<ul style="list-style-type: none"> AppEvent (Backup) .evt AppEvent (Backup) .txt SysEvent (Backup) .evt SysEvent (Backup) .txt 	Y
Crash dump#3	<i>user-specified-folder</i> \user.dmp	user.dmp	Y#4
jp1hosts2 information registered on the host	• jbshosts2export execution result	<ul style="list-style-type: none"> jbshosts2export.log (standard output) jbshosts2export_err.log (standard error) 	Δ
	• jbshosts2export -h <i>logical-host-name</i> execution result	<ul style="list-style-type: none"> jbshosts2export.log (standard output) jbshosts2export_err.log (standard error) 	--
Media sense functionality's ON/OFF information	Content of the registry HKEY_LOCAL_MACHINE\System \CurrentControlSet\Services \Tcpip\Parameters \DisableDHCPMediaSense displayed by the reg command	DisableDHCPMediaSense_reg.txt	--
Server certificate information (CN and SAN settings and expiration dates)	openssl x509 -noout -in <i>server-certificate-file</i> -subject -dates execution result	<ul style="list-style-type: none"> openssl_x509_server.log (standard output) openssl_x509_server_err.log (standard error) 	--
Server certificate and private key compatibility information (modulus)	<ul style="list-style-type: none"> openssl rsa -noout -in <i>private-key-file</i> -modulus execution result openssl x509 -noout -in <i>server-certificate-file</i> -modulus execution result 	<ul style="list-style-type: none"> openssl_keymatching.log (standard output) openssl_keymatching_err.log (standard error) 	--

Legend:

Y: Collected by the jcoview_log.bat command.

Δ: Collected by the jcoview_log.bat command only when JP1/Base and JP1/IM - Manager are installed on the same host as JP1/IM - View.

--: Not collected by the jcoview_log.bat command.

#1: Indicates the storage destination file name after a data collection tool is executed. For details about the storage destination, see the following sections:

- *jim_log.bat* (Windows only) (in Chapter 1. Commands) in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*
- *jcoview_log.bat* (Windows only) (in Chapter 1. Commands) in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*

#2: Can be collected when data in a logical host (cluster) environment is being collected.

#3: The output destination must be specified in advance. (See 1.18.2(1) *Preparations for collecting data in the event of a failure* in the JP1/Integrated Management - Manager Configuration Guide.)

#4: JP1/IM - View and JP1/IM - Manager for Windows do not collect crash dumps.

#5: Can be collected only when *Console-path\log\action\action-information-file-name* exists.

(2) JP1 information

You need to collect the JP1-related information listed in the table below. These types of information can be collected using a data collection tool. If a network connection problem has occurred, you must also collect files from the machine at the connection destination.

The two data collection tools (the *jim_log.bat* command and the *jcoview_log.bat* command) collect different types of data. When the *jim_log.bat* command is executed, all of the data listed in the table below is collected. The data that can be collected by executing the *jcoview_log.bat* command is indicated in the far-right column.

Table 10–14: JP1 information (Windows)

Information type		Collected data	File name#1	View
Common to JP1/IM and JP1/Base	Integrated trace log	<i>system-drive</i> :Program Files\Hitachi\HNTRLib2\spool	The following files in the default mode: hntr2[1 2 3 4].log	Y
JP1/IM - Manager (common to components)	Patch information	<i>Manager-path</i> \PATCHLOG.TXT	Patchlog_jplimm.txt	--
	Model name and version information	<i>Manager-path</i> \Version.txt	Version.txt	--
	License type and expiration date	<i>Manager-path</i> \ProductInfo.txt	ProductInfo.txt	--
	Settings and definition file	Files under <i>Manager-path</i> \conf\	Copies of the files indicated at left	--
	Log file	Files under <i>Manager-path</i> \log\	Copies of the files indicated at left	--
	Operation log file	Files under the folder specified in the following common definition: [JP1_DEFAULT\JP1IMM\OPERATION] "LOGFILEDIR"	Copies of the files indicated at left	--
JP1/IM - Manager (Central Console)	Settings and definition file	Files under <i>Console-path</i> \conf\	Copies of the files indicated at left	--
		Files under <i>shared-folder</i> \JP1Cons\conf\#2	Copies of the files indicated at left	--
	Common definition information	Files under <i>Console-path</i> \default\	Copies of the files indicated at left	--
	Log file	Files under <i>Console-path</i> \log\	Copies of the files indicated at left	--

Information type		Collected data	File name#1	View
		Files under <i>shared-folder</i> \JP1Cons\log\ \#2	Copies of the files indicated at left	--
	File for accumulated response-waiting events#3	Files under <i>Console-path</i> \log\response\ \	Copies of the files indicated at left	--
		Files under <i>shared-folder</i> \jplcons\log\ \response\ \	Copies of the files indicated at left	--
	Correlation event generation history file	Files under <i>Console-path</i> \operation\ \evgen\ \	Copies of the files indicated at left	--
		Files under <i>shared-folder</i> \JP1Cons\ \operation\evgen\#2	Copies of the files indicated at left	--
	Common exclusion history file, and common exclusion-conditions definition history file	Files under <i>Console-path</i> \operation\ \comexclude\ \	Copies of the files indicated at left	--
		Files under <i>shared-folder</i> \JP1Cons\ \operation\comexclude\#2	Copies of the files indicated at left	--
JP1/IM - Manager (Central Scope)	Settings and definition file	Files under <i>Scope-path</i> \conf\ \	Copies of the files indicated at left	--
		Files under <i>shared-folder</i> \JP1Scope\ \conf\#2	Copies of the files indicated at left	--
	Common definition information	Files under <i>Scope-path</i> \default\ \	Copies of the files indicated at left	--
	Log file	Files under <i>Scope-path</i> \log\ \	Copies of the files indicated at left	--
		Files under <i>shared-folder</i> \JP1Scope\ \log\ \#2	Copies of the files indicated at left	--
	Database information	Files under <i>Scope-path</i> \database\ \	Copies of the files indicated at left	--
Files under <i>shared-folder</i> \JP1Scope\ \database\#2		Copies of the files indicated at left	--	
JP1/IM - Manager (IM Configuration Management)	Settings and definition file	Files under <i>Manager-path</i> \conf\imcf\ \	Copies of the files indicated at left	--
		Files under <i>shared-folder</i> \jplimm\conf\ \imcf\#2	Copies of the files indicated at left	--
	Common definition information	Files under <i>Manager-path</i> \system\ \default\new\imcf\ \	Copies of the files indicated at left	--
	Log file	Files under <i>Manager-path</i> \log\imcf\ \	Copies of the files indicated at left	--
		Files under <i>shared-folder</i> \jplimm\ \log\ \imcf\#2	Copies of the files indicated at left	--
JP1/IM - View	Patch information	<i>View-path</i> \Patchlog.txt	Patchlog_jplcoview.txt	Y

Information type		Collected data	File name#1	View
	Model name and version information	<i>View-path</i> \Version.txt	Version.txt	--
	License type and expiration date	<i>View-path</i> \ProductInfo.txt	ProductInfo.txt	--
	Settings and definition file	Files under <i>View-path</i> \conf\	Copies of the files indicated at left	Y
		Files under <i>system-drive</i> :\ProgramData\Hitachi\jp1\jp1_default\JP1CoView\conf\	Copies of the files indicated at left	Y
	Common definition information	Files under <i>View-path</i> \default\	Copies of the files indicated at left	Y
	Log file	Files under <i>system-drive</i> :\ProgramData\Hitachi\jp1\jp1_default\JP1CoView\log\	Copies of the files indicated at left	Y
JP1/Base	Patch information	<i>Base-path</i> \PatchLog.txt	Patchlog_jp1base.txt	--
	Model name and version information	<i>Base-path</i> \Version.txt	Version.txt	--
	License type and expiration date	<i>Base-path</i> \ProductInfo.txt	ProductInfo.txt	--
	Settings and definition file	Files under <i>Base-path</i> \conf\	Copies of the files indicated at left	--
		Files under <i>shared-folder</i> \JP1Base\conf\#2	Copies of the files indicated at left	--
	Common definition information	Files under <i>Base-path</i> \default\	Copies of the files indicated at left	--
	Log file	Files under <i>Base-path</i> \log\	All files under the folder indicated at left, excluding COMMAND	--
		Files under <i>shared-folder</i> \JP1Base\log\#2	All files under the folder indicated at left, excluding COMMAND	--
	Plug-in service settings file	Files under <i>Base-path</i> \plugin\conf\	Copies of the files indicated at left	--
	Log and temporary file	Files under <i>Base-path</i> \sys\tmp\	Copies of the files indicated at left	--
		<i>shared-folder</i> \JP1Base\event#2	All files under the folder indicated at left, excluding IMEvent*. *	--
	Command execution log file	Files under <i>Base-path</i> \log\COMMAND\	Copies of the files indicated at left	--
		Files under <i>shared-folder</i> \JP1Base\log\COMMAND\#2	Copies of the files indicated at left	--

Information type		Collected data	File name ^{#1}	View
	Event database	Files under <i>Base-path</i> \sys\event \servers\default\	Copies of the files indicated at left	--
		<i>shared-folder</i> \JP1Base\event ^{#2}	IMEvent*.*	--

Legend:

Y: Collected by the `jcoview_log.bat` command.

--: Not collected by the `jcoview_log.bat` command.

#1: Indicates the storage destination file name after a data collection tool is used. For details about the storage destination, see the following sections:

- *jim_log.bat* (Windows only) (in *Chapter 1. Commands*) in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*
- *jcoview_log.bat* (Windows only) (in *Chapter 1. Commands*) in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*

#2: Can be collected when data in a logical host (cluster) environment is being collected.

#3: The file for accumulated response-waiting events is created when you enable the response-waiting event management function. You can prevent the `jim_log.bat` command from collecting this file by specifying a command option. For details, see *9.5.2 jim_log.bat* (Windows only).

(3) Operation content

You need the following types of information related to the operation that was being performed when the problem occurred:

- Operation content details
- Time of problem occurrence
- Machine configuration (version of each OS, host name, and Central Console configuration)
- Reproducibility
- Login user name that was used to log in from JP1/IM - View

(4) Error information on the screen

Collect a hard copy of the following:

- Error dialog box (and the content displayed by the **Details** button, if available)

(5) Information related to the Web version of JP1/IM - View

If a problem occurs while you are using the Web version of JP1/IM - View, you need to collect the following data.

View side

- Java stack trace log
Before you can collect a Java stack trace log, you must set up the system such that the Java Console window can be opened. For details, see *4.19.4 Specifying display settings for the Java Console window* in the *JP1/Integrated Management - Manager Configuration Guide*.
- Java trace file of Java™ Plug-in[#]
The Java trace file is located in the following directory:

Java™ Plug-in 1.4.2:

system-drive: \Documents and Settings*login-user-name*\Application Data\Sun\Java
\Deployment\log\

#: You do not need to collect this data if you use the web-based version of JP1/IM - View in plug-in free mode.

Manager side

- HTTP server error log
- HTTP server access log

(6) User dump (only for Windows)

If a JP1/IM - View process stops due to an application error in Windows, collect a user dump.

(7) RAS information during remote monitoring

If a problem occurs during remote monitoring, the user must collect RAS information. For details about how to collect RAS information, see [10.4.1\(8\) Collecting RAS information](#).

10.3.2 In UNIX

(1) OS system information

You need to collect the OS-related information listed in the table below. These types of information can be collected using data collection tools.

Table 10–15: OS system information (UNIX)

Information type	Collected data	File name ^{#1}
Installed Hitachi product information	/etc/.hitachi/pplistd/pplistd	<ul style="list-style-type: none">• jpl_default_imm_1st.tar.{Z gz}• pplistd
Information about products installed by Hitachi PP Installer	Output based on /etc/.hitachi/bin/ SHOWPP	<ul style="list-style-type: none">• jpl_default_imm_1st.tar.{Z gz}• SHOWPP
Hitachi PP Installer installation log file	/etc/.hitachi/.install.log*	<ul style="list-style-type: none">• jpl_default_imm_1st.tar.{Z gz}• .install.log*
Hitachi PP Installer uninstallation log file	/etc/.hitachi/.uninstall.log*	<ul style="list-style-type: none">• jpl_default_imm_1st.tar.{Z gz}• .uninstall.log*
Common definition information	Files under /opt/jpl/hcclibcnf/	<ul style="list-style-type: none">• jpl_default_imm_1st.tar.{Z gz}• Copies of the files indicated at left
JP1/IM - Manager (Central Console) core analysis information (back trace) ^{#6}	Analysis result from seraph /var/opt/jplcons	<ul style="list-style-type: none">• jpl_default_imm_1st.tar.{Z gz}• core_<i>module-name</i>.log
	Analysis result from seraph <i>shared-directory</i> /jplcons/log ^{#2}	<ul style="list-style-type: none">• <i>logical-host-name</i>_imm_1st.tar.{Z gz}• core_<i>module-name</i>.log

Information type	Collected data	File name#1
JP1/IM - Manager (Central Scope) core analysis information (back trace)#6	Analysis result from seraph /var/opt/jplscope	<ul style="list-style-type: none"> • jpl_default_imm_1st.tar.{Z gz} • core_module-name.log
	Analysis result from seraph shared-directory/jplscope/log#2	<ul style="list-style-type: none"> • logical-host-name_imm_1st.tar.{Z gz} • core_module-name.log
JP1/IM - Manager distribution release file	Information for identifying which distribution the execution environment is	<ul style="list-style-type: none"> • Linux /etc/redhat-release • Oracle Linux /etc/oracle-release • CentOS 7 /etc/centos-release • SUSE Linux /etc/SuSE-release
JP1/Base installation log file	/tmp/HITACHI_JP1_INST_LOG/ jplbase_inst{1 2 3 4 5}.log	<ul style="list-style-type: none"> • jpl_default_imm_1st.tar.{Z gz} • jplbase_inst{1 2 3 4 5}.log
JP1/IM - Manager installation log file	/tmp/HITACHI_JP1_INST_LOG/ jplimm_inst{1 2 3 4 5}.log	<ul style="list-style-type: none"> • jpl_default_imm_1st.tar.{Z gz} • jplimm_inst{1 2 3 4 5}.log
File list	<ul style="list-style-type: none"> • ls -lRa /opt/jplimm execution result • ls -lRa /var/opt/jplimm execution result • ls -lRa /opt/jplcons execution result • ls -lRa /etc/opt/jplcons execution result • ls -lRa /var/opt/jplcons execution result • ls -lRa /opt/jplscope execution result • ls -lRa /etc/opt/jplscope execution result • ls -lRa /var/opt/jplscope execution result • ls -lRa /opt/jplbase execution result • ls -lRa /etc/opt/jplbase execution result • ls -lRa /var/opt/jplbase execution result • ls -lRa user-specified -IMDBENVDIR-value-in-setup-information-file execution result • ls -lRa user-specified -IMDBDIR-value-in-setup-information-file execution result • ls -lRa /etc/opt/jplimm execution result • ls -lRa /tmp/ HITACHI_JP1_INST_LOG execution result • ls -lRa /etc/.hitachi execution result • ls -lRa /etc/opt/.hlic execution result • ls -lRa operation-log-output-destination execution result#4 	<ul style="list-style-type: none"> • jpl_default_imm_1st.tar.{Z gz} • inst_dir.log

Information type	Collected data	File name#1
	<ul style="list-style-type: none"> • <code>ls -lRa shared-directory/jplcons</code> execution result#2 • <code>ls -lRa shared-directory/jplscope</code> execution result#2 • <code>ls -lRa shared-directory/jplbase</code> execution result#2 • <code>ls -lRa shared-directory/event</code> execution result#2 • <code>ls -lRa operation-log-output-destination</code> execution result#5 	<ul style="list-style-type: none"> • <code>logical-host-name_imm_1st.tar.{Z gz}</code> • <code>share_dir.log</code>
File list (with the <code>-L</code> option added for referencing the file or folder at the symbolic link destination)	<ul style="list-style-type: none"> • <code>ls -lRaL /opt/jplimm</code> execution result • <code>ls -lRaL /var/opt/jplimm</code> execution result • <code>ls -lRaL /opt/jplcons</code> execution result • <code>ls -lRaL /etc/opt/jplcons</code> execution result • <code>ls -lRaL /var/opt/jplcons</code> execution result • <code>ls -lRaL /opt/jplscope</code> execution result • <code>ls -lRaL /etc/opt/jplscope</code> execution result • <code>ls -lRaL /var/opt/jplscope</code> execution result • <code>ls -lRaL /opt/jplbase</code> execution result • <code>ls -lRaL /etc/opt/jplbase</code> execution result • <code>ls -lRaL /var/opt/jplbase</code> execution result • <code>ls -lRaL user-specified -IMDBENVDIR-value-in-setup-information-file</code> execution result • <code>ls -lRaL user-specified -IMBDBDIR-value-in-setup-information-file</code> execution result • <code>ls -lRaL /etc/opt/jplimm</code> execution result • <code>ls -lRaL /tmp/HITACHI_JP1_INST_LOG</code> execution result • <code>ls -lRaL /etc/.hitachi</code> execution result • <code>ls -lRaL /etc/opt/.hlic</code> execution result • <code>ls -lRaL operation-log-output-destination</code> execution result#4 	<ul style="list-style-type: none"> • <code>jpl_default_imm_1st.tar.{Z gz}</code> • <code>inst_dir_lRaL.log</code>
	<ul style="list-style-type: none"> • <code>ls -lRaL shared-directory/jplcons</code> execution result • <code>ls -lRaL shared-directory/jplscope</code> execution result • <code>ls -lRaL shared-directory/jplbase</code> execution result 	<ul style="list-style-type: none"> • <code>logical-host-name_imm_1st.tar.{Z gz}</code> • <code>share_lRaL_dir.log</code>

Information type	Collected data	File name#1
	<ul style="list-style-type: none"> • <code>ls -lRaL shared-directory/event</code> execution result • <code>ls -lRaL operation-log-output-destination</code> execution result#5 	
Data collection date/time	date execution result	<ul style="list-style-type: none"> • <code>jp1_default_imm_1st.tar.{Z gz}</code> • <code>jp1_default_imm_2nd.tar.{Z gz}</code> • <code>logical-host-name_imm_1st.tar.{Z gz}</code> • <code>logical-host-name_imm_2nd.tar.{Z gz}</code> • <code>date.log</code>
Disk information	<code>df -k</code> execution result	<ul style="list-style-type: none"> • <code>jp1_default_imm_1st.tar.{Z gz}</code> • <code>df.log</code>
btrfs file system information	Only when btrfs is installed in Linux <ul style="list-style-type: none"> • <code>btrfs filesystem show --all-device</code> result 	<ul style="list-style-type: none"> • <code>Linux:jp1_default_imm_1st.tar.gz</code> • <code>df.log</code>
Information about process operation based on the automated startup service (systemd)	Only when systemd is installed in Linux <code>systemctl --all,</code> <code>systemctl list-unit-files,</code> <code>systemctl status jp1_base,</code> <code>systemctl status jp1_cons,</code> <code>systemctl status /usr/lib/systemd/system/2248-*</code> <code>start.service</code> result	<ul style="list-style-type: none"> • <code>jp1_default_imm_1st.tar.gz</code> • <code>systemctl.log</code>
Machine's environment variable	<code>env</code> execution result	<ul style="list-style-type: none"> • <code>jp1_default_imm_1st.tar.{Z gz}</code> • <code>env.log</code>
Host name settings that are set in the machine	<ul style="list-style-type: none"> • <code>/etc/hosts</code> (AIX) • <code>/etc/hosts</code>(Linux) 	<ul style="list-style-type: none"> • <code>jp1_default_imm_1st.tar.{Z gz}</code> • <code>hosts</code>
Status of shared memory for inter-process communication	<code>ipcs -ma</code> execution result	<ul style="list-style-type: none"> • <code>jp1_default_imm_1st.tar.{Z gz}</code> • <code>ipcs.log</code>
Host name for resolving network address	<code>jbsgethostbyname</code> execution result	<ul style="list-style-type: none"> • <code>jp1_default_imm_1st.tar.{Z gz}</code> • <code>jbsgethostbyname.log</code> (standard output) • <code>jbsgethostbyname_err.log</code> (standard error)
	<code>jbsgethostbyname logical-host-name</code> execution result#2	<ul style="list-style-type: none"> • <code>logical-host-name_imm_1st.tar.{Z gz}</code> • <code>jbsgethostbyname_logical-host-name.log</code>
Health check	<code>jbshcstatus -debug -a</code> execution result	<ul style="list-style-type: none"> • <code>jp1_default_imm_1st.tar.{Z gz}</code> • <code>jbshcstatus.log</code> (standard output) • <code>jbshcstatus_err.log</code> (standard error)
	<code>jbshcstatus -debug -a -h logical-host-name</code> execution result#2	<ul style="list-style-type: none"> • <code>logical-host-name_imm_1st.tar.{Z gz}</code> • <code>jbshcstatus.log</code> (standard output) • <code>jbshcstatus_err.log</code> (standard error)
Process operation status of Event Service	<code>jevstat</code> execution result	<ul style="list-style-type: none"> • <code>jp1_default_imm_1st.tar.{Z gz}</code> • <code>jevstat.log</code> (standard output) • <code>jevstat_err.log</code> (standard error)
	<code>jevstat logical-host-name</code> execution result	<ul style="list-style-type: none"> • <code>logical-host-name_imm_1st.tar.{Z gz}</code> • <code>jevstat.log</code> (standard output)

Information type	Collected data	File name#1
		<ul style="list-style-type: none"> • jevstat_err.log (standard error)
Process operation status of items other than Event Service	jbs_spmd_status execution result	<ul style="list-style-type: none"> • jp1_default_imm_1st.tar.{Z gz} • jbs_spmd_status.log (standard output) • jbs_spmd_status_err.log (standard error)
	jbs_spmd_status -h <i>logical-host-name</i> execution result#2	<ul style="list-style-type: none"> • <i>logical-host-name</i>_imm_1st.tar.{Z gz} • jbs_spmd_status.log (standard output) • jbs_spmd_status_err.log (standard error)
Automated action execution result	jcashowa execution result#3	<ul style="list-style-type: none"> • jp1_default_imm_1st.tar.{Z gz} • jcashowa.log (standard output) • jcashowa_err.log (standard error)
	jcashowa -h <i>logical-host-name</i> execution result#2, #3	<ul style="list-style-type: none"> • <i>logical-host-name</i>_imm_1st.tar.{Z gz} • jcashowa.log (standard output) • jcashowa_err.log (standard error)
Automated action function status	jcastatus execution result	<ul style="list-style-type: none"> • jp1_default_imm_1st.tar.{Z gz} • jcastatus.log (standard output) • jcastatus_err.log (standard error)
	jcastatus -h <i>logical-host-name</i> execution result#2	<ul style="list-style-type: none"> • <i>logical-host-name</i>_imm_1st.tar.{Z gz} • jcastatus.log (standard output) • jcastatus_err.log (standard error)
Automated action definition file content	jcastatus -d execution result	<ul style="list-style-type: none"> • jp1_default_imm_1st.tar.{Z gz} • jcastatus_d.log (standard output) • jcastatus_d_err.log (standard error)
	jcastatus -d -h <i>logical-host-name</i> execution result#2	<ul style="list-style-type: none"> • <i>logical-host-name</i>_imm_1st.tar.{Z gz} • jcastatus_d.log (standard output) • jcastatus_d_err.log (standard error)
Event Generation Service status	jcoegsstatus execution result	<ul style="list-style-type: none"> • jp1_default_imm_1st.tar.{Z gz} • jcoegsstatus.log (standard output) • jcoegsstatus_err.log (standard error)
	jcoegsstatus -h <i>logical-host-name</i> execution result#2	<ul style="list-style-type: none"> • <i>logical-host-name</i>_imm_1st.tar.{Z gz} • jcoegsstatus.log (standard output) • jcoegsstatus_err.log (standard error)
Process operation status	jco_spmd_status execution result	<ul style="list-style-type: none"> • jp1_default_imm_1st.tar.{Z gz} • jco_spmd_status.log (standard output) • jco_spmd_status_err.log (standard error)
	jco_spmd_status -h <i>logical-host-name</i> execution result#2	<ul style="list-style-type: none"> • <i>logical-host-name</i>_imm_1st.tar.{Z gz} • jco_spmd_status.log (standard output) • jco_spmd_status_err.log (standard error)
Data collection command execution result	jim_log.sh command execution result	<ul style="list-style-type: none"> • jp1_default_imm_1st.tar.{Z gz} • jim_log_result.log
IP address acquisition	ifconfig -a	<ul style="list-style-type: none"> • jp1_default_imm_1st.tar.{Z gz} • ifconfig.log
	For Linux only	For Linux only

Information type	Collected data	File name#1
	<ul style="list-style-type: none"> ip addr show 	<ul style="list-style-type: none"> jp1_default_imm_1st.tar.gz ip_addr_show.log
NIC installation status	netstat -ai execution result	<ul style="list-style-type: none"> jp1_default_imm_1st.tar.{Z gz} netstat_ai.log
	For Linux only <ul style="list-style-type: none"> ip -s link 	For Linux only <ul style="list-style-type: none"> jp1_default_imm_1st.tar.gz ip_s_link.log
Network statistical information	For AIX <ul style="list-style-type: none"> netstat -naA execution result Result of executing rmsock on the tcp socket displayed in the above result For Linux <ul style="list-style-type: none"> netstat -nap execution result 	<ul style="list-style-type: none"> jp1_default_imm_1st.tar.{Z gz} netstat_na.log
	For Linux only <ul style="list-style-type: none"> ss -nap 	For Linux only <ul style="list-style-type: none"> jp1_default_imm_1st.tar.gz ss_na.log
List of users that are set in the machine	/etc/passwd	<ul style="list-style-type: none"> jp1_default_imm_1st.tar.{Z gz} passwd
Process list	ps -elfa execution result	<ul style="list-style-type: none"> jp1_default_imm_1st.tar.{Z gz} ps.log
Service port settings that are set in the machine	<ul style="list-style-type: none"> /etc/services (AIX) /etc/services (Linux) 	<ul style="list-style-type: none"> jp1_default_imm_1st.tar.{Z gz} services
Memory information	<ul style="list-style-type: none"> lspcs -s execution result (AIX) cat /proc/meminfo (Linux) 	<ul style="list-style-type: none"> jp1_default_imm_1st.tar.{Z gz} swapinfo.log
System diagnostic information	<ul style="list-style-type: none"> alog -o -t boot execution result (AIX) dmesg execution result (Linux) 	<ul style="list-style-type: none"> jp1_default_imm_1st.tar.{Z gz} sys_info.log
Syslog (syslog)	<ul style="list-style-type: none"> /var/adm/messages (AIX) /var/log/messages (Linux) 	<ul style="list-style-type: none"> jp1_default_imm_1st.tar.{Z gz} syslog.log
JP1/IM - Manager (Central Console) core analysis information (back trace) output by the jcogencore command#6	Analysis result from seraph /var/opt/jp1cons	<ul style="list-style-type: none"> jp1_default_imm_1st.tar.{Z gz} trace_<i>module-name</i>.log
	Analysis result from seraph <i>shared-directory</i> /jp1cons/log (core output by jcogencore)#2	<ul style="list-style-type: none"> <i>logical-host-name</i>_imm_1st.tar.{Z gz} trace_<i>module-name</i>.log
OS version information	uname -a execution result	<ul style="list-style-type: none"> jp1_default_imm_1st.tar.{Z gz} uname_a.log
Kernel parameter information	In AIX: <ul style="list-style-type: none"> lsattr -E -l sys0 execution result ulimit -a execution result /etc/security/limits execution result In Linux: <ul style="list-style-type: none"> sysctl -a execution result ulimit -a execution result 	<ul style="list-style-type: none"> jp1_default_imm_1st.tar.{Z gz} In AIX: <ul style="list-style-type: none"> isattr.log ulimit.log limits In Linux: <ul style="list-style-type: none"> sysctl.log ulimit.log

