

JP1 Version 13

**JP1/Integrated Management 3 - Manager
Administration Guide**

3021-3-L04-20(E)

Notices

■ Relevant program products

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

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

P-2A2C-8EDL JP1/Integrated Management 3 - Manager 13-10

The above product includes the following:

P-CC2A2C-9MDL JP1/Integrated Management 3 - Manager 13-10 (for Windows Server 2022, Windows Server 2019, Windows Server 2016)

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

P-CC2A2C-9GDL JP1/Integrated Management 3 - Agent 13-10 (for Windows Server 2022, Windows Server 2019, Windows Server 2016)

P-CC842C-9GDL JP1/Integrated Management 3 - Agent 13-10 (for Linux 9, Linux 8, Linux 7, Oracle Linux 9, Oracle Linux 8, Oracle Linux 7, SUSE Linux 15, SUSE Linux 12, Amazon Linux 2023)

P-CC2A2C-6LDL JP1/Base 13-10 (for Windows Server 2022, Windows Server 2019, Windows Server 2016)

P-CC842C-6LDL JP1/Base 13-10 (for Linux 9, Linux 8, Linux 7, Oracle Linux 9, Oracle Linux 8, Oracle Linux 7, SUSE Linux 15, SUSE Linux 12, Amazon Linux 2023)

P-CC1M2C-6LDL JP1/Base 13-10 (for AIX)

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

P-842C-8EDL JP1/Integrated Management 3 - Manager 13-10

The above product includes the following:

P-CC842C-9MDL JP1/Integrated Management 3 - Manager 13-10 (for Linux 9, Linux 8, Linux 7, Oracle Linux 9, Oracle Linux 8, Oracle Linux 7)

P-CC9W2C-9MDL JP1/Integrated Management 3 - Manager 13-10 (for SUSE Linux 15, SUSE Linux 12)

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

P-CC2A2C-9GDL JP1/Integrated Management 3 - Agent 13-10 (for Windows Server 2022, Windows Server 2019, Windows Server 2016)

P-CC842C-9GDL JP1/Integrated Management 3 - Agent 13-10 (for Linux 9, Linux 8, Linux 7, Oracle Linux 9, Oracle Linux 8, Oracle Linux 7, SUSE Linux 15, SUSE Linux 12, Amazon Linux 2023)

P-CC2A2C-6LDL JP1/Base 13-10 (for Windows Server 2022, Windows Server 2019, Windows Server 2016)

P-CC842C-6LDL JP1/Base 13-10 (for Linux 9, Linux 8, Linux 7, Oracle Linux 9, Oracle Linux 8, Oracle Linux 7, SUSE Linux 15, SUSE Linux 12, Amazon Linux 2023)

P-CC1M2C-6LDL JP1/Base 13-10 (for AIX)

■ Trademarks

HITACHI, HiRDB, JP1, uCosminexus are either trademarks or registered trademarks of Hitachi, Ltd. in Japan and 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/>).

1. This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (<http://www.openssl.org/>)

2. This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)

3. This product includes software written by Tim Hudson (tjh@cryptsoft.com)

4. This product includes the OpenSSL Toolkit software used under OpenSSL License and Original SSLeay License. OpenSSL License and Original SSLeay License are as follow:

LICENSE ISSUES

=====

The OpenSSL toolkit stays under a double license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit.

See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL License

/* =====

* Copyright (c) 1998-2018 The OpenSSL Project. All rights reserved.

*

* Redistribution and use in source and binary forms, with or without

* modification, are permitted provided that the following conditions

* are met:

*

* 1. Redistributions of source code must retain the above copyright

* notice, this list of conditions and the following disclaimer.

*

* 2. Redistributions in binary form must reproduce the above copyright

* notice, this list of conditions and the following disclaimer in

* the documentation and/or other materials provided with the

* distribution.

*

* 3. All advertising materials mentioning features or use of this software must display the following acknowledgment:

* "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (<http://www.openssl.org/>)"

* 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.

* 5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.

* 6. Redistributions of any form whatsoever must retain the following acknowledgment:

* "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>)"

* THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

* This product includes cryptographic software written by Eric Young (ey@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

*/

Original SSLeay License

/* Copyright (C) 1995-1998 Eric Young (ey@cryptsoft.com)

* All rights reserved.

*
 * This package is an SSL implementation written
 * by Eric Young (eay@cryptsoft.com).
 * The implementation was written so as to conform with Netscapes SSL.
 *
 * This library is free for commercial and non-commercial use as long as
 * the following conditions are aheared to. The following conditions
 * apply to all code found in this distribution, be it the RC4, RSA,
 * lhash, DES, etc., code; not just the SSL code. The SSL documentation
 * included with this distribution is covered by the same copyright terms
 * except that the holder is Tim Hudson (tjh@cryptsoft.com).
 *
 * Copyright remains Eric Young's, and as such any Copyright notices in
 * the code are not to be removed.
 * If this package is used in a product, Eric Young should be given attribution
 * as the author of the parts of the library used.
 * This can be in the form of a textual message at program startup or
 * in documentation (online or textual) provided with the package.
 *
 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions
 * are met:
 * 1. Redistributions of source code must retain the copyright
 * notice, this list of conditions and the following disclaimer.
 * 2. Redistributions in binary form must reproduce the above copyright
 * notice, this list of conditions and the following disclaimer in the
 * documentation and/or other materials provided with the distribution.
 * 3. All advertising materials mentioning features or use of this software
 * must display the following acknowledgement:
 * "This product includes cryptographic software written by
 * Eric Young (eay@cryptsoft.com)"
 * The word 'cryptographic' can be left out if the rouines from the library
 * being used are not cryptographic related :-).
 * 4. If you include any Windows specific code (or a derivative thereof) from
 * the apps directory (application code) you must include an acknowledgement:
 * "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"
 *
 * THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS" AND
 * ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
 * IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
 * ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE
 * FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL

- * DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
- * OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
- * HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
- * LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
- * OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
- * SUCH DAMAGE.

- *
- * The licence and distribution terms for any publically available version or
- * derivative of this code cannot be changed. i.e. this code cannot simply be
- * copied and put under another distribution licence
- * [including the GNU Public Licence.]
- */

This product includes software developed by Andy Clark.

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

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

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

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



■ Microsoft product name abbreviations

This manual uses the following abbreviations for Microsoft product names.

Abbreviation	Full name or meaning
Hyper-V	Microsoft ^(R) Windows Server ^(R) 2012 Hyper-V ^(R)

Abbreviation	Full name or meaning
SCVMM	Microsoft ^(R) System Center Virtual Machine Manager 2012
Windows 10	Windows ^(R) 10 Enterprise 64-bit
	Windows ^(R) 10 Home 64-bit
	Windows ^(R) 10 Pro 64-bit
Windows 11	Windows ^(R) 11 Enterprise
	Windows ^(R) 11 Home
	Windows ^(R) 11 Pro
Windows Server 2016	Microsoft ^(R) Windows Server ^(R) 2016 Datacenter
	Microsoft ^(R) Windows Server ^(R) 2016 Standard
Windows Server 2019	Microsoft ^(R) Windows Server ^(R) 2019 Datacenter
	Microsoft ^(R) Windows Server ^(R) 2019 Standard
Windows Server 2022	Microsoft ^(R) Windows Server ^(R) 2022 Datacenter
	Microsoft ^(R) Windows Server ^(R) 2022 Standard

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

■ Restrictions

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

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

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

■ Issued

Sep. 2024: 3021-3-L04-20(E)

■ Copyright

Copyright (C) 2023, 2024 Hitachi, Ltd.

Copyright (C) 2023, 2024 Hitachi Solutions, Ltd.

Summary of amendments

The following table lists changes in this manual (3021-3-L04-20(E)) and product changes related to this manual.

Changes	Location
<p>Added a function (Web scenario monitoring function) to monitor the operation playback time of user operations (initial screen and series of operations from login to logoff) in a Web browser based on Web scenarios. In addition, the following functions were added.</p> <ul style="list-style-type: none"> Trace viewer function to visually check the actions recorded in the trace by executing web scenarios Web operation information collection function (Web exporter) added to performance monitoring function of JP1/IM - Agent <p>Along with this, an explanation on the operation of Web exporter and Web scenario monitoring function was added.</p>	<p><i>1.1.1(1), 1.1.2(3)(a), 1.5.1(9)(c), 2.1.1(3), 10.1, 12.3.1(1)(b), 12.3.1(2)(b), 12.5.1(12)</i></p>
<p>VMware performance information collection function (VMware exporter) has been added to the performance monitoring function of JP1/IM - Agent.</p> <p>Along with this, an explanation on the operation of VMware exporter was added.</p>	<p><i>1.1.1(1), 1.1.1(3), 1.1.2(3)(a), 1.1.2(3)(b), 10.1, 12.3.1(1)(b), 12.3.1(2)(b), 12.5.1(13)</i></p>
<p>Added a function (event-forwarding relay function) in which JP1/IM - Manager (Intelligent Integrated Management Base) on a host in the cloud environment creates an IM management node for JP1/Base on monitored hosts in your on-premises environment, and display JP1 events generated on that node in the integrated operation viewer.</p> <p>Along with this, an explanation on the operation of the event-forwarding relay function was added.</p>	<p><i>1.1.1(1), 1.1.1(3), 2.2.1(3)(a), 2.2.1(3)(d), 2.3.1(3)(a), 2.11, 12.5.3(84), 12.5.3(85)</i></p>

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

Preface

This manual explains administration, operations, and troubleshooting for JP1/Integrated Management 3 - Manager and JP1/Integrated Management 3 - View. In this manual, JP1/Integrated Management 3 - Manager and JP1/Integrated Management 3 - View are generically referred to as *JP1/Integrated Management* or *JP1/IM*. In addition, in this manual, read JP1/Integrated Management - Manager and JP1/Integrated Management - View as JP1/Integrated Management 3 - Manager and JP1/Integrated Management 3 - View, respectively.

■ 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.

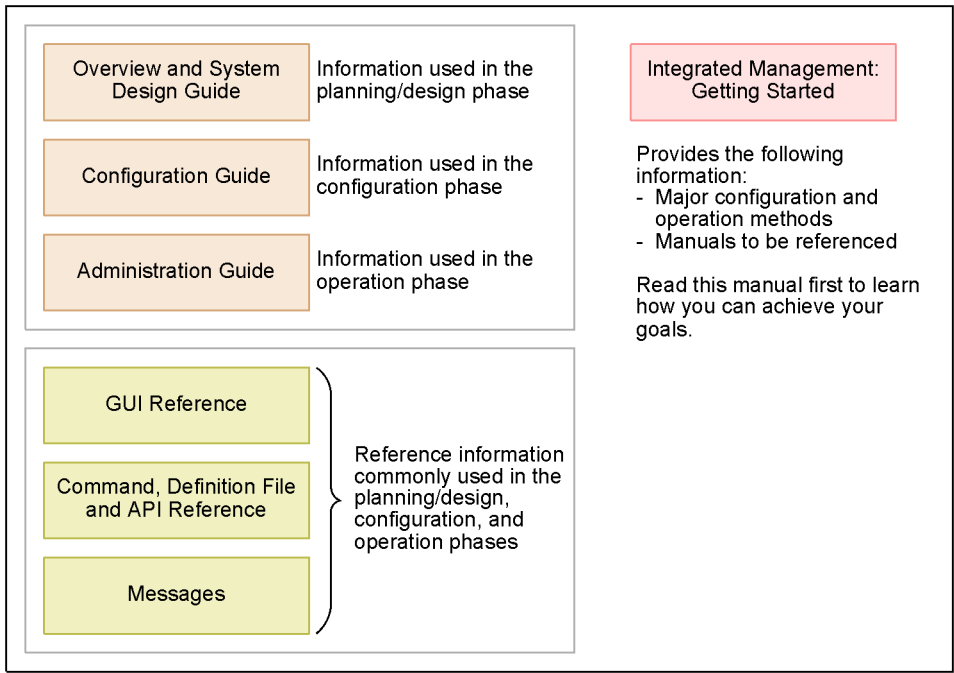
PART 4. Troubleshooting

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

■ Manual suite






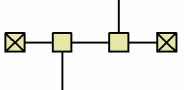


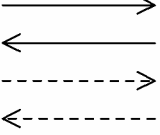
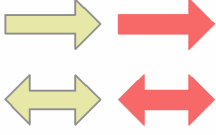


JP1/IM manuals provide necessary information according to the phase in the system life cycle (the phases include planning/design, configuration, and operation). Read the manual appropriate for the purpose.

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/IM - Agent	<i>Agent-path</i>	<i>system-drive</i> : \Program Files\Hitachi\JP1IMA
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**.
- In Integrated Operation Viewer Window, choose **Help** and then **Online manual**.

Note:

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

■ Output destinations of Integrated trace log file

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

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

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

- IM database
- Central Scope Service
- Process management
- Command execution
- Automatic action
- Installation and Setup

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

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

Contents

Notices	2
Summary of amendments	8
Preface	9

Part 1: Administration

1	JP1/IM System Maintenance	22
1.1	Managing the configuration information	23
1.1.1	JP1/IM - Manager backups and recoveries	23
1.1.2	Backing Up and Recovering of JP1/IM - Agent	38
1.2	Managing the databases	52
1.2.1	Database reorganization	52
1.2.2	Database backup and recovery	54
1.2.3	Re-creating a database and changing its settings	63
1.3	Managing the disk capacity	75
1.3.1	Managing the IM database capacity	75
1.3.2	Managing the log file size	78
1.3.3	Managing dump files	81
1.4	Using historical reports	82
1.4.1	Outputting events to a CSV file	82
1.4.2	Correlation event generation history	82
1.4.3	Exclusion history and definition history of common exclusion conditions	83
1.5	Migrating the configuration information and databases	84
1.5.1	Configuration information and databases to be migrated	84
1.6	Managing certificates for the communication encryption function	90
1.6.1	Managing the effective duration of the server certificate	90
1.6.2	Managing keystores	90
2	Changing the Configuration of JP1/IM	92
2.1	Changing the JP1/IM settings information	93
2.1.1	Changing the JP1/IM - Agent settings with integrated agent host	93
2.1.2	Changing the Integration Manager Host JP1/IM - Agent settings	96
2.2	Tasks necessary when a host name is changed	97
2.2.1	When you are using JP1/IM - Agent as agent	97
2.2.2	When you are using JP1/Base as agent	102
2.2.3	Tasks to be performed when the host name of a mail server is changed	105
2.2.4	Tasks to be performed before a logical host name is changed in a cluster system	105

2.3	Tasks necessary when an IP address is changed	107
2.3.1	When JP1/IM - Agent is used as agent	107
2.3.2	When JP1/Base is used as agent	109
2.3.3	Tasks to be performed when the IP address of a mail server is changed	110
2.4	Tasks necessary when the date of a manager or agent is changed	111
2.4.1	Resetting the date/time of a manager or agent to a past date/time	111
2.4.2	Advancing the system time	114
2.5	Required steps to change integrated agent host system date and time	115
2.5.1	Changing integrated agent host system date and time	115
2.5.2	Changing the system date and time on a cluster system	115
2.5.3	Changing the system date and time in a container	116
2.6	Tasks necessary when the date of a monitored host in a remote monitoring configuration is changed	117
2.6.1	Resetting the date/time of a monitored host in a remote monitoring configuration to a past date/time	117
2.6.2	Advancing the date/time of a monitored host in a remote monitoring configuration	117
2.7	Tasks necessary when the passwords of a monitored host in a remote monitoring configuration are changed	118
2.8	Notes on changing the monitoring configuration from remote to agent	119
2.8.1	Notes on JP1/Base log file traps	119
2.8.2	Notes on JP1/Base event log traps	119
2.9	Tasks necessary when an Port number is changed	120
2.10	Tasks to be performed when changing the locale of integrated agent host	121
2.10.1	Changing the locale of integrated agent host	121
2.10.2	Changing the locale on a cluster system	122
2.10.3	Changing the locale in a container	122
2.11	Tasks necessary when configuration of event-forwarding relay source for integrated agent host is changed	123
2.12	Duplicate an integrated agent host	124
2.12.1	Replicating physical hosts	124
2.12.2	Duplicate AWS/EC2 instance after operation starts	124

Part 2: Operation

3	Starting and Stopping JP1/IM - Manager	126
3.1	Starting JP1/IM - Manager	127
3.1.1	In Windows	127
3.1.2	In UNIX	128
3.1.3	Operations in a cluster system	130
3.1.4	Operating a logical host in a non-cluster system	130
3.2	Stopping JP1/IM - Manager	132
3.2.1	In Windows	132
3.2.2	In UNIX	132

3.2.3	Operations in a cluster system	133
3.2.4	Operating a logical host in a non-cluster system	134
3.3	Automatic startup and automatic stop setting examples when a logical host operates in a non-cluster system	135
3.3.1	Setting up automatic startup and automatic stop when a logical host operates in a non-cluster system (for Windows)	135
3.3.2	Setting up automatic startup and automatic stop when a logical host operates in a non-cluster system (for Linux)	135
3.3.3	Setting up automatic startup and automatic stop on both the physical host and the logical host	137
3.4	Notes on starting and stopping	139
4	JP1/IM - Manager Login and Logout	141
4.1	Logging in to JP1/IM - Manager	142
4.1.1	Using a Web browser to log in to JP1/IM - Manager (Intelligent Integrated Management Base)	142
4.1.2	Using the GUI to log in to JP1/IM - Manager	142
4.1.3	Using a command to log in to JP1/IM - Manager	144
4.2	Logging out of JP1/IM - Manager	145
5	System Monitoring from the Intelligent Integrated Management Base	146
5.1	Viewing the system status	147
5.1.1	What Intelligent Integrated Management Base can monitor	147
5.1.2	Items displayed in the sunburst chart or the tree chart	147
5.2	Viewing JP1 events (Events window)	150
5.2.1	Items displayed in the events list	151
5.2.2	Displaying Repeated event list window	153
5.2.3	Displaying detailed JP1 event information	153
5.3	Add metric for Trend Viewing and Alerting	155
5.4	How to look at the dashboard	157
5.4.1	For viewing dashboards	157
5.4.2	IM management node status monitoring	158
5.4.3	Monitoring with alert information	160
5.4.4	Checking various IT resources	160
5.4.5	Flow of Problem Investigation and Response Based on Dashboard	161
5.4.6	Notes	164
5.5	Viewing links with other products	166
5.5.1	Using signs to avoid failures (link with JP1/AJS)	166
5.5.2	Understanding how extensive a problem that occurred during operation of a job is and handling it (link with JP1/AJS)	166
5.5.3	Understanding in advance which root jobnets are affected before the definition or content of a job is changed (link with JP1/AJS)	167
5.5.4	Checking performance data and handling the problem (link with JP1/PFM)	167
5.5.5	Handling errors by viewing suggestions	167

- 5.5.6 Logging in to the system with single sign-on through linkage with external products using OIDC authentication 168
- 5.5.7 Sharing information using a direct access URL 169
- 5.6 Notes on operating the Intelligent Integrated Management Base 171
- 5.6.1 Notes on when there is a link with JP1/AJS 171
- 5.6.2 Notes on using event receiver filters 173

- 6 System Monitoring from Central Console 174**
- 6.1 Viewing JP1 events 175
- 6.1.1 Items displayed in the events list 175
- 6.1.2 Events displayed in the events list in the Event Console window 179
- 6.1.3 Applying a filter 183
- 6.2 Displaying detailed JP1 event information 184
- 6.2.1 Editing JP1 memo entries 186
- 6.3 Setting JP1 event response statuses 187
- 6.3.1 Settings for JP1 event response statuses 187
- 6.3.2 Setting a response status for JP1 events from the events list 188
- 6.3.3 Deleting severe events from the Severe Events page 188
- 6.4 Operating JP1 events from the Related Events window 189
- 6.4.1 Checking detailed information about repeated events and changing the response status 189
- 6.4.2 Checking detailed information about a correlation event and changing the response status 190
- 6.5 Applying a JP1/IM filter 193
- 6.5.1 Enabling a view filter to display only certain JP1 events 193
- 6.5.2 Displaying only severe events 193
- 6.5.3 Switching the event acquisition filter to be applied 194
- 6.5.4 Setting an additional common exclusion-condition to exclude a JP1 event from the monitoring target or action execution 198
- 6.6 Displaying an event by specifying an event display start-time 200
- 6.7 Narrowing the JP1 events to be displayed by specifying a time period 201
- 6.8 Searching for JP1 events 203
- 6.8.1 Search method 203
- 6.8.2 Displaying the search results 205
- 6.9 Customizing JP1 event information by operation 208
- 6.9.1 Displaying program-specific extended attributes of JP1 events (displaying program-specific extended attributes) 208
- 6.9.2 Displaying extended attributes of JP1 events (mapping of event information) 208
- 6.9.3 Adding a user-defined extended attribute to JP1 events that match a condition 211
- 6.9.4 Changing the severity level of JP1 events 212
- 6.9.5 Changing the message displayed for a JP1 event 215
- 6.10 Taking actions for the generation of a large number of events 219
- 6.10.1 General procedures and preparation for handling occurrence a large number of events 219
- 6.10.2 Preparing to suppress event forwarding from an agent 221

- 6.10.3 Handling the occurrence of a large number of events by suppressing event forwarding from an agent 224
- 6.10.4 Handling the occurrence of a large number of events by consolidating them on the manager 228
- 6.10.5 Setting a threshold for automatically suppressing event forwarding on an agent 229
- 6.10.6 Specifying repeated event conditions 230
- 6.10.7 Stopping, on the manager, a log file trap that issues a large numbers of events 235
- 6.10.8 Consolidated display when events with the same attributes occur consecutively 236
- 6.11 Handling JP1 events by linking with other products 238
- 6.11.1 Registering JP1 events as incidents in JP1/IM - Service Support (linking with JP1/IM - Service Support) 238
- 6.11.2 Displaying operating procedures for JP1 events (linking with JP1/Navigation Platform) 239
- 6.11.3 Opening a monitor window of the application that issued JP1 events 239
- 6.11.4 Displaying performance reports for JP1 events when linking with JP1/PFM 240
- 6.12 Notes for Central Console 241
- 6.13 Notes on using the Central Console - View 242

7 System Monitoring from Central Scope 243

- 7.1 Monitoring from the Monitoring Tree window 244
 - 7.1.1 Changing the status of monitoring nodes 244
 - 7.1.2 Changing the monitoring status of monitoring nodes 245
 - 7.1.3 Searching for monitoring nodes 246
 - 7.1.4 Searching for status-change events 246
 - 7.1.5 Displaying the attributes of monitoring nodes 247
 - 7.1.6 Displaying guide information 247
 - 7.1.7 Opening the Visual Monitoring window 248
 - 7.1.8 Displaying a login user list 248
 - 7.1.9 Saving the information in the Monitoring Tree window on the local host 248
- 7.2 Monitoring from the Visual Monitoring window 249
 - 7.2.1 Opening the Monitoring Tree window from the Visual Monitoring window 249
 - 7.2.2 Changing the status of monitoring nodes 250
 - 7.2.3 Changing the monitoring status of monitoring nodes 250
 - 7.2.4 Searching for monitoring nodes 251
 - 7.2.5 Searching for status-change events 251
 - 7.2.6 Displaying the attributes of monitoring nodes 252
 - 7.2.7 Displaying guide information 252
- 7.3 Cautions on integrated scope 254

8 System Operation Using JP1/IM 258

- 8.1 Executing a command 259
 - 8.1.1 Executing a command by using Command Execution 259
 - 8.1.2 Executing a command by using the Command button 261
 - 8.1.3 User that executes commands 263

- 8.1.4 Checking command execution status and deleting a command 263
- 8.2 Executing automated actions and taking necessary steps 265
- 8.2.1 Checking the execution status of an automated action 265
- 8.2.2 Checking the execution results of automated actions 266
- 8.2.3 Checking the operating status of the automated action function 271
- 8.3 Opening other application windows from the Tool Launcher 273
- 8.3.1 Operations in the Tool Launcher window 273
- 8.3.2 Functions that can be operated from the Tool Launcher window 274

9 Managing the System Hierarchy Using IM Configuration Management 277

- 9.1 Managing hosts 278
- 9.2 Managing the system hierarchy 279
- 9.3 Managing the configuration of a virtual system 280
- 9.3.1 Registering a virtual system host 280
- 9.3.2 Displaying host information in a virtual system 280
- 9.3.3 Applying the management information to the Central Scope monitoring tree 280
- 9.4 Managing business groups 282
- 9.5 Managing profiles 283
- 9.6 Managing service operation status 284
- 9.6.1 Collecting service operation information 284
- 9.6.2 Service operation information display 285
- 9.7 Exporting and importing management information of IM Configuration Management 286
- 9.7.1 Exporting management information of IM Configuration Management 286
- 9.7.2 Importing management information of IM Configuration Management 290
- 9.7.3 Applying the imported management information of IM Configuration Management to a system 300
- 9.8 Cautions on the IM configuration 303

10 Starting and Stopping JP1/IM - Agent 304

- 10.1 Service of JP1/IM - Agent 305
- 10.2 Starting the Service 307
- 10.3 Stopping the service 308
- 10.4 Optional Functions in JP1/IM - Agent 309
- 10.4.1 Servicing OracleDB exporter 309
- 10.4.2 Servicing Node exporter for AIX 310
- 10.5 When operating in a cluster system 317
- 10.5.1 Starting the Service 317
- 10.5.2 Stopping the service 317
- 10.5.3 Settings of auto start 317
- 10.5.4 Auto-Stop at OS Shutdown 317