Information type	Collected data	File name#1
Page size information	<ul style="list-style-type: none"> • <code>pagesize</code> execution result (AIX) • Nothing (Linux) 	<ul style="list-style-type: none"> • <code>jp1_default_imm_1st.tar.{Z gz}</code> • <code>pagesize.log</code>
OS patch application information	<p>In AIX:</p> <ul style="list-style-type: none"> • <code>instfix -a -icv</code> execution result • <code>lslpp -l -a</code> execution result <p>In Linux:</p> <ul style="list-style-type: none"> • <code>rpm -qa</code> execution result 	<p>In AIX:</p> <ul style="list-style-type: none"> • <code>instfix.log</code> • <code>lslpp.log</code> <p>In Linux:</p> <ul style="list-style-type: none"> • <code>rpm.log</code>
Distribution information	<p>For Linux only</p> <ul style="list-style-type: none"> • <code>/etc/*-release</code> 	<p>For Linux only</p> <ul style="list-style-type: none"> • <code>*-release</code>
JP1/IM - Manager license information	Trace logs and error logs that are output by the license library (HLICLIB) at installation	<ul style="list-style-type: none"> • <code>jp1_default_imm_1st.tar.{Z gz}</code> • <code>hlicliberr{n}.log</code> • <code>hliclibmgrerr{n}.log</code> • <code>hliclibtrc{n}.log</code> • <code>hliclibmgrtrc{n}.log</code>
Process startup information used by the <code>init</code> daemon	<ul style="list-style-type: none"> • <code>/etc/inittab</code> (AIX) • Files under <code>/etc/init</code> (Linux) <p>In Linux, this information is collected only in Linux 6.</p>	<ul style="list-style-type: none"> • <code>jp1_default_imm_1st.tar.{Z gz}</code> • <code>inittab</code> (AIX) • For the Linux version described at left, files under the <code>init</code> directory (Linux)
Disk mounting information	<ul style="list-style-type: none"> • <code>/etc/filesystems</code> (AIX) • <code>/etc/fstab</code> (Linux) 	<ul style="list-style-type: none"> • <code>jp1_default_imm_1st.tar.{Z gz}</code> • <code>fstab</code> • <code>filesystems</code>
jp1hosts2 information registered on the host	<code>jbshosts2export</code> execution result	<ul style="list-style-type: none"> • <code>jp1_default_imm_1st.tar.{Z gz}</code> • <code>jbshosts2export .log</code> (standard output) • <code>jbshosts2export_err.log</code> (standard error)
	<code>jbshosts2export -h logical-host-name</code> execution result	<ul style="list-style-type: none"> • <code>logical-host-name_imm_1st.tar.{Z gz}</code> • <code>jbshosts2export .log</code> (standard output) • <code>jbshosts2export_err.log</code> (standard error)
Server certificate information (CN and SAN settings and expiration dates)	<code>openssl x509 -noout -in server-certificate-file -subject -dates</code> execution result	<ul style="list-style-type: none"> • <code>jp1_default_imm_1st.tar.{Z gz}</code> • <code>openssl_x509_server.log</code> (standard output) • <code>openssl_x509_server_err.log</code> (standard error)
Server certificate and private key compatibility information (modulus)	<ul style="list-style-type: none"> • <code>openssl rsa -noout -in private-key-file -modulus</code> execution result • <code>openssl x509 -noout -in server-certificate-file -modulus</code> execution result 	<ul style="list-style-type: none"> • <code>jp1_default_imm_1st.tar.{Z gz}</code> • <code>openssl_keymatching.log</code> (standard output) • <code>openssl_keymatching_err.log</code> (standard error)

#1: Indicates the name of the compressed file and uncompressed file after a data collection tool is used (with the compressed file described first, followed by the uncompressed file).

The compressed file is created in `.tar.Z` format for Windows and AIX, and created in `.tar.gz` format for Linux.

For details about the internal directory configuration of the compressed file, see `jim_log.sh` (UNIX only) (in Chapter 1. Commands) in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

#2: Can be collected when data in a logical host (cluster) environment is being collected.

#3: Can be collected only when `/var/opt/jp1cons/log/action/action-information-file-name` exists.

#4: `operation-log-output-destination` indicates the directory specified in the following common definition:

```
[JP1_DEFAULT\JP1IMM\OPERATION]
"LOGFILEDIR"
```

#5: *operation-log-output-destination* indicates the directory specified in the following common definition:

```
[logical-host-name\JP1IMM\OPERATION]
"LOGFILEDIR"
```

#6: Core dump files might not be generated if the operating system is configured to restrict generating core dump files. For details about the settings for core dump files, see 2.17.4 *Specifying settings for handling JP1/IM - Manager failures (for UNIX)* in the *JP1/Integrated Management - Manager Configuration Guide*.

(2) JP1 information

You need to collect the JP1-related information listed in the table below. These types of information can be collected using a data collection tool. If a network connection problem has occurred, you must also collect files from the machine at the connection destination.

Table 10–16: JP1 information (UNIX)

Information type		Collected data	File name ^{#1}
Common to JP1/IM and JP1/Base	Integrated trace log	All files under /var/opt/hitachi/HNTRLib2/spool/	<ul style="list-style-type: none"> jp1_default_imm_1st.tar.{Z gz} The following files in the default mode: hntr2[1 2 3 4].log
	Patch application history Patch log information License type and expiration date Managed-node count log file Operation log file	/opt/jp1imm/patch_history /opt/jp1imm/update.log /var/opt/jp1imm/log/ProductInfo /var/opt/jp1imm/log/nodccount	<ul style="list-style-type: none"> jp1_default_imm_1st.tar.{Z gz} patch_history jp1_default_imm_1st.tar.{Z gz} update.log jp1_default_imm_1st.tar.{Z gz} ProductInfo jp1_default_imm_1st.tar.{Z gz} jimmnodecount_cmd{1 2}.log
JP1/IM - Manager (common to components)	Operation log file	Files under the directory specified in the following common definition: [JP1_DEFAULT\JP1IMM\OPERATION] "LOGFILEDIR"	<ul style="list-style-type: none"> jp1_default_imm_1st.tar.{Z gz} Copies of the files indicated at left
		Files under the directory specified in the following common definition: [logical-host-name\JP1IMM\OPERATION] "LOGFILEDIR"	<ul style="list-style-type: none"> logical-host-name_imm_1st.tar.{Z gz} Copies of the files indicated at left
JP1/IM - Manager (Central Console) ^{#4}	Automatic startup and automatic termination script	Files under /etc/opt/jp1cons/	<ul style="list-style-type: none"> jp1_default_imm_1st.tar.Z Copies of the files indicated at left
	Settings and definition file	Files under /etc/opt/jp1cons/conf/	<ul style="list-style-type: none"> jp1_default_imm_1st.tar.{Z gz} Copies of the files indicated at left
		Files under <i>shared-directory</i> /jp1cons/conf/ ^{#2}	<ul style="list-style-type: none"> logical-host-name_imm_1st.tar.{Z gz} Copies of the files indicated at left

Information type		Collected data	File name ^{#1}
	Common definition information	Files under <code>/etc/opt/jplcons/default/</code>	<ul style="list-style-type: none"> • <code>jpl_default_imm_1st.tar.{Z gz}</code> • Copies of the files indicated at left
	Log file	Files under <code>/var/opt/jplcons/log/</code>	<ul style="list-style-type: none"> • <code>jpl_default_imm_1st.tar.{Z gz}</code> • Copies of the files indicated at left
		Files under <code>shared-directory/jplcons/log/#2</code>	<ul style="list-style-type: none"> • <code>logical-host-name_imm_1st.tar.{Z gz}</code> • Copies of the files indicated at left
	File for accumulated response-waiting events ^{#3}	Files under <code>/var/opt/jplcons/log/response/</code>	<ul style="list-style-type: none"> • <code>jpl_default_imm_1st.tar.{Z gz}</code> • Copies of the files indicated at left
		Files under <code>shared-directory/jplcons/log/response/</code>	<ul style="list-style-type: none"> • <code>jpl_default_imm_1st.tar.{Z gz}</code> • Copies of the files indicated at left
	Core analysis information (CAR file) output by the <code>jcogencore</code> command	car command result <code>/var/opt/jplcons/log</code> (core output by <code>jcogencore</code>)	<ul style="list-style-type: none"> • <code>jpl_default_imm_2nd.tar.{Z gz}</code> • <code>car_module-name.tar.Z</code>
		car command result <code>shared-directory/jplcons/log</code> (core output by <code>jcogencore</code>) ^{#2}	<ul style="list-style-type: none"> • <code>logical-host-name_imm_2nd.tar.{Z gz}</code> • <code>car_module-name.tar.Z</code>
	Core analysis information (CAR file)	car command result <code>/var/opt/jplcons/log</code>	<ul style="list-style-type: none"> • <code>jpl_default_imm_2nd.tar.{Z gz}</code> • <code>core_module-name_car.tar.Z</code>
		car command result <code>shared-directory/jplcons/log#2</code>	<ul style="list-style-type: none"> • <code>logical-host-name_imm_2nd.tar.{Z gz}</code> • <code>core_module-name_car.tar.Z</code>
	Correlation event generation history file	Files under <code>/var/opt/jplcons/operation/evgen/</code>	<ul style="list-style-type: none"> • <code>jpl_default_imm_2nd.tar.{Z gz}</code> • Copies of the files indicated at left
		<code>shared-directory/jplcons/operation/evgen#2</code>	<ul style="list-style-type: none"> • <code>logical-host-name_imm_2nd.tar.{Z gz}</code> • Copies of the files indicated at left
	Common exclusion history file, and common exclusion-conditions definition history file	Files under <code>/var/opt/jplcons/operation/comexclude/</code>	<ul style="list-style-type: none"> • <code>jpl_default_imm_2nd.tar.{Z gz}</code> • Copies of the files indicated at left
<code>shared-directory/jplcons/operation/comexclude#2</code>		<ul style="list-style-type: none"> • <code>logical-host-name_imm_2nd.tar.{Z gz}</code> • Copies of the files indicated at left 	
JP1/IM - Manager (Central Scope) ^{#4}	Settings and definition file	Files under <code>/etc/opt/jplscope/conf/</code>	<ul style="list-style-type: none"> • <code>jpl_default_imm_1st.tar.{Z gz}</code> • Copies of the files indicated at left
		Files under <code>shared-directory/jplscope/conf/#2</code>	<ul style="list-style-type: none"> • <code>logical-host-name_imm_1st.tar.{Z gz}</code> • Copies of the files indicated at left

Information type		Collected data	File name#1
	Common definition information	Files under <code>/etc/opt/jplscope/default/</code>	<ul style="list-style-type: none"> • <code>jp1_default_imm_1st.tar.{Z gz}</code> • Copies of the files indicated at left
	Log file	Files under <code>/var/opt/jplscope/log/</code>	<ul style="list-style-type: none"> • <code>jp1_default_imm_1st.tar.{Z gz}</code> • Copies of the files indicated at left
		Files under <code>shared-directory/jplscope/log/#2</code>	<ul style="list-style-type: none"> • <code>logical-host-name_imm_1st.tar.{Z gz}</code> • Copies of the files indicated at left
	Core analysis information (CAR file)	car command result <code>/var/opt/jplscope/log</code>	<ul style="list-style-type: none"> • <code>jp1_default_imm_2nd.tar.{Z gz}</code> • <code>core_module-name_car.tar.Z</code>
		car command result <code>shared-directory/jplscope/log#2</code>	<ul style="list-style-type: none"> • <code>logical-host-name_imm_2nd.tar.{Z gz}</code> • <code>core_module-name_car.tar.Z</code>
	Database information	Files under <code>/var/opt/jplscope/database/</code>	<ul style="list-style-type: none"> • <code>jp1_default_imm_2nd.tar.{Z gz}</code> • Copies of the files indicated at left
		Files under <code>shared-directory/jplscope/database/#2</code>	<ul style="list-style-type: none"> • <code>logical-host-name_imm_2nd.tar.{Z gz}</code> • Copies of the files indicated at left
	JP1/IM - Manager (IM Configuration Management)#4	Settings and definition files	Files under <code>/etc/opt/jplimm/conf/imcf/</code>
Files under <code>shared-directory/jplimm/conf/imcf/#2</code>			<ul style="list-style-type: none"> • <code>logical-host-name_imm_1st.tar.{Z gz}</code> • Copies of the files indicated at left
Common definition information		Files under <code>/etc/opt/jplimm/default/imcf/</code>	<ul style="list-style-type: none"> • <code>jp1_default_imm_1st.tar.{Z gz}</code> • Copies of the files indicated at left
Log file		Files under <code>/var/opt/jplimm/log/imcf/</code>	<ul style="list-style-type: none"> • <code>jp1_default_imm_1st.tar.{Z gz}</code> • Copies of the files indicated at left
		Files under <code>shared-directory/jplimm/log/imcf/#2</code>	<ul style="list-style-type: none"> • <code>logical-host-name_imm_1st.tar.{Z gz}</code> • Copies of the files indicated at left
Core analysis information (CAR file)		car command result <code>/var/opt/jplimm/log</code>	<ul style="list-style-type: none"> • <code>jp1_default_imm_2nd.tar.{Z gz}</code> • <code>./var/opt/jplimm/log/_jp1_default/core/core_module-name_car.tar.Z</code>
		car command result <code>shared-directory/jplimm/log#2</code>	<ul style="list-style-type: none"> • <code>logical-host-name_imm_2nd.tar.{Z gz}</code> • <code>./var/opt/jplimm/log/_logical-host-name/core/core_module-name_car.tar.Z</code>

Information type		Collected data	File name#1
JP1/Base	Automatic startup and automatic termination script	Files under /etc/opt/jp1base/	<ul style="list-style-type: none"> jp1_default_imm_1st.tar.{Z gz} Copies of the files indicated at left
	Settings and definition file	Files under /etc/opt/jp1base/conf/	<ul style="list-style-type: none"> jp1_default_imm_1st.tar.{Z gz} Copies of the files indicated at left
		Files under <i>shared-directory</i> /jp1base/conf/#2	<ul style="list-style-type: none"> <i>logical-host-name</i>_imm_1st.tar.{Z gz} Copies of the files indicated at left
	Common definition information	Files under /etc/opt/jp1base/default/	<ul style="list-style-type: none"> jp1_default_imm_1st.tar.{Z gz} Copies of the files indicated at left
	Plug-in service settings file	Files under /opt/jp1base/conf/plugin/	<ul style="list-style-type: none"> jp1_default_imm_1st.tar.{Z gz} Copies of the files indicated at left
	Patch application history	/opt/jp1base/PatchInfo	<ul style="list-style-type: none"> jp1_default_imm_1st.tar.{Z gz} PatchInfo
	Patch log information	/opt/jp1base/PatchLog	<ul style="list-style-type: none"> jp1_default_imm_1st.tar.{Z gz} PatchLog
	Log file	/var/opt/jp1base/log	<ul style="list-style-type: none"> jp1_default_imm_1st.tar.{Z gz} All files under the directory indicated at left, except COMMAND
		<i>shared-directory</i> /jp1base/log#2	<ul style="list-style-type: none"> <i>logical-host-name</i>_imm_1st.tar.{Z gz} All files under the directory indicated at left, except COMMAND
	Log and temporary file	Files under /var/opt/jp1base/sys/tmp/	<ul style="list-style-type: none"> jp1_default_imm_1st.tar.{Z gz} Copies of the files indicated at left
		<i>shared-directory</i> /event#2	<ul style="list-style-type: none"> <i>logical-host-name</i>_imm_1st.tar.{Z gz} All files under the directory indicated at left, except IMEvent*
	SES settings file	<ul style="list-style-type: none"> /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 	<ul style="list-style-type: none"> jp1_default_imm_2nd.tar.{Z gz} Copies of the files indicated at left
	Command execution history file	Files under /var/opt/jp1base/log/COMMAND/	<ul style="list-style-type: none"> jp1_default_imm_2nd.tar.{Z gz} Copies of the files indicated at left
Files under <i>shared-directory</i> /jp1base/log/COMMAND/#2		<ul style="list-style-type: none"> <i>logical-host-name</i>_imm_2nd.tar.{Z gz} 	

Information type		Collected data	File name ^{#1}
			<ul style="list-style-type: none"> Copies of the files indicated at left
	Event database	Files under <code>/var/opt/jp1base/sys/event/servers/default/</code>	<ul style="list-style-type: none"> <code>jp1_default_imm_2nd.tar.{Z gz}</code> Copies of the files indicated at left
		<code>shared-directory/event</code> ^{#2}	<ul style="list-style-type: none"> <code>logical-host-name_imm_2nd.tar.{Z gz}</code> <code>IMEvent*.*</code>

^{#1}: Indicates the name of the compressed file and uncompressed file after a data collection tool is executed (with the compressed file described first, followed by the uncompressed file).

The compressed file is created in `.tar.Z` format for AIX, and in `.tar.gz` format for Linux.

For details about the internal directory configuration of the compressed file, see `jim_log.sh (UNIX only)` (in *Chapter 1. Commands*) in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

^{#2}: Can be collected when data in a logical host (cluster) environment is being collected.

^{#3}: The file for accumulated response-waiting events is created when you enable the response-waiting event management function. You can prevent the `jim_log.sh` command from collecting this file by specifying a command option. For details, see *9.5.3 jim_log.sh (UNIX only)*.

^{#4}: Core dump files might not be generated if the operating system is configured to restrict generating core dump files.

For details about the settings for core dump files, see *2.17.4 Specifying settings for handling JP1/IM - Manager failures (for UNIX)* in the *JP1/Integrated Management - Manager Configuration Guide*.

(3) Operation content

You need the following types of information related to the operation that was being performed when the problem occurred:

- Operation content details
- Time of problem occurrence
- Machine configuration (version of each OS, host name, and Central Console configuration)
- Reproducibility
- Login user name that was used to log in from JP1/IM - View

(4) Error information on the screen

Collect a hard copy of the following:

- Error dialog box

(5) Information related to the Web version of JP1/IM - View

If a problem occurs while you are using the Web version of JP1/IM - View, you need to collect the following data.

View side

- Java stack trace log

Before you can collect a Java stack trace log, you must set up the system such that the Java Console window can be opened. For details, see *4.19.4 Specifying display settings for the Java Console window* in the *JP1/Integrated Management - Manager Configuration Guide*.
- Java trace file of Java™ Plug-in[#]

The Java trace file is located in the following directory:

```
system-drive:\Documents and Settings\login-user-name\Application Data\Sun\Java  
\Deployment\log\
```

#: You do not need to collect this data if you use the web-based version of JP1/IM - View in plug-in free mode.

Manager side

- HTTP server error log
- HTTP server access log

(6) RAS information during remote monitoring

If a problem occurs during remote monitoring, the user must collect RAS information. For details about how to collect RAS information, see [10.4.2\(7\) Collecting RAS information](#).

10.4 Collecting data

This section explains how to collect data when a problem occurs.

10.4.1 In Windows

(1) Checking the process status

Using Windows Task Manager, check the operating status of processes. This subsection shows the processes that are displayed when the programs are running normally.

(a) JP1/IM - Manager

For details about JP1/IM - Manager processes, see *Appendix B.1 (1) JP1/IM - Manager* in the *JP1/Integrated Management - Manager Overview and System Design Guide*.

(b) JP1/IM - View

For details about JP1/IM - View processes, see *Appendix B.1 (1) JP1/IM - Manager* in the *JP1/Integrated Management - Manager Overview and System Design Guide*.

(c) JP1/IM - IM Configuration Management - View

The table below shows the processes of JP1/IM - IM Configuration Management - View. The value inside parentheses () indicates the number of processes that execute simultaneously.

Table 10–17: JP1/IM - IM Configuration Management - View processes

Parent process name	Function	Child process name	Function
jcfvview.exe (3)	Controls the JP1/IM - IM Configuration Management - View window.	jcfvview_evt.exe (3)	Sends thread dump output events.
		java.exe (3)	Controls the JP1/IM - IM Configuration Management - View window.

You can start a maximum of three JP1/IM - IM Configuration Management - View instances when you log in from a single machine. Each time JP1/IM - IM Configuration Management - View is started, one process starts.

(2) Outputting a thread dump for JP1/IM

(a) JP1/IM - View

Follow the procedure described below to output a dump file.

1. Start Task Manager.
2. On the Applications page, select JP1/IM - View, and then from the pop-up menu, choose **Bring To Front**.
In this way, you can determine whether JP1/IM - View is disabled. If you have identified a disabled JP1/IM - View, proceed to the next step.
3. From the pop-up menu, choose **Go To Process**.

The display switches to the **Process** page. Since `java.exe` of JP1/IM - View is displayed in the selected state, use this to identify the process ID (PID).[#]

[#]: If no PID is displayed, from the menu, choose **Display** and then **Select Columns**, and then, from the Select Columns window, select the **PID (Process Identifier)** check box.

4. Using the process ID that has been identified as the argument, execute the `jcothreaddmp` command.

For details about the `jcothreaddmp` command, see *jcothreaddmp (Windows only)* (in *Chapter 1. Commands*) in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

(b) JP1/IM - Manager

When the health check function detects an abnormality in Event Console Service, Event Base Service or Event Generation Service of JP1/IM - Manager, output a dump file for JP1/IM - Manager. Execute the `jcogencore` command as follows.

```
jcogencore
```

For details about the `jcogencore` command, see *jcogencore* (in *Chapter 1. Commands*) in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

(3) Collecting information related to the Web version of JP1/IM - View

When a problem occurs in the Web version of JP1/IM - View, collect the following data in addition to the data described in this section.

View side

- Java stack trace log

The collection procedure follows:

1. Choose the Java Console window and enter `v`.

The Java stack trace log is output to the Java Console window.

2. Copy the log and manually paste it to a text file, for example.
3. Save the text file.

- Java trace file of Java™ Plug-in[#]

The Java trace file is located in the following directory:

```
system-drive:\Documents and Settings\login-user-name\Application Data\Sun\Java  
\Deployment\log\
```

[#]: You do not need to collect this data if you use the web-based version of JP1/IM - View in plug-in free mode.

Important

The Java trace file of Java™ Plug-in is erased when Java™ Plug-in restarts. Therefore, if a problem occurs, save the content of this file to another file before restarting.

Manager side

- HTTP server error log
- HTTP server access log

(4) Executing the data collection tool

This subsection describes execution of the data collection tool (`jim_log.bat` or `jcoview_log.bat`).

When you execute the `jim_log.bat` command, which is provided by JP1/IM - Manager, you can collect the data necessary for troubleshooting JP1/IM - Manager and JP1/IM - View on the same host.

If you execute the `jcoview_log.bat` command, which is provided by JP1/IM - View, you can collect the data necessary for troubleshooting JP1/IM - View.

Use one of above commands according to the application that is being used.

Because the total volume of data collected by a data collection tool is massive, you need to estimate it before you execute the command and make sure the machine you are using has sufficient free space.

For the volume of data that will be collected by the `jim_log.bat` command, see the JP1/IM - Manager release notes.

For the volume of data that will be collected by the `jcoview_log.bat` command, see the JP1/IM - View release notes.

A tool execution example follows.

```
C:\>"C:\Program Files\Hitachi\JP1IMM\tools\jim_log.bat" -f data-storage-folder
```

Specify the data storage folder as an absolute path. If the data storage folder path contains a space, enclose the path in double quotation marks.

When you execute the tool, the `jp1_default` folder is created under the folder specified as the data storage folder, and the collected data is copied into this folder. Use a data-compression tool to compress the collected data.

(5) Checking the operation content

Check the content of the operation that was taking place when the problem occurred, and record it. The following types of information must be checked:

- Operation content details
- Time of problem occurrence
- Reproducibility
- Login user name that was used to log in from JP1/IM - View
- Machine configuration (version of each OS, host name, and Central Console configuration)

(6) Collecting the error information on the screen

If an error is displayed on the screen, collect that information as well. Collect a hard copy of the following:

- Error dialog box
Copy the content displayed by the **Details** button, if available.

(7) Collecting a user dump (Windows only)

If a JP1/IM - View process stops due to an application error in Windows, while the error dialog box is displayed, use the following procedure to collect a user dump:

1. Start Task Manager.

You can use either of the following procedures to start Task Manager:

- Right-click a blank area on the task bar and choose **Task Manager**.
- Press **Ctrl + Shift + Esc** keys to start Task Manager.

2. Click the **Process** tab.

3. Right-click the name of the JP1/IM - View process that was stopped by an application error, and then choose **Create Dump File**.

4. When a dialog box showing the user dump output destination path opens, collect a dump from there.

Important

If the error dialog box is closed, a normal dump cannot be collected, and consequently you will not be able to collect a user dump. If you closed the error dialog box by mistake (by clicking **OK**, for example) before collecting a user dump, reproduce the error and then collect a user dump.

(8) Collecting RAS information

If a problem occurs during remote monitoring, collect RAS information on the manager host and monitored host.

How to collect the information differs depending on the method of connecting monitored hosts. For collecting information from remotely-monitored hosts, the connection method differs depending on the log information to be collected and the OSs on the manager host and monitored hosts. For details about the connection methods for remote monitoring, see *6.6.2 Collectable log information and connection methods for remote monitoring* in the *JP1/Integrated Management - Manager Overview and System Design Guide*.

The following describes how to collect information when the OS on the manager host is Windows.

Table 10–18: References about how to collect RAS information (when the OS on the manager host is Windows)

Connection method	Host for collecting data (OS)	References about the collection method
WMI connection	Manager host (Window)	<i>Table 10-20 Collecting data on the Windows manager host (for WMI connection)</i>
	Monitored host (Windows)	<i>Table 10-21 Collecting data on the Windows monitored host (for WMI connection)</i>
NetBIOS connection	Manager host (Windows)	<i>Table 10-22 Collecting data on the Windows manager host (for NetBIOS connection)</i>
	Monitored host (Windows)	<i>Table 10-23 Collecting data on the Windows monitored host (for NetBIOS connection)</i>
SSH connection	Manager host (Windows)	<i>Table 10-24 Collecting data on the Windows manager host (for SSH connection)</i>
	Monitored host (UNIX)	<i>Table 10-27 Collecting data on the UNIX monitored host (for SSH connection)</i>

#: To collect host information from remotely monitored hosts, use WMI and WMI/NetBIOS (NetBIOS over TCP/IP) if the OS on the monitored hosts is Windows, and use SSH if the OS on the monitored hosts is UNIX. For details about the connection methods for remote monitoring, see 6.6.2 Collectable log information and connection methods for remote monitoring in the *JPI/Integrated Management - Manager Overview and System Design Guide*.