Part 3: Linking with Other Products

11	Linking with BJEX or JP1/AS	318
11.1	Overview of BJEX and JP1/AS linkage	319
11.1.1	System configuration when linking JP1/IM with a batch job execution system	319
11.2	JP1/IM functionality for BJEX and JP1/AS linkage	322
11.2.1	Handling response-waiting events in JP1/IM	322
11.2.2	Monitoring response-waiting events	324
11.2.3	Accumulation of response-waiting events	327
11.2.4	Responding to response-waiting events	328
11.2.5	Canceling response-waiting events	330
11.3	Configuring JP1/IM to link with BJEX and JP1/AS	332
11.3.1	Configuring JP1/IM - Manager	332
11.3.2	Configuring JP1/IM - View	333
11.3.3	Configuring JP1/Base	334
11.3.4	Communication settings between BJEX or JP1/AS and JP1/IM - Manager	334
11.3.5	Configuring BJEX or JP1/AS	335
11.4	Working with response-waiting events	336
11.4.1	Flow of tasks for responding to response-waiting events	336
11.4.2	Responding to response-waiting events	339
11.4.3	Manually releasing response-waiting events from the hold-and-accumulate state	339
11.4.4	Resuming monitoring of events in the hold-and-accumulate state	340
11.5	Command usage when linking with BJEX or JP1/AS	341
11.5.1	jcoimdef	341
11.5.2	jim_log.bat (Windows only)	341
11.5.3	jim_log.sh (UNIX only)	342

Part 4: Troubleshooting

12	Troubleshooting	343
12.1	Troubleshooting procedure	344
12.2	Log information types	345
12.2.1	JP1/IM - Manager log information	345
12.2.2	JP1/IM - Agent log information	385
12.3	Data that needs to be collected when a problem occurs	391
12.3.1	Information about JP1/IM - Manager	391
12.3.2	Data about JP1/IM - Agent	420
12.4	Collecting data	421
12.4.1	How to collect JP1/IM - Manager data	421
12.4.2	How to collect JP1/IM - Agent data	432
12.5	Troubleshooting	442
12.5.1	How to isolate faults	442

- 12.5.2 What happens and how to recover from major input errors 475
- 12.5.3 Dealing with common problems 477
- 12.5.4 Actions to take when the JP1/IM - Agent cannot connect to the JP1/IM - Manager 553

Index 555

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. It cannot be used for server-to-server replication and file migration.

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 JP1/IM - Manager backups and recoveries

(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*.

In addition, backing up and recovering JP1/IM - Agent product plugin follows JP1/IM - Manager backup and recovery.

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* and replace *Manager-path* with *shared-folder\JP1IMM*.

Table 1–1: JP1/IM files to back up

Product name	File name	Description
Common to all products	Backup files created in 7.3.4 Copying the common definition information during new installation of JP1/IM - Manager (for Windows) in the JP1/Integrated Management 3 - Manager Configuration Guide	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:</p>

Product name	File name	Description	
		JP1_DEFAULT\JP1BASE\SSL\CACERTIFICATEFILE#2	
JP1/IM - Manager	Intelligent Integrated Management Base	<i>Manager-path</i> \conf\imdd\imdd.properties	Intelligent Integrated Management Base definition file
		<i>Manager-path</i> \conf\imdd\systemnode.conf	System node definition file
		<i>Manager-path</i> \conf\imdd\category_name.conf	Category name definition file for IM management nodes
		<i>Manager-path</i> \conf\imdd\target_host.conf	Target host definition file for configuration collection
		<i>Manager-path</i> \conf\imdd\imdd_host_name.conf	Host name definition file
		<i>Manager-path</i> \conf\imdd\imdd_nodeLink_def.conf	IM management node link definition file
		<i>Manager-path</i> \conf\imdd\imdd_sso_mapping.properties	Single sign-on mapping definition file
		<i>Manager-path</i> \conf\imdd\plugin\jplajs*.conf	Plug-in definition file for JP1/AJS
		<i>Manager-path</i> \conf\imdd\plugin\jplpfm*.conf	Plug-in definition file for JP1/PFM
		<i>Manager-path</i> \data\imdd\eventForward\imdd_event-forwarding-relay-source-host-name_jbsrt.dat	Event-forwarding relay source IM configuration information file
		<i>Manager-path</i> \data\imdd\eventForward\imdd_event-forwarding-relay-source-host-name_alconfig.dat	Event-forwarding relay source remote monitoring information file
		<i>Manager-path</i> \conf\imdd\user-created-plug-ins	User-created plug-ins
		<i>Manager-path</i> \public\customUI\user-created-folders-for-custom-UIs	Storage folder for custom UI files
		<i>Manager-path</i> \conf\imdd\suggestion\template\en\imdd_suggestion_a js_check_failed_agent_jobnet_en.conf	English suggestion template files for JP1/AJS
		<i>Manager-path</i> \conf\imdd\suggestion\template\en\imdd_suggestion_a js_check_failed_agent_list_en.conf	
		<i>Manager-path</i> \conf\imdd\suggestion\template\en\imdd_suggestion_p fm_cpu_event_en.conf	English suggestion template files for JP1/PFM
<i>Manager-path</i> \conf\imdd\suggestion\template\en\imdd_suggestion_p fm_set_status_of_events_to_processed_en.conf			
<i>Manager-path</i> \conf\imdd\suggestion\template\en\imdd_suggestion_p fm_suspend_monitoring_en.conf			

Product name	File name	Description
	<i>Manager-path</i> \conf\imdd\suggestion\template\ja\imdd_suggestion_a js_check_failed_agent_jobnet_ja.conf	Japanese suggestion template files for JP1/AJS
	<i>Manager-path</i> \conf\imdd\suggestion\template\ja\imdd_suggestion_a js_check_failed_agent_list_ja.conf	
	<i>Manager-path</i> \conf\imdd\suggestion\template\ja\imdd_suggestion_p fm_cpu_event_ja.conf	Japanese suggestion template files for JP1/PFM
	<i>Manager-path</i> \conf\imdd\suggestion\template\ja\imdd_suggestion_p fm_set_status_of_events_to_processed_ja.conf	
	<i>Manager-path</i> \conf\imdd\suggestion\template\ja\imdd_suggestion_p fm_suspend_monitoring_ja.conf	
	<i>any-path</i> \suggestion-definition-files	Suggestion definition file
	<i>Manager-path</i> \conf\imdd\responseaction\autoactconf.json	Auto response Action definition file
	<i>Manager-path</i> \conf\imdd\responseaction\responseactionnotice.conf	Response Action state monitoring definition file
Central Console	<i>Console-path</i> \conf\jp1co_env.conf	IM environment definition file
	<i>Console-path</i> \conf\jp1co_param.conf	IM parameter definition file
	<i>Console-path</i> \conf\jp1co_param_V7.conf	IM parameter definition file
	<i>Console-path</i> \conf\jp1co_service.conf	Extended startup process definition file
	<i>Console-path</i> \conf\jp1co_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

Product name	File name	Description
	<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_JP1-user-name	JP1/IM - View user profile
	<i>Console-path</i> \conf\console\profile\systemColor.conf	System color definition file
	<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

Product name	File name	Description
	<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</i> .conf	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
	<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
	<i>Console-path</i> \conf\console\performance\performance.conf	Performance report display definition file
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

Product name	File name	Description
	<i>user-selected-folder\user-selected-file-name</i>	Definition file for monitoring object initialization mode
	<i>Scope-path\conf\auto_dbbackup_on.conf</i>	Backup recovery settings file for monitored object database
	<i>Scope-path\conf\auto_dbbackup_off.conf</i>	
	<i>Scope-path\conf\evhist_warn_event_on.conf</i>	Settings file for the maximum number of status change events
	<i>Scope-path\conf\evhist_warn_event_off.conf</i>	
	<i>user-selected-folder\user-selected-file-name</i>	Guide message file
	<i>user-selected-folder\user-selected-file-name</i>	Definition file for on memory mode of status change condition
IM Configuration Management	<i>Manager-path\conf\imcf\jplcf_applyconfig.conf</i>	Apply-IM-configuration-method definition file
	<i>Manager-path\conf\imcf\jplcf_treedefaultpolicy.csv</i>	Default monitoring policy definition file
	<i>Manager-path\conf\agtless\targets\wmi.ini</i>	Definition files regarding WMI authentication information
	<i>Manager-path\conf\agtless\targets\ssh.ini</i>	Definition files regarding SSH authentication information
JP1/IM - Agent product plugin	<i>Manager-path\conf\imdd\plugin\jplpccs\aws_settings.conf</i>	AWS definition file
	<i>Manager-path\conf\imdd\plugin\jplpccs\property_labels.conf</i>	Property displayed character column definition file
	<i>Manager-path\conf\imdd\plugin\jplpccs\metrics_node_exporter.conf</i>	Node exporter metric definition file
	<i>Manager-path\conf\imdd\plugin\jplpccs\metrics_windows_exporter.conf</i>	Windows exporter metric definition file
	<i>Manager-path\conf\imdd\plugin\jplpccs\metrics_windows_exporter_process.conf</i>	Windows exporter (process monitoring) metric definition file
	<i>Manager-path\conf\imdd\plugin\jplpccs\metrics_blackbox_exporter.conf</i>	Blackbox exporter metric definition file
	<i>Manager-path\conf\imdd\plugin\jplpccs\metrics_ya_cloudwatch_exporter.conf</i>	Yet another cloudwatch exporter metric definition file
	<i>Manager-path\conf\imdd\plugin\jplpccs\metrics_kubernetes.conf</i>	Container monitoring metric definition file
	<i>Manager-path\conf\imdd\plugin\jplpccs\metrics_fluentd.conf</i>	Fluentd metric definition file

Product name	File name	Description
	<i>Manager-path</i> \conf\imdd\plugin\jplpccs\metrics_ <i>Any-Prometheus-trend-name</i> .conf	User-specific metric definition file
	<i>Manager-path</i> \conf\imdd\plugin\jplpccs\metrics_process_exporter.conf	Process exporter metric definition file
	<i>Manager-path</i> \conf\imdd\plugin\jplpccs\metrics_promitor.conf	Promitor metric definition file
	<i>Manager-path</i> \conf\imdd\plugin\jplpccs\metrics_script_exporter.conf	Script exporter metric definition file
	<i>Manager-path</i> \conf\imdd\plugin\jplpccs\metrics_web_exporter.conf	Web exporter metric definition file
	<i>Manager-path</i> \conf\imdd\plugin\jplpccs\metrics_vmware_exporter_host.conf	VMware exporter metric definition file for host
	<i>Manager-path</i> \conf\imdd\plugin\jplpccs\metrics_vmware_exporter_vm.conf	VMware exporter metric definition file for VM
	<i>Manager-path</i> \conf\imdd\plugin\jplpccs\user\metrics_ <i>Any-Prometheus-trend-name</i> .conf	User-specific metric definition file
	<i>Manager-path</i> \conf\imdd\imagent\jpc_imbase.json	imbase configuration file
	<i>Manager-path</i> \conf\imdd\imagent\jpc_imbaseproxy.json	imbaseproxy configuration file
	<i>Manager-path</i> \conf\imdd\imagent\server-certificate-file	Server certificate file for JP1/IM agent management base
	<i>Manager-path</i> \conf\imdd\imagent\server-certificate-key-file	Server certificate key file for JP1/IM agent management base
JP1/IM - View	<i>View-path</i> \conf\webdata\en*.html <i>View-path</i> \conf\webdata\ja*.html <i>View-path</i> \conf\webdata\zh*.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 <i>View-path</i> \conf\sovtoolexec\ja\!JP1_CS_APP0.conf <i>View-path</i> \conf\sovtoolexec\zh\!JP1_CS_APP0.conf	Start program definition file
	<i>View-path</i> \conf\sovtoolitem\en\!JP1_CS_FTOOL0.conf <i>View-path</i> \conf\sovtoolitem\ja\!JP1_CS_FTOOL0.conf <i>View-path</i> \conf\sovtoolitem\zh\!JP1_CS_FTOOL0.conf	Toolbar definition file

Product name	File name	Description
	<i>View-path</i> \conf\sovtoolitem\en\!JP1_CS_FTREE0.conf <i>View-path</i> \conf\sovtoolitem\ja\!JP1_CS_FTREE0.conf <i>View-path</i> \conf\sovtoolitem\zh\!JP1_CS_FTREE0.conf	Icon operation definition file
	<i>View-path</i> \conf\appexecute\en*.conf <i>View-path</i> \conf\appexecute\ja*.conf <i>View-path</i> \conf\appexecute\zh*.conf	Definition file for executing applications
	<i>View-path</i> \conf\function\en*.conf <i>View-path</i> \conf\function\ja*.conf <i>View-path</i> \conf\function\zh*.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\sovsystem\en\system.conf	System profile of the Central Scope viewer
	<i>View-path</i> \conf\sovsystem\ja\system.conf	
	<i>View-path</i> \conf\sovsystem\zh\system.conf	

#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 7.1.3(5) *Setting common definition information* in the *JP1/Integrated Management 3 - 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.

(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.

(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*.

In addition, backing up and recovering JP1/IM - Agent product plugin follows JP1/IM - Manager backup and recovery.

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 `/var/opt` and `/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 8.3.4 <i>Copying the common definition information during new installation of JP1/IM - Manager (for UNIX) in the JP1/Integrated Management 3 - 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

1. JP1/IM System Maintenance

Product name		File name	Description
			<p>Server certificate used by the communication encryption function</p> <p>File specified for the following common definition information: JP1_DEFAULT\JP1BASE\SSL\CERTIFICATEFILE#2</p>
			<p>Root certificate used by the communication encryption function</p> <p>File specified for the following common definition information: JP1_DEFAULT\JP1BASE\SSL\CACERTIFICATEFILE#2</p>
JP1/IM - Manager	Intelligent Integrated Management Base	/etc/opt/jplimm/conf/imdd/imdd.properties	Intelligent Integrated Management Base definition file
		/etc/opt/jplimm/conf/imdd/imdd_systemnode.conf	System node definition file
		/etc/opt/jplimm/conf/imdd/imdd_category_name.conf	Category name definition file for IM management nodes
		/etc/opt/jplimm/conf/imdd/imdd_target_host.conf	Target host definition file for configuration collection
		/etc/opt/jplimm/conf/imdd/imdd_host_name.conf	Host name definition file
		/etc/opt/jplimm/conf/imdd/imdd_nodeLink_def.conf	IM management node link definition file
		/etc/opt/jplimm/conf/imdd/imdd_sso_mapping.properties	Single sign-on mapping definition file
		/etc/opt/jplimm/conf/imdd/plugin/jplajs/*.conf	Plug-in definition file for JP1/AJS
		/etc/opt/jplimm/conf/imdd/plugin/jplpfm/*.conf	Plug-in definition file for JP1/PFM
		/var/opt/jplimm/data/imdd/eventForward/imdd_event-forwarding-relay-source-host-name_jbsrt.dat	Event-forwarding relay source IM configuration information file
		/var/opt/jplimm/data/imdd/eventForward/imdd_event-forwarding-relay-source-host-name_alconfig.dat	Event-forwarding relay source remote monitoring information file
		/etc/opt/jplimm/plugin/imdd/user-created-plug-ins	User-created plug-ins
		/opt/jplimm/public/custumUI/user-created-folders-for-custom-UIs	Storage folder for custom UI files
		/etc/opt/jplimm/conf/imdd/suggestion/template/en/imdd_suggestion_ajs_check_failed_agent_jobnet_en.conf	English suggestion template files for JP1/AJS
/etc/opt/jplimm/conf/imdd/suggestion/template/en/			

Product name	File name	Description
	imdd_suggestion_ajs_check_failed_agent_list_en.conf	
	/etc/opt/jplimm/conf/imdd/suggestion/template/en/ imdd_suggestion_pfm_cpu_event_en.conf	English suggestion template files for JP1/PFM
	/etc/opt/jplimm/conf/imdd/suggestion/template/en/ imdd_suggestion_pfm_set_status_of_events_to_processed_en.conf	
	/etc/opt/jplimm/conf/imdd/suggestion/template/en/ imdd_suggestion_pfm_suspend_monitoring_en.conf	
	/etc/opt/jplimm/conf/imdd/suggestion/template/ja/ imdd_suggestion_ajs_check_failed_agent_jobnet_ja.conf	Japanese suggestion template files for JP1/AJS
	/etc/opt/jplimm/conf/imdd/suggestion/template/ja/ imdd_suggestion_ajs_check_failed_agent_list_ja.conf	
	/etc/opt/jplimm/conf/imdd/suggestion/template/ja/ imdd_suggestion_pfm_cpu_event_ja.conf	Japanese suggestion template files for JP1/PFM
	/etc/opt/jplimm/conf/imdd/suggestion/template/ja/ imdd_suggestion_pfm_set_status_of_events_to_processed_ja.conf	
	/etc/opt/jplimm/conf/imdd/suggestion/template/ja/ imdd_suggestion_pfm_suspend_monitoring_ja.conf	
	<i>any-path/suggestion-definition-files</i>	Suggestion definition file
	/etc/opt/jplimm/conf/imdd/responseaction/autoactconf.json	Auto response Action definition file
	/etc/opt/jplimm/conf/imdd/responseaction/responseactionnotice.conf	Response Action state monitoring definition file
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

Product name	File name	Description
	/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
	/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
	/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

Product name	File name	Description
	/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
	/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
	/etc/opt/jplcons/conf/console/performance/performance.conf	Performance report display definition file
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

Product name	File name	Description
	/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
	/etc/opt/jplimm/conf/ imcf/jplcf_treedefaultpolicy.csv	Default monitoring policy definition file
	All files under /var/opt/jplimm/data/imcf/	System management information
	/etc/opt/jplimm/conf/agtless/targets/ssh.ini	Definition files regarding SSH authentication information
JP1/IM - Agent product plugin	/opt/jplimm/conf/imdd/plugin/ jplpccs/aws_settings.conf	AWS definition file
	/opt/jplimm/conf/imdd/plugin/ jplpccs/property_labels.conf	Property displayed character column definition file
	/opt/jplimm/conf/imdd/plugin/ jplpccs/metrics_node_exporter.conf	Node exporter metric definition file
	/opt/jplimm/conf/imdd/plugin/ jplpccs/metrics_windows_exporter.conf	Windows exporter metric definition file
	/opt/jplimm/conf/imdd/plugin/jplpccs/ metrics_windows_exporter_process.conf	Windows exporter (process monitoring) metric definition file
	/opt/jplimm/conf/imdd/plugin/ jplpccs/metrics_blackbox_exporter.conf	Blackbox exporter metric definition file
	/opt/jplimm/conf/imdd/plugin/ jplpccs/metrics_ya_cloudwatch_exporter.conf	Yet another cloudwatch exporter metric definition file
	/opt/jplimm/conf/imdd/plugin/ jplpccs/metrics_kubernetes.conf	Container monitoring metric definition file
	/opt/jplimm/conf/imdd/plugin/ jplpccs/metrics_fluentd.conf	Fluentd metric definition file
	/opt/jplimm/conf/imdd/plugin/ jplpccs/metrics_Any-Prometheus-trend-name.conf	User-specific metric definition file
	/opt/jplimm/conf/imdd/plugin/ jplpccs/metrics_process_exporter.conf	Process exporter metric definition file
	/opt/jplimm/conf/imdd/plugin/ jplpccs/metrics_promitor.conf	Promitor metric definition file
	/opt/jplimm/conf/imdd/plugin/ jplpccs/metrics_script_exporter.conf	Script exporter metric definition file
	/etc/opt/jplimm/conf/imdd/plugin/ jplpccs/metrics_vmware_exporter_host.conf	VMware exporter metric definition file for host

Product name	File name	Description
	/etc/opt/jplimm/conf/imdd/plugin/jplpccs/metrics_vmware_exporter_vm.conf	VMware exporter metric definition file for VM
	/opt/jplimm/conf/imdd/plugin/jplpccs/user/metrics_ <i>Any-Prometheus-trend-name</i> .conf	User-specific metric definition file
	/opt/jplimm/conf/imdd/imagent/jplpccs/jpc_imbase.json	imbase configuration file
	/opt/jplimm/conf/imdd/imagent/jpc_imbaseproxy.json	imbaseproxy configuration file
	/opt/jplimm/conf/imdd/imagent/ <i>server-certificate-file</i>	Server certificate file for JP1/IM agent management base
	/opt/jplimm/conf/imdd/imagent/ <i>server-certificate-key-file</i>	Server certificate key file for JP1/IM agent management base

#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 7.1.3(5) *Setting common definition information* in the *JP1/Integrated Management 3 - 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) 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.

1.1.2 Backing Up and Recovering of JP1/IM - Agent

(1) Backup

Back up JP1/IM - Agent if the settings have been changed. Backup can be performed even during operation.

(a) Normal host

1. Back up JP1/IM - Agent files to be backed up.

Back up the files to be backed up in the corresponding OS in "1.1.2(3) File to be backed up" table.

2. If you want to save Alertmanager's silence settings, back up by acquiring silence with REST API.
For details about REST API for obtaining silence, see *Get silence of Alertmanager* in *Chapter 5. API* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

(b) Cluster environment

This is the same as the procedure in *1.1.2(1)(a) Normal host*.

However, note the following:

- Make a backup of both the running server and the standby server.
- The shared directory must also be backed up.

(c) Container environment

Back up Docker image and Podman image.

(d) Backing up optional functions

Back up your JP1/IM-Agent and JP1/IM-Manager separately.

■ OracleDB exporter

Back up the following files:

For Windows

- Service definition file of OracleDB exporter
*OracleDB-exporter-location\oracledb_exporter_windows\jplima\bin\oracledb_exporter_*_service.xml*
1

For Linux

- Unit definition file of OracleDB exporter
/usr/lib/systemd/system/oracledb_exporter_.service*

■ Node exporter for AIX

There are no files to back up.

(2) Recovery

(a) Normal host

■ For Windows

1. Prepare a machine with the same hostname and IP address as the backup definition file.
2. Install the same version of JP1/IM - Agent as the backup definition file.
3. Overwrites the backup definition file to the installation destination.
Update the certificate used for communication encryption if necessary.
4. If the service to be used was already registered, register it to Windows service again.

To register the service again, you must disable and re-enable the service registration.

For details on how to enable or disable add-on program service registration, see *1.21.1(1) Enable or disable add-on program* in the *JP1/Integrated Management 3 - Manager Configuration Guide*.

5. Start the service.

6. Register silence settings for Alertmanager.

Use API for silence creation in Alertmanager. For details, see *5.21.4 Silence creation of Alertmanager* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

Note that you cannot create a silence that has expired.

■ For Linux

1. Prepare a machine with the same hostname and IP address as the backup definition file.

2. Install the same version of JP1/IM - Agent as the backup definition file.

3. Overwrite the backup definition file to the install destination and `"/usr/lib/systemd/system"`.

4. Run the following command.

```
# systemctl daemon-reload
```

5. Start the service.

6. Register silence settings for Alertmanager.

Use API for silence creation in Alertmanager. For details, see *5.21.4 Silence creation of Alertmanager* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

Note that you cannot create a silence that has expired.

(b) Cluster environment

■ For Windows

1. Prepare a machine with the same hostname and IP address as the backup definition file.

Prepare both the running server and the standby server.

2. Install the same version of JP1/IM - Agent as the backup definition file.

This command is executed on both the running server and the standby server.

3. Build a logical host with the same logical host name as the backup.

4. Overwrites the backup definition file to the installation destination and shared directory.

This command is executed on both the running server and the standby server.

5. If the service to be used was already registered, register it to Windows service again.

To register the service again, you must disable and re-enable the service registration.

This command is executed on both the running server and the standby server.

6. Register services for JP1/IM - Agent logical hosts in the cluster software.

For details on registering JP1/IM - Agent service to the cluster software, see *7.5 Registering into the cluster software during new installation and setup (for Windows)* in the *JP1/Integrated Management 3 - Manager Configuration Guide*.

7. Start JP1/IM - Agent from the cluster software.
8. Register silence settings for Alertmanager.
Use API for silence creation in Alertmanager.
Note that you cannot create a silence that has expired.

■ For Linux

1. Prepare a machine with the same hostname and IP address as the backup definition file.
Prepare both the running server and the standby server.
2. Install the same version of JP1/IM - Agent as the backup definition file.
Prepare both the running server and the standby server.
3. Overwrites the backup definition files to the install destination,
4. `"/usr/lib/systemd/system"`, and shared directories.
5. Run the following command.

```
# systemctl daemon-reload
```

6. Start the service.
7. Register silence settings for Alertmanager.
Use API for silence creation in Alertmanager.
Note that you cannot create a silence that has expired.

(c) Container environment

Recover from a backup Docker image or Podman image.

(d) Optional Function Recovery

■ OracleDB exporter

For Windows

1. You install OracleDB exporter.
2. Add a OracleDB exporter target.
When you add a target, you use the backed-up service definition file as a step in creating service definition file.

For Linux

1. You install OracleDB exporter.
2. Add a OracleDB exporter target.
When you add a target, you use the backed-up service definition file as a step in creating unit definition file.

■ Node exporter for AIX

Monitored AIX hosts

1. You install Node exporter for AIX.
For information about installing Node exporter for AIX, see *1.23.2 (2) Installing Node exporter for AIX* in the *JP1/Integrated Management 3 - Manager Configuration Guide*.

2. If you need to change the port number of Node exporter for AIX, change the port number.

For details on changing the port number of Node exporter for AIX, see *1.23.2(4)(b) Changing the port on Node exporter for AIX (optional)* in the *JP1/Integrated Management 3 - Manager Configuration Guide*.