(a) For WMI connection

The following table describes how to collect data on the manager host (Windows) if a problem occurs in WMI connection.

Table 10–19: Collecting data on the Windows manager host (for WMI connection)

No.	Procedure
1	<p>From the command prompt, execute the following commands, and then collect the results:</p> <ul style="list-style-type: none"> • <code>whoami /all</code> • <code>nslookup <i>monitored-host-name</i></code> • <code>netsh advfirewall firewall show rule name=all</code> • <code>netsh advfirewall show allprofiles</code> • <code>tasklist <i>monitored-host-name</i></code> • <code>systeminfo</code> • <code>wmic qfe</code> • <code>reg export HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\ CurrentVersion\Policies\System <i>output-file</i></code> • <code>reg export HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Ole <i>output-file</i></code> • <code>reg export HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\System <i>output-file</i></code> • <code>wmic /node:"<i>monitored-host-name</i>" /user:<i>user-name</i> /password:<i>password</i> port (user-specified WMI command)</code> • Commands to be executed on the manager host: <ul style="list-style-type: none"> <code>date /t</code> <code>time /t</code> • Command to be executed on the monitored host connected via WMI: <ul style="list-style-type: none"> <code>wmic /node:"<i>monitored-host-name</i>" /user:<i>user-name</i> /password:<i>password</i> path Win32_LocalTime</code>
2	<p>Collect the authentication information for WMI connection.</p> <ul style="list-style-type: none"> • For physical hosts: <ul style="list-style-type: none"> <code><i>Manager-path</i>\conf\agtless\targets\wmi.ini</code> • For logical hosts: <ul style="list-style-type: none"> <code><i>shared-folder</i>\JP1IMM\conf\agtless\targets\wmi.ini</code>
3	<p>Collect the WMI connection log.</p> <ul style="list-style-type: none"> • Log file under the directory specified in <code>HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\CIMOM\Logging Directory#</code>
4	<p>Obtain a screenshot showing that <code>runas /user:<i>user-name</i> wbemtest</code> has been executed from the command prompt on the manager host.</p> <p>Make sure that the value of <i>user-name</i> is the same as that specified in the User name text box on the IM Host Account page in the System Common Settings window. If you are prompted to enter a password after executing the command, specify the value set in the Password text box on the IM Host Account page.</p>
5	<p>Obtain a screenshot showing the user-specified values for the namespace and credentials displayed when the Connect button is clicked in the dialog box opened by <code>wbemtest</code>.</p>
6	<p>Obtain a screenshot of the status after the Connect button is clicked in the dialog box opened by <code>wbemtes</code>. The status indicating that connection is established correctly is displayed, or an error message is displayed.</p>
7	<p>In the dialog box opened by <code>wbemtest</code>, click the Query button. In the dialog box that opens, enter the query as follows, and then click the Apply button:</p> <ul style="list-style-type: none"> • <code>Select * From Win32_NTLogEvent Where (Logfile='System' Or Logfile='Application')</code> <p>After the query is performed, obtain a screenshot of the query results indicated in the Query Result widow.</p>

#: If HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\CIMOM\Logging is set to 0 (default value), no data is output to the log. If the value of Logging is 1, only error information is output. If the value of Logging is 2, detailed information is output.

The following table describes how to collect data on the monitored host (Windows) if a problem occurs in WMI connection.

Table 10–20: Collecting data on the Windows monitored host (for WMI connection)

No.	Procedure
1	<p>Log in to the monitored host as the monitored user, execute the following commands from the command prompt, and then collect the results:</p> <ul style="list-style-type: none"> • hostname • whoami /all • nslookup <i>manager-host-name</i> • ipconfig /all • netstat -na • netsh advfirewall firewall show rule name=all • netsh advfirewall show allprofiles • tasklist <i>monitored-host-name</i> • systeminfo • %ProgramFiles%\Common Files\Microsoft Shared\MSInfo\msinfo32.exe /report <i>output-file</i> • wmic qfe • tasklist <i>monitored-host-name</i> • reg export HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System <i>output-file</i> • reg export HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Ole <i>output-file</i>
2	<p>Collect the WMI connection log.</p> <ul style="list-style-type: none"> • Log file under the directory specified in HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\CIMOM\Logging Directory#
3	<ul style="list-style-type: none"> • If a firewall is disabled: Collect the data indicating that the Windows firewall is disabled. • If a firewall is enabled: From the command prompt, execute the following command, and then collect the result: reg export HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsFirewall\StandardProfile\RemoteAdminSettings <i>output-file</i>
4	<p>Collect the data indicating that the event log is correctly created on the monitored host.</p> <ul style="list-style-type: none"> • Click Administrative Tools, and then Event Viewer. Then, in the dialog box that opens, application, system, and security event logs in both binary and text formats.

#: If HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\CIMOM\Logging is set to 0 (default value), no data is output to the log. If the value of Logging is 1, only error information is output. If the value of Logging is 2, detailed information is output.

(b) For NetBIOS connection

The following table describes how to collect data on the manager host (Windows) if a problem occurs in NetBIOS connection.

Table 10–21: Collecting data on the Windows manager host (for NetBIOS connection)

No.	Procedure
1	<p>From the command prompt, execute the following commands, and then collect the results:</p> <ul style="list-style-type: none"> • whoami • nslookup <i>monitored-host-name</i>

No.	Procedure
	<ul style="list-style-type: none"> • nbtstat -s • netsh advfirewall firewall show rule name=all • netsh advfirewall show allprofiles • net use • systeminfo • wmic qfe • date /t# • time /t#
2	Click Administrative Tools, Local Security Policy, Security Settings, Local Policies , and then User Rights Assignment , and then right-click Access this computer from the network . In the menu that opens, select Properties , and then obtain a screenshot that indicates the user name you specified.
3	Log in with the user name specified on the IM Host Account page. In the address bar of Explorer, enter <code>\\remotely-monitored-host-name</code> to establish a connection. Then, obtain a screenshot that indicates that the monitored file has been viewed successfully.

#: Execute the same commands also on the monitored host, and then check the time difference between the manager host and the monitored host. Do not provide a long interval between executions.

The following table describes how to collect data on the monitored host (Windows) if a problem occurs in NetBIOS connection.

Table 10–22: Collecting data on the Windows monitored host (for NetBIOS connection)

No.	Procedure
1	Log in to the monitored host as the monitored user, execute the following commands from the command prompt, and then collect the results: <ul style="list-style-type: none"> • hostname • nslookup <i>manager-host-name</i> • ipconfig /all • netsh advfirewall firewall show rule name=all • netsh advfirewall show allprofiles • net session • systeminfo • %ProgramFiles%\Common Files\Microsoft Shared\MSInfo\msinfo32.exe /report <i>output-file</i> • wmic qfe • cacls <i>monitored-file</i> • dir /A <i>directory-containing-the-monitored-file</i> • net share <i>shared-folder-name</i> • reg export HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanmanServer\Parameters <i>output-file</i> • date /t# • time /t#
2	Select Administrative Tools, Local Security Policy, Security Settings, Local Policies, User Rights Assignment , and then right-click Access this computer from the network . In the menu that opens, select Properties , and then obtain a screenshot that indicates the user name you specified.
3	Collect the monitored file.

#: Execute the same commands also on the monitored host to check the time difference between the manager host and the monitored host. Do not provide a long interval between executions.

(c) For SSH connection

The following table describes how to collect data on the manager host (Windows) if a problem occurs in SSH connection.

Table 10–23: Collecting data on the Windows manager host (for SSH connection)

No.	Procedure
1	<p>From the command prompt, execute the following commands, and then collect the results:</p> <ul style="list-style-type: none">• <code>whoami</code>• <code>nslookup <i>monitored-host-name</i></code>• <code>netsh advfirewall firewall show rule name=all</code>• <code>netsh advfirewall show allprofiles</code>• <code>systeminfo</code>• <code>wmic qfe</code>• Commands to be executed on the manager host: <code>date /t</code> <code>time /t</code>• Commands to be executed on the monitored host connected via SSH: <code>date</code>• <code>dir /A <i>directory-containing-the-private-key</i></code>
2	<p>Collect the authentication information for SSH connection.</p> <ul style="list-style-type: none">• For physical hosts: <code>Manager-path\conf\agtless\targets\ssh.ini</code>• For logical hosts: <code>shared-folder\JP1IMM\conf\agtless\targets\ssh.ini</code>
3	<p>Collect the data indicating that an SSH connection with the remotely-monitored host was successfully established by using the private key placed on the host.</p>

For details about how to collect data on a monitored host (UNIX) if a problem occurs in SSH connection, see [Table 10-27 Collecting data on the UNIX monitored host \(for SSH connection\)](#) in [10.4.2\(7\)\(a\) For SSH connection](#).

10.4.2 In UNIX

(1) Checking the process status

The process names that are displayed when the `ps` command is executed are shown below. In UNIX, by using the data collection tool (`jim_log.sh`), you can collect the execution results of the `ps` command along with other data.

(a) JP1/IM - Manager

For details about JP1/IM - Manager processes, see [Appendix B.2 \(1\) JP1/IM - Manager](#) in the *JP1/Integrated Management - Manager Overview and System Design Guide*.

(2) Outputting a dump file for JP1/IM

(a) JP1/IM - Manager

You only need to output a dump file for JP1/IM - Manager when the health check function detects an abnormality in JP1/IM - Manager. Execute the `jcogencore` command as follows.

jcogencore

When you execute the `jcogencore` command, a message appears asking you to select the process from which to output a dump file. Select the process that is included in the message information issued by the health check function. If a dump file already exists, an overwrite confirmation message is displayed. If you choose not to overwrite the dump file, choose `n` and terminate the command. Next, save the dump file and then re-execute the `jcogencore` command.

For details about the `jcogencore` command, see *jcogencore* (in *Chapter 1. Commands*) in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

(3) Collecting information related to the Web version of JP1/IM - View

When a problem occurs in the Web version of JP1/IM - View, collect the following data in addition to the data described in this section.

View side

- Java stack trace log

The collection procedure follows:

1. Choose the Java Console window and enter `v`.

The Java stack trace log is output to the Java Console window.

2. Copy the log and manually paste it to a text file, for example.
3. Save the text file.

- Java trace file of Java™ Plug-in#

The Java trace file is located in the following directory:

```
system-drive:\Documents and Settings\login-user-name\Application Data\Sun\Java
\Deployment\log\
```

#: You do not need to collect this data if you use the web-based version of JP1/IM - View in plug-in free mode.

Important

The Java trace file of Java™ Plug-in is erased when Java™ Plug-in restarts. Therefore, if a problem occurs, save the content of this file to another file before restarting.

Manager side

- HTTP server error log
- HTTP server access log

(4) Executing the data collection tool

This subsection describes execution of the data collection tool (`jim_log.sh`).

When you execute the `jim_log.sh` command, which is provided by JP1/IM - Manager, you can collect the data necessary for troubleshooting JP1/IM - Manager and JP1/Base on the same host.

Because the total volume of data collected by a data collection tool is massive, you need to estimate it before you execute the command and make sure the machine you are using has sufficient free space. For the volume of data that will be collected by the `jim_log.bat` command, see the JP1/IM - Manager release notes.

A tool execution example follows.

```
# /opt/jplimm/tools/jim_log.sh -f data-storage-directory
```

When you execute the tool, the collected data is summarized in the `tar` format and output as compressed data.

(5) Checking the operation content

Check the content of the operation that was taking place when the problem occurred, and record it. The following types of information must be checked:

- Operation content details
- Time of problem occurrence
- Reproducibility
- Login user name that was used to log in from JP1/IM - View
- Machine configuration (version of each OS, host name, and Central Console configuration)

(6) Collecting the error information on the screen

If an error is displayed on the screen, collect that information as well. Collect a hard copy of the following:

- Error dialog box
If the **Details** button is available, copy its content as well.

(7) Collecting RAS information

If a problem occurs during remote monitoring, collect RAS information on the manager host and monitored host.

How to collect the information differs depending on the method of connecting monitored hosts. For collecting information from remotely-monitored hosts, the connection method differs depending on the log information to be collected and the OSs on the manager host and monitored hosts. For details about the connection methods for remote monitoring, see *6.6.2 Collectable log information and connection methods for remote monitoring* in the *JP1/Integrated Management - Manager Overview and System Design Guide*.

The following describes how to collect information when the OS on the manager host is UNIX.

Table 10–24: References about how to collect RAS information (when the OS on the manager host is UNIX)

Connection method	Host for collecting information (OS)	References about the collection method
SSH connection	Manager host (UNIX)	<i>Table 10-26 Collecting data on the UNIX manager host (for SSH connection)</i>
	Monitored host (UNIX)	<i>Table 10-27 Collecting data on the UNIX monitored host (for SSH connection)</i>

(a) For SSH connection

The following table describes how to collect data on the manager host (UNIX) if a problem occurs in SSH connection.

Table 10–25: Collecting data on the UNIX manager host (for SSH connection)

No.	Procedure
1	<p>From the console, execute the following commands, and then collect the results:</p> <ul style="list-style-type: none"> • <code>whoami</code> • <code>nslookup <i>monitored-host-name</i></code> • Command to be executed on the manager host: <code>date</code> • Command to be executed on the monitored host connected via SSH: <code>Date</code> • <code>ls -al <i>directory-containing-the-private-key</i></code>
2	<p>Collect the authentication information for SSH connection.</p> <ul style="list-style-type: none"> • For physical hosts: <code><i>Manager-path</i>\conf\agtless\targets\ssh.ini</code> • For logical hosts: <code><i>shared-folder</i>\JP1IMM\conf\agtless\targets\ssh.ini</code>
3	<p>Collect the data indicating that an SSH connection with the remotely-monitored host was successfully established by using the private key placed on the host.</p>

The following table describes how to collect data on the monitored host (UNIX) if a problem occurs in SSH connection.

Table 10–26: Collecting data on the UNIX monitored host (for SSH connection)

No.	Procedure
1	<p>Log in to the monitored host as the monitored user, execute the following commands from the console, and then collect the results:</p> <ul style="list-style-type: none"> • <code>uname -a</code> • <code>nslookup <i>manager-host-name</i></code> • <code>ifconfig -a</code> • <code>netstat -i</code> • <code>netstat -na</code> • <code>iptables --list</code> • <code>env</code> • <code>which <i>command-name</i></code> (specify one of the following for <i>command-name</i>) <code>uname</code> <code>ls</code> <code>wc</code> <code>tail</code> <code>head</code> <code>grep</code> <code>find</code> • <code>ls -ail <i>directory-containing-the-monitored-file</i></code> • <code>ls -al <i>higher-directory-of-the-directory-specified-for-AuthorizedKeysFile-in-the-sshd_config-file</i></code> • <code>ls -al <i>directory-specified-for-AuthorizedKeysFile-in-the-sshd_config-file</i></code> • In AIX: <code>alog -o -t boot</code> <code>instfix -a -icv</code> <code>lslpp -l -a</code> <code>oslevel -s</code> • In Linux: <code>dmesg</code> <code>rpm -qa</code>

No.	Procedure
2	<p>Collect the following files:</p> <ul style="list-style-type: none">• /etc/hosts.allow• /etc/hosts.deny• Monitored file• In AIX:<ul style="list-style-type: none">/etc/netshvc.conf/etc/ssh/sshd_config/var/adm/messages/var/log/authlog• In Linux:<ul style="list-style-type: none">/etc/nsswitch.conf/etc/issue/etc/ssh/sshd_config/var/log/messages/var/log/secure

10.5 Troubleshooting

10.5.1 Dealing with common problems

This section explains how to correct the problems that can generally be anticipated.

(1) Actions to take when you cannot log in from JP1/IM - View

The actions to take differ depending on the message that is output.

The message KAVB1200-E: Communication error occurred in establishing the connection. is output.

Cause

The following are possible causes:

- JP1/IM - Manager has not been started.
- The host name at the connection destination is invalid.

Corrective action

Take the corrective action that matches the cause.

- Start JP1/IM - Manager.
- Make sure that the host name at the connection destination is correct.

The message KAVB0104-E: Failed to authenticate the user. is output.

Cause

The user name or password for the connection destination is invalid.

Corrective action

Make sure that the user name or password for the connection destination is valid.

*The message KAVB0109-E: Communication error occurred between the connecting host and the authentication server. Connecting host: **connecting-host** or KAVB0111-E: A connection to the authentication server could not be established. is output.*

Cause

The authentication server that is set at the connection-destination host has not been started.

Corrective action

Make sure of the following and take appropriate action.

- The authentication server has been started.
- Communication between the connection host and the authentication server is possible.
- The authentication server settings are not incorrect.

The message KNAN20100-E: Address resolution for the specified connection destination host name failed. is output.

Cause

The following are possible causes:

- The target host name is invalid.
- The target host has not been started.

- An error occurred in communications with the target host.

Corrective action

Take the corrective action that matches the cause.

- Make sure that the target host name is correct.
- Make sure that the target host has been started.
- Make sure that there are no communication problems with the target host.

The message KNAN20101-E: Communication error occurred in establishing the connection.

Cause

The following are possible causes:

- The target host name is invalid.
- The target host has not been started.
- An error occurred in communications with the target host.

Corrective action

Take the corrective action that matches the cause.

- Make sure that the target host name is correct.
- Make sure that the target host has been started.
- Make sure that there are no communication problems with the connection-target host.

The message KNAN20102-E: Communication error occurred in establishing the connection. *is output.*

Cause

The following are possible causes:

- The target host name is invalid.
- The port number is invalid.
- The target host has not been started.
- An error occurred in communications with the target host.

Corrective action

Take the corrective action that matches the cause.

- Make sure that the target host name is correct.
- Make sure that the port number is available.
- Make sure that the target host has been started.
- Make sure that there are no communication problems with the connection-destination host.

The message KNAN20103-E: A communication error occurred while sending data. *is output.*

Cause

A communication error occurred between the connecting host and the authentication server.

Corrective action

Check the following, and then retry the operation:

- Make sure that the name of the connecting host is correct.
- Make sure that the connecting host is running.
- Make sure that there are no communication problems with the connecting host.

The message KNAN20104-E: A communication error occurred while receiving data . *is output.*

Cause

A communication error occurred during an attempt to connect to the host.

Corrective action

Check the following, and then retry the operation:

- Make sure that the target host name is correct.
- Make sure that the port number is correct.
- Make sure that the target host has been started.
- Make sure that there are no communication problems with the target host.

(2) Actions to take when an attempt to connect to the event service fails

Cause 1

The event service on the manager host is not running.

Corrective action 1

Use the `jbs_spmd_status` command to check whether the event service is running on the manager host.

If the service is not running, start the service.

Cause 2

The `server` parameter is set incorrectly in the API settings file (`api`).

Corrective action 2

Match the setting of the `server` parameter in the API settings file (`api`) to the setting of the `ports` parameter in the event server settings file (`conf`).

If a host name is specified as the address in the `server` parameter in the API settings file (`api`) or the `ports` parameter in the event server settings file (`conf`), the host name might not resolve to the correct IP address. This is because the resolution process depends on the operating system.

For details about the API settings file (`api`) and the event server settings file (`conf`), see the chapters on these files in the *JP1/Base User's Guide*.

Cause 3

JP1/IM - Manager is running on an IPv6 host.

Corrective action 3

JP1/IM - Manager does not support IPv6 hosts. Therefore, when the monitored host is an IPv6 host, install JP1/IM - Manager on an IPv4/IPv6 host. Follow the instructions in error messages to take corrective action.

(3) Actions to take when the definition menu is not displayed in the Event Console window

In the **Options** menu of the Event Console window, menu-related definitions are disabled.

Cause

The JP1 resource group settings are invalid.

Corrective action

Make sure that in the JP1 resource group settings, the group name `JP1_Console` is specified for the JP1 resource group of the logged-in JP1 user, and `JP1_Console_Admin` or `JP1_Console_Operator` is specified for the permission level.

(4) Actions to take when the trapped JP1 event message indicates unreadable characters

The following are possible causes:

- The character encoding of the monitored log file does not match the encoding specified on the **Configuration File** page.
- The specified character encoding is not supported on the agent host.

The corrective action to take for each case is described as follows:

*The character encoding of the monitored log file does not match the encoding specified on the **Configuration File** page.*

Correct the character encoding of monitored log file, and then retry the operation.

Note that this problem can also occur in remote monitoring.

The specified character encoding is not supported on the agent host.

Even when the character encoding is supported by JP1/IM - Manager, it might not be specifiable for the version of JP1/Base installed on the agent host. Check the version of JP1/Base installed on the agent host, and set a supported character encoding. Then retry the operation.

(5) Actions to take when you cannot execute a command

*In the Execute Command window, the message KAVB0415-E: The command cannot be executed because the business group or monitoring group specified for the execution host name is not defined. (execution host name = *execution-host-name*) is output.*

Cause

The business group or monitoring group specified for the execution host name is not defined.

Corrective action

Review the business group or monitoring group, and then re-execute the command. Note that the information in this message cannot be checked by using the `jcocmdshow` command of JP1/Base.

If you are still unable to execute the command, contact the system administrator and confirm the settings of the business group.

*In the Execute Command window, the message KAVB0416-E: The command cannot be executed because the host specified for the execution host name is not a management target. (execution host name = *execution-host-name*) is output.*

Cause

The host specified for the execution host name is not a managed host.

Corrective action

Check the type of host and then re-execute the command. Note that the information in this message cannot be checked by using the `jcocmdshow` command of JP1/Base.

If you are still unable to execute the command, contact the system administrator and check the settings of the business group.

*In the Execute Command window, the message KAVB0417-E: The command cannot be executed because the user does not have the permissions necessary to execute it on the business group specified in the execution host name. (execution host name = *execution-host-name*) is output.*

Cause

No permission is required for executing the command for the business group specified for the execution host name.

Corrective action

Review the business group or monitoring group, and then re-execute the command. Note that the information in this message cannot be checked by using the `jcocmdshow` command of JP1/Base.

If you are still unable to execute the command, contact the system administrator and check the settings of the business group.

*In the Execute Command window, the message KAVB0418-E: The command cannot be executed because the user does not have the permissions necessary to execute on the host specified in the execution host name. (execution host name = *execution-host-name*) is output.*

Cause

No permission is required for executing the command on the host specified for the execution host name.

Corrective action

Review the host and then re-execute the command. Note that the information in this message cannot be checked by using the `jcocmdshow` command of JP1/Base.

If you are still unable to execute the command, contact the system administrator and check the settings of the business group.

*In the Execute Command window, the message KAVB0419-E: The command cannot be executed because a host group is defined with the same name as the host name specified for the execution host name. (execution host name = *execution-host-name*) is output.*

Cause

The host group name specified for the destination host name is the same as the execution host name.

Corrective action

Confirm that no host group has the same name as the host name specified for the execution host name. If there is such a host group, change either name of the host or of the host group.

*In the Execute Command window, the message KAVB0422-E: A host is not defined for the business group or monitoring group. (group name = *group-name*) is output.*

Cause

No host is defined for the business group or monitoring group specified for the execution host name.

Corrective action

Define a host for the specified business group or monitoring group. Also review the coding of the business group or monitoring group path.

*In the Execute Command window, the message KAVB0423-E: The business group or monitoring group is not defined. (group name = *group-name*) is output.*

Cause

The business group or monitoring group specified for the execution host name is not defined.

Corrective action

Define the specified business group or monitoring group. Also review the coding of the business group or monitoring group path.

In the Execute Command window, the message KAVB2027-E: Cannot execute the command. Failed to simulate the user `user-name` environment. is output.

Cause

The user mapping setting is invalid.

Corrective action

Check the user mapping setting. If it is not set, set it. This setting is required in Windows.

When the host specified for the mapping source server name is using DNS, a domain name must be included in the setting. If the host name is correct but the simulation still fails, check whether DNS is being used. For details about the user mapping setting, see the chapter related to user mapping in the *JP1/Base User's Guide*.

In the Execute Command window, the message KAVB2031-E: Cannot execute the command. The host (`host-name`) is not managed by JP1/Console. is output.

Cause

The definition of the configuration definition file is invalid. Alternatively, the executing host name cannot be resolved.

Corrective action

- Make sure the configuration information is defined in the configuration definition file.
- Make a correction so that the executing host name can be resolved.
- If this message is output in an environment in which both a physical host and a logical host are started under Windows, the network settings are insufficient. For details, see the section on building both a physical host environment and a logical host environment on the same host, in the notes related to cluster operation (Windows only) in the *JP1/Base User's Guide*.

In the Execute Command window, the message KAVB8452-E: The operation cannot be executed because the reference/operation permission function of the business group changed from active to inactive while logged in. is output.

Cause

The reference/operation permission of the business group changed from active to inactive while JP1/IM - View was connected.

Corrective action

Restart and log in to JP1/IM - View, and then re-execute the command.

The execution result from the DOS prompt differs from the execution result in the Execute Command window, or it differs from the execution result of an automated action.

Cause

The OS user environment used for execution is invalid.

Corrective action

Enable the `-loaduserprofile` option of the `jcocmddef` command. For details, see 7.4.4(3)(c) *Environment for command execution* in the *JP1/Integrated Management - Manager Overview and System Design Guide*. See also the chapter that explains commands in the *JP1/Base User's Guide*.

When the command is executed from the Preview Command Execution Content window, the message KAVB0002-E is output, and then the command is suspended.

Cause

The name of an execution host or an execution command was not specified.

Corrective action

Specify an execution host or a command, and then re-execute the command.

When the command is executed from the Preview Command Execution Content window, the message KAVB1037-E is output, and then the command is suspended.

Cause

The value specified for the execution host name, execution command, or environment variable file exceeds the upper limit.

Corrective action

Correct the value of the item that exceeds the upper limit, and then re-execute the command.

The Execute Command window cannot be started, and the message KAVB1046-E is output.

Cause

An I/O error occurred when the configuration file for converting information was read.

Corrective action

Make sure that the necessary permission is set for the configuration file for converting information, and then re-execute the command.

If you are still unable to perform the operation, contact the system administrator.

(6) Actions to take when event information cannot be inherited

The attribute value is not inherited. Furthermore, warning information is displayed in the Preview Command Execution Content window.

Cause

The event has no attribute corresponding to the variable.

Alternatively, there is no attribute value corresponding to the variable.

Corrective action

Check the specified event and the execution content of the command for which the variable is specified, and re-execute the command.

The event to be inherited is not displayed in the Execute Command window.

Cause

The menu or button that was clicked was not one for which events are inherited.

Corrective action

Select an event that can be inherited, and then click the menu or button for inheriting it.

A special character in the event inheritance information is not converted. Furthermore, the message KAVB1040-W, KAVB1041-W, KAVB1042-W, KAVB1043-W, or KAVB1044-W is output.

Cause

The configuration file for converting information is invalid.

Corrective action

Review the configuration file for converting information, and restart the Execute Command window.

All of the characters before cutoff are not displayed in the Preview Command Execution Content window. Furthermore, the message KAVB1036-W is output.

Cause

The number of characters before truncation after variables are replaced exceeds the maximum number of characters that can be displayed in the text area in the Preview Command Execution Content window.

Corrective action

Review the execution content of the command for which the variables are specified, and then re-execute the command.

(7) Actions to take when you cannot execute a command from the Command button

The message KAVB1035-E is output, and the command is suspended.

Cause

Although the executed command is set to inherit an event, nothing is specified as the event to be inherited.

Corrective action

Specify an event to be inherited, and then re-execute the command.

The message KAVB0002-E is output, and the command is suspended.

Cause

After the event information is inherited, the value of the execution host name or execution command is an empty string.

Corrective action

Make sure that the variable names of the items set for the executing command and the event to be inherited are correct, and then re-execute the command.

The message KAVB1037-E is output, and the command is suspended.

Cause

After the event information is inherited, the value specified for the execution host name, execution command, or environment variable file exceeds the upper limit.

Corrective action

Review the value of the item that exceeds the upper limit, and then re-execute the command.

(8) Actions to take when you cannot start a client application

In the Execute Command window, the message KAVB1034-E is output, and the command is suspended.

The following are possible causes:

- The path to the command execution file was not found.
- You do not have the necessary permission for executing the command.
- An I/O error occurs when the command process starts.

The following describes the corrective action to take for each case:

The path to the command execution file is not found.

Review the command line and make sure that the command can be executed at the command prompt. Then re-execute the command.

You do not have permissions necessary for executing the command.

Confirm that you have execution permission for the command to be executed and make sure that the command can be executed at the command prompt. Then re-execute the command.

An I/O error occurs when the command process starts.

Make sure that the command to be executed can be executed at the command prompt, and then re-execute the command.

(9) Actions to take when a command execution log file is damaged

If an operation to write data into a command execution log file is interrupted by, for example, a machine stoppage caused by a power failure, the command execution log file for automated actions or the command execution log file for command execution may be damaged.

In such cases, the following messages are issued:

- In the Action Log Details window of JP1/IM - View, or when the `jcashowa` command is executed to display the execution result of an automated action, the message `KAVB5151-W Failed to get data from Command Executed log file .` is displayed as the execution result.

The command execution log file for automated actions may be damaged.

- When the `jcocmdlog` command is executed, the message `KAVB2523-E The command-execution log file for the executed command cannot be opened .` is output.

The command execution log file for command execution may be damaged.

- When the `jcocmdlog` command is executed, the message `KAVB2525-E The command-execution log file for the automatic action cannot be opened .` is output.

The command execution log file for automated actions may be damaged.

- When the `jcocmdlog` command is executed, the message `KAVB2527-E An attempt to read the command-execution log file has failed .` is output.

- If `-act` is specified for the option, the command execution log file for automated actions may be damaged.
- If `-window` is specified for the option, the command execution log file for command execution may be damaged.
- If neither `-act` nor `-window` is specified for the option, the command execution log file for automated actions or command execution may be damaged.

- The message `KAVB2064-E Error in writing execution results to Command execution log .` is output to the integrated trace log.

The command execution log file for automated actions or the command execution log file for command execution may be damaged.

If any of these messages is output, use the following procedure to check the status of the command execution log file.

1. Use the procedure in (a) below to check the file that may have been damaged.
2. If it is not damaged, take the correction action prescribed in each message.
3. If it is damaged, restore it using the procedure described in (b).
4. If the file cannot be restored using the procedure in (b), follow the procedure in (c) to delete the command execution log file.

(a) How to check the command execution log files

Checking the command execution log file for automated actions

- In Windows

From the command prompt, execute the following commands:

```
cd Base-path\log\COMMAND
```

(For a logical host: `cd shared-folder\jplbase\log\COMMAND`)

`Jischk -l3 Base-path\log\COMMAND\ACTISAMLOGV8`

- In UNIX

Execute the following command:

`cd /var/opt/jplbase/log/COMMAND`

(For a logical host: `cd shared-directory/jplbase/log/COMMAND`)

`/opt/jplbase/bin/Jischk -l3 actisamlogv8`

Checking the command execution log file for command execution

- In Windows

From the command prompt, execute the following commands:

`cd Base-path\log\COMMAND`

(For a logical host: `cd shared-folder\jplbase\log\COMMAND`)

`Jischk -l3 Base-path\log\COMMAND\CMDISAMLOGV8`

- In UNIX

Execute the following command:

`cd /var/opt/jplbase/log/COMMAND`

(For a logical host: `cd shared-directory/jplbase/log/COMMAND`)

`/opt/jplbase/bin/Jischk -l3 cmdisamlogv8`

If the `Jischk` command does not detect file invalidity, the command execution log file is not damaged. If the `Jischk` command detects file invalidity, follow the procedure described in (b) below to restore the command execution log file.

For details about the `Jischk` command, see the *JPI/Base User's Guide*.

(b) How to restore the command execution log files

Restoring the command execution log file for automated actions

- In Windows

Perform the following operations with Administrator permissions. Also, for the restoration operation you need free space that is approximately three times the size of `ACTISAMLOGV8.DRF`.

1. Stop JP1/IM - Manager.
2. Stop JP1/Base.
3. From the command prompt, execute the commands listed below to restore the command execution log file.

For details about the `Jiscond` command, see the *JPI/Base User's Guide*.

`cd Base-path\log\COMMAND`

(For a logical host: `cd shared-folder\jplbase\log\COMMAND`)

`Jiscond ACTISAMLOGV8`

4. From the command prompt, execute the following command to check whether the command execution log file has been normally restored:

`Jischk -l3 ACTISAMLOGV8`

If the `Jischk` command detects file invalidity, the command execution log file cannot be restored. If the file cannot be restored, follow the procedure described in (c) below to delete the command execution log file for automated actions.

5. Start JP1/Base.
6. Start JP1/IM - Manager.

- In UNIX

Perform the following operations with superuser permissions. Also, for the restoration operation you need free space that is approximately three times the size of `actisamlogv8.DAT`.

1. Stop JP1/IM - Manager.
2. Stop JP1/Base.
3. Execute the commands listed below to restore the command execution log file.

For details about the `Jiscond` command, see the *JP1/Base User's Guide*.

```
cd /var/opt/jplbase/log/COMMAND
```

(For a logical host: `cd shared-directory/jplbase/log/COMMAND`)

```
/opt/jplbase/bin/Jiscond actisamlogv8
```

4. From the command prompt, execute the following command to check whether the command execution log file has been normally restored:

```
/opt/jplbase/bin/Jischk -l3 actisamlogv8
```

If the `Jischk` command detects file invalidity, the command execution log file cannot be restored. If the file cannot be restored, follow the procedure in (c) to delete the command execution log file for automated actions.

5. Start JP1/Base.
6. Start JP1/IM - Manager.

Restoring the command execution log file for command execution

- In Windows

Perform the following operations with Administrator permissions. Also, for the restoration operation you need free space that is approximately three times the size of `CMDISAMLOGV8.DRF`.

1. Stop JP1/IM - Manager.
2. Stop JP1/Base.
3. From the command prompt, execute the commands listed below to restore the command execution log file.

For details about the `Jiscond` command, see the *JP1/Base User's Guide*.

```
cd Base-path\log\COMMAND
```

(For a logical host: `cd shared-folder\jplbase\log\COMMAND`)

```
Jiscond CMDISAMLOGV8
```

4. From the command prompt, execute the following command to check whether the command execution log file has been normally restored:

```
Jischk -l3 CMDISAMLOGV8
```

If the `Jischk` command detects file invalidity, the command execution log file cannot be restored. If the file cannot be restored, follow the procedure described in (c) below to delete the command execution log file for command execution.

5. Start JP1/Base.
6. Start JP1/IM - Manager.

- In UNIX

Perform the following operations with superuser permissions. Also, for the restoration operation you need free space that is approximately three times the size of `cmdisamlogv8.DAT`.

1. Stop JP1/IM - Manager.
2. Stop JP1/Base.
3. Execute the following command:

```
cd /var/opt/jp1base/log/COMMAND
```

 (For a logical host: `cd shared-directory/jp1base/log/COMMAND`)

```
/opt/jp1base/bin/Jiscond cmdisamlogv8
```
4. From the command prompt, execute the following command to check whether the command execution log file has been normally restored:

```
/opt/jp1base/bin/Jischk -l3 cmdisamlogv8
```

 If the `Jischk` command detects file invalidity, the command execution log file cannot be restored. If the file cannot be restored, follow the procedure described in (c) below to delete the command execution log file for command execution.
5. Start JP1/Base.
6. Start JP1/IM - Manager.

(c) How to delete the command execution log files

Deleting the command execution log file for automated actions

When you delete the command execution log file for automated actions, all history on past automated actions is lost. Therefore, if deletion will cause a problem, back up the files. For details, see [1.2.2 Database backup and recovery](#).

1. Stop JP1/IM - Manager.
2. Stop JP1/Base.
3. Delete the command execution log file.

Delete the files listed in the table below if you could not restore the command execution log file for automated actions. For details about the command execution log file, see the *JP1/Base User's Guide*.

In Windows

Table 10–27: Locations of files to be deleted (Windows)

File name	Location
Command execution log file for automated actions	<ul style="list-style-type: none"> • <i>Base-path</i>\log\COMMAND\ACTISAMLOGV8.DRF • <i>Base-path</i>\log\COMMAND\ACTISAMLOGV8.K01 • <i>Base-path</i>\log\COMMAND\ACTISAMLOGV8.KDF
	<ul style="list-style-type: none"> • <i>shared-folder</i>\jp1base\log\COMMAND\ACTISAMLOGV8.DRF • <i>shared-folder</i>\jp1base\log\COMMAND\ACTISAMLOGV8.K01 • <i>shared-folder</i>\jp1base\log\COMMAND\ACTISAMLOGV8.KDF
Action information file	<i>Console-path</i> \log\action\actinf.log
	<i>shared-folder</i> \jp1cons\log\action\actinf.log
Action host name file	<i>Console-path</i> \log\action\acttxt{1 2}.log
	<i>shared-folder</i> \jp1cons\log\action\acttxt{1 2}.log

In UNIX

Table 10–28: Locations of files to be deleted (UNIX)

File name	Location
Command execution log file for automated actions	<ul style="list-style-type: none"> • /var/opt/jplbase/log/COMMAND/actisamlogv8.DAT • /var/opt/jplbase/log/COMMAND/actisamlogv8.K01 • /var/opt/jplbase/log/COMMAND/actisamlogv8.DEF
	<ul style="list-style-type: none"> • <i>shared-directory</i>/jplbase/log/COMMAND/actisamlogv8.DAT • <i>shared-directory</i>/jplbase/log/COMMAND/actisamlogv8.K01 • <i>shared-directory</i>/jplbase/log/COMMAND/actisamlogv8.DEF
Action information file	/var/opt/jplcons/log/action/actinf.log
	<i>shared-directory</i> /jplcons/log/action/actinf.log
Action host name file	/var/opt/jplcons/log/action/acttxt{1 2}.log
	<i>shared-directory</i> /jplcons/log/action/acttxt{1 2}.log

4. Start JP1/Base.

5. Start JP1/IM - Manager.

Deleting the command execution log file for command execution

When you delete the command execution log file for command execution, all history on past command execution is lost. Therefore, if deletion will cause a problem, back up the files. For details, see [1.2.2 Database backup and recovery](#).

1. Stop JP1/IM - Manager.

2. Stop JP1/Base.

3. Delete the command execution log file.

Delete the files listed in the table below if you could not restore the command execution log file for command execution. For details about the command execution log file, see the *JP1/Base User's Guide*.

In Windows

Table 10–29: Locations of files to be deleted (Windows)

File name	Location
Command execution log file for command execution	<ul style="list-style-type: none"> • <i>Base-path</i>\log\COMMAND\CMDISAMLOGV8.DRF • <i>Base-path</i>\log\COMMAND\CMDISAMLOGV8.K01 • <i>Base-path</i>\log\COMMAND\CMDISAMLOGV8.KDF
	<ul style="list-style-type: none"> • <i>shared-folder</i>\jplbase\log\COMMAND\CMDISAMLOGV8.DRF • <i>shared-folder</i>\jplbase\log\COMMAND\CMDISAMLOGV8.K01 • <i>shared-folder</i>\jplbase\log\COMMAND\CMDISAMLOGV8.KDF

In UNIX

Table 10–30: Locations of files to be deleted (UNIX)

File name	Location
Command execution log file for command execution	<ul style="list-style-type: none"> • /var/opt/jplbase/log/COMMAND/cmdisamlogv8.DAT • /var/opt/jplbase/log/COMMAND/cmdisamlogv8.K01 • /var/opt/jplbase/log/COMMAND/cmdisamlogv8.DEF
	<ul style="list-style-type: none"> • <i>shared-directory</i>/jplbase/log/COMMAND/cmdisamlogv8.DAT

File name	Location
	<ul style="list-style-type: none"> <i>shared-directory</i>/jplbase/log/COMMAND/cmdisamlogv8.K01 <i>shared-directory</i>/jplbase/log/COMMAND/cmdisamlogv8.DEF

4. Start JP1/Base.

5. Start JP1/IM - Manager.

(10) Actions to take when Unknown is displayed as the automated action execution status

There may be inconsistencies among the files in which automated action execution results are saved (action information file, action host name file, and command execution log file).

If so, you need to delete the files in which automated action execution results are saved. If you delete these files, you will no longer be able to view past automated action execution results. Therefore, if deletion will cause a problem, back up the files. For details, see [1.2.2 Database backup and recovery](#).

The deletion procedure follows:

1. Stop JP1/IM - Manager and then stop JP1/Base.

In the case of a cluster configuration, operate the cluster software to stop the logical hosts. After you have confirmed that they have stopped, mount a shared disk in the shared directory.

2. Delete the action information file, action host name file, and command execution log file.

The table below shows the locations of the files to delete.

In Windows

Table 10–31: Locations of files to delete (Windows)

File name	Location
Action information file	<i>Console-path</i> \log\action\actinf.log
	<i>shared-folder</i> \jplcons\log\action\actinf.log
Action host name file	<i>Console-path</i> \log\action\acttxt{1 2}.log
	<i>shared-folder</i> \jplcons\log\action\acttxt{1 2}.log
Command execution log file	All files under <i>Base-path</i> \log\COMMAND\
	All files under <i>shared-folder</i> \jplbase\log\COMMAND\

In UNIX

Table 10–32: Locations of files to delete (UNIX)

File name	Location
Action information file	/var/opt/jplcons/log/action/actinf.log
	<i>shared-directory</i> /jplcons/log/action/actinf.log
Action host name file	/var/opt/jplcons/log/action/acttxt{1 2}.log
	<i>shared-directory</i> /jplcons/log/action/acttxt{1 2}.log

File name	Location
Command execution log file	All files under <code>/var/opt/jplbase/log/COMMAND/</code>
	All files under <code>shared-directory/jplbase/log/COMMAND/</code>

3. Start JP1/Base and then start JP1/IM - Manager.

In the case of a cluster configuration, unmount the shared disk and then operate the cluster software to start the logical hosts.

(11) Actions to take when an automated action is delayed

When the automated action status remains Running.

First, use the `jcocmdshow` command[#] to check the command status. The action to take differs depending on the result. The possible cause for each obtained result and the action to take in each case are explained below.

There is a command whose command execution lapse time (ETIME) is too long.

Cause

A command is executing that does not terminate, or that is taking a long time.

Corrective action

Using the `jcocmddel` command,[#] delete the command that does not terminate. For details, see [7.1.4 Checking command execution status and deleting a command](#) in this manual, and see [7.4.4\(6\) Commands for troubleshooting](#) in the *JP1/Integrated Management - Manager Overview and System Design Guide*.

The message KAVB2239-E: A network connection with the connected host could not be established. is displayed.

Cause

JP1/Base on the executing host stopped while the command was being executed.

Corrective action

Restart JP1/Base on the executing host.

As a means of monitoring JP1/Base, the JP1/Base health check function is available. For details, see [7.4.8 JP1/Base health check function](#) in the *JP1/Integrated Management - Manager Overview and System Design Guide*.

There are a large number of commands whose execution status (STATUS) is Q.

Cause

The number of automated actions to be executed is too large.

Corrective action

Check the automated actions being executed and reassess the following:

- Were any unnecessary automated actions set?
- Is it possible to narrow the JP1 events for which automated actions are to be set?

If there are no unnecessary automated actions, use the `jcocmddef` command[#] to increase the number of commands that can be executed simultaneously. For details, see [12.7.6 Command execution environment](#) in the *JP1/Integrated Management - Manager Overview and System Design Guide*.

#

For details about the `jcocmdshow` command, `jcocmddel` command, and `jcocmddef` command, see the chapter explaining commands in the *JP1/Base User's Guide*.

(12) Actions to take when the monitored object database is damaged

Messages such as KAVB7247-E: JP1/IM-CS could not execute the operation request (request-name) from JP1/IM-View. (Cause: The record in the database is invalid) . and KAVB7248-E: JP1/IM-CS could not execute the operation request (request-name) from JP1/IM-View. (Cause: The database cannot be operated) . are output.

Cause

The following is the possible cause:

- Logical conflict has occurred in the monitored object database of JP1/IM - Manager.

Corrective action

Take the following steps:

1. Stop JP1/IM - Manager.
2. Collect a backup of the *Scope-path*\database folder for problem investigation.
3. Execute the `jcsdbsetup -f` command.
4. Delete all files from the *Scope-path*\database\jcshosts folder.
5. Execute the `jcshostsimpport -r jcshosts` command.
6. Start JP1/IM - Manager.

(13) Actions to take when the monitored object database cannot be unlocked

The monitored object database stays locked.

Cause

The following is the possible cause:

- An attempt to acquire a lock on the monitored object database of JP1/IM - Manager failed.

Corrective action

Take the following steps:

1. Execute the `jco_spm�_status` command to make sure the `jcsmain` process is not active.
2. Execute the `Jismlcktr` command.
3. Determine which process has locked the files under *Scope-path*\database.
4. Execute the `Jislckfree -p PID` command on the process ID determined in Step 3.

The `Jismlcktr` and `Jislckfree` commands are provided by JP1/Base. For details, see the chapter that explains commands in the *JP1/Base User's Guide*.

(14) Actions to take when KAVB5150-W is displayed in the detailed information (message) for the action result

When the Action Log Details window is opened, the message KAVB5150-W: There is no applicable data in the Command Executed log file. is displayed in the message column.

Cause

The command execution log file (ISAM) may have wrapped. If it has wrapped, automated action execution results cannot be displayed.

Corrective action

If this phenomenon occurs frequently, consider increasing the upper limit for the record count in the command execution log file. Keep in mind, however, that increasing the record count will also use more disk space.

The procedure follows:

Changing the upper limit for the record count

When you increase the upper limit for the record count, you must delete the command execution log file to enable the new setting. When you delete the command execution log file, all history on past automated actions and command execution is lost. Therefore, if deletion will cause a problem, back up the files. For details, see [1.2.2 Database backup and recovery](#).

1. Execute the `jcocmddef` command to change the record count in the command execution log file.
2. Stop JP1/IM - Manager and JP1/Base.

In the case of a cluster configuration, operate the cluster software to stop the logical hosts.

After you have confirmed that they have stopped, mount a shared disk in the shared directory.

3. Delete the command execution log files.

This means all files under the command execution log folder. The default command execution log folder is described below.

In Windows

Table 10–33: Locations of command execution log files (Windows)

File name	Location
Command execution log file	All files under <i>Base-path</i> \log\COMMAND\
	All files under <i>shared-folder</i> \jplbase\log\COMMAND\

In UNIX

Table 10–34: Locations of command execution log files (UNIX)

File name	Location
Command execution log file	All files under <i>/var/opt/jplbase/log/COMMAND/</i>
	All files under <i>shared-directory/jplbase/log/COMMAND/</i>

For details about the command execution log file, see the *JP1/Base User's Guide*.

4. Start JP1/Base and JP1/IM - Manager.

In the case of a cluster configuration, unmount the shared disk and then operate the cluster software to start the logical hosts.

For details about the `jcocmddef` command, see the chapter that explains commands in the *JP1/Base User's Guide*.

(15) Actions to take when an earlier version of JP1/IM - Manager or JP1/IM - View is being used

The actions to take differ depending on the message that is output.

The message KAVB6060-E: The connection destination server did not respond. *is displayed.*

Cause

The version of JP1/IM - Manager is earlier than the version of JP1/IM - View, or an earlier version of the monitored object database is being used.

Corrective action

When the version of JP1/IM - Manager is earlier than the version of JP1/IM - View:

Use the following procedure to upgrade the JP1/IM - Manager version.

1. In the Monitoring Tree (Editing) window, choose **File** and then **Save Tree**, and save the edited monitoring tree in the `CSV` file.
2. Upgrade JP1/IM - Manager to the same version as JP1/IM - View.
3. In the Monitoring Tree (Editing) window, choose **File** and then **Open Tree**, and load the `CSV` file that was saved.
4. In the Monitoring Tree (Editing) window, choose **File** and then **Update Server Tree** to update the server tree.

When the version of JP1/IM - View is the same as the version of JP1/IM - Manager Scope, but an earlier version of the monitored object database is being used:

Follow the procedure below to upgrade the monitored object database version.

1. In the Monitoring Tree (Editing) window, choose **File** and then **Save Tree**, and save the edited monitoring tree in the `CSV` file.
2. Upgrade the monitored object database version.
3. In the Monitoring Tree (Editing) window, choose **File** and then **Open Tree**, and load the `CSV` file that was saved.
4. In the Monitoring Tree (Editing) window, choose **File** and then **Update Server Tree** to update the server tree.

For details about upgrading the monitored object database version, see the following sections:

- For a physical host
 - Windows: *1.18.3(1) Executing the Central Scope upgrade command in the JP1/Integrated Management - Manager Configuration Guide*
 - UNIX: *2.17.5(2) Executing the Central Scope upgrade command in the JP1/Integrated Management - Manager Configuration Guide*
- For a logical host
 - Windows: *6.5 Upgrade installation and setup of logical hosts (for Windows) in the JP1/Integrated Management - Manager Configuration Guide*
 - UNIX: *7.5 Upgrade installation and setup of logical hosts (for UNIX) in the JP1/Integrated Management - Manager Configuration Guide*

When the version of JP1/IM - Manager is later than the version of JP1/IM - View, and an earlier version of the monitored object database is being used:

Follow the procedure below to upgrade the JP1/IM - View version.

1. In the Monitoring Tree (Editing) window, choose **File** and then **Save Tree**, and save the edited monitoring tree in the `CSV` file.
2. Uninstall JP1/IM - Manager.
3. Delete the JP1/IM - Manager installation directory.
4. Install the version of JP1/IM - Manager or JP1/IM - Central Scope that matches the version of JP1/IM - View.
5. In the Monitoring Tree (Editing) window, choose **File** and then **Open Tree**, and load the `CSV` file that was saved.
6. In the Monitoring Tree (Editing) window, choose **File** and then **Update Server Tree** to update the server tree.

7. Upgrade JP1/IM - Manager to the later version.
8. Upgrade JP1/IM - View to the same version as JP1/IM - Manager.

The message KAVB6046-E: The user (*user*) does not have permission necessary for operations. *is displayed.*

Cause

The version of JP1/IM - View is earlier than the version of JP1/IM - Manager, or the edited data in JP1/IM - View is from an earlier version.

Corrective action

Follow the procedure below to upgrade the version of JP1/IM - View.

1. In the Monitoring Tree (Editing) window, choose **File** and then **Save Tree**, and save the edited monitoring tree in the `csv` file.
2. Uninstall JP1/IM - Manager.
3. Delete the JP1/IM - Manager installation directory.
4. Install the JP1/IM - Manager version that is the same version as JP1/IM - View.
5. In the Monitoring Tree (Editing) window, choose **File** and then **Open Tree**, and load the `csv` file that was saved.
6. In the Monitoring Tree (Editing) window, choose **File** and then **Update Server Tree** to update the server tree.
7. Upgrade JP1/IM - Manager to the later version.
8. Upgrade JP1/IM - View to the same version as JP1/IM - Manager.

(16) Actions to take when many JP1 events occurred for which correlation events were generated

If an operation such as system maintenance generates a large number of JP1 events for which correlation events are generated, the correlation event generation process may become overloaded.

The following two methods are available for avoiding this situation:

- Pause the correlation event generation process.
- Stop JP1/IM - Manager.

Stop JP1/IM - Manager only if the problem cannot be avoided even after the correlation event generation process has been paused.

Pausing the correlation event generation process

Pause the correlation event generation process, and resume it once the situation has improved.

The procedure follows:

1. Execute the `jcoegsstop` command to pause correlation event generation processing.
Executing the `jcoegsstop` command places Event Generation Service in standby status. This means that JP1 events generated during this period are not processed.
Since the command stops only the processing without actually stopping the service, operations can continue without failover during cluster operation.
2. To resume correlation event generation processing, execute the `jcoegsstart` command.

Stopping JP1/IM - Manager

When you stop JP1/IM - Manager, if the startup option is set to `cold`, there is no need to perform the procedure described below. Perform it only when the startup option is set to `warm`.

The procedure follows:

1. Edit the correlation event generation system profile (`egs_system.conf`) and then change the startup option to `cold`.
2. Restart JP1/IM - Manager.
3. Edit the correlation event generation system profile (`egs_system.conf`) and then change the startup option back to `warm`.
4. Execute the `jco_spmd_reload` command to enable the startup option setting.

(17) Actions to take when correlation events cannot be displayed in JP1/IM - View

The following are possible causes:

- Correlation event generation is not enabled.
- Correlation event generation definition has not been created.
- Correlation events are being filtered.
- The applied correlation event generation definition is damaged.

The action to take in response to each cause is described below.

Correlation event generation is not enabled.

Event Generation Service is an optional function and thus does not start by default. If Event Generation Service is not set to start, execute the `jcoimdef` command to set up the service to start. Event Generation Service will now start when JP1/IM - Manager is restarted.

To check whether the correlation event generation process is running, first restart JP1/IM - Manager and then execute the `jcoegsstatus` command to check whether Event Generation Service is in `RUNNING` status.

A correlation event generation definition has not been created.

Event Generation Service generates correlation events according to the correlation event generation definition. Since the correlation event generation definition is not created by default, correlation events are not generated.

After you have created the correlation event generation definition file, execute the `jcoegschange` command to apply the correlation event generation definition to Event Generation Service. You can use the `jcoegsstatus` command to check the correlation event generation definition that has been applied.