(3) File to be backed up

(a) For Windows

Table 1–3: Files to be backed up on the physical hosts of JP1/IM - Agent (Windows)

File name	Description
<i>Agent-path</i> \conf\jpc_imagentcommon.json	imagent common configuration file
<i>Agent-path</i> \conf\jpc_imagent.json	imagent configuration file
<i>Agent-path</i> \conf\jpc_imagentproxy.json	imagentproxy configuration file
<i>Agent-path</i> \conf\jpc_imagentaction.json	imagentaction configuration file
<i>Agent-path</i> \conf\jpc_alertmanager.yml	Alertmanager configuration file
<i>Agent-path</i> \conf\jpc_prometheus_server.yml	Prometheus configuration file
<i>Agent-path</i> \conf\jpc_alerting_rules.yml	Alert configuration file
<i>Agent-path</i> \conf\jpc_file_sd_config_windows.yml	Windows exporter discovery configuration file
<i>Agent-path</i> \conf\jpc_file_sd_config_blackbox_http.yml	Blackbox exporter (HTTP/HTTPS monitoring) discovery configuration file
<i>Agent-path</i> \conf\jpc_file_sd_config_blackbox_icmp.yml	Blackbox exporter (ICMP monitoring) discovery configuration file
<i>Agent-path</i> \conf\user\file_sd_config_blackbox_any-name.yml	Blackbox exporter Monitored target (User-Defined) Discovery configuration file
<i>Agent-path</i> \conf\jpc_file_sd_config_cloudwatch.yml	Yet another cloudwatch exporter discovery configuration file
<i>Agent-path</i> \conf\user\file_sd_config_any-name.yml	User-specific discovery configuration file
<i>Agent-path</i> \conf\jpc_file_sd_config_process.yml	Process exporter discovery configuration file
<i>Agent-path</i> \conf\jpc_file_sd_config_promitor.yml	Promitor discovery configuration file
<i>Agent-path</i> \conf\jpc_file_sd_config_web.yml	Web exporter discovery configuration file
<i>Agent-path</i> \conf\jpc_file_sd_config_vmware.yml	VMware exporter discovery configuration file
<i>Agent-path</i> \conf\jpc_file_sd_config_script.yml	Script exporter discovery configuration file
<i>Agent-path</i> \conf\jpc_windows_exporter.yml	Windows exporter configuration file
<i>Agent-path</i> \conf\jpc_blackbox_exporter.yml	Blackbox exporter configuration file
<i>Agent-path</i> \conf\jpc_ya_cloudwatch_exporter.yml	Yet another cloudwatch exporter configuration file
<i>Agent-path</i> \conf\jpc_script_exporter.yml	Script exporter configuration file
<i>Agent-path</i> \conf\jpc_web_exporter.yml	Web exporter configuration file
<i>Agent-path</i> \conf\jpc_playwright.config.ts	Playwright configuration file
<i>Agent-path</i> \conf\jpc_vmware_exporter.yml	VMware exporter configuration file
<i>Agent-path</i> \conf\jpc_fluentd_common.conf	Log monitoring common definition file

File name	Description
<i>Agent-path</i> \conf\jpc_fluentd_common_list.conf	Log Monitor Target Definition File
<i>Agent-path</i> \conf\jpc_fluentd_common_wevt_rendered.conf	Rendering information acquisition definition file
<i>Agent-path</i> \conf\fluentd_@@trapname@@_tail.conf.template	Text-formatted log file monitoring definition file Templates
<i>Agent-path</i> \conf\fluentd_@@trapname@@_wevt.conf.template	Windows event-log monitoring definition file Templates
<i>Agent-path</i> \conf\user\fluentd_log-monitor-name_tail.conf	Text-formatted log file monitoring definition file
<i>Agent-path</i> \conf\user\fluentd_log-monitor-name_wevt.conf	Windows event-log monitoring definition file
<i>Agent-path</i> \conf\user\fluentd_any-name_logmetrics.conf	Log metrics definition file
<i>Agent-path</i> \conf\jpc_user_deffile_list.json	User-created-definition file list definition file
<i>Agent-path</i> \conf\promitor\scraper\metrics-declaration.yaml	Promitor Scraper configuration file
<i>Agent-path</i> \conf\promitor\scraper\runtime.yaml	Promitor Scraper runtime configuration file
<i>Agent-path</i> \conf\promitor\resource-discovery\resource-discovery-declaration.yaml	Promitor Resource Discovery configuration file
<i>Agent-path</i> \conf\promitor\resource-discovery\runtime.yaml	Promitor Resource Discovery runtime configuration file
<i>Agent-path</i> \conf\user\cert\CA-certificate-file	CA certificate for Black exporter file
<i>Agent-path</i> \conf\user\cert\client-certificate-file	Client certificate for Black exporter file
<i>Agent-path</i> \conf\user\secret\client-certificate-key-file	Client certificate for Black exporter key file
<i>Agent-path</i> \conf\user\secret\password-file	Password for Black exporter file
<i>Agent-path</i> \conf\jpc_file_sd_config_off\jpc_file_sd_config_windows.yml	Windows exporter discovery configuration file
<i>Agent-path</i> \conf\jpc_file_sd_config_off\jpc_file_sd_config_blackbox_http.yml	Blackbox exporter (HTTP/HTTPS monitoring) discovery configuration file
<i>Agent-path</i> \conf\jpc_file_sd_config_off\jpc_file_sd_config_blackbox_icmp.yml	Blackbox exporter (ICMP monitoring) discovery configuration file
<i>Agent-path</i> \conf\jpc_file_sd_config_off\jpc_file_sd_config_cloudwatch.yml	Yet another cloudwatch exporter discovery configuration file
<i>Agent-path</i> \conf\jpc_file_sd_config_off\jpc_file_sd_config_promitor.yml	Promitor's discovery configuration file
<i>Agent-path</i> \conf\jpc_file_sd_config_off\jpc_file_sd_config_node_aix.yml	Node exporter for AIX discovery configuration file
<i>Agent-path</i> \conf\jpc_file_sd_config_off\jpc_file_sd_config_oracledb.yml	OracleDB exporter discovery configuration file

File name	Description
<i>Agent-path</i> \conf\jpc_file_sd_config_off\jpc_file_sd_config_web.yml	Web exporter discovery configuration file
<i>Agent-path</i> \conf\jpc_file_sd_config_off\jpc_file_sd_config_vmware.yml	VMware exporter discovery configuration file
<i>Agent-path</i> \bin\jpc_imagent_service.xml	Service of imagent definition file
<i>Agent-path</i> \bin\jpc_imagent_service_logical-host-name.xml	Service of imagent for Logical Hosts definition file
<i>Agent-path</i> \bin\jpc_imagentproxy_service.xml	Service of imagentproxy definition file
<i>Agent-path</i> \bin\jpc_imagentproxy_service_logical-host-name.xml	Service of imagentproxy for Logical Hosts definition file
<i>Agent-path</i> \bin\jpc_imagentaction_service.xml	Service of imagentaction definition file
<i>Agent-path</i> \bin\jpc_imagentaction_service_logical-host-name.xml	Service of imagentaction for Logical Hosts definition file
<i>Agent-path</i> \bin\jpc_alertmanager_service.xml	Service of Alertmanager definition file
<i>Agent-path</i> \bin\jpc_alertmanager_service_logical-host-name.xml	Service of Alertmanager for Logical Hosts definition file
<i>Agent-path</i> \bin\jpc_prometheus_server_service.xml	Service of Prometheus server definition file
<i>Agent-path</i> \bin\jpc_prometheus_server_service_logical-host-name.xml	Service of Prometheus server for Logical Hosts definition file
<i>Agent-path</i> \bin\jpc_windows_exporter_service.xml	Service of Windows exporter definition file
<i>Agent-path</i> \bin\jpc_windows_exporter_service_logical-host-name.xml	Service of Windows exporter for Logical Hosts definition file
<i>Agent-path</i> \bin\jpc_blackbox_exporter_service.xml	Service of Blackbox exporter definition file
<i>Agent-path</i> \bin\jpc_blackbox_exporter_service_logical-host-name.xml	Service of Blackbox exporter for Logical Hosts definition file
<i>Agent-path</i> \bin\jpc_ya_cloudwatch_exporter_service.xml	Service of Yet another cloudwatch exporter definition file
<i>Agent-path</i> \bin\jpc_ya_cloudwatch_exporter_service_logical-host-name.xml	Service of Yet another cloudwatch exporter for Logical Hosts definition file
<i>Agent-path</i> \bin\jpc_promitor_scraper_service.xml	Service of Promitor Scraper definition file
<i>Agent-path</i> \bin\jpc_promitor_scraper_service_logical-host-name.xml	Service of Promitor Scraper for Logical Hosts definition file
<i>Agent-path</i> \bin\jpc_promitor_resource_discovery_service.xml	Service of Promitor Resource Discovery definition file
<i>Agent-path</i> \bin\jpc_promitor_resource_discovery_service_logical-host-name.xml	Service of Promitor Resource Discovery for Logical Hosts definition file
<i>Agent-path</i> \bin\jpc_script_exporter_service.xml	Service of Script exporter definition file
<i>Agent-path</i> \bin\jpc_script_exporter_service_logical-host-name.xml	Service of Script exporter for Logical Hosts definition file

File name	Description
<i>Agent-path</i> \bin\jpc_fluentd_service.xml	Service of Fluentd definition file
<i>Agent-path</i> \bin\jpc_fluentd_service_logical-host-name.xml	Service of Fluentd for Logical Hosts definition file

Table 1–4: Files to be backed up by logical hosts in the JP1/IM - Agent (Windows)

File name	Description
<i>Shared-folder</i> \jplima\conf\jpc_imagentcommon.json	imagent common configuration file
<i>Shared-folder</i> \jplima\conf\jpc_imagent.json	imagent configuration file
<i>Shared-folder</i> \jplima\conf\jpc_imagentproxy.json	imagentproxy configuration file
<i>Shared-folder</i> \jplima\conf\jpc_imagentaction.json	imagentaction configuration file
<i>Shared-folder</i> \jplima\conf\jpc_alertmanager.yml	Alertmanager configuration file
<i>Shared-folder</i> \jplima\conf\jpc_prometheus_server.yml	Prometheus configuration file
<i>Shared-folder</i> \jplima\conf\jpc_alerting_rules.yml	Alert configuration file
<i>Shared-folder</i> \jplima\conf\jpc_file_sd_config_windows.yml	Windows exporter discovery configuration file
<i>Shared-folder</i> \jplima\conf\jpc_file_sd_config_blackbox_http.yml	Blackbox exporter (HTTP/HTTPS monitoring) discovery configuration file
<i>Shared-folder</i> \jplima\conf\jpc_file_sd_config_blackbox_icmp.yml	Blackbox exporter (ICMP monitoring) discovery configuration file
<i>Shared-folder</i> \jplima\conf\user\file_sd_config_blackbox_any-name.yml	Blackbox exporter Monitored target (User-Defined) Discovery configuration file
<i>Shared-folder</i> \jplima\conf\jpc_file_sd_config_cloudwatch.yml	Yet another cloudwatch exporter discovery configuration file
<i>Shared-folder</i> \jplima\conf\user\file_sd_config_any-name.yml	User-specific discovery configuration file
<i>Shared-folder</i> \jplima\conf\jpc_file_sd_config_process.yml	Process exporter discovery configuration file
<i>Shared-folder</i> \jplima\conf\jpc_file_sd_config_web.yml	Web exporter discovery configuration file
<i>Shared-folder</i> \jplima\conf\jpc_file_sd_config_vmware.yml	VMware exporter discovery configuration file
<i>Shared-folder</i> \jplima\conf\jpc_file_sd_config_promitor.yml	Promitor discovery configuration file
<i>Shared-folder</i> \jplima\conf\jpc_windows_exporter.yml	Windows exporter configuration file
<i>Shared-folder</i> \jplima\conf\jpc_blackbox_exporter.yml	Blackbox exporter configuration file
<i>Shared-folder</i> \jplima\conf\jpc_ya_cloudwatch_exporter.yml	Yet another cloudwatch exporter configuration file
<i>Shared-folder</i> \jplima\conf\jpc_script_exporter.yml	Script exporter configuration file
<i>Shared-folder</i> \jplima\conf\jpc_web_exporter.yml	Web exporter configuration file
<i>Shared-folder</i> \jplima\conf\jpc_playwright.config.ts	Playwright configuration file

File name	Description
<i>Shared-folder</i> \jplima\conf\jpc_vmware_exporter.yml	VMware exporter configuration file
<i>Shared-folder</i> \jplima\conf\jpc_fluentd_common.conf	Log monitoring common definition file
<i>Shared-folder</i> \jplima\conf\jpc_fluentd_common_list.conf	Log Monitor Target Definition File
<i>Shared-folder</i> \jplima\conf\jpc_fluentd_common_wevt_rendered.conf	Rendering information acquisition definition file
<i>Shared-folder</i> \jplima\conf\fluentd_@@trapname@@_tail.conf.template	Text-formatted log file monitoring definition file Templates
<i>Shared-folder</i> \jplima\conf\fluentd_@@trapname@@_wevt.conf.template	Windows event-log monitoring definition file Templates
<i>Shared-folder</i> \jplima\conf\jpc_user_deffile_list.json	User-created-definition file list definition file
<i>Shared-folder</i> \jplima\conf\promitor\scraper\metrics-declaration.yaml	Promitor Scraper configuration file
<i>Shared-folder</i> \jplima\conf\promitor\scraper\runtime.yaml	Promitor Scraper runtime configuration file
<i>Shared-folder</i> \jplima\conf\promitor\resource-discovery\resource-discovery-declaration.yaml	Promitor Resource Discovery configuration file
<i>Shared-folder</i> \jplima\conf\promitor\resource-discovery\runtime.yaml	Promitor Resource Discovery runtime configuration file
<i>Shared-folder</i> \jplima\conf\user\cert\CA-certificate-file	CA certificate for Black exporter file
<i>Shared-folder</i> \jplima\conf\user\cert\client-certificate-file	Client certificate for Black exporter file
<i>Shared-folder</i> \jplima\conf\user\secret\client-certificate-key-file	Client certificate for Black exporter key file
<i>Shared-folder</i> \jplima\conf\user\secret\password-file	Password for Black exporter file
<i>Shared-folder</i> \jplima\conf\jpc_file_sd_config_off\jpc_file_sd_config_windows.yml	Windows exporter discovery configuration file
<i>Shared-folder</i> \jplima\conf\jpc_file_sd_config_off\jpc_file_sd_config_blackbox_http.yml	Blackbox exporter (HTTP/HTTPS monitoring) discovery configuration file
<i>Shared-folder</i> \jplima\conf\jpc_file_sd_config_off\jpc_file_sd_config_blackbox_icmp.yml	Blackbox exporter (ICMP monitoring) discovery configuration file
<i>Shared-folder</i> \jplima\conf\jpc_file_sd_config_off\jpc_file_sd_config_cloudwatch.yml	Yet another cloudwatch exporter discovery configuration file
<i>Shared-folder</i> \jplima\conf\jpc_file_sd_config_off\jpc_file_sd_config_promitor.yml	Promitor discovery configuration file
<i>Shared-folder</i> \jplima\conf\jpc_file_sd_config_off\jpc_file_sd_config_node_aix.yml	Node exporter for AIX discovery configuration file
<i>Shared-folder</i> \jplima\conf\jpc_file_sd_config_off\jpc_file_sd_config_oracledb.yml	OracleDB exporter discovery configuration file

File name	Description
<i>Shared-folder</i> \jplima\conf\jpc_file_sd_config_off\jpc_file_sd_config_web.yml	Web exporter discovery configuration file
<i>Shared-folder</i> \jplima\conf\jpc_file_sd_config_off\jpc_file_sd_config_vmware.yml	VMware exporter discovery configuration file

(b) For UNIX

Table 1–5: Files to be backed up on the physical hosts of the JP1/IM - Agent (UNIX)

File name	Description
/opt/jplima/conf/jpc_imagentcommon.json	imagent common configuration file
/opt/jplima/conf/jpc_imagent.json	imagent configuration file
/opt/jplima/conf/jpc_imagentproxy.json	imagentproxy configuration file
/opt/jplima/conf/jpc_imagentaction.json	imagentaction configuration file
/opt/jplima/conf/jpc_alertmanager.yml	Alertmanager configuration file
/opt/jplima/conf/jpc_prometheus_server.yml	Prometheus configuration file
/opt/jplima/conf/jpc_alerting_rules.yml	Alert configuration file
/opt/jplima/conf/jpc_file_sd_config_node.yml	Node exporter discovery configuration file
/opt/jplima/conf/jpc_file_sd_config_blackbox_http.yml	Blackbox exporter (HTTP/HTTPS monitoring) discovery configuration file
/opt/jplima/conf/jpc_file_sd_config_blackbox_icmp.yml	Blackbox exporter (ICMP monitoring) discovery configuration file
/opt/jplima/conf/jpc_file_sd_config_cloudwatch.yml	Yet another cloudwatch exporter discovery configuration file
/opt/jplima/conf/user/file_sd_config_blackbox_any-name.yml	Blackbox exporter Monitored target (User-Defined) Discovery configuration file
/opt/jplima/conf/user/file_sd_config_any-name.yml	User-specific discovery configuration file
/opt/jplima/conf/jpc_file_sd_config_process.yml	Process exporter discovery configuration file
/opt/jplima/conf/jpc_file_sd_config_promitor.yml	Promitor discovery configuration file
/opt/jplima/conf/jpc_file_sd_config_script.yml	Script exporter discovery configuration file
/opt/jplima/conf/jpc_file_sd_config_vmware.yml	VMware exporter discovery configuration file
/opt/jplima/conf/jpc_blackbox_exporter.yml	Blackbox exporter configuration file
/opt/jplima/conf/jpc_ya_cloudwatch_exporter.yml	Yet another cloudwatch exporter configuration file
/opt/jplima/conf/jpc_process_exporter.yml	Process exporter configuration file
/opt/jplima/conf/jpc_script_exporter.yml	Script exporter configuration file
/opt/jplima/conf/jpc_vmware_exporter.yml	VMware exporter configuration file
/opt/jplima/conf/jpc_fluentd_common.conf	Log monitoring common definition file
/opt/jplima/conf/jpc_fluentd_common_list.conf	Log Monitor Target Definition File
/opt/jplima/conf/fluentd_@@trapname@@_tail.conf.template	Text-formatted log file monitoring definition file Templates

File name	Description
/opt/jplima/conf/fluentsd_log-monitor-name_tail.conf	Text-formatted log file monitoring definition file
/opt/jplima/conf/user/fluentsd_any-name_logmetrics.conf	Log metrics definition file
/opt/jplima/conf/jpc_user_deffile_list.json	User-created-definition file list definition file
/opt/jplima/conf/promitor/scrapper/metrics-declaration.yaml	Promitor Scrapper configuration file
/opt/jplima/conf/promitor/scrapper/runtime.yaml	Promitor Scrapper runtime configuration file
/opt/jplima/conf/promitor/resource-discovery/resource-discovery-declaration.yaml	Promitor Resource Discovery configuration file
/opt/jplima/conf/promitor/resource-discovery/runtime.yaml	Promitor Resource Discovery runtime configuration file
/opt/jplima/conf/user/cert/CA-certificate-file	CA certificate for Black exporter file
/opt/jplima/conf/user/cert/client-certificate-file	Client certificate for Black exporter file
/opt/jplima/conf/user/secret/client-certificate-key-file	Client certificate for Black exporter key file
/opt/jplima/conf/user/secret/password-file	Password for Black exporter file
/opt/jplima/conf/jpc_file_sd_config_off/jpc_file_sd_config_node.yaml	Node exporter discovery configuration file
/opt/jplima/conf/jpc_file_sd_config_off/jpc_file_sd_config_blackbox_http.yaml	Blackbox exporter (HTTP/HTTPS monitoring) discovery configuration file
/opt/jplima/conf/jpc_file_sd_config_off/jpc_file_sd_config_blackbox_icmp.yaml	Blackbox exporter (ICMP monitoring) discovery configuration file
/opt/jplima/conf/jpc_file_sd_config_off/jpc_file_sd_config_cloudwatch.yaml	Yet another cloudwatch exporter discovery configuration file
/opt/jplima/conf/jpc_file_sd_config_off/jpc_file_sd_config_process.yaml	Process exporter discovery configuration file
/opt/jplima/conf/jpc_file_sd_config_off/jpc_file_sd_config_promitor.yaml	Promitor Process exporter discovery configuration file
/opt/jplima/conf/jpc_file_sd_config_off/jpc_file_sd_config_node_aix.yaml	Node exporter for AIX discovery configuration file
/opt/jplima/conf/jpc_file_sd_config_off/jpc_file_sd_config_oracledb.yaml	OracleDB exporter discovery configuration file
/opt/jplima/conf/jpc_file_sd_config_off/jpc_file_sd_config_windows.yaml	VMware exporter discovery configuration file
/usr/lib/systemd/system/jpc_imagentaction.service	Unit definition file of imagentaction
/usr/lib/systemd/system/jpc_alertmanager.service	Unit definition file of Alertmanager
/usr/lib/systemd/system/jpc_prometheus_server.service	Unit definition file of Prometheus server
/usr/lib/systemd/system/jpc_node_exporter.service	Unit definition file of Node exporter
/usr/lib/systemd/system/jpc_blackbox_exporter.service	Unit definition file of Blackbox exporter
/usr/lib/systemd/system/jpc_ya_cloudwatch_exporter.service	Unit definition file of Yet another cloudwatch exporter

File name	Description
/usr/lib/systemd/system/jpc_fluentd.service	Unit definition file of Fluentd
/usr/lib/systemd/system/jpc_imagent_logical-host-name.service	Unit definition file of imagent for Logical Hosts
/usr/lib/systemd/system/jpc_imagentproxy_logical-host-name.service	Unit definition file of imagentproxy for Logical Hosts
/usr/lib/systemd/system/jpc_imagentaction_logical-host-name.service	Unit definition file of imagentaction for Logical Hosts
/usr/lib/systemd/system/jpc_alertmanager_logical-host-name.service	Unit definition file of Alertmanager for Logical Hosts
/usr/lib/systemd/system/jpc_prometheus_server_logical-host-name.service	Unit definition file of Prometheus server for Logical Hosts
/usr/lib/systemd/system/jpc_node_exporter_logical-host-name.service	Unit definition file of Node exporter for Logical Hosts
/usr/lib/systemd/system/jpc_blackbox_exporter_logical-host-name.service	Unit definition file of Blackbox exporter for Logical Hosts
/usr/lib/systemd/system/jpc_ya_cloudwatch_exporter_logical-host-name.service	Unit definition file of Yet another cloudwatch exporter for Logical Hosts
/usr/lib/systemd/system/jpc_process_exporter_logical-host-name.service	Unit definition file of Process exporter for Logical Hosts
/usr/lib/systemd/system/jpc_promitor_scraper_logical-host-name.service	Unit definition file of Promitor Scraper for Logical Hosts
/usr/lib/systemd/system/jpc_promitor_resource_discovery_logical-host-name.service	Unit definition file of Promitor Resource Discovery for Logical Hosts
/usr/lib/systemd/system/jpc_script_exporter_logical-host-name.service	Unit definition file of Script exporter for Logical Hosts
/usr/lib/systemd/system/jpc_fluentd_logical-host-name.service	Unit definition file of Fluentd for Logical Hosts

Table 1–6: Files to be backed up by the logical host of the JP1/IM - Agent (UNIX)

File name	Description
Shared-directory/jplima/conf/jpc_imagentcommon.json	imagent common configuration file
Shared-directory/jplima/conf/jpc_imagent.json	imagent configuration file
Shared-directory/jplima/conf/jpc_imagentproxy.json	imagentproxy configuration file
Shared-directory/jplima/conf/jpc_imagentaction.json	imagentaction configuration file
Shared-directory/jplima/conf/jpc_alertmanager.yml	Alertmanager configuration file
Shared-directory/jplima/conf/jpc_prometheus_server.yml	Prometheus configuration file
Shared-directory/jplima/conf/jpc_alerting_rules.yml	Alert configuration file
Shared-directory/jplima/conf/jpc_file_sd_config_node.yml	Node exporter discovery configuration file

File name	Description
<i>Shared-directory/jplima/conf/jpc_file_sd_config_blackbox_http.yml</i>	Blackbox exporter (HTTP/HTTPS monitoring) discovery configuration file
<i>Shared-directory/jplima/conf/jpc_file_sd_config_blackbox_icmp.yml</i>	Blackbox exporter (ICMP monitoring) discovery configuration file
<i>Shared-directory/jplima/conf/user/file_sd_config_blackbox_any-name.yml</i>	Blackbox exporter Monitored target (User-Defined) Discovery configuration file
<i>Shared-directory/jplima/conf/jpc_file_sd_config_cloudwatch.yml</i>	Yet another cloudwatch exporter discovery configuration file
<i>Shared-directory/jplima/conf/user/file_sd_config_any name.yml</i>	User-specific discovery configuration file
<i>Shared-directory/jplima/conf/jpc_file_sd_config_process.yml</i>	Process exporter discovery configuration file
<i>Shared-directory/jplima/conf/jpc_file_sd_config_promitor.yml</i>	Promitor discovery configuration file
<i>Shared-directory/jplima/conf/jpc_blackbox_exporter.yml</i>	Blackbox exporter configuration file
<i>Shared-directory/jplima/conf/jpc_ya_cloudwatch_exporter.yml</i>	Yet another cloudwatch exporter configuration file
<i>Shared-directory/jplima/conf/jpc_process_exporter.yml</i>	Process exporter configuration file
<i>Shared-directory/jplima/conf/jpc_script_exporter.yml</i>	Script exporter configuration file
<i>Shared-directory/jplima/conf/jpc_fluentd_common.conf</i>	Log monitor common definition file
<i>Shared-directory/jplima/conf/jpc_fluentd_common_list.conf</i>	Log Monitor Target Definition File
<i>Shared-directory/jplima/conf/jpc_fluentd_common_wevt_rendered.conf</i>	Rendering information acquisition definition file
<i>Shared-directory/jplima/conf/fluentd_@@trapname@@_tail.conf.template</i>	Text-formatted log file monitoring definition file Templates
<i>Shared-directory/jplima/conf/fluentd_@@trapname@@_wevt.conf.template</i>	Windows event-log monitoring definition file Templates
<i>Shared-directory/jplima/conf/jpc_user_deffile_list.json</i>	User-created-definition file list definition file
<i>Shared-directory/jplima/conf/promitor\scraper\metrics-declaration.yml</i>	Promitor Scraper configuration file
<i>Shared-directory/jplima/conf/promitor\scraper\runtime.yml</i>	Promitor Scraper runtime configuration file
<i>Shared-directory/jplima/conf/promitor\resource-discovery\resource-discovery-declaration.yml</i>	Promitor Resource Discovery configuration file
<i>Shared-directory/jplima/conf/promitor\resource-discovery\runtime.yml</i>	Promitor Resource Discovery runtime configuration file
<i>Shared-directory/jplima/conf/user/cert/CA-certificate file</i>	CA certificate for Black exporter file
<i>Shared-directory/jplima/conf/user/cert/Client-Certificate-File</i>	Client certificate for Black exporter file
<i>Shared-directory/jplima/conf/user/secret/Client-Certificate-Key-File</i>	Client certificate for Black exporter key file
<i>Shared-directory/jplima/conf/user/secret/Password-File</i>	Password for Black exporter file