Correlation events are being filtered.

Check whether correlation events are not being filtered by an event acquisition filter, a user filter, a severe event filter, or a view filter.

Like normal JP1 events, correlation events are also filtered by an event acquisition filter, a user filter, a severe event filter, and a view filter. Furthermore, events for which no severity level has been defined are filtered by an event acquisition filter (in the default setting).

The applied correlation event generation definition is damaged.

If the message described below is output to the integrated trace log, the correlation event generation definition that was applied to Event Generation Service by the `jcoegschange` command may have been damaged.

- KAJV2246-E An incorrect definition was detected because the correlation event generation definition storage file is corrupt. (line = *line-number*, incorrect contents = *invalid-content*)

If this message is output, execute the `jcoegschange` command and apply the correlation event generation definition again.

(18) Actions to take when the JP1/IM - View window cannot be displayed after you log in to JP1/IM - View

After you log in to JP1/IM - View, the JP1/IM - View window is not displayed. The task bar shows the JP1/IM - View task bar button.

Cause

When you perform the following operation, the JP1/IM - View window is not displayed after you log in to JP1/IM - View:

- Terminating JP1/IM - View while a screen area was displayed in which JP1/IM - View was not shown because of the virtual window configuration.#

#

This configuration, by having more desktops than the display windows in the memory and by displaying each of the partitioned areas as a single virtual desktop, allows the user to use multiple desktops by switching among the windows.

This configuration is also called a *virtual desktop*.

Corrective action

Take one of the following corrective actions:

Corrective action 1

1. Press the **Alt + Tab** keys and select JP1/IM - View.
2. From the task bar, choose **Cascade Windows** to display all windows in a cascade.
3. Change the display positions and sizes of the JP1/IM - View and other windows.

Corrective action 2

1. Press the **Alt + Tab** keys and select JP1/IM - View.
2. From the task bar, choose **Tile Windows Horizontally** to display all windows as horizontal tiles.
3. Change the display positions and sizes of the JP1/IM - View and other windows.

Corrective action 3

1. Press the **Alt + Tab** keys and select JP1/IM - View.
2. From the task bar, choose **Tile Windows Vertically** and display all windows as vertical tiles.
3. Change the display positions and sizes of the JP1/IM - View and other windows.

Corrective action 4

1. Press the **Alt + Tab** keys and select JP1/IM - View.
2. From the Context menu of JP1/IM - View, choose **Move** and then use the cursor key to adjust the position.
3. Once you have decoded the position of the displayed window or its frame, press the **Enter** key.

Corrective action 5

1. Press the **Alt + Tab** keys and select JP1/IM - View.

2. From the Context menu of JP1/IM - View, choose **Maximize**, and with the window maximized, log out of JP1/IM - View.
3. After you log in to JP1/IM - View again, change the window's display position and size.

(19) Actions to take when command execution or a batch file executed in an automated action does not terminate normally (Windows only)

Cause

If all of the following conditions are present, batch file processing is interrupted and cannot be normally executed.

- The OS of the host specified as the command execution destination is Windows 2000.
- A batch file uses the FOR /F command.
- After the execution of the FOR /F command, the result is output to standard error.

Corrective action

Take one of the following corrective actions:

- Do not use the FOR /F command.
- Do not output the result to standard error after execution of the FOR /F command.

(20) Actions to take when an additional common exclusion-condition cannot be set

The message KAVB1155-E is output, and the additional common exclusion-condition cannot be registered.

Cause

The number of defined common exclusion-conditions had already reached the maximum number when an attempt was made to display the Common Exclusion-Condition Settings (Extended) window from the **Exclude by Common Exclusion-Conditions** menu, or to register the additional common exclusion-condition.

Corrective action

Delete unnecessary common exclusion-conditions groups.

The message KAVB1163-E is output, and the additional common exclusion-condition cannot be registered.

Cause

The following are possible causes:

- The event acquisition filter is operating in compatibility mode, or the common exclusion-conditions are operating in basic mode.
- The definition file is invalid.
- An attempt to switch the event acquisition filter failed.

Corrective action

Take the corrective action that matches the cause.

- If the common exclusion-conditions of JP1/IM - Manager do not operate in extended mode, check the operating mode of the common exclusion-conditions of JP1/IM - Manager and change the mode to extended mode. Then restart JP1/IM - View and retry the operation.
- Stop JP1/IM - Manager, change the operating mode of the common exclusion-conditions to basic mode. Next, change the mode back to extended mode and then initialize the definition of the common exclusion-conditions (extended).

- Confirm that the KAVB4003-I message is output to an integrated trace log of the manager, and then retry the operation. If the KAVB4003-I message has not been output and the integrated management database is being used, execute the `jimdbstatus` command to check the status of the IM database service. Confirm that the IM database service is running, confirm that the KAVB4003-I message has been output to an integrated trace log, and then retry the operation.

For other causes, check whether OS resources, such as file descriptors, are insufficient.

- For Windows: Windows event log
- For UNIX: Syslog

If OS resources are sufficient, use the data collection tool to collect data and then contact the system administrator.

The message KAVB1157-E is output, and the additional common exclusion-condition cannot be registered.

Cause

The filter of the common exclusion-conditions had already reached the maximum size when an attempt was made to display the Common Exclusion-Condition Settings (Extended) window from the **Exclude by Common Exclusion-Conditions** menu, or to register the additional common exclusion-condition.

Corrective action

Delete unnecessary common exclusion-conditions groups, or define the common exclusion-conditions groups so that they are within the maximum size of the filter.

The message KAVB0256-E is output, and the additional common exclusion-condition cannot be registered.

Cause

The specified common exclusion-conditions group name already existed when an attempt was made to register the additional common exclusion-condition.

Corrective action

Specify a different common exclusion-conditions group name, and then retry the operation.

The message KAVB1153-E is output in a log, and the attribute conditions set in the common-exclusion-conditions auto-input definition file are not automatically displayed in Event conditions when you display the Common Exclusion-Condition Settings (Extended) window from the Exclude by Common Exclusion-Conditions menu.

Cause

The common-exclusion-conditions auto-input definition file does not exist.

Corrective action

Make sure that:

- There is a common-exclusion-conditions auto-input definition file.
- You have permission to access the common-exclusion-conditions auto-input definition file.

Next, execute the `jco_spmc_reload` command or restart JP1/IM - Manager to reload the common-exclusion-conditions auto-input definition file.

The message KAVB1154-W is output in a log, and the automatically-specified conditions are not displayed in Event conditions when you display the Common Exclusion-Condition Settings (Extended) window from the Exclude by Common Exclusion-Conditions menu.

Cause

An attempt to read the common-exclusion-conditions auto-input definition file failed.

Corrective action

Check whether OS resources are insufficient.

- For Windows: Windows event log

- For UNIX: Syslog

If OS resources are sufficient, use the data collection tool to collect data, and then contact the system administrator.

The message KAVB1158-W is output in a log, and the automatically-specified conditions are not displayed in Event conditions when you display the Common Exclusion-Condition Settings (Extended) window from the Exclude by Common Exclusion-Conditions menu.

Cause

The common-exclusion-conditions auto-input definition file contains no definitions.

Corrective action

Set an attribute name in the common-exclusion-conditions auto-input definition file, and then either execute the `jco_spmc_reload` command or restart JP1/IM - Manager to reload the common-exclusion-conditions auto-input definition file.

The message KAVB1159-W or KAVB1160-W is output in a log, and the automatically-specified conditions are not displayed in Event conditions when you display the Common Exclusion-Condition Settings (Extended) window from the Exclude by Common Exclusion-Conditions menu.

Cause

The following are possible causes:

- An invalid attribute name is defined in the common-exclusion-conditions auto-input definition file.
- Duplicate attribute names are defined in the common-exclusion-conditions auto-input definition file.

Corrective action

Define a valid attribute name in the common-exclusion-conditions auto-input definition file, and then either execute the `jco_spmc_reload` command or restart JP1/IM - Manager to reload the common-exclusion-conditions auto-input definition file.

The message KAVB1161-W is output in a log, and the whole of Common exclusion-conditions group name in the Common Exclusion-Condition Settings (Extended) window is not displayed.

Cause

The common exclusion-conditions group name defined in the common-exclusion-conditions auto-input definition file exceeds 40 bytes.

Corrective action

Define the common exclusion-conditions group name in the common-exclusion-conditions auto-input definition file with no more than 40 bytes, and then either execute the `jco_spmc_reload` command or restart JP1/IM - Manager to reload the common-exclusion-conditions auto-input definition file.

The message KAVB1162-W is output in a log, and Common exclusion-conditions group name in the Common Exclusion-Condition Settings (Extended) window is displayed incorrectly.

Cause

A character that cannot be used in a common exclusion-conditions group name in the common-exclusion-conditions auto-input definition file was used.

Corrective action

Correct the common exclusion-conditions group name in the common-exclusion-conditions auto-input definition file, and then either execute the `jco_spmc_reload` command or restart JP1/IM - Manager to reload the common-exclusion-conditions auto-input definition file.

(21) Actions to take when processing of JP1 events received by JP1/IM - Manager (Central Scope) is delayed

Cause

Name resolution of the character string (host name or IP address) specified as an attribute value of the individual condition in the status-change condition settings may have failed.

Corrective action

The host name that could not be resolved is output to the following logs:

In Windows

```
Scope-path\log\jcsmain_trace{1|2|3}.log#
```

In UNIX

```
/var/opt/jp1scope/log/jcsmain_trace{1|2|3}.log#
```

#

Do not specify this log as the monitoring target of the JP1/Base log file trapping function.

If name resolution failed, one of the following messages is output in the aforementioned log file:

```
...fs_jcsHostsAccessPtr->getHostByName() is failed. (host = host-name-for-which-name-resolution-failed, jplerror = 2001)...
```

or

```
...fs_jcsHostsAccessPtr->getHostByAddr() is failed. (host = IP-address-for-which-name-resolution-failed, jplerror = 2001)...
```

Check one of these messages and specify **Host name comparison** as the individual condition. Then, use one of the methods described below to enable name resolution of the host name or IP address specified as the attribute value.

- Register in the host information database the host name or IP address specified as the attribute value of the individual condition.
- Register in the `jp1hosts` information or the `jp1hosts2` information of JP1/Base the host name or IP address specified as the attribute value of the individual condition.
- Register in `hosts` or DNS the host name or IP address specified as the attribute value of the individual condition.

(22) Actions to take when no response-waiting events are displayed in JP1/IM - View

Cause

The following are possible causes:

- The response-waiting event management function is disabled.
OFF might be specified as the value of the `-resevent` option of the `jcoimdef` command.
- No response-waiting events have been issued.
- Response-waiting events have been issued but were filtered by JP1/IM - Manager.

Corrective action

If the response-waiting event management function is disabled, enable it by executing the `jcoimdef` command with ON specified in the `-resevent` option.

If the response-waiting event management function is enabled, follow the steps below to identify the cause of the problem:

1. Check whether response-waiting events are registered in the event database on the JP1/IM - Manager host.

As a JP1 user such as the administrator who is not subject to an event receiver filter, check whether response-waiting events are registered in the event database by conducting an event search.

If there are no response-waiting events registered in the database, investigate further according to Step 2 below.

If there are response-waiting events in the database, a filter (an event acquisition filter or an event receiver filter) is filtering the events in JP1/IM - Manager. In this case, review the filter conditions.

2. Check the log files on the BJEX or JP1/AS host for BJEX errors, JP1/AS errors, or communication errors.

If an error message was output, take action as described in the message. BJEX or JP1/AS might have been set up incorrectly, or a communication error might have occurred.

(23) Actions to take when response-waiting events are displayed in JP1/IM - View but as ordinary JP1 events (the arrow icon does not appear and you cannot enter a response)

Cause

The following are possible causes:

- The response-waiting event management function is disabled.
OFF might be specified as the value of the `-resevent` option of the `jcoimdef` command.
- The JP1/IM - Manager host name is specified incorrectly in the BJEX or JP1/AS configuration.
An IP address might be specified instead of a host name.
- The response-waiting event was forwarded to a JP1/IM - Manager host other than the one set up in BJEX or JP1/AS.

Corrective action

Take the corrective action that matches the cause.

- Enable the response-waiting event management function.
Execute the `jcoimdef` command with ON specified in the `-resevent` option.
- Specify the correct JP1/IM - Manager host name in the settings of BJEX or JP1/AS.
- To respond to the response-waiting event, log in to the JP1/IM - Manager host specified in the BJEX or JP1/AS settings.

(24) Actions to take when no JP1 event is displayed in the Event Console window

Cause

Because no condition is specified in the exclusion-conditions or valid common exclusion-conditions for a filter, all JP1 events are excluded.

Corrective action

When a common exclusion-condition is used in extended mode, check the common exclusion history file to know whether a common exclusion-condition prevents JP1 events from being collected. If JP1 events are excluded, review the common exclusion-condition.

When no common exclusion-condition is used in extended mode or when the problem remains after you review common exclusion-conditions in extended mode, review the following filter exclusion conditions and common exclusion-conditions enabled in basic mode:

- Event acquisition filter
- User filter

- Severe event filter
- View filter

(25) Actions to take when a JP1 event is displayed late in the Event Console window

Cause

The following are possible causes:

- When regular expressions are used for event conditions (filter conditions[#], execution conditions for automated actions, event attribute conditions of the correlation event generation conditions, event conditions of the severity changing function, and event conditions of the mapping function of the event source host), the match processing when JP1 events are received might take a long time.

#

Indicates the pass conditions, exclusion-conditions, or valid common exclusion-conditions for the following filters:

- Event acquisition filter
- User filter
- Severe event filter
- When you set `local` as the method for obtaining the event-issuing host name in the automated action environment definition, reverse lookup of the host name from the source IP address of the event attributes might take a long time during the match processing of an automated action.
- When Central Scope is used, it might take a long time for JP1 events to be displayed in the Event Console window due to a possible failure to resolve the character string (host name or IP address) specified as an attribute value of the individual condition in the status-change condition settings, or due to the status change condition of the monitoring node.
- The `server` parameter might be set incorrectly in the API settings file (`api`), which might cause frequent communication errors while JP1/IM - Manager events are received due to a shortage of ports.

Corrective action

Take the corrective action that matches the cause.

- When regular expressions are used for event conditions (filter conditions[#], execution conditions for automated actions, event attribute conditions of correlation event generation conditions, event conditions of the severity changing function, and event conditions of the mapping function of the event source host), review the regular expressions and then restart JP1/IM - Manager. In addition, if you are using Central Scope and you use the status change condition of the monitoring node as an event condition, also review the regular expressions, and then restart JP1/IM - Manager.

#

Indicates the pass conditions, exclusion-conditions, or valid common exclusion-conditions for the following filters:

- Event acquisition filter
- User filter
- Severe event filter

If you use many regular expressions that are matched recursively, such as the expression `.*` (matches all characters), the match processing might take a long time. For details, see *Appendix G.4 Tips on using regular expressions* in the *JP1/Integrated Management - Manager Overview and System Design Guide*.

- When you set `local` as the method for obtaining the event-issuing host name in the automated action environment definition, the host name is resolved from the source IP address of the event attributes. In order to

shorten the time for reverse lookup of the host name, review the settings of the `hosts` file of the OS, or change the method of the event-issuing host name to `remote`, and then restart JP1/IM - Manager. For details about the method for obtaining the event-issuing host name, see *Automated action environment definition file (action.conf.update)* in *Chapter 2. Definition Files* of the manual *JP1/Integrated Management - Manager Command and Definition File Reference*. For details about the `hosts` setting of the OS, see *12.4.1 Host names and IP addresses* in the *JP1/Integrated Management - Manager Overview and System Design Guide*.

- When you use JP1/IM - Central Scope, in addition to the actions above, confirm whether name resolution of the character string (host name or IP address) specified as an attribute value of the individual condition in the status-change condition settings can be performed promptly. For details, see *10.5.1(21) Actions to take when processing of JP1 events received by JP1/IM - Manager (Central Scope) is delayed*.

Furthermore, if you use the memory-resident function for the status change condition of the monitoring object, the match processing time for a change of monitoring object status takes less time. When you estimate the memory requirements for securing sufficient memory, we recommend that you set this function. For details about the memory-resident function for the status change condition of the monitoring object, see *4.2.3 Status change conditions* in the *JP1/Integrated Management - Manager Overview and System Design Guide*.

- If the communication type of the `server` parameter is set to `close` in the API settings file (`api`), a temporary port is used each time JP1/IM - Manager receives an event, so temporary ports will run short. As a result, a communication error or delay in receiving events might occur. On the event server to which JP1/IM - Manager connects, in the API settings file (`api`), make sure that you set the communication type of the `server` parameter to `keep-alive`.

(26) Actions to take when a status cannot be changed

The following are possible causes:

- Connection cannot be established between the event console and Central Console. Alternatively, connection cannot be established between the event console and the `jcochstat` command.
- The specified JP1 event was an event that cannot be changed.
- Connection cannot be established between Event Console Service and Event Service.
- Connection cannot be established between Event Console Service and Event Base Service.
- Connection cannot be established between Event Base Service and the IM database service.

The action to take in response to each cause is described below.

Connection cannot be established between the event console and Central Console. Alternatively, connection cannot be established between the event console and the `jcochstat` command.

The event console on the manager may not have been started, the system (host or network) may be under a heavy workload, or the network settings may be invalid.

- Corrective action

Execute the `jco_spmd_status` command to check whether the event console on the manager has started, and then try to change the status again.

Alternatively, use the `ping` command, for example, to check whether the logged-in host is running normally, and then try to change the status again.

The specified JP1 event was an event that cannot be changed.

- Corrective action

Reassess the serial number inside the event database and then try to change the status again.

Connection cannot be established between Event Console Service and Event Service.

- Corrective action
Check whether Event Service has started, and then try to change the status again.

Connection cannot be established between Event Console Service and Event Base Service.

Event Base Service may not have been started, or the system (host or network) may be under a heavy workload.

- Corrective action
Execute the `jco_spmd_status` command to check whether Event Base Service on the manager has started, and then try to change the status again.

Connection cannot be established between the Event Base Service and the IM database service.

The IM database service may not have been started, or the system (host or network) may be under a heavy workload.

- Corrective action
First start the IM database service, and then try to change the status again.

(27) Actions to take when an event search cannot be performed

The following are possible causes:

- Connection cannot be established between the event console and the viewer.
- Connection cannot be established between Event Base Service and Event Console Service.
- Connection cannot be established between Event Base Service and the integrated monitoring database.
- Connection cannot be established between Event Console Service and Event Service.
- A JP1 event search was performed using an unsupported condition.
- The regular expression specified for performing the event search was invalid.
- When an event search was performed with an exclusion-condition specified, the JP1/Base version of the search host was 08-11 or earlier.

The action to take in response to each cause is described below.

Connection cannot be established between the event console and the viewer.

The event console on the manager may not have been started, the system (host or network) may be under a heavy workload, or the network settings may be invalid.

- Corrective action
Execute the `jco_spmd_status` command to check whether the event console on the manager has started, and then perform the event search again.
Alternatively, use the `ping` command, for example, to check whether the logged-in host is running normally, and then perform the event search again.

Connection cannot be established between Event Base Service and Event Console Service.

Event Base Service may not have been started, or the system (host or network) may be under a heavy workload.

- Corrective action
Execute the `jco_spmd_status` command to check whether Event Base Service has started on the manager, and then perform the event search again.

Connection cannot be established between Event Base Service and the integrated monitoring database.

The integrated monitoring database may not have been started, or the system (host or network) may be under a heavy workload.

- Corrective action

First start the integrated monitoring database, and then perform the event search again.

Connection cannot be established between Event Console Service and Event Service.

The Event Service instance at the target host may not have been started, the system (host or network) may be under a heavy workload, or the network settings may be invalid.

- Corrective action

Execute the `jevstat` command to check whether the Event Service instance at the target host has started, and then perform the event search again. For details about the `jevstat` command, see the *JP1/Base User's Guide*.

Alternatively, use the `ping` command or other means on the manager host to check whether the target host is running normally, and then perform the event search again.

A JP1 event search was performed using an unsupported condition.

A JP1 event search was performed using an unsupported condition (**Is contained**, **Is not contained**, **Regular expression**, or multiple statuses specified) for Event Service of JP1/Base Version 06-00 or earlier. Alternatively, a JP1 event search was performed using an unsupported condition (**Regular expression** specified) for Event Service of JP1/Base Version 06-51 or earlier.

- Corrective action

Make sure that **Is contained**, **Is not contained**, **Regular expression**, or multiple statuses are not selected, and then perform the search again.

The regular expression specified for performing the event search was invalid.

- Corrective action

Make sure the displayed regular expression is valid, and then re-execute the search.

When an event search was executed with an exclusion-condition specified, and the JP1/Base version of the target host was 08-11 or earlier.

- Corrective action

Check the version of JP1/Base on the host that is specified as the event search target, and if it is 08-11 or earlier, execute the search without using an exclusion-condition.

(28) Actions to take when memo entries cannot be set up

The following are possible causes:

- Connection cannot be established between the event console and Central Console - View.
- Connection cannot be established between Event Console Service and Event Base Service.
- Connection cannot be established between Event Base Service and the integrated monitoring database.

The action to take in response to each cause is described below.

Connection cannot be established between the event console and Central Console - View.

The event console on the manager may not have been started, the system (host or network) may be under a heavy workload, or the network settings may be invalid.

- Corrective action

Make sure that Event Console Service or the host is running normally, and then set up memory entries.

Execute the `jco_spmd_status` command to check whether the event console on the manager has started, and then set up memory entries again.

Alternatively, use the `ping` command, for example, to check whether the logged-in host is running normally, and then set up memory entries again.

Connection cannot be established between Event Console Service and Event Base Service.

Event Base Service may not have been started, or the system (host or network) may be under a heavy workload.

- Corrective action

Execute the `jco_spmd_status` command to check whether Event Base Service on the manager has started, and then set up memory entries again.

Connection cannot be established between Event Base Service and the integrated monitoring database.

The integrated monitoring database may not have been started, or the system (host or network) may be under a heavy workload.

- Corrective action

After starting the integrated monitoring database, set up memory entries again.

(29) Actions to take when the IM database cannot be terminated

Cause

There is a JP1/IM - Manager process that is currently connected.

Corrective action

Check whether JP1/IM - Manager is running. If it is, terminate it first and then terminate the IM database.

(30) Actions to take when you cannot connect to the IM database

The following are possible causes:

- The system is not set up to use the IM database.
- The IM database has not been started.
- The port number setting is invalid.
- When a logical host in a non-cluster system was set up, `standby` was specified for the `-c` option of the `jcfdbsetup` or `jcodbsetup` command.

The action to take in response to each cause is described below.

The system is not set up to use the IM database.

- Corrective action

Execute the `jcoimdef` command without specifying any option, and check whether `S_DB` is set to `ON`. For details about the `jcoimdef` command, see `jcoimdef` (in *Chapter 1. Commands*) in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

The IM database has not been started.

- Corrective action

Make sure that the IM database has been started.

The port number setting is invalid.

- Corrective action

Make sure that the specified port number is not the same as any of the following port numbers:

- Port number specified during the setup of another logical host
- Port number described in the `services` file
- Port number that is used by a HiRDB instance bundled with another product
- Temporary port number that is used by another product or by the OS, for example

When a logical host in a non-cluster system was set up, standby was specified for the `-c` option of the `jcfdbsetup` or `jcodbsetup` command.

- Corrective action
When setting up a logical host of a non-cluster system, specify `online` for the `-c` option of the `jcfdbsetup` or `jcodbsetup` command.

(31) Actions to take when JP1/IM - Manager cannot be uninstalled

The message `KAVB9940-E: Unsetup has not been performed for the IM database service on the physical host.` or `KAVB9941-E: Unsetup has not been performed for the IM database service on the logical host. (Logical host name: logical-host-name) is output.`

Cause

The IM database has not been unset up.

Corrective action

Make sure that the integrated monitoring database and the IM Configuration Management database have been unset up.

(32) Actions to take when an error message indicating an invalid port number is issued after the IM database has been set up

The message `KNAN11044-E: The setup information file does not exist. is output.`

Cause

The specified port number is the same as a port number being used elsewhere.

Corrective action

Make sure that the specified port number is not the same as any of the following port numbers:

- Port number specified during the setup of another logical host
- Port number described in the `services` file
- Port number that is used by a HiRDB instance bundled with another product
- Temporary port number that is used by another product or the OS, for example

(33) Actions to take when IM database setup fails

The message `KNAN11084-E: Creation of a database file system area has failed. is output.`

The following are possible causes:

- The file system in the path specified in `IMDBDIR` or `SHAREDDBDIR` does not support large files.
- The kernel parameters have not been set correctly.
- The host name specified in `LOGICALHOSTNAME` or `ONLINEHOSTNAME` is invalid.

The action to take in response to each cause is described below.

The file system in the path specified in `IMDBDIR` or `SHAREDDBDIR` does not support large files.

- Corrective action
In the target OS, enable the large file setting.

The kernel parameters have not been set correctly.

- Corrective action

Make sure that the kernel parameters have been set correctly. For details about kernel parameters, see the JP1/IM - Manager release notes.

The host name specified in LOGICALHOSTNAME or ONLINEHOSTNAME is invalid.

- Corrective action

Check the following items:

- Is the host name specified in LOGICALHOSTNAME or ONLINEHOSTNAME appropriate?
- Is the host name specified in the -h option of database-related commands appropriate?
- Is the host name specified in the hosts file described? Are there any duplicate host names?
- Is the IP address corresponding to the specified host name appropriate? Are there any duplicate IP addresses?

(34) Actions to take when the setup information file is output as invalid during IM database setup

One of the following messages is output:

- KNAN11030-E A required key is not specified in the setup information file. (key = *item-name*)
- KNAN11038-E A key specified in the setup information file is invalid. (key = *item-name*)
- KNAN11047-E A key name specified in the setup information file is invalid. (key = *item-name*)
- KNAN11048-E A key name specified in the setup information file is duplicated. (key = *item-name*)

The following are possible causes:

- A required item or value is not specified.
- The character string specified for the item name is invalid.
- An invalid value is specified.
- An unnecessary space is inserted before or after the equal sign (=).

The action to take in response to each cause is described below.

A required item or value is not specified.

- Corrective action

Check the setup information file and the cluster information file, and specify all required items.

The character string specified for the item name is invalid.

- Corrective action

Check the setup information file and the cluster information file, and specify all required items.

An invalid value is specified.

- Corrective action

Check the specified value and correct it if necessary.

An unnecessary space is inserted before or after the equal sign (=).

- Corrective action

Check whether there is a space before or after the equal sign (=) and delete it if present.

(35) Actions to take when the IM database cannot be started or database-related commands cannot be executed

When executing a database-related command, the message KNAN11037-E: The data storage directory of the IM database service cannot be accessed. or KNAN11143-E: Configuration of the IM database service is invalid. is output.