File name	Description
<i>Shared-directory</i> /jplima/conf/ jpc_file_sd_config_off/jpc_file_sd_config_node.yml	Node exporter discovery configuration file
<i>Shared-directory</i> /jplima/conf/jpc_file_sd_config_off/ jpc_file_sd_config_blackbox_http.yml	Blackbox exporter (HTTP/HTTPS monitoring) discovery configuration file
<i>Shared-directory</i> /jplima/conf/jpc_file_sd_config_off/ jpc_file_sd_config_blackbox_icmp.yml	Blackbox exporter (ICMP monitoring) discovery configuration file
<i>Shared-directory</i> /jplima/conf/jpc_file_sd_config_off/ jpc_file_sd_config_cloudwatch.yml	Yet another cloudwatch exporter discovery configuration file
<i>Shared-directory</i> /jplima/conf/jpc_file_sd_config_off/ jpc_file_sd_config_process.yml	Process exporter discovery configuration file
<i>Shared-directory</i> /jplima/conf/jpc_file_sd_config_off/ jpc_file_sd_config_promitor.yml	Promitor Process exporter discovery configuration file
<i>Shared-directory</i> /jplima/conf/jpc_file_sd_config_off/ jpc_file_sd_config_node_aix.yml	Node exporter for AIX discovery configuration file
<i>Shared-directory</i> /jplima/conf/jpc_file_sd_config_off/ jpc_file_sd_config_oracledb.yml	OracleDB exporter discovery configuration file
<i>Shared-directory</i> /jplima/conf/jpc_file_sd_config_off/ jpc_file_sd_config_vmware.yml	VMware exporter discovery configuration file

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
- Intelligent Integrated Management 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, 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/IM3-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/IM3-Manager DB Server) is running.
 - Check whether the JP1/IM3-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/IM3-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 *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.
4. Start the JP1/IM3-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/IM3-Manager DB Server_*logical-host-name*) is running.
 - Check whether the JP1/IM3-Manager service and the cluster service (JP1/IM3-Manager DB Cluster Service_*logical-host-name*) 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. Using the `jimdborg` command, reorganize the database.

For details about the `jimdborg` command, see *jimdborg* in *Chapter 1. Commands* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

3. Start the JP1/IM3-Manager service and the cluster service (JP1/IM3-Manager DB Cluster Service *_logical-host-name*) of the IM database 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.

(6) Reorganization for Intelligent Integrated Management Database

Because the Intelligent Integration Management Database is reorganized automatically, there is no need for user reorganization.

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 1–7: 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

Information type	Files to back up
	<i>shared-folder</i> \jplcons\log\action\acttxt{1 2}.log

In UNIX:

Table 1–8: Files to back up (UNIX)

Information type	Files to back up
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

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 1–9: Files to back up

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

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 1–10: 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 <i>/var/opt/jp1scope/database/jcshosts/</i>
		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 1–11: 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/IM3-Manager DB Server) is running.
2. Stop the following services:
 - JP1/IM3-Manager service
 - In Windows, the cluster service (JP1/IM3-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 *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.
4. Back up the target files.
For details about which files to back up, see *1.1.1(1) Backup (in Windows)* and *1.1.1(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/IM3-Manager DB Server) is running.
2. Stop the following services:
 - JP1/IM3-Manager service
 - In Windows, the cluster service (JP1/IM3-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 *JP1/Integrated Management 3 - Manager Command, Definition File and API 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. When you are using the Intelligent Integrated Management Base, delete the file shown in the table below.

OS	Files to delete
Windows	<i>Manager-path</i> \data\imdd\actevent.ser
	<i>Manager-path</i> \data\imdd\imdd_nodeStatus.ser

OS	Files to delete
	<i>Manager-path</i> \data\imdd\jddactseq.ser
UNIX	/var/opt/jplimm/data/imdd/actevent.ser
	/var/opt/jplimm/data/imdd/imdd_nodeStatus.ser
	/var/opt/jplimm/data/imdd/jddactseq.ser

6. Start the services that were stopped in step 2.

7. When you use the Intelligent Integrated Management Base, execute the `jddupdate tree` command in the new and rebuilding mode.

(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/IM3-Manager service and the cluster service (JP1/IM3-Manager DB Cluster Service *_logical-host-name*) of the IM database.

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

3. Back up the target files.

For details about which files to back up, see *1.1.1(1) Backup (in Windows)* and *1.1.1(3) Backup (in UNIX)*.

4. Start the JP1/IM3-Manager service and the cluster service (JP1/IM3-Manager DB Cluster Service *_logical-host-name*) of the IM database 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/IM3-Manager service and the cluster service (JP1/IM3-Manager DB Cluster Service *_logical-host-name*) of the IM database.

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 *JP1/Integrated Management 3 - Manager Command, Definition File and API 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. When you are using the Intelligent Integrated Management Base, delete the file shown in the table below.

OS	Files to delete
Windows	<i>shared-folder\data\imdd\actevent.ser</i>
	<i>shared-folder\data\imdd\imdd_nodeStatus.ser</i>
	<i>shared-folder\data\imdd\jddactseq.ser</i>
UNIX	<i>shared-directory/jplimm/data/imdd/actevent.ser</i>
	<i>shared-directory/jplimm/data/imdd/imdd_nodeStatus.ser</i>
	<i>shared-directory/jplimm/data/imdd/jddactseq.ser</i>

5. Start the JP1/IM3-Manager service and the cluster service (JP1/IM3-Manager DB Cluster Service *_logical-host-name*) of the IM database 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.

6. When you use the Intelligent Integrated Management Base, execute the `jddupdate tree` command in the new and rebuilding mode.

(7) Backup and recovery procedure of Intelligent Integrated Management Database

Perform regular backups as a means of recovery in the event of a failure of the Intelligent Integrated Management Database. The way to get a backup is an offline backup.

Describes how to perform offline backups and recovery while Intelligent Integrated Management Database services are stopped, when Intelligent Integrated Management Database services can be stopped, for example, due to planned outages.

When copying files and directories, in the case of Linux, please copy them while preserving the directory and file attributes.

(a) Backup procedure

The procedure for offline backup of the Intelligent Integration Management Database is as follows:

1. Stop JP1/IM - Manager services.

For details on how to stop Intelligent Integrated Management Database service, see [3.2 Stopping JP1/IM - Manager](#).

2. Stop Intelligent Integrated Management Database service.

For Windows

To stop Intelligent Integrated Management Database service and trend data management service, select [Control Panel]-[Management tools]-[Service] and then stop the trend data management service and Intelligent Integrated Management Database service.

For Linux

As JP1/IM - Manager goes down, Intelligent Integrated Management Database, and Trend Data Management services are also stopped. For details, see [3.2.2 In UNIX](#).

3. Back up IM database (Integrated Monitoring DB) for disaster recovery (when backing up the Integrated Monitoring DB according to Intelligent Integrated Management Database).

For details on how to back up, see [1.2.2\(6\)\(a\) Procedures for backing up and recovering the IM database on a physical host](#) and [1.2.2\(6\)\(b\) Procedures for backing up and recovering the IM database in a cluster environment](#).

4. Back up Intelligent Integrated Management Database for disaster recovery using `jimgndbbackup` command-with MAINT in the parameter-m.

For details and examples of the `jimgndbbackup` command, see `jimgndbbackup` in *Chapter 1. Commands* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

5. Start the services in the Intelligent Integrated Management Database.

For Windows

To start Intelligent Integrated Management Database service, start Intelligent Integrated Management Database service and Trend Data Management Service in order from [Control Panel]-[Management tools]-[Service] (There is a dependency. When you start the Trend Data Management Service, Intelligent Integrated Management Database service starts automatically.)

For Linux

As JP1/IM - Manager starts, Intelligent Integrated Management Database, and Trend Data Management Services are also started. For details, see [3.1.2 In UNIX](#).

6. Start JP1/IM - Manager services.

For details about how to start, see [3.1 Starting JP1/IM - Manager](#).

(b) Recovery procedure

Following are the steps to recover a backup of an Intelligent Integrated Management Database taken by an offline backup:

1. Stop JP1/IM - Manager services.

For details on how to stop Intelligent Integrated Management Database service, see [3.2 Stopping JP1/IM - Manager](#).

2. Stop JP/IM - Agent service.

For details, see [10.3 Stopping the service](#)

3. Delete Intelligent Integrated Management Database.

For details, see [1.25.1 \(1\) The procedure for delete Intelligent Integrated Management Database](#) and [2.23.1 \(1\) The procedure for delete Intelligent Integrated Management Database](#) in the *JP1/Integrated Management 3 - Manager Configuration Guide*.

4. Construct Intelligent Integrated Management Database.

For details, see [1.5 Construction of Intelligent Integrated Management Database \(for Windows\)](#) and [2.5 Construction of Intelligent Integrated Management Database \(for UNIX\)](#) in the *JP1/Integrated Management 3 - Manager Configuration Guide*.

5. Stop Intelligent Integrated Management Database service.

For Windows

To stop Intelligent Integrated Management Database service and trend data management service, select [Control Panel]-[Management tools]-[Service] and then stop the trend data management service and Intelligent Integrated Management Database service.

For Linux

As JP1/IM - Manager goes down, Intelligent Integrated Management Database, and Trend Data Management services are also stopped. For details, see [3.2.2 In UNIX](#).

6. Perform disaster recovery for IM database (Integrated Monitoring DB) if you want to recover the Integrated Monitoring DB for Intelligent Integrated Management Database.

For recovery methods, see *1.2.2(6)(a) Procedures for backing up and recovering the IM database on a physical host* and *1.2.2(6)(b) Procedures for backing up and recovering the IM database in a cluster environment*.

- Use `jimgndbrestore` command-with MAINT in the parameter-m-to perform disaster recovery for Intelligent Integrated Management Database.

For details and examples of the `jimgndbrestore` command, see *jimgndbrestore* in *Chapter 1. Commands* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

- Start Intelligent Integrated Management Database service.

For Windows

To start Intelligent Integrated Management Database service, start Intelligent Integrated Management Database service and Trend Data Management Service in order from [Control Panel]-[Management tools]-[Service] (There is a dependency. When you start the Trend Data Management Service, Intelligent Integrated Management Database service starts automatically.)

For Linux

As JP1/IM - Manager starts, Intelligent Integrated Management Database, and Trend Data Management Services are also started. For details, see *3.1.2 In UNIX*.

- Start JP/IM - Agent service.

For details, see *10.2 Starting the Service*.

- Start JP1/IM - Manager service.

For how to start Intelligent Integrated Management Database service, see *3.1 Starting JP1/IM - Manager*.

- Execute `jddupdatetree` command in the new/rebuild mode.

For details about the `jddupdatetree` command, see *jddupdatetree* in *Chapter 1. Commands* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

If you also want to perform IM database (integrated monitoring DB) recovery, perform it after performing IM database (integrated monitoring DB) recovery.

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:

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

In Windows:

Table 1–12: 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> \jp1base\log\COMMAND
Action information file	<i>Console-path</i> \log\action\actinf.log

Information type	Files to delete
	<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 1–13: 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\jcshosts\ 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. Note that when you are using the Intelligent Integrated Management Base, after setting up the integrated monitoring database again, and then before start JP1/IM - Manager, you need to delete the file shown in the table below.

OS	Files to delete
Windows	<i>Manager-path</i> \data\imdd\actevent.ser
	<i>Manager-path</i> \data\imdd\imdd_nodeStatus.ser
	<i>Manager-path</i> \data\imdd\jddactseq.ser
	<i>shared-folder</i> \data\imdd\actevent.ser
	<i>shared-folder</i> \data\imdd\imdd_nodeStatus.ser
	<i>shared-folder</i> \data\imdd\jddactseq.ser
UNIX	/var/opt/jplimm/data/imdd/actevent.ser
	/var/opt/jplimm/data/imdd/imdd_nodeStatus.ser
	/var/opt/jplimm/data/imdd/jddactseq.ser
	<i>shared-directory</i> /jplimm/data/imdd/actevent.ser
	<i>shared-directory</i> /jplimm/data/imdd/imdd_nodeStatus.ser
	<i>shared-directory</i> /jplimm/data/imdd/jddactseq.ser

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.