The following are possible causes:

- In UNIX, the IM database installation directory or data storage directory has been unmounted.
- The host name has been changed.
- The IM database is using a port number that is being used by another product.

The action to take in response to each cause is described below.

In UNIX, the IM database installation directory or data storage directory has been unmounted.

- Corrective action

Check whether you can access the directory. If you cannot, mount the directory.

The host name has been changed.

- Corrective action

Restore the host name to the previous name, and then change the host name by following the host name change procedure for the IM database.

The IM database is using a port number that is being used by another product.

- Corrective action

Make sure that the specified port number is not the same as any of the following port numbers:

- Port number specified during the setup of another logical host
- Port number described in the `services` file
- Port number that is used by a HiRDB instance bundled with another product
- Temporary port number that is used by another product or by the OS, for example

(36) Actions to take when IM Configuration Management fails to apply the system hierarchy

Cause

The following are possible causes:

- JP1/Base is not running on the following hosts on which the system hierarchy is to be applied.
 - Batch distribution method
 - All hosts included in the system hierarchy
 - Differential distribution method
 - Hosts whose system hierarchy is to be changed and their higher-level manager hosts
- The host onto which the system hierarchy is to be applied is already included in another system hierarchy.

- Name resolution cannot occur among the integrated manager, relay manager, and agent.

Corrective action

Take the corrective action that matches the cause.

- Make sure that JP1/Base is running on the following hosts for which a system hierarchy could not be applied, and then retry the operation.
 - Batch distribution method
 - All hosts included in the system hierarchy
 - Differential distribution method
 - Hosts whose system hierarchy is to be changed and their higher-level manager hosts
- Execute the `jbsrt_get` command on the host for which system hierarchy application failed, and then check whether the host is included in another system hierarchy. If the host is included in another system hierarchy, delete it from that system hierarchy, apply the desired system hierarchy, and then re-execute the command.
- Check whether host name resolution among various hosts was successful. If it was unsuccessful, change the settings so that name resolution can take place, and then retry the operation.

(37) Actions to take when IM Configuration Management fails to collect the operation definition file for the log file trap

Cause

The action definition file for a log file trap must be unique within the agent. Multiple log file traps may have been started using the same settings file, or multiple log file traps may have been started using action definition files that have the same name but are in different directories.

Corrective action

Follow the steps described below.

1. On the agent, stop the log file trap.
2. Set up the action definition file for a log file trap such that it has a unique name within the agent, and then restart the log file trapping function.
3. In the Display/Edit Profiles window of IM Configuration Management - View, from the **Operation** menu, choose **Rebuild Profile Tree** to rebuild the profile tree.

(38) Actions to take when JP1/IM - View cannot display any of the log file traps that are active

Cause

The following are possible causes:

- After the log file trapping function was started, the profile tree was not rebuilt.
The log file trap may have been started or restarted after the Display/Edit Profiles window was started, after the profile tree was rebuilt, or after batch collection of profiles was executed.
- The action definition file specified during startup of the log file trap is not found under *JP1-Base-path*\conf.

Corrective action

Take the corrective action that matches the cause.

- You need to collect the latest profile list. In the Display/Edit Profiles window of IM Configuration Management - View, from the **Operation** menu, choose **Rebuild Profile Tree** to rebuild the profile tree.

- Place the action definition file for the log file trap under *JP1-Base-path\conf*, and then restart the log file trapping function.

After the log file trap is started, in the Display/Edit Profiles window of IM Configuration Management - View, from the **Operation** menu, choose **Rebuild Profile Tree** to rebuild the profile tree.

(39) Actions to take when the content of the profile settings file does not match the content of the valid configuration information

Cause

The following are possible causes:

- After the settings file was edited, the edited content was not applied or the application operation failed.
- Part of the description of the settings file is invalid.

If part of the description of the settings file is invalid, the agent sometimes skips the invalid description when it applies the settings file. In this case, if you perform an application operation from IM Configuration Management - View, an error dialog box opens.

Corrective action

Take the corrective action that matches the cause.

- In the Display/Edit Profiles window of IM Configuration Management - View, verify the content of the settings file, and then execute profile application and make sure that the application operation terminates normally.
- If application of the settings file fails, services may not operate according to the description in the settings file. Correct the description errors and then retry the operation.

(40) Actions to take when menu items such as Register Host and Edit Agent Configuration are disabled in IM Configuration Management - View

Cause

Because the JP1 user who logged in to IM Configuration Management - View is not assigned IM Configuration Management permissions (*JP1_CF_Admin*, *JP1_CF_Manager*, or *JP1_CF_User*), the only operation that is allowed is viewing. The following are possible causes:

- The instance of JP1/Base specified in the authentication server is Version 8 or earlier.
- After the instance of JP1/Base specified in the authentication server was upgraded from Version 8 or earlier by means of overwrite installation, the JP1 user was not assigned IM Configuration Management permissions (*JP1_CF_Admin*, *JP1_CF_Manager*, or *JP1_CF_User*).
- The JP1 user is not assigned IM Configuration Management permissions (*JP1_CF_Admin*, *JP1_CF_Manager*, or *JP1_CF_User*).

Corrective action

Take the corrective action that matches the cause.

- Upgrade the instance of JP1/Base specified on the authentication server to version 9 or later.
- Set *JP1_Console* for the JP1 resource group name of the JP1 user that logs in, assign one of the IM Configuration Management permissions (*JP1_CF_Admin*, *JP1_CF_Manager*, or *JP1_CF_User*) to the JP1 user, and then have the user log in again.

The scope of a menu's operations differs according to the permission levels of IM Configuration Management. For details, see *Appendix E.3 Operating permissions required for IM Configuration Management* in the *JP1/Integrated Management - Manager Overview and System Design Guide*.

(41) Actions to take when virtualization system configuration cannot be obtained in IM Configuration Management

The message KNAN22062-E: Collection of the virtualization configuration failed for the host "host-name" because the communication type is not supported. *is output.*

Cause

The following are possible causes:

- The destination host name is different from the intended one.
- The name of the destination host has not been resolved.
- The destination host is not running.
- vCenter, JP1/SC/CM, SCVMM, HCSM, or KVM has not been started or set up on the destination host.
- Communication with the destination host failed.

Corrective action

Take the corrective action that matches the cause.

- Make sure that the destination host name is correct.
- Make sure that the destination host is running.
- Make sure that vCenter, JP1/SC/CM, SCVMM, HCSM, or KVM has been started and set up on the destination host.
- Make sure that there are no communication problems with the destination host. If the destination VMM host is a KVM, make sure that the SSH connection is set up correctly.

(42) Actions to take when valid configuration information of a remote monitoring log file trap or a remote monitoring event log trap cannot be viewed in IM Configuration Management

The message KNAN22422-E: Collection of operation definition information for *Log File Trapping* failed. (Detail information: A required service or process is not running.) *or* KNAN22422-E Collection of operation definition information for *Event Log Trapping* failed. (Detail information: A required service or process is not running.) *is output.*

Cause

The following are possible causes:

- Because of an error while the remote monitoring log file trap was running, the remote monitoring log file trap stopped.
- Because of an error while the remote monitoring event log trap was running, the remote monitoring event log trap stopped.

Corrective action

A description of the error occurring while the remote monitoring log file trap or the remote monitoring event log trap is running is output to the integrated log. See the corrective action for the error message output to the integrated log and remove the cause of the error. After correcting the error, stop the remote monitoring log file trap or the remote monitoring event log trap and then restart it.

(43) Actions to take if JP1 events are not received even when the remote monitoring log file trap is running in IM Configuration Management

Cause

The following are possible causes:

- The specification of the filter (`filter` to `end-filter`) in the remote-monitoring log file trap action-definition file is incorrect.
- Because the monitoring interval of the remote monitoring log file trap is long, differences occurring in log files have not been monitored.
- Although the remotely monitored host or monitored log file is invalid, an error does not occur because, on the **Valid Configuration Information** page in the Display/Edit Profiles window, you selected the sequence **Log File Trapping - Startup Options** and then enabled **Retry specification for opening a log file [-r]** or because you executed the `jcfallogstart` command with the `-r` option specified.
- Because the filter specification of the startup option for the remote monitoring log file trap is incorrect, the monitored log file data was not transferred from the monitored host.

Corrective action

- Check whether the specification of the filter (`filter` to `end-filter`) in the remote-monitoring log file trap action-definition file is correct.
- Check whether JP1 events still cannot be received even when a time greater than the file monitoring interval specified by the `-t` option of the `jcfallogstart` command has passed.
- If the remotely monitored host is a Windows host, check whether the NetBIOS (NetBIOS over TCP/IP) settings for monitoring logs on the remotely monitored host are correct. For details about NetBIOS (NetBIOS over TCP/IP), see *1.17.2 NetBIOS settings (NetBIOS over TCP/IP) (for Windows)* in the *JP1/Integrated Management - Manager Configuration Guide*.
- If the remotely monitored host is UNIX, check whether the SSH settings for monitoring logs on the remotely monitored host are correct. For details about SSH settings, see *2.16.1 Configuring SSH (for UNIX)* in the *JP1/Integrated Management - Manager Configuration Guide*.
- Make sure that the monitored log file is in a readable state.
- When the `stty`, `tty`, `tset`, or `script` command, which requires interactive operation, is coded in the login script of an SSH-connection user, log files might not be able to be read. In such cases, create a new SSH-connection user for remote monitoring, or change the login script of the SSH-connection user so that these commands are not executed.
- Check whether the filter specification of the startup option for the remote monitoring log file trap is correct. If the filter specification is correct, check whether users who use SSH connection on the remotely monitored host can execute the following command:

For Linux:

```
/bin/grep -E 'regular-expression-character-string-specified-in-filter' path-to-monitored-log-file
```

For Solaris:

```
/usr/xpg4/bin/grep -E 'regular-expression-character-string-specified-in-filter' path-to-monitored-log-file
```

For OSs other than Linux and Solaris:

```
/usr/bin/grep -E 'regular-expression-character-string-specified-in-filter' path-to-monitored-log-file
```

Furthermore, check whether the data in a monitored log file is excluded because of the filter specification.

- If you specify `-r` as an additional option, check the items listed below.

See *10.5.1(50) Actions to take when the remote monitored log file name is incorrect*, and then check whether the path is specified correctly.

- Make sure that the file access permission is set correctly.
- Operation of the log file trap without the `-r` option is effective when you check for errors.
- If none of the above actions resolves the problem, use the data collection tool to collect data on the JP1/IM - Manager host and the monitored host. The following table shows data that needs to be collected on the monitored host.

OS on monitored host	Data to be collected	Method
Windows	System information	<ol style="list-style-type: none"> 1. Choose Run from the start menu. 2. Enter <code>msinfo32</code> in the text box and then click the OK button. 3. In the System Information window, select File and then Export to save the system information to a text file.
	Monitored log file	If there are multiple log files, obtain all of them.
	Windows application and system event logs	<ol style="list-style-type: none"> 1. In Event Viewer, select the relevant event log. 2. Select Save Log File As, and specify <code>evt</code> for the output format.
UNIX	Monitored log file	If there are multiple log files, obtain all of them.
	Syslog	Obtain the syslog messages. For details, see <i>10.3.2 In UNIX</i> .

(44) Actions to take if JP1 events are not received even when the remote monitoring event log trap is running in IM Configuration Management

Cause

- The time settings of the remotely monitored host and the JP1/IM - Manager host are different.
- On a remotely monitored host, there is an event log whose time is later than the current time of the monitored host
- The filter specification is incorrect.

Corrective action

- Set the time of both the remotely monitored host and the JP1/IM - Manager host to the correct current time.
- Make sure that the remotely monitored host does not have any event logs that have a time that is later than the current time of the monitored host.
- Set the filter so that the content indicated in the condition sentence of the filter information displayed in **Valid Configuration Information** can be obtained.
- If none of the above actions resolves the problem, use the data collection tool to collect data on the JP1/IM - Manager host and the monitored host. The following table shows the data to be collected on the monitored host.

Data to be collected	Method
System information	<ol style="list-style-type: none"> 1. Choose Run from the start menu. 2. Enter <code>msinfo32</code> in the text box and then click the OK button. 3. In the System Information window, select File and then Export to save the system information in a text file.

Data to be collected	Method
Windows application and system event logs	<ol style="list-style-type: none"> 1. Select the target event log from Event Viewer. 2. Select Save Log File As, and specify <code>evt</code> for the output format.

(45) Actions to take when the Processing dialog box continues to open in IM Configuration Management - View

Cause

The JP1/IM - Manager host or the agent for the target operation has stopped.

Corrective action

Check whether the JP1/IM - Manager host or the agent for the target operation has stopped.

If it has stopped, click the × (Close) button in the Processing dialog box to forcibly terminate IM Configuration Management - View.

If it has not stopped, IM Configuration Management processing is in progress. Wait until this processing finishes.

(46) Actions to take when the tree area on the IM Configuration page in IM Configuration Management - View is displayed in gray

When you execute Collect IM Configuration in IM Configuration Management - View, the tree area is displayed in grey.

Cause

The following is the possible cause:

- The `jbsrt_del` command was executed on the manager host, but JP1/Base does not hold any configuration definition information.

Corrective action

Execute **Apply Agent Configuration** in IM Configuration Management - View.

When you log in or execute Verify IM Configuration in IM Configuration Management - View, the tree area is displayed in grey.

Cause

The configuration definition information held by the IM Configuration Management database does not match the configuration definition information held by JP1/Base. The following are possible causes:

- The agent configuration has not been applied because the action immediately follows an import by the `jcfimport` command.
- The `jbsrt_del` command was executed on the manager host, but JP1/Base does not hold any configuration definition information.
- The configuration definition information held by JP1/Base has changed because the `jbsrt_distrib` command was executed.
- The agent configuration has not been applied.
- When you manage the system for each site by using a site manager, the procedure described in 3.2.4(3) *Applying a system hierarchy to a system managed by IM Configuration Management* in the *JP1/Integrated Management - Manager Configuration Guide* has not been performed.

Corrective action

Take the corrective action that matches the cause.

- If the agent configuration has not been applied, execute **Apply Agent Configuration** in IM Configuration Management - View.
- Execute **Collect IM Configuration** in IM Configuration Management - View. When the configuration is not the configuration you expect from the operation, execute **Apply Agent Configuration**.

(47) Actions to take when the same JP1 event is received redundantly in the remote monitoring log file trap of IM Configuration Management

Cause

- When a log is output during log processing, the same log might be trapped twice.

Corrective action

- No action is required. You can safely ignore the redundant JP1 events.

(48) Actions to take when an attempt to start the profile of a remote monitoring log file trap fails in IM Configuration Management

The message KNAN26039-E: The specified remote log-file trap failed to start. (Host name: Host-name, Monitoring-target-name: monitoring-target-name, Details: message) is output, and an attempt to start the profile fails.

See the actions for *KNAN26039-E* in *2.13 Messages related to IM Configuration Management (KNAN22000 to KNAN26999)* in the manual *JP1/Integrated Management - Manager Messages*.

If you are still unable to resolve the problem, take action as follows.

How you handle the problem depends on the detailed information.

Cannot connect to the monitored host.

Cause

- A connection to the monitored host has not been established.

Corrective action

- See *10.5.1(51) Actions to take when you cannot connect to the remotely monitored host* to check connectivity with the remotely monitored host.

Cannot access the log file of the monitoring target.

Cause

- The path to the log file is not set correctly.

Corrective action

- See *10.5.1(50) Actions to take when the remote monitored log file name is incorrect* to check correct setting of the path.

(49) Notes applying before starting a remote monitoring log file trap by using IM Configuration Management

Note:

- Make sure that the file type of the log file is correct.
- Make sure that the size of the log file is not too large.

- Make sure that the header size of the log file is not too large.
- Make sure that the JP1/Base LogTrap service does not stop.

(50) Actions to take when the remote monitored log file name is incorrect

Check whether items are set correctly.

To do so, see *Table 4-31 Items additionally displayed on the Configuration File page (when an item under Log File Trapping selected)* in *4.9.2 Configuration File page* in the manual *JP1/Integrated Management - Manager GUI Reference*.

The following are examples of mistakes that are easy to make:

- When the remotely monitored host is a Windows host, the path is not set in `\shared-folder-name\file-name` format.
- When the remotely monitored host is a UNIX host, the full path is not set as the path.
- The path indicates a folder.

(51) Actions to take when you cannot connect to the remotely monitored host

Check whether the following items are set correctly.

When the JP1/IM - Manager host is a Windows host:

See the following subsections in the *JP1/Integrated Management - Manager Configuration Guide*:

- *1.17.1 Configuring WMI (for Windows)*
- *1.17.2 NetBIOS settings (NetBIOS over TCP/IP) (for Windows)*
- *1.17.3 Configuring SSH (for Windows)*

When the JP1/IM - Manager host is a UNIX host:

2.16.1 Configuring SSH (for UNIX) in the *JP1/Integrated Management - Manager Configuration Guide*

Check for the following problems:

- The monitored host is not running.
- Name resolution of the monitored host cannot be performed from the JP1/IM - Manager host.

(52) Actions to take when an attempt to collect host information in IM Configuration Management fails

How you resolve the problem depends on the message type.

The message KNAN22017-E: Collection of host information failed because a connection could not be established with the host "host-name". is output, and an attempt to collect host information fails.

Cause

The following are possible causes:

- The destination host name is different from the intended one.
- The name of the destination host has not been resolved.
- The destination host is not running.

- JP1/Base on the destination host is not running.
- Communication with the destination host failed.
- The version of JP1/Base on the destination host is earlier than 07-00.

Corrective action

Take the corrective action that matches the cause.

- Execute the command below on the JP1/IM - Manager host to check whether the name of the host registered in IM Configuration Management can be resolved, and whether communication with the host registered in IM Configuration Management is possible. If the system operates in an IPv6 environment, check whether the IPv6 address is the primary IP address (whether the IPv6 address is first address displayed in Resolved Host List that is displayed by executing the following command), and whether communication is possible using the IPv6 address.

- jplping *host-name-registered-in-IM-Configuration-Management*

Execute the following command on the JP1/IM - Manager host to check whether communication with the host registered in IM Configuration Management is possible for the specified port number.

- telnet *agent-host-name or IP-address* 20306

If the system operates in an IPv6 environment, specify the IPv6 address as the destination address of the telnet command. By default, the port number to be used for collecting host information is 20306/tcp. If communication with the destination is not possible, a message to that effect is output. If communication with the destination is possible, a black window is displayed.

On a Windows host running Windows Server 2008 R2 or later, no telnet client has been installed by default. You can install a telnet client by using the Windows **Add or Remove Programs** function.

- Check whether the version of JP1/Base on the destination host is 07-00 or later. If the system operates in an IPv6 environment, check whether the version of JP1/Base on the destination host is Version 10 or later.

- Execute the following commands to check whether JP1/Base on the destination host is running.

- jbs_spmc_status (for a logical host: jbs_spmc_status -h *logical-host-name*)

- jevstat (for a logical host: jevstat *logical-host-name*)

- Execute the following command on the destination host to check whether the name the JP1/IM - Manager host can be resolved, and whether communication with the JP1/IM - Manager host is possible. If the system operates in an IPv6 environment, check whether the IPv6 address is the primary IP address (whether the IPv6 address is first address displayed in Resolved Host List that is displayed by executing the following command), and whether communication is possible using the IPv6 address.

- jplping *JP1/IM - Manager-host-name*

- If the system operates in an IPv6 environment and the communication method on the JP1/IM - Manager host is set to ANY bind address, use the following steps to check whether the version settings of the IP address to be bound are correct.

1. Execute the jbsgetcnf command.

jbsgetcnf > config.txt

2. Open config.txt in a text editor.

3. Check whether the value of [JP1_DEFAULT\JP1BASE\JP1_ANY_BIND] is ALL.

- If the system operates in an IPv6 environment and the communication method on the collection-destination host is set to ANY bind address, use the following steps to check whether the version settings of the IP address to be bound are correct.

1. Execute the jbsgetcnf command.

jbsgetcnf > config.txt

2. Open config.txt in a text editor.

3. Check whether the value of [JP1_DEFAULT\JP1BASE\JP1_ANY_BIND] is ALL or IPv6.

- Make sure that IP address resolved from the short name of the destination host matches the IP address resolved from the FQDN.

The following message is output, and an attempt to collect host information fails.

- KNAN21400-W Collection of host information from host "*host-name*" partially succeeded.

Collection of host information from JP1/Base succeeded while collection of host information from the remote host failed.

Details: *details*

KNAN21402-E The collection of host information for a host "*host-name*" failed.

The collection of host information failed from JP1/Base.

Detailed information: *details*

The collection of remote host information failed.

Detailed information: *details*

- KNAN21403-E Host "*host-name*" failed to collect host information from the remote host.

Details: *details*

Cause

When an attempt to collect host information fails in remote monitoring, the following are possible causes:

- The remote communication configuration has not been set.
- A connection to the monitored host cannot be established.
- The collection of log files timed out.
- Authentication processing failed.
- The private key does not exist.
- The creation of the remote monitoring process failed.

Corrective action

Take the corrective action that matches the cause.

- Set remote communication on the monitored host, and then retry the operation.
- Check the connection with the remotely monitored host. For details about the method, see [10.5.1\(51\) Actions to take when you cannot connect to the remotely monitored host](#).
- Check the following:

When the OS of the host of the monitored host name is a Windows host:

- Whether communication with the host that has the monitored host name is possible
- Whether the password of the user who logs in to the monitored host has expired
- Whether the remote communication type of the host that has the monitored host name is set correctly
- Whether the WMI service is running

At this point, if there is no problem, check whether the WMI connection is set normally.

When the OS of the host of the monitored host name is a UNIX host:

- Whether communication with the host that has the monitored host name is possible
- Whether the remote communication type of the host that has the monitored host name is set correctly
- Whether the SSH server is running on the host that has the monitored host name

At this point, if there is no problem, check whether the SSH connection is set correctly.

- Check the following:
 - When the OS of the host of the monitored host name is a Windows host:
 - Whether the user name, password, and domain name in the System Common Settings window or the Remote Monitoring Settings window are set correctly
 - Whether DCOM is set correctly on the host that has the monitored host name
 - Whether DCOM is set correctly on the JP1/IM - Manager host
 - At this point, if there is no problem, check whether the WMI connection is set correctly.
 - When the OS of the host of the monitored host name is a UNIX host:
 - Whether the SSH authentication settings are correct
 - At this point, if there is no problem, check whether the SSH connection is set correctly.
- Check whether the private key exists.
- Check the settings on the **IM Host Account** page in the System Common Settings window.

(53) Actions to take when the source host name is different from the host name registered in IM Configuration Management

Corrective action

Take corrective action according to the version. For details, see *12.3.11(2)(b) Changing JP1 event attributes (Setting for JP1/IM - Manager)* in the *JP1/Integrated Management - Manager Overview and System Design Guide*.

- For a new installation or an overwrite installation of JP1/IM - Manager, perform the following steps:
 1. Check the content of the common definition configuration file for changes in the JP1 event attributes.
 2. Execute the `jbsetcnf` command.
 3. Restart JP1/IM - Manager.
- When the version of JP1/IM - Manager is earlier than 10-00, register the host name in IM Configuration Management with both its short name and FQDN name.

(54) Actions to take when the filter does not work correctly because the source host name is different from the monitored host name

Corrective action

For details about how to resolve the problem, see *10.5.1(53) Actions to take when the source host name is different from the host name registered in IM Configuration Management*.

(55) Actions to take when JP1/IM - Manager does not start, or JP1/IM - View cannot be operated after the OS starts or the network settings are changed in Windows

Cause

The following are possible causes:

- After OS startup, JP1/IM - Manager startup processing started before the network became available.

The time from OS startup until the network becomes available depends on the environment. In an environment in which teaming is used, a few minutes might be needed before the network becomes available. Also, in a teaming environment, JP1/IM - Manager startup processing might start before the network becomes available (for example, when JP1/IM - Manager is started automatically by the startup control function of JP1/Base).

- The network settings (such as the teaming settings) were changed during JP1/IM - Manager startup.

Corrective action

On the physical host and all logical hosts, terminate JP1/IM - Manager, JP1/IM - View, JP1/Base, and any programs that require JP1/Base. Execute `jp1ping local-host-name` to make sure that the local host name can be resolved to the intended IP address, and then start JP1/IM - Manager, JP1/IM - View, JP1/Base, and the programs requiring JP1/Base.

The following describes the appropriate actions to be taken in each case.

- After OS startup, JP1/IM - Manager startup processing starts before the network became available
To automatically start JP1/IM - Manager when the OS starts, use the startup control function of JP1/Base. To do so, configure the settings so that the timing of startup of the JP1/IM - Manager service is delayed to postpone JP1/IM - Manager startup until after the network becomes available. For details about the settings, see the chapter related to the explanation for setting the timing of the startup of services in the *JP1/Base User's Guide*.
- The network settings, such as the teaming settings, were changed during JP1/IM - Manager startup
To change the network settings, such as the teaming settings, terminate on the physical host and all logical hosts JP1/IM - Manager, JP1/IM - View, JP1/Base, and programs that require JP1/Base. Also, if you are connected to JP1/IM - View, log out.

(56) Actions to take if characters are unreadable when JP1/SES-format events are received

Cause

JP1/SES-format events (events output by an older version of a JP1 product, or events output by products that do not support JP1 event output, such as JP1/Open Job Entry) do not have character encoding information.

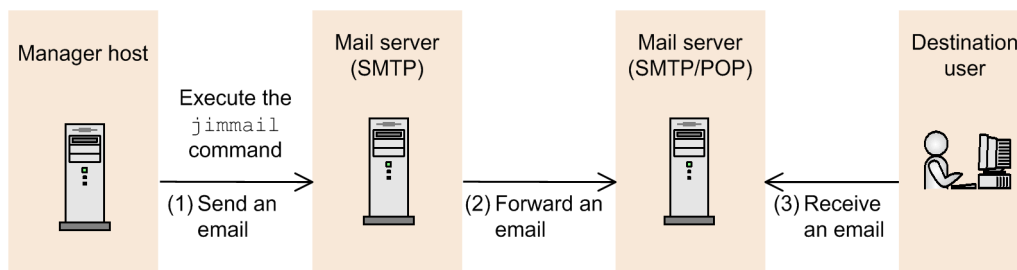
JP1/IM - Manager interprets JP1/SES-format events by using the character encoding that JP1/IM - Manager uses to operate. Therefore, if the character encoding of a JP1/SES-format event is different from the JP1/IM - Manager encoding, the displayed JP1/SES-format event might be unreadable or contain some characters that are not the intended characters.

Corrective action

Take either of the following actions to resolve the problem:

- Use the same character encoding for JP1/SES-format events and operation of JP1/IM - Manager.
- Use local actions on JP1/Base operating with the same character encoding as that of JP1/SES-format events so that JP1 events are issued when JP1/SES-format events are received. These JP1 events are then forwarded to the JP1/IM - Manager host. For details about local actions, see the chapter related to the explanation of local actions in *JP1/Base User's Guide*.

(57) Actions to take when an email does not reach the destination in the email notification function of JP1/IM - Manager



JP1/IM - Manager

If the `jimmail` command terminates normally, but an email does not reach the destination:

Cause 1

The destination address of the email is incorrect.

Corrective action 1

The destination address of the email might be incorrect. Check the destination email address specified for the `-to` option of the `jimmail` command, or for `DefaultTo` in the email environment definition file.

If the destination email address is specified for both the `-to` option of the `jimmail` command and `DefaultTo` in the email environment definition file, the destination email address specified for the `-to` option of the `jimmail` command takes precedence.

Cause 2

An error occurred between the mail server (SMTP) and the mail server (SMTP/POP3), and forwarding email failed.

Corrective action 2

Make sure that the following conditions are satisfied, and then re-execute the `jimmail` command:

- The mail server (SMTP/POP3) is running.
- No error occurs in the mail server (SMTP) log.
- Transit through a port in the firewall is allowed.
- Host name resolution for the mail server is enabled.

Cause 3

Receiving an email between the mail server (SMTP/POP3) and a mail client failed.

Corrective action 3

The error cannot be checked in JP1/IM - Manager because the communication is between the mail server and the mail client.

Check the messages and logs on the mail server and the mail client.

Also, make sure that the mail client settings (POP3 server name, POP3 account name, password, and port number) are correct.

If the `jimmail` command terminates abnormally:

Cause

The mail server (SMTP) cannot be connected.

Corrective action

The `jimmail` command outputs an error message according to the contents of the error. Take action according to the output message, make sure that the conditions below are satisfied, and then re-execute the `jimmail` command.

For details about messages, see *Chapter 2. List of Messages* in the manual *JP1/Integrated Management - Manager Messages*.

- The mail server (SMTP) is running.
- No error occurs in the mail server (SMTP) log.
- Transit through a port in the firewall is allowed.
- Host name resolution for the mail server (SMTP) is enabled.
- The authentication account and password in the email environment definition file is correct.

(58) Actions to take when an error is displayed on JP1/IM - Manager in which the communication encryption function is enabled

How you handle the problem depends on the message that is output.

If JP1/IM - Manager does not start:

- The following message might be output: KAVB8817-E A file specified for a parameter of the communication encryption function for JP1/IM - Manager could not be read. (parameter = *parameter-name*, parameter value = *parameter-value*)
- The following message might be output: KAVB8818-E A private key specified for a parameter of the communication encryption function for JP1/IM - Manager could not be read. (parameter for the private key = *parameter-name*, parameter value for the private key = *parameter-value*, parameter for the server authentication certificate = *parameter-name*, parameter value for the server authentication certificate = *parameter-value*)

Cause

The following are possible causes:

- The file specified by a parameter of JP1/IM - Manager's communication encryption function cannot be read.
- The private key specified by a parameter of JP1/IM - Manager's communication encryption function cannot be read or is not paired with a server certificate.

Corrective action

Take the corrective action that matches the cause.

- Make sure that a server certificate is paired with a private key. If this is not the case, provide a server certificate and a private key that form a pair.
- Make sure that the file format of the private key is valid.
- If a passphrase is set for the private key, cancel the passphrase.
- Check the following operating system logs, and make sure that no shortage has occurred in OS resources such as file descriptors:
 - For Windows: Windows event log
 - For UNIX: syslog

If execution of the `jcochfilter` or `jcochstat` command fails:

- The following message might be output: KAVB1956-E An error occurred during the initialization of the communication encryption function for the command "*command-name*". (cause = *cause*, file = *file-name*)
- The following message might be output: KAVB1957-E Failed to encrypt communications by using the communication encryption function for the command "*command-name*". (host name of connection destination = *connection-destination-host-name*, cause = *cause*)

Cause

The following are possible causes:

- The root authentication certificate was not found.
- The root authentication certificate could not be read.
- The CN or SAN of the server authentication certificate does not match with the host name of the connection destination.
- A communication error occurred.

- A system error occurred.

Corrective action

Take the corrective action that matches the cause.

- If a root certificate is available, check whether you have read permission for the root certificate. If not, set read permission for the root certificate.
- If no root certificate was found, provide one.
- Make sure that the root certificate file is valid.
- Check the following operating system logs, and make sure that no shortage has occurred in OS resources such as file descriptors:
 - For Windows: Windows event log
 - For UNIX: syslog
- Make sure that the manager host name specified in the `-h` option of the `jcochstat` command matches the CN or SAN in the server certificate of the manager host at the connection destination. Then, re-execute the command.
- Verify the following and then re-execute the command:
 - In the case of the `jcochstat` command, make sure that the host on which the command is executed has a root certificate corresponding to the server certificate of the manager host specified by the `-h` option of the `jcochstat` command. If not, provide an appropriate root certificate.
 - In the case of the `jcochstat` command, make sure that the communication encryption function of the manager host specified in the `-h` option is enabled. If not, enable it.
 - In the case of the `jcochstat` command, make sure that the server certificate of the manager host specified in the `-h` option is has not expired. If it has expired, update the server certificate.
 - The settings for the communication encryption function might have been modified after JP1/IM - Manager startup. Restart JP1/Base and JP1/IM - Manager to apply the settings for the communication encryption function.
- If a system error occurred, use the data collection tool to collect data, and then contact the system administrator.

If the following warning message is output during the execution of the `jcochfilter` or `jcochstat` command:

```
KAVB1972-W The root authentication certificate used by the communication encryption function for the command "command-name" is no longer valid. (file=file-name)
```

Cause

The following is a possible cause:

- The root certificate used by the communication encryption function has expired.

Corrective action

Take the corrective action that matches the cause.

- Check whether there is a problem with using the expired root certificate. If there is a problem, contact the system administrator and update the root certificate.

If execution of a command (`jcschstat`, `jcsdbexport`, or `jcsdbimport`) fails:

- The following message might be output: `KAVB7602-E Command execution will stop because memory is insufficient.`
- The following message might be output: `KAVB7810-E An error occurred during the initialization of the communication encryption function for the command "command-name". (cause = cause)`

- The following message might be output: KAVB7818-E A library required for the command "*command-name*" was not found.
- The following message might be output: KAVB7812-E Failed to encrypt communications by using the communication encryption function for the command "*command-name*". (host name of connection destination = *connection-destination-host-name*, cause = *cause*)

Cause

The following are possible causes:

- There is insufficient memory for executing the command.
- The library required by the command was not found.
- A communication error occurred.
- A system error occurred.

Corrective action

The settings for the communication encryption function might have been modified after startup of JP1/IM - Manager. Restart JP1/Base and JP1/IM - Manager to apply the settings for the communication encryption function, and then re-execute the command. If the problem persists, use the data collection tool to collect data, and then contact the system administrator.

If execution of any of the following commands fails:

jcfvirtualchstat, jcfexport, jcfimport, jcfaleltdef, jcfaleltreload, jcfaleltstart, jcfaleltstat, jcfaleltstop, jcfallogdef, jcfallogreload, jcfallogstart, jcfallogstat, and jcfallogstop

- The following message is output: KNAN24155-E Failed to encrypt communications by using the communication encryption function for the command "*command-name*". (host name of connection destination = *connection-target-host-name*, cause = *cause*)

Cause

The following are possible causes:

- A communication error occurred.
- A system error occurred.

Corrective action

Take the corrective action that matches the cause.

- The settings for the communication encryption function might have been modified after startup of JP1/IM - Manager. Restart JP1/Base and JP1/IM - Manager to apply the settings for the communication encryption function, and then re-execute the command. If the problem persists, use the data collection tool to collect data, and then contact the system administrator.

If execution of IM configuration synchronization fails:

- The following message might be output: KNAN29095-E An error occurred during the initialization of the communication encryption function for the IM Configuration Management Service. (cause = *cause*, file = *file-name*)
- The following message might be output: KNAN29098-E Failed to encrypt communications by using the communication encryption function for the IM Configuration Management Service. (host name of connection destination = *connection-target-host-name*, cause = *cause*)

Cause

The following are possible causes:

- The root authentication certificate was not found.
- The root authentication certificate could not be read.
- The CN or SAN of the server authentication certificate does not match with the host name of the connection destination.
- A communication error occurred.
- A system error occurred.

Corrective action

Take the corrective action that matches the cause.

- Check whether you have read permission for the root certificate. If not, set read permission for the root certificate.
- If no root certificate was found, provide one.
- Make sure that the root certificate file is valid.
- Check the following operating system logs, and make sure that no shortage has occurred in OS resources such as file descriptors:
 - For Windows: Windows event log
 - For UNIX: syslog
- Make sure that the host name of the connection destination matches the CN or SAN in the server certificate of the manager host at the connection destination, and then re-execute the command.
- Check whether the message `Failed to read some of the root authentication certificates` was output to the integrated trace log. If it was output, take action as described in the message.
- Check whether the manager host has a root certificate corresponding to the server certificate of the connection destination host. If not, provide one.
- Check whether the server certificate of the connection destination host has expired. If it has expired, update the server certificate.
- If a system error occurred, use the data collection tool to collect data, and then contact the system administrator.

If a warning message is output during execution of IM configuration synchronization:

- The following message is output: `KNAN29097-W The root authentication certificate used by the communication encryption function for the IM Configuration Management Service is no longer valid. (file = file-name)`

Cause

The following is a possible cause:

- The root certificate used by the communication encryption function has expired.

Corrective action

Take the corrective action that matches the cause.

- Check whether there is a problem with using the expired root certificate. If there is a problem, contact the system administrator and update the root certificate.

(59) Actions to take when an error is displayed in JP1/IM - View when the communication encryption function is enabled

How you handle the problem depends on the message that is output.

If you cannot log in to JP1/IM - View:

- The following message might be output: KAVB1958-E An error occurred during the initialization of the communication encryption function for JP1/IM-View. (cause = *cause*, directory = *directory-name*)
- The following message might be output: KAVB6601-E An error occurred during the initialization of the communication encryption function for JP1/IM-View. (cause = *cause*, directory = *directory*)
- The following message might be output: KNAN20121-E An error occurred during the initialization of the communication encryption function for CF - View. (cause = *cause*, directory = *directory-name*)
- The following message might be output: KNAN20141-E An error occurred during the initialization of the communication encryption function for CF - View for the base manager. (cause = *cause*, directory = *directory-name*)

Cause

The following are possible causes:

- No root authentication certificates were found.
- None of the root authentication certificates could be read.
- The placement directory for root authentication certificates could not be found.

Corrective action

Take the corrective action that matches the cause.

- If no root certificates could be found, check the following and then log in again.
Check whether a root certificate is available. If a root certificate is available, check whether you have read permission for the root certificate. If not, set read permission for the root certificate. If no root certificate was found, provide one.
- If none of the root certificates could be read, check the following and then log in again.
 - Check whether a root certificate is available. If a root certificate is available, check whether you have read permission for the root certificate. If not, set read permission for the root certificate.
 - Make sure that the root certificate file is valid.
 - Check the Windows event log and make sure that no shortage has occurred in OS resources such as file descriptors.
- If no root certificate directory exists, create one and place root certificates in it.

If connection to the manager fails:

- The following message might be output: KAVB1959-E Failed to encrypt communications by using the communication encryption function for JP1/IM - View. (host name of connection destination = *connection-destination-host-name*, cause = *cause*)
- The following message might be output: KAVB6602-E Failed to encrypt communications by using the communication encryption function for JP1/IM - View. (host name of connection destination = *connection-destination-host-name*, cause = *cause*)
- The following message might be output: KNAN20122-E Failed to encrypt communications by using the communication encryption function for CF - View. (host name of connection destination = *connection-target-host-name*, cause = *cause*)

- The following message might be output: KNAN20142-E Failed to encrypt communications by using the communication encryption function for CF - View for the base manager. (host name of connection destination = *connection-target-host-name*, cause = *cause*)

Cause

The following are possible causes:

- The CN or SAN of the server authentication certificate does not match with the host name of the connection destination.
- A communication error occurred.
- A system error occurred.

Corrective action

Take the corrective action that matches the cause.

- Make sure that the host name of the viewer's connection-destination of the viewer matches the CN or SAN in the server certificate of the manager host at the connection destination, and then log in again.
- Make sure that the communication encryption function of the manager at the connection destination is enabled. If it is enabled, make sure that the host name of the manager at the connection destination is not specified in the non-encryption communication host configuration file.
- Check whether the message Failed to read some of the root authentication certificates is output to the integrated trace log. If it is output, take action as described in the message.
- Check whether a root certificate corresponding to the manager host at the connection destination is provided in JP1/IM - View. If not, provide one.
- Check whether the server certificate of the manager host at the connection destination has expired. If it has expired, update it.
- If a system error occurred, use the data collection tool to collect data, and then contact the system administrator.

If a warning message is output:

- The following message might be output: KAVB1969-W Failed to read some of the root authentication certificates used by the communication encryption function for JP1/IM - View. (directory = *directory-name*, file = *file-name*, *file-name*, ...)
- The following message might be output: KAVB1971-W The root authentication certificate used by the communication encryption function for JP1/IM - View is no longer valid. (directory = *directory-name*, file = *file-name*, *file-name*, ...)
- The following message might be output: KAVB6603-W Failed to read some of the root authentication certificates used by the communication encryption function for JP1/IM - View. (directory = *directory-name*, file = *file-name*, *file-name*, ...)
- The following message might be output: KNAN20123-W Failed to read some of the root authentication certificates used by the communication encryption function for CF - View. (directory = *directory-name*, file = *file-name*, *file-name*, ...)
- The following message might be output: KNAN20124-W The root authentication certificate used by the communication encryption function for CF - View is no longer valid. (directory = *directory-name*, file = *file-name*, *file-name*, ...)
- The following message might be output: KNAN20143-W Failed to read some of the root authentication certificates used by the communication encryption function for CF - View for the base manager. (directory = *directory-name*, file = *file-name*, *file-name*, ...)

- The following message might be output: KNAN20144-W The root authentication certificate used by the communication encryption function for CF - View for the base manager is no longer valid. (directory = *directory-name*, file = *file-name*, *file-name*, ...)

Cause

The following are possible causes:

- Reading of some of the root certificates used by the communication encryption function of JP1/IM - View failed.
- The root certificate used by the communication encryption function of JP1/IM - View has expired.

Corrective action

Take the corrective action that matches the cause.

- Check whether you have read permission for the root certificate. If not, set read permission for the root certificate.
- Check the Windows event log and make sure that no shortage has occurred in OS resources such as file descriptors.
- Make sure that the root certificate file is valid.
- Check whether there is a problem with using the expired root certificate. If there is a problem, update the root certificate.

If acquisition of remote monitoring configuration fails during IM configuration synchronization:

This subsection describes the causes related to the communication encryption function when the following message is output, along with the actions to take:

- The following message is output: KNAN21404-E There is a host for which IM configuration synchronization failed. Take action according to the manual, and then retry IM configuration synchronization.

Cause

The following are possible causes:

- No root certificate file was found on the connection destination manager.
- The root certificate file on the connection destination manager could not be read.
- The host name of the site manager does not match the CN or SAN in the server certificate of the site manager.
- The server certificate of the site manager has expired.

Corrective action

Take the corrective action that matches the cause.

- If no root certificate was found, provide one, and set its location in JP1/Base.
- Check whether you have read permission for the root certificate. If not, set read permission for the root certificate.
- Make sure that the root certificate file is valid.
- Check the following operating system logs, and make sure that no shortage has occurred in OS resources such as file descriptors:
 - For Windows: Windows event log
 - For UNIX: syslog
- Make sure that the host name of the site manager matches the CN or SAN in the server certificate of the site manager.

- Check whether the message Failed to read some of the root authentication certificates was output to the integrated trace log of the connection destination manager. If it was output, take action as described in the message.
- Check whether the manager at the connection destination has a root certificate corresponding to the server certificate of the site manager. If not, obtain a root certificate and set its location in JP1/Base.
- Check whether the server certificate of the site manager has expired. If it has expired, update it.

(60) Actions to take if extended recovery fails

Check the IM database log and determine whether message KFPL15308-E was output.

- In Windows

1. Execute the following command to set up environment variables:

```
set PDDIR=<IM-database-service-installation-directory>\JM<n>
set PDUXPLDIR=%PDDIR%\UXPLDIR
<IM-database-service-installation-directory>\JM<n>\bin\pdcat
```

- In Linux

1. Execute the following command to set up environment variables:

```
export PDDIR=<IM-database-service-installation-directory>/JM<n>
export LD_LIBRARY_PATH=$PDDIR/lib/:$LD_LIBRARY_PATH
```

2. Execute the following command to display the IM database log:

```
$PDDIR/bin/pdcat
```

- In AIX

1. Execute the following command to set up environment variables:

```
export PDDIR=<IM-database-service-installation-directory>/JM<n>
export LIBPATH=$PDDIR/lib/:$LIBPATH
```

2. Execute the following command to display the IM database log:

```
$PDDIR/bin/pdcat
```

<IM-database-service-installation-directory>:

Path specified in the item IMDBENVDIR of the setup information file

<n>:

For a physical host, *n* is 0. For a logical host, *n* is the value specified for LOGICALHOSTNUMBER in the cluster setup information file.

If message KFPL15308-E is output to the IM database log, you need to match the table schema used for backup file acquisition to the table schema of the IM database service.

Check whether you need to update the IM database by executing the `j imdbupdate` command, and perform a recovery operation according to the following procedure.

If message KNAN11201-I, indicating that the IM database is the latest, is displayed:

1. Perform `unsetup` for the integrated monitoring database.
2. In Windows, restart the OS.
3. Execute the `j codbsetup` command with the `-v` option specified.

4. Execute the `jimdbrecovery` command with both the backup file for which extended recovery failed and the `-m EXPAND` option specified.

5. Update the table schema of the database.

Execute the `jimdbupdate` command with the `-i` option specified.

If message `KNAN11201-I`, indicating that the IM database is the latest, is not displayed:

1. Update the table schema of the database.

Execute the `jimdbupdate` command with the `-i` option specified.

2. Execute the `jimdbrecovery` command with both the backup file for which extended recovery failed and the `-m EXPAND` option specified.

If message `KFPL15308-E` is not output, check the following and then re-execute the `jimdbrecovery` command:

- Is the backup file acquired by the same OS specified?
- Is the database configuration the same as when the backup was collected?
- Is the size of the current IM database smaller than when the backup was collected?
- Was the recovery operation performed after the IM database was set up again?
- Is there sufficient space available in the IM database installation directory? Approximately 1 gigabyte is required if the database size is S or M, and 4 gigabytes are required if the database size is L.

(61) How to extend logs when a log from the time an event occurred cannot be collected because logs for the Central Console viewer or Central Scope viewer wrapped around, causing older logs to be overwritten

You can extend process-specific trace logs for the Central Console viewer or the Central Scope viewer by specifying the following common definition information in a file on the machine on which JP1/IM - View is installed, and then using the `jbssetcnf` command to apply the information:

Format

```
[JP1_DEFAULT\JP1CONSOLEVIEW\LOG_CONTROL\VIEW]
"LOGFILENUM"=dword:hexadecimal-value
"LOGSIZE"=dword:hexadecimal-value
"JP1COVIEW_LOGNUM"= dword:hexadecimal-value
"JP1COVIEW_LOGSIZE"= dword:hexadecimal-value
"JP1COVIEW_APILOGNUM"= dword:hexadecimal-value
"JP1COVIEW_APILOGSIZE"= dword:hexadecimal-value
[JP1_DEFAULT\JP1CONSOLEVIEW]
"JP1COVIEW_LOGSIZE"=dword:hexadecimal-value
"JP1COVIEW_APILOGSIZE"=dword:hexadecimal-value
```

Estimate the values according to the number of JP1/IM - View instances that will be connected concurrently, so that the maximum amount of disk space to be allocated for each process-specific trace log (*maximum size x number of files*) is equal to *default value x maximum number of JP1/IM - View instances that can be connected concurrently*.

This action requires free disk space equivalent to the space to be allocated for the trace log.

Specification

Specify the following values:

[JP1_DEFAULT\JP1CONSOLEVIEW\LOG_CONTROL\VIEW]

This is a key name in the JPI/IM - View environment settings; this value is fixed.

"LOGFILENUM"=dword:*hexadecimal-value*

Specifies the number of VIEWn.log files for the process-specific trace log.

Specify a hexadecimal value in the range from 1 to 16. The default value is dword:00000003 (3 files).

"LOGSIZE"=dword:*hexadecimal-value*

Specifies the maximum size of each VIEWn.log for the process-specific trace log.

Specify a hexadecimal value in bytes in the range from 4,096 to 2,147,483,647 bytes. The default value is dword:00A00000 (10,485,760 bytes, or 10 MB).

"JP1COVIEW_LOGNUM"= dword:*hexadecimal-value*

Specifies the number of jplconvn.log files for the process-specific trace log.

Specify a hexadecimal value in the range from 2 to 100. The default value is dword:00000008 (8 files).

"JP1COVIEW_LOGSIZE"= dword:*hexadecimal-value*

Specifies the maximum size of each jplconvn.log file for the process-specific trace log.

Specify a hexadecimal value in bytes in the range from 4,096 to 104,857,600 bytes. The default value is dword:00500000 (5,242,880 bytes, or 5 MB).

"JP1COVIEW_APILOGNUM"= dword:*hexadecimal-value*

Specifies the number of jplconvMn.log files for the process-specific trace log.

Specify a hexadecimal value in the range from 2 to 100. The default value is dword:0000003C (60 files).

"JP1COVIEW_APILOGSIZE"= dword:*hexadecimal-value*

Specifies the maximum size of each jplconvMn.log file for the process-specific trace log.

Specify a hexadecimal value in bytes in the range from 4,096 to 104,857,600.

The default value is dword:00500000 (5,242,880 bytes, or 5 MB).

[JP1_DEFAULT\JP1CONSOLEVIEW]

This is a key name in the JPI/IM - View environment settings; this value is fixed.

"JP1COVIEW_LOGSIZE"=dword:*hexadecimal-value*

Specifies the maximum size of the jplcsov[_old].log file for the process-specific trace log.

Specify a hexadecimal value in the range from 512 to 2,097,152 KB. The default value is dword:00300000 (3,145,728 bytes, or 3 MB).

"JP1COVIEW_APILOGSIZE"=dword:*hexadecimal-value*

Specifies the maximum size of the jplcsovM[_old].log file for the process-specific trace log.

Specify a hexadecimal value in the range from 512 to 2,097,152 KB. The default value is dword:00600000 (6,291,456 bytes, or 6 MB).

Procedures for extending logs

To extend the process-specific trace logs:

1. Stop any of the following that are running on the host for which logs are to be extended: Central Console viewer, Central Scope viewer, and any monitoring tree editing viewers. Do this even when you are connecting to the host via Remote Desktop.
2. Check the *system-drive*: \ProgramData\Hitachi\jpl\jpl_default\JP1CoView\log\mmap folder and its subfolders, and if the VIEW.mm file exists, manually delete it.
3. Use the jbssetcnf command to apply the file in which the common definition information is set.
For details about the jbssetcnf command, see the *JPI/Base User's Guide*.

(62) How to extend logs when a log from the time an event occurred cannot be collected because logs for the IM Configuration Management viewer wrapped around, causing older logs to be overwritten

You can extend process-specific trace logs for the IM Configuration Management viewer by modifying the following file on the machine on which JP1/IM - View is installed, and then restarting the machine.

- The process-specific log settings definition file (`jcfview_reg.conf`) for the IM Configuration Management viewer

File name

`jcfview_reg.conf`

Directory

View-path\conf\jcfview\

Format

```
"TRACELEVEL"=dword:00000028
"SHMTHRESHOLD"=dword:0000001E
"FILETHRESHOLD"=dword:00000000
"LOGFILENUM"=dword:hexadecimal-value
"LOGSIZE"=dword:hexadecimal-value
```

Estimate the values according to the number of JP1/IM - View instances that will be connected concurrently, so that the maximum amount of disk space to be allocated for each process-specific trace log (*maximum size x number of files*) is equal to *default value x maximum number of JP1/IM - View instances that can be connected concurrently*.

This action requires free disk space equivalent to the space to be allocated for the trace logs.

Specification

Specify the following values:

`"TRACELEVEL"=dword:00000028`

This parameter is fixed. Do not change it.

`"SHMTHRESHOLD"=dword:0000001E`

This parameter is fixed. Do not change it.

`"FILETHRESHOLD"=dword:00000000`

This parameter is fixed. Do not change it.

`"LOGFILENUM"=dword:hexadecimal-value`

Specifies the maximum number of `VIEWn.log` files for the process-specific trace log.

Specify a hexadecimal value in the range from 1 to 16. The default value is `dword:00000003` (3 files).

`"LOGSIZE"=dword:hexadecimal-value`

Specifies the maximum size of each `VIEWn.log` file for the process-specific trace log.

Specify a hexadecimal value in the range from 4,096 to 16,777,216. The default value is `dword:00A00000` (10,485,760 bytes, or 10 MB).

Procedures for extending logs

To extend the process-specific trace logs:

1. Stop any IM Configuration Management viewers that are running on the host for which logs are to be extended. Do this even when you are connecting to the host via Remote Desktop.
2. Check the *system-drive*: \ProgramData\Hitachi\jpl\jpl_default\JP1CoView\log\jcfview\mmap folder and its subfolders, and if the VIEW.mm file exists, manually delete it.
3. In the process-specific log settings definition file (jcfview_reg.conf) for the IM Configuration Management viewer, set the values for the parameters that are required to expand the logs.

(63) Actions to take when an automated action is not executed

Cause

The following are possible causes:

- A common exclusion-condition excludes a collected JP1 event from automated-action execution.
- The automated action definition is disabled.
- No collected JP1 event satisfies the action execution condition in the automated action definition.

Corrective action

Take the corrective action that matches the cause.

- When a common exclusion-condition is used in extended mode, check the common exclusion history file to know whether a common exclusion-condition excludes JP1 events from automated-action execution. If JP1 events are excluded, review the common exclusion-condition.
- Check that the automated action definition is not disabled.
- Review action execution conditions in the automated action definition.