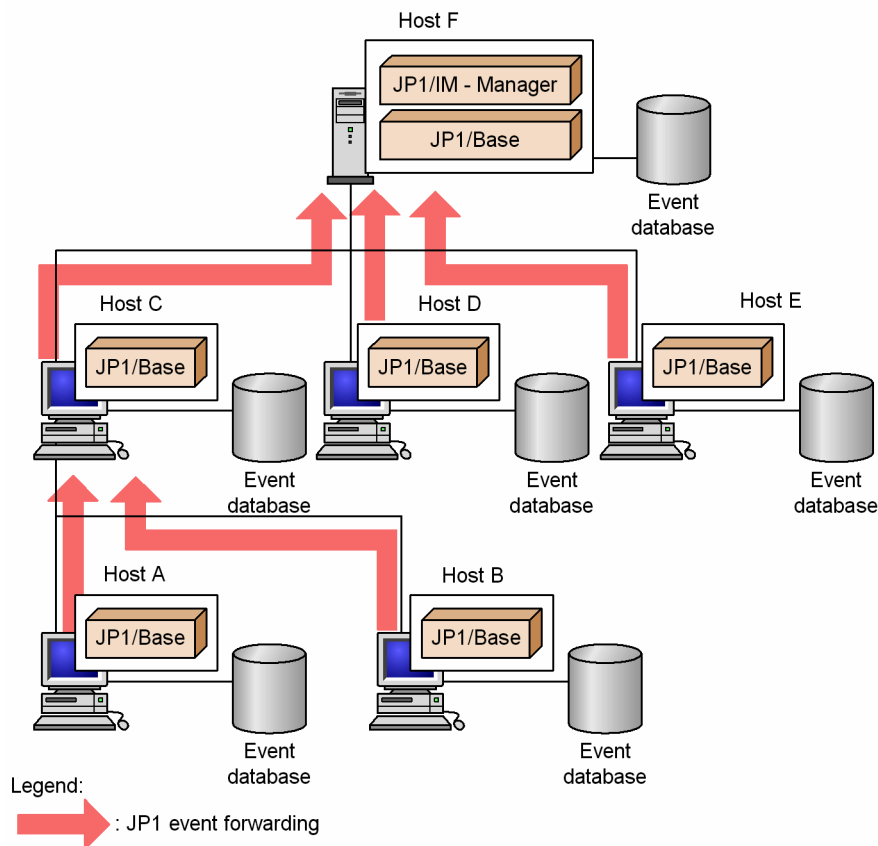
To re-create event databases:

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 `jevexport` 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 `jevexport` 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 1–14: 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/</i> resevent.dat
	<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 *JP1/Integrated Management 3 - Manager Command, Definition File and API 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 *JP1/Integrated Management 3 - Manager Command, Definition File and API 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. Stop JP1/IM - Manager.

6. Stop JP1/Base.

7. Restart the OS.

8. Start JP1/Base.

9. Start JP1/IM - Manager.

10. 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.

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

12. Restart the JP1/IM3-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 JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

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

13. When you are using the Intelligent Integrated Management Base, execute the `jddupdatetree` command in new and rebuilding mode.

For details about the `jddupdatetree` command, see *jddupdatetree* in *Chapter 1. Commands in the JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

- Procedure when stopping system monitoring via Central Console

1. Stop the JP1/IM3-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 JP1/Integrated Management 3 - Manager Command, Definition File and API 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. Stop JP1/Base.

6. Restart the OS.

7. Start JP1/Base.

8. 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.

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

10. Start the JP1/IM3-Manager service.

11. When you are using the Intelligent Integrated Management Base, execute the `jddupdatetree` command in new and rebuilding mode.

For details about the `jddupdatetree` command, see *jddupdatetree* in *Chapter 1. Commands in the JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

(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 JP1/Integrated Management 3 - Manager Command, Definition File and API 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 service (JP1/IM3-Manager DB Cluster Service_*logical-host-name*) of the IM database.

Stop the cluster service (JP1/IM3-Manager DB Cluster Service_*logical-host-name*) of the IM database 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 JP1/Integrated Management 3 - Manager Command, Definition File and API 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. Stop JP1/IM - Manager.
 7. Stop JP1/Base.
 8. Restart the OS.
 9. Start JP1/Base.
 10. Start JP1/IM - Manager.
 11. 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.
 12. 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 *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

13. Start the cluster service (JP1/IM3-Manager DB Cluster Service_ *logical-host-name*) of the IM database.
Start the cluster service (JP1/IM3-Manager DB Cluster Service_ *logical-host-name*) of the IM database you stopped in Step 2.
 14. Restart the JP1/IM3-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 *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

If JP1/IM - MO is being used, also start the JP1/IM - Message Optimizer service of JP1/IM - MO on the connection source.
 15. When you are using the Intelligent Integrated Management Base, execute the `jddupdatetree` command in new and rebuilding mode.
For details about the `jddupdatetree` command, see *jddupdatetree* in *Chapter 1. Commands* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.
- Procedure when stopping system monitoring via Central Console
 1. Stop the JP1/IM3-Manager service and the cluster service (JP1/IM3-Manager DB Cluster Service_ *logical-host-name*) of the IM database.
Stop the JP1/IM3-Manager service and the cluster service (JP1/IM3-Manager DB Cluster Service_ *logical-host-name*) of the IM database 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 *JP1/Integrated Management 3 - Manager Command, Definition File and API 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. Stop JP1/Base.
 6. Restart the OS.
 7. Start JP1/Base.
 8. 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.
 9. 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 JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

10. Start the JP1/IM3-Manager service and the cluster service (JP1/IM3-Manager DB Cluster Service_ *logical-host-name*) of the IM database.
Start the JP1/IM3-Manager service and cluster service (JP1/IM3-Manager DB Cluster Service_ *logical-host-name*) of the IM database you stopped in Step 1.
11. When you are using the Intelligent Integrated Management Base, execute the `jddupdatetree` command in new and rebuilding mode.
For details about the `jddupdatetree` command, see *jddupdatetree* in *Chapter 1. Commands in the JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

(6) Procedure for changing the IM database port

To change the IM database port:

1. Stop JP1/IM3-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 JP1/Integrated Management 3 - Manager Command, Definition File and API 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. Stop JP1/Base.
6. Restart the OS.
7. Start JP1/Base.
8. 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.
9. 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 JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.
10. 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.
11. When you are using the Intelligent Integrated Management Base, execute the `jddupdatetree` command in new and rebuilding mode.

For details about the `jddupdatetree` command, see *jddupdatetree* in *Chapter 1. Commands in the JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

(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/IM3-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. Stop JP1/Base.
6. Restart the OS.
7. Start JP1/Base.
8. 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.
9. When you are using the Intelligent Integrated Management Base, delete the file shown in the table below.

OS	Files to delete
Windows	<i>Manager-path</i> \data\imdd\actevent.ser
	<i>Manager-path</i> \data\imdd\imdd_nodeStatus.ser
	<i>Manager-path</i> \data\imdd\jddactseq.ser
	<i>shared-folder</i> \data\imdd\actevent.ser
	<i>shared-folder</i> \data\imdd\imdd_nodeStatus.ser
	<i>shared-folder</i> \data\imdd\jddactseq.ser
UNIX	/var/opt/jplimm/data/imdd/actevent.ser
	/var/opt/jplimm/data/imdd/imdd_nodeStatus.ser
	/var/opt/jplimm/data/imdd/jddactseq.ser
	<i>shared-directory</i> /jplimm/data/imdd/actevent.ser
	<i>shared-directory</i> /jplimm/data/imdd/imdd_nodeStatus.ser
	<i>shared-directory</i> /jplimm/data/imdd/jddactseq.ser

10. 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.

11. When you are using the Intelligent Integrated Management Base, execute the `jddupdatetree` command in new and rebuilding mode.

For details about the `jddupdatetree` command, see *jddupdatetree* in *Chapter 1. Commands in the JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

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

(1) Managing 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 1–15: 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 *JP1/Integrated Management 3 - Manager Command, Definition File and API 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 JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

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

(2) Intelligent Consolidated Management Database Capacity Management

Running out of PostgreSQL disk space as an Intelligent Integrated Management Database can cause the following problems:

- Cannot write, browse, or delete trend data
- Forcibly terminate database
- Corruption of trend data[#]

#

In the Intelligent Integration Management Database (PostgreSQL), disk access when trend data is written is reduced as much as possible so that database processing can be performed at high speed, and the contents of update operations (transactions) to the database are written to a log called WAL (write-ahead log). I'm going to write it down to disk in units that are organized to some extent. Depending on when the disk is full, it may fail to write to this WAL, or the WAL file itself may be corrupted.

In order to prevent such problems, it is necessary to operate to monitor the free space of the disk.

If the number of data items is reached the upper limit of registration, only for data that is registered frequently in the database, the old data judging from registration date and time will be deleted and new data will be registered.

Monitor the free disk space in "JP1/IM - Directories monitored by Manager" shown in the following table.

Areas to be monitored	Monitored directory in JP1/IM - Manager
Database cluster area	Where to store data files in the Intelligent Integrated Management Database ^{#1}
TABLESPACE area	
Temporary space in the database	
WAL storage	

1. JP1/IM System Maintenance

Areas to be monitored		Monitored directory in JP1/IM - Manager
Database log storage		
Storage space for server logs	Individual logs of operational commands	Where to store individual logs of operational commands ^{#1}
	Trend Data Management Service Log	Where to store trend data management service ^{#1}
Logging OS	Windows event log	<i>System-drive</i> : \Windows\System32\winevt\Logs
	syslog	/var/log ^{#2}
System log (syslog)		/var/log ^{#2}

#1

See 2.7.1(1)(d) *Where related files are stored in the JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

#2

For Linux 7 and later, the storage destination can be changed by "/etc/syslog.conf" or "/etc/rsyslog.conf". When the storage destination is changed, set the destination directory as the monitoring target.

Note:

Because the database is reorganized automatically, there is no need for user reorganization.

If you are using per-user disk quotas, monitor disk usage and usage limits for users who start trend data management DB. In addition to being able to cope with the lack of disk space with plenty of time, it is recommended that you use a guide in advance, for example, to deal with the available disk space when it interrupts 20% of the total.

Alevere trend data managed by the Intelligent Integrated Management Database is deleted after a certain period of time (the default retention period is 32 days), there is a risk that the disk will be depleted by inserting a large amount of trend data into the Intelligent Integrated Management Database before the trend data is deleted in the following cases:

- Set a longer retention period for trend data
- Extremely large number of monitored or samples

Consider planning to deal with disk shortages in advance, such as assuming a disk full state based on the amount of disk usage before and after operation after a certain period of time (1 day, 1 week, etc.).

(a) Recovering from Disk Full State

Here are the steps to recover when the disk is full:

1. Verify that the service is stopped.

If the event that the disk becomes full, it is necessary to take action once the request from the monitoring agent is not accepted, so make sure that the service of the intelligent integrated management database[#] is stopped. Also, please stop the trend data management service.

#

If the service is in a disk full state, the service may have been terminated, but if the service has not stopped, stop it.

2. Free up disk space

Remove unnecessary files and add disk space (OS functions such as LVM) to free up enough disk space.

3. Start the service.

Start intelligent integrated management database services and trend data management services.

If the above steps do not recover, delete and rebuild the Intelligent Integrated Management database. When backing up regularly, you can recover from the backup and # to the status at the time of the last backup.

#

Basically, if the disk is full, the recovery of the trend data collected so much cannot be guaranteed.

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) Checking the log output by Intelligent Integrated Management Database

Depending on the PostgreSQL configuration, the following Intelligent Integrated Management Database logs are output. For details about setting PostgreSQL, see *Intelligent Integrated Management Database configuration file (postgresql.conf)* in Chapter 2. *Definition Files* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

- Storage destination

In Windows

Storage-destination-of-Intelligent-Integrated-Management-Database-data-file#\log

In UNIX

Storage-destination-of-Intelligent-Integrated-Management-Database-data-file#/log

#

See 2.7.1(1)(d) *Where related files are stored* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

- File name

postgresql-%a#.log

#

"%a" contains three letters representing the day of the week in the GMT time zone (Mon, Tue, Wed, Thu, Fri, Sat, or Sun).

- Contents of the output

The format of the log output line is as follows:

YYYY-MM-DD HH:MM:SS.FFF GMT [Process-ID] SQL-Statement Logging-Message

In the "*YYYY-MM-DD HH:MM:SS.FFF GMT [Process-ID] SQL-Statement*" part, the timestamp, process ID, and SQL statement of the GMT time zone are output as prefixes.

- Estimating