Index

A

actions to take when

additional common exclusion-conditions cannot be set [326](#)

attempt to start profile of remote monitoring log file trap fails in IM Configuration Management [345](#)

automated action is delayed [319](#)

characters are unreadable JP1/SES-format events are received [350](#)

command execution log file is damaged [313](#)

command execution or batch file executed in automated action does not terminate normally [326](#)

connection to JP1/Base fails [307](#)

correlation events cannot be displayed in JP1/IM - View [324](#)

definition menu is not displayed in Event Console window [307](#)

earlier version of JP1/IM - Manager or JP1/IM - View is being used [321](#)

email does not reach destination in email notification function of JP1/IM - Manager [350](#)

error message indicating invalid port number is issued after IM database has been set up [336](#)

event information cannot be inherited [311](#)

event search cannot be executed [333](#)

filter does not work correctly because source host name is different from monitored host name [349](#)

IM Configuration Management failed to apply system hierarchy [338](#)

IM Configuration Management failed to collect operation definition file for log file trap [339](#)

IM database cannot be started or database-related commands cannot be executed [338](#)

IM database cannot be terminated [335](#)

IM database setup fails [336](#)

JP1/IM - Manager cannot be uninstalled [336](#)

JP1/IM - View cannot display any log file traps that are active [339](#)

JP1/IM - View window cannot be displayed after you have logged in [325](#)

JP1 events are displayed late in Event Console window [331](#)

KAVB5150-W is displayed in detailed information for action result [320](#)

many JP1 events occurred for which correlation events were generated [323](#)

memo entries cannot be set up [334](#)

menu items such as Register Host and Edit Agent Configuration are disabled in IM Configuration Management - View [340](#)

monitored object database cannot be unlocked [320](#)

monitored object database is damaged [320](#)

no JP1 event is displayed in Event Console window [330](#)

no response-waiting events are displayed in JP1/IM - View [329](#)

Processing dialog box continues to open in IM Configuration Management - View [344](#)

profile settings file does not match valid configuration information [340](#)

remote monitored log file name is incorrect [346](#)

response-waiting events are displayed as ordinary events [330](#)

same JP1 event is received redundantly in remote monitoring log file trap of IM Configuration Management [345](#)

setup information file is output as invalid during IM database setup [337](#)

source host name is different from host name registered in IM Configuration Management [349](#)

status cannot be changed [332](#)

trapped JP1 event message shows unreadable characters [308](#)

tree area on IM Configuration page in IM Configuration Management - View is displayed in gray [344](#)

unknown is displayed as automated action execution status [318](#)

valid configuration information of remote monitoring log file trap or remote monitoring event log trap cannot be viewed in IM Configuration Management [341](#)

virtualization system configuration cannot be collected in IM Configuration Management [341](#)

you cannot connect to IM database [335](#)

you cannot connect to remotely monitored host [346](#)

you cannot execute command [308](#)

you cannot execute commands from Command button [312](#)

you cannot log in from JP1/IM - View [305](#)

you cannot start client applications [312](#)

Actions to take when an automated action is not executed [363](#)

actions to take when filter does not work correctly because source host name is different from monitored host name [349](#)

- additional common exclusion-condition
 - changing additional common exclusion-condition to common exclusion-condition 112
 - Setting an additional common exclusion-condition to exclude a JP1 event from the monitoring target or action execution 111
- additional common exclusion-conditions
 - setting additional common exclusion-conditions by using JP1 events that have occurred 111
 - trouble shooting (additional common exclusion-conditions cannot be set) 326
- additional common exclusion-condition to common exclusion-condition
 - changing 112
- applying edited settings file information 193
- automated actions
 - canceling 179
 - checking execution results of 176
 - checking execution status of 175
 - checking operating status of 181
 - executing 175
 - re-executing 180
 - setting up 175
- automatic startup and stop, examples of 77

B

- backing up 32
 - command execution log 33
 - configuration information (UNIX) 25
 - configuration information (Windows) 19
 - database 32
 - event database 35
 - file for accumulated response-waiting events 36
 - host information database 35
 - IM database 36
 - monitored object database 34
- batch file, abnormally terminated 326
- batch job execution system 214
 - system configuration when linking with batch job execution systems 214
- BJEX linkage commands
 - jcoimdef 236
 - jim_log.bat (Windows only) 236
 - jim_log.sh (UNIX only) 237
- business groups
 - managing 192

C

- canceling automated actions 179
- Central Console
 - JP1 event grouping 124
- Central Console, monitoring system from 87
- Central Scope
 - monitoring from Monitoring Tree window 158
 - monitoring from Visual Monitoring window 163
 - monitoring system from 157
- changing
 - additional common exclusion-condition to common exclusion-condition 112
 - changing JP1 event display messages 128
 - database settings 38
 - JP1/IM settings 57
 - monitoring status of monitoring nodes 159, 164
 - status of monitoring nodes 158, 164
- changing monitoring configuration
 - notes on changing monitoring configuration from remote to agent 69
- changing response status
 - changing 101
- Changing the message displayed for a JP1 event 128
- checking
 - command execution status 173
 - execution results of automated actions 176
 - execution status of automated actions 175
 - operating status of automated actions 181
- Checking detailed information about a correlation event and changing the response status 103
- cluster system, operations in 73, 76
- collecting (UNIX)
 - RAS information 302
- collecting (Windows)
 - RAS information 296
- command, executing
 - by using Command button 171
 - by using command line 169
 - defined on source host of selected event 172
- command execution log
 - backing up 33
 - procedures for backing up and recovering 33
 - recovering 33
 - re-creating 38
 - reorganizing 30
- command execution status, checking 173
- commands

- actions to take when you cannot execute 308
- deleting 173
- user who executes 173
- commands, executing 169
- common exclusion-condition
 - using command to switch 110
- configuration information
 - managing 19
 - migrating 52
- consolidated
 - consolidated display when events with same attributes occur consecutively 149
- consolidated display
 - consolidated display when events with same attributes occur consecutively 149
- consolidated event
 - setting response status for repeated events 102
- consolidated events in events list, displaying 94
- conventions
 - diagrams 8
 - fonts and symbols 9
 - mathematical expressions 10
 - version numbers 10
- correlation event generation history 50
- correlation events in events list, displaying 95
- correlation source event
 - displaying 104
 - from Related Events (Correlation) or Related Events (Correlation fails) window, deleting 105
 - from Related Events (Correlation) or Related Events (Correlation fails) window, setting response status for 104
- CSV file
 - outputting events to 50

D

- data, collecting 293
- database management 30
 - backing up command execution log 33
 - backing up event database 35
 - backing up file for accumulated response-waiting events 36
 - backing up host information database 35
 - backing up IM database 36
 - backing up monitored object database 34
 - changing IM database port 46
 - expanding IM database size 43
 - recovering command execution log 33

- recovering event database 35
- recovering file for accumulated response-waiting events 36
- recovering host information database 35
- recovering IM database 36
- recovering monitored object database 34
- reorganizing event database 30
- reorganizing file for accumulated response-waiting events 30
- reorganizing IM database 30
- databases
 - backing up 32
 - changing settings of 38
 - managing 30
 - migrating 52
 - recovering 32
 - re-creating 38
 - reorganizing 30
- data collection tool
 - executing (UNIX) 301
 - executing (Windows) 295
- deleting commands 173
- detailed information about repeated events
 - checking, and changing the response status for 102
- diagram conventions 8
- disk capacity, managing 48
- displaying
 - attributes of monitoring nodes 161, 166
 - consolidated events 149
 - guide information 161, 166
 - login user list 162
- displaying, detailed JP1 event information 97
- Displaying extended attributes of JP1 events (mapping of event information) 121
- displaying performance reports for JP1 events when linking with JP1/PFM 156
- displaying search results (JP1 event) 118
- dump files, managing 49

E

- email notification function
 - actions to take when email does not reach destination 350
- error information
 - collecting (UNIX) 302
 - collecting (Windows) 295
- event

- event by specifying event display start-time, displaying 113
- consolidated display when events with same attributes occur consecutively 149
- forwarding from agent, preparing to suppress 134
- severity level of, changing 125
- event acquisition filter
 - applying filter 96
 - switching 107
 - using jcochfilter command to switch 109
- Event Console window
 - actions to take when definition menu is not displayed in 307
 - actions to take when no JP1 event is displayed in 330
 - events displayed in events list in 92
- event database
 - backing up 35
 - procedures for backing up and recovering 35
 - recovering 35
 - re-creating 40
 - reorganizing 30
- event display
 - displaying event by specifying event display start-time 113
- event forwarding
 - handling occurrence of large number of events by suppressing event forwarding from agent 137
 - on agent, setting threshold for automatically suppressing 142
- event information
 - actions to take when event information cannot be inherited 311
- events
 - occurrence of, handling large number of 132
 - occurrence of by suppressing event forwarding from agent, handling large number of 137
 - outputting (to CSV file) 50
 - stopping, on manager, log file trap that issues large numbers of 148
- event search direction 118
- event service
 - actions to take when connection to JP1/Base fails 307
- Exclusion history and definition history of common exclusion conditions 51
- executing
 - automated actions 175
 - commands (on agent or manager host) 171
- extended recovery

- failed, actions to take for 359

F

- file for accumulated response-waiting events 222
 - backing up 36
 - procedures for backing up and recovering 36
 - recovering 36
 - re-creating 42
 - reorganizing 30
- filter 106
 - applying 96
- font conventions 9

G

- grouping
 - JP1 event 124
- guide information, displaying 161, 166

H

- handling
 - general procedures and preparation for handling occurrence of large number of events 132
 - handling occurrence of large number of events 132
- historical reports, using 50
- host information
 - collecting 188
- host information database
 - backing up 35
 - procedures for backing up and recovering 35
 - recovering 35
 - re-creating 39
 - reorganizing 30
- host management
 - changing information 188
 - collecting information 188
 - deleting (IM Configuration Management window) 188
 - displaying lists 188
 - registering 188
- host name
 - actions to take when source host name is different from host name registered in IM Configuration Management 349
 - changing 58
 - cluster system, logical 60
 - mail server 60
 - of manager or agent 58
- host name, changing 58

- host name of manager or agent
 - tasks necessary after changing 58
- host name of manager or agent, procedure for redistributing system configuration after changing 60
- hosts
 - managing 188
- How to extend logs
 - when a log from the time an even occurred cannot be collected because logs for IM Configuration Management viewer wrap around, causing older logs to be overwritten 362

I

- IM Configuration Management
 - actions to take when attempt to start profile of remote monitoring log file trap fails in IM Configuration Management 345
 - actions to take when same JP1 event is received redundantly in remote monitoring log file trap of IM Configuration Management 345
 - actions to take when virtualization system configuration cannot be collected in IM Configuration Management 341
 - applying imported management information of 210
 - applying management information to Central Scope monitoring tree 190
 - exporting and importing management information of IM Configuration Management 196
 - exporting management information of 196
 - importing management information of 200
 - managing business groups 192
 - managing hosts 188
 - managing profiles 193
 - managing service operation status 194
 - managing system hierarchy using 187
- IM Configuration Management - View
 - actions to take when menu items such as Register Host and Edit Agent Configuration are disabled in IM Configuration Management - View 340
 - actions to take when Processing dialog box continues to open in IM Configuration Management - View 344
- IM Configuration page
 - actions to take when tree area on IM Configuration page in IM Configuration Management - View is displayed in gray 344
- IM database
 - actions to take when IM database cannot be started or database-related commands cannot be executed 338
 - backing up 36

- changing port of 46
- expanding size of 43
- recovering 36
- reorganizing 30
- IM database capacity
 - managing 48
- IM database setup
 - actions to take when error message indicating invalid port number is issued after IM database has been set up 336
 - actions to take when IM database setup fails 336
 - actions to take when setup information file is output as invalid during IM database setup 337
- incident
 - displaying JP1/Service Support from Event Details window 152
 - displaying JP1/Service Support from pages of Event Console window 151
 - displaying JP1/Service Support from Related Events window 151
- IP address
 - changing 62
 - of mail server 63
 - of manager or agent 62
- IP address, changing 62
- IP address of manager or agent, procedure for restarting the system after changing 62
- items, displayed in events list 88

J

- JP1/AS linkage commands
 - jcoimdef 236
 - jim_log.bat (Windows only) 236
 - jim_log.sh (UNIX only) 237
- JP1/IM
 - changing configuration of 56
 - changing severity level of JP1 events 125
 - collecting data 293
 - correcting problems 305
 - data that needs to be collected when problem occurs 269
 - editing JP1 memo entries 99
 - linking with BJEX 213
 - logging in 83
 - logging in to JP1/IM - Manager 83
 - logging out 86
 - logging out of JP1/IM - Manager 86
 - log information types 240

- managing configuration information 19
- managing databases 30
- managing disk capacity 48
- monitoring from Monitoring Tree window 158
- monitoring from Visual Monitoring window 163
- monitoring system from Central Scope 157
- opening monitor window of application that issued JP1 events 155
- opening other application windows from Tool Launcher 183
- outputting dump file for (UNIX) 300
- outputting thread dump for (Windows) 293
- searching for JP1 events 116
- settings information, changing 57
- starting 71
- stopping 75
- switching event acquisition filter to be applied 107
- system maintenance 18
- system operation using 168
- troubleshooting 238
- troubleshooting procedure 239
- using historical reports 50
- JP1/IM files for backup 20, 26
- JP1/IM filter
 - applying 106
- JP1/IM - Manager
 - in which communication encryption function is enabled, actions to take when error is displayed on 352
 - log files (Central Console) (UNIX) 257
 - log files (Central Console) (Windows) 243
 - log files (Central Scope) (UNIX) 264
 - log files (Central Scope) (Windows) 250
 - log files and folders (IM Configuration Management) (UNIX) 265
 - log files and folders (IM Configuration Management) (Windows) 251
 - logging in to 83
 - logging out of 86
 - login and logout 82
 - notes on starting 81
 - notes on stopping 81
 - starting 70–72
 - stopping 70, 75
 - using command to log in to 84
 - using GUI to log in to 83
- JP1/IM - Rule Operation
 - checking rule startup request status 152
 - displaying Rule Log Details window of 153
 - operating 152
- JP1/IM system
 - applying system hierarchy 189
 - collecting system hierarchy information 189
 - displaying system hierarchy 189
 - editing system hierarchy 189
 - synchronizing system hierarchies 189
 - verifying system hierarchy 189
- JP1/IM - View
 - actions to take when no response-waiting events are displayed in 329
 - actions to take when response-waiting events are displayed as ordinary events 330
 - actions to take when you cannot log in from 305
 - collecting information related to web version of (UNIX) 301
 - collecting information related to web version of (Windows) 294
 - executing commands by using Command button 171
 - executing commands by using Command Execution 169
 - log files and folders 255
 - opening monitor window of application that issued JP1 events 155
 - opening other application windows from Tool Launcher 183
 - switching common exclusion-condition from Event Acquisition Conditions List window 108
 - switching common exclusion-condition from System Environment Settings window 108
 - switching event acquisition filter from Event Acquisition Conditions List window 108
 - switching event acquisition filter from System Environment Settings window 107
 - system operation 168
 - when communication encryption function is enabled, actions to take when error is displayed in 355
- JP1/Navigation Platform
 - displaying operating procedures for JP1 events (linking with JP1/Navigation Platform) 152
- JP1/PFM
 - displaying performance reports for JP1 events when linking with JP1/PFM 156
 - operating 156
- JP1/Service Support
 - from Event Details window, displaying 152
 - from pages of Event Console window, displaying 151
 - from Related Events window, displaying 151
 - operating 151

registering JP1 events as incidents in JP1/IM - Service Support (linking with JP1/IM - Service Support) 151

JP1 event

as incidents in JP1/IM - Service Support (linking with JP1/IM - Service Support), registering 151

by linking with other products, handling 151

changing severity level of JP1 events 125

displaying 88

displaying detailed information 97

displaying only severe events 106

displaying operating procedures for (linking with JP1/Navigation Platform) 152

displaying program-specific extended attributes of (displaying program-specific extended attributes) 121

displaying program-specific extended attributes of (mapping event information) 121

displaying search results 118

display messages, changing 128

grouping 124

opening monitor window of application that issued 155

program-specific extended attributes of (displaying program-specific extended attributes) 91

program-specific extended attributes of (event information mapping) 92

response status 92

searching for 116

search method 116

search procedure 116

setting JP1 event response statuses 100

to be displayed by specifying time period, narrowing 114

viewing 88

JP1 event information

by operation, customizing 121

JP1 event response status

setting 100

settings for 100

JP1 events

actions to take if JP1 events are not received even when remote monitoring event log trap is running in IM Configuration Management 343

actions to take if JP1 events are not received even when remote monitoring log file trap is running in IM Configuration Management 342

items that can be displayed 89

using historical information of 50

JP1 events response status

from events list, setting 101

JP1 memo entry

editing 99

K

KAVB0002-E 310

KAVB0104-E 305

KAVB0109-E 305

KAVB0256-E 327

KAVB0415-E 308

KAVB0416-E 308

KAVB0417-E 309

KAVB0418-E 309

KAVB0419-E 309

KAVB0422-E 309

KAVB0423-E 309

KAVB1034-E 312

KAVB1036-W 311

KAVB1037-E 311, 312

KAVB1040-W 311

KAVB1041-W 311

KAVB1042-W 311

KAVB1043-W 311

KAVB1044-W 311

KAVB1046-E 311

KAVB1153-E 327

KAVB1154-W 327

KAVB1155-E 326

KAVB1157-E 327

KAVB1158-W 328

KAVB1159-W 328

KAVB1160-W 328

KAVB1161-W 328

KAVB1162-W 328

KAVB1163-E 326

KAVB1200-E 305

KAVB1956-E 352

KAVB1957-E 352

KAVB1958-E 356

KAVB1959-E 356

KAVB1969-W 357

KAVB1971-W 357

KAVB1972-W 353

KAVB2027-E 310

KAVB2031-E 310

KAVB2239-E 319

KAVB6601-E 356

KAVB6602-E 356
 KAVB6603-W 357
 KAVB7247-E 320
 KAVB7248-E 320
 KAVB7602-E 353
 KAVB7810-E 353
 KAVB7812-E 354
 KAVB7818-E 354
 KAVB8452-E 310
 KAVB8817-E 352
 KAVB8818-E 352
 KNAN20100-E 305
 KNAN20101-E 306
 KNAN20102-E 306
 KNAN20103-E 306
 KNAN20104-E 307
 KNAN20121-E 356
 KNAN20122-E 356
 KNAN20123-W 357
 KNAN20124-W 357
 KNAN20141-E 356
 KNAN20142-E 357
 KNAN20143-W 357
 KNAN20144-W 358
 KNAN21400-W 348
 KNAN21402-E 348
 KNAN21403-E 348
 KNAN21404-E 358
 KNAN22017-E 346
 KNAN24155-E 354
 KNAN26039-E 345
 KNAN29095-E 354
 KNAN29097-W 355
 KNAN29098-E 354

L

linkage

- BJEX configuration 230
- BJEX linkage configuration 227
- BJEX or JP1/AS configuration 230
- BJEX or JP1/AS linkage configuration 227
- communication settings between BJEX and JP1/IM - Manager 229
- JP1/AS configuration 230
- JP1/AS linkage configuration 227
- JP1/IM functionality for BJEX linkage 217
- JP1/IM functionality for BJEX or JP1/AS linkage 217

- JP1/IM functionality for JP1/AS linkage 217
- linking with BJEX 236
- linking with BJEX or JP1/AS 236
- linking with JP1/AS 236
- overview of BJEX linkage 214
- overview of BJEX or JP1/AS linkage 214
- overview of JP1/AS linkage 214

linked products

- BJEX 213
- linking with JP1/AS 213

linking

- handling JP1 events by linking with other products 151
- with BJEX or JP1/AS 213
- with JP1/AS 213

linking with JP1/Navigation Platform

- operating 152

log

- common message 240
- files and directory list 242
- integrated trace 240
- operation 242
- types of information 240

log file size, managing 49

log file trap

- stopping, on manager, log file trap that issues large numbers of events 148

login 83

- using GUI 83

login user list, displaying 162

logout 86

M

maintenance 18

management information, exporting and importing 196

manager or agent, IP address of

- tasks after changing 62

manager or agent, resetting the date/time of

- returning the time 64

manager or agent, tasks required when date of is changed 64

managing

- business groups 192
- configuration information 19
- configuration of virtual system 190
- databases 30
- disk capacity 48

- hosts 188
- IM database capacity 48
- profiles 193
- service operation status 194
- mathematical expression conventions 10
- message
 - changing JP1 event display messages 128
- migrating configuration information and databases 52
- monitored host in a remote monitoring configuration, tasks required when date of is changed 67
- monitored object database
 - backing up 34
 - procedures for backing up and recovering 34
 - recovering 34
 - re-creating 39
 - reorganizing 30
- monitoring
 - from Monitoring Tree window 158
 - from Visual Monitoring window 163
- monitoring nodes
 - changing monitoring status of 159, 164
 - changing status of 158, 164
 - displaying attributes of 161, 166
 - searching for 160, 165
- monitoring tree
 - changing monitoring status of monitoring nodes in 159
 - changing status of monitoring nodes in 158
 - displaying attributes of monitoring nodes in 161
 - displaying guide information in 161
 - searching for monitoring nodes in 160
 - searching for status-change events in 160
- Monitoring Tree window
 - monitoring from 158
 - opening, from Visual Monitoring window 163
 - saving information in 162
- monitor window 155
- monitor window of application, opening 155

N

- non-cluster system
 - logical host, operating (startup) 74
 - logical host, operating (termination) 76
- notes on
 - starting JP1/IM - Manager 81
 - stopping JP1/IM - Manager 81

O

- opening
 - Monitoring Tree window from Visual Monitoring window 163
 - other application windows from Tool Launcher 183
 - Visual Monitoring window 162
- opening monitor window
 - opening monitor window of application that issued JP1 events 155
- operating
 - changing severity level of JP1 events 125
 - checking rule startup request status 152
 - deleting severe events 101
 - displaying detailed JP1 event information 97
 - displaying JP1 event search results 118
 - displaying only severe events 106
 - displaying operating procedures for JP1 events (linking with JP1/Navigation Platform) 152
 - displaying performance reports for JP1 events when linking with JP1/PFM 156
 - editing memo entry 99
 - executing commands by using Command button 171
 - executing commands by using Command Execution 169
 - making rule startup request 152
 - opening monitor window 155
 - registering JP1 events as incidents in JP1/IM - Service Support (linking with JP1/IM - Service Support) 151
 - searching for JP1 events 116
 - setting response status for JP1 events from events list 101
 - switching event acquisition filter 107
- operation content
 - checking (UNIX) 302
 - checking (Windows) 295
- operations
 - displaying login user list 162
 - login 83
 - logout 86
 - opening Visual Monitoring window 162
 - saving information in Monitoring Tree window on local host 162
 - searching for monitoring nodes 165
 - searching for monitoring nodes from monitoring tree 160
 - starting JP1/IM - Manager 71
 - stopping JP1/IM - Manager 75

- Tool Launcher window 183
- using command to log in 84
- using GUI to log in 83

P

- passwords of a monitored host in a remote monitoring configuration, tasks required when changed 68

- preparing

- general procedures and preparation for handling occurrence of large number of events 132
 - preparing to suppress event forwarding from agent 134

- procedures

- changing IM database port 46
 - expanding IM database size 43
 - troubleshooting 239

- process status, checking 293, 300

- profiles, managing 193

- displaying profiles 193
 - editing settings files 193
 - obtaining list of profiles 193
 - obtaining profiles 193

- program-specific extended attributes of JP1 events

- displaying (displaying program-specific extended attributes) 121
 - displaying (mapping event information) 121

R

- RAS information

- collecting (UNIX) 302
 - collecting (Windows) 296

- recovering 32

- command execution log 33
 - configuration information (UNIX) 29
 - configuration information (Windows) 25
 - database 32
 - event database 35
 - file for accumulated response-waiting events 36
 - host information database 35
 - IM database 36
 - monitored object database 34

- re-creating

- command execution log 38
 - databases 38
 - event database 40
 - file for accumulated response-waiting events 42
 - host information database 39

- monitored object database 39
- re-executing automated actions 180
- regular expression
 - to specify search conditions, using (event search) 118

- Related Events window

- operating JP1 events from 102

- remote monitoring log file trap

- notes applying before starting remote monitoring log file trap by using IM Configuration Management 345

- reorganizing 30

- command execution log 30

- event database 30

- file for accumulated response-waiting events 30

- host information database 30

- IM database 30

- monitored object database 30

- repeated events

- consolidated event 102

- repeated events that are consolidated into consolidated event

- checking detailed information about 102
 - setting response status for 102

- response-waiting event management function 214, 218

- response-waiting events 214

- accumulating 222

- canceling 225

- handling in JP1/IM 217

- issuing paths 217

- manually removing from accumulation 234

- monitoring 219

- monitoring in Central Console 231

- monitoring in Central Scope 233

- responding to 223, 234

- resuming monitoring in hold-and-accumulate state 235

- rule startup request

- checking rule startup request status and making rule startup request (linking with JP1/IM - Rule Operation) 152

S

- saving information in Monitoring Tree window on local host 162

- searching

- monitoring nodes 160, 165

- status-change events 165

- status-change events from monitoring tree 160

- searching for
 - JP1 event 116
- searching for JP1 events
 - operating 116
 - search procedure 116
- search method (JP1 event) 116
- service operation information
 - displaying 195
 - managing 194
- setting
 - setting additional common exclusion-conditions by using JP1 events that have occurred 111
 - setting threshold for automatically suppressing event forwarding on agent 142
- setting additional common exclusion-conditions by using JP1 events that have occurred 111
- Setting an additional common exclusion-condition to exclude a JP1 event from the monitoring target or action execution 111
- settings information, changing 57
- severe event
 - displaying 106
- severe event filter
 - applying filter 96
- Severe Events page
 - deleting severe events from 101
- specifying
 - specifying repeated event conditions 143
- starting
 - JP1/IM - Manager 71
 - notes on 81
- status-change events, searching 160, 165
- stopping
 - JP1/IM - Manager 75
 - notes on 81
 - stopping, on manager, log file trap that issues large numbers of events 148
- suppressing
 - handling occurrence of large number of events by suppressing event forwarding from agent 137
 - preparing to suppress event forwarding from agent 134
- symbol conventions 9
- system date, changing of 64
- system hierarchies
 - managing 187, 189
- system monitoring from Central Console 87
- system time, resetting of

- advancing the time 66

T

- Taking actions for the generation of a large number of events 132
- threshold
 - setting threshold for automatically suppressing event forwarding on agent 142
- Tool Launcher
 - functions that can be operated from 184
 - opening other application windows from 183
 - operations in 183
- troubleshooting 238, 305
 - corrective actions 305
 - data collection method 293
 - data that needs to be collected 269
 - log information types 240
 - procedure 239

U

- unreadable characters
 - actions to take when trapped JP1 event message shows unreadable characters 308
- user-defined extended attribute to JP1 events that match condition, adding 124
- user dump
 - collecting (Windows only) 295
- user who executes commands 173

V

- version number conventions 10
- view filter
 - applying filter 96
- viewing, JP1 events 88
- virtual host, registering 190
- virtual system
 - displaying host information in 190
 - managing configuration of 190
- Visual Monitoring window
 - changing monitoring status of monitoring nodes in 164
 - changing status of monitoring nodes in 164
 - displaying attributes of monitoring nodes from 166
 - displaying guide information from 166
 - monitoring from 163
 - opening 162
 - opening Monitoring Tree window from 163

searching for monitoring nodes in [165](#)

searching for status-change events in [165](#)

W

Web version of JP1/IM - View [83](#)

when a log from the time an even occurred cannot be collected because logs for Central Console viewer or Central Scope viewer wrap around, causing older logs to be overwritten [360](#)

 **Hitachi, Ltd.**

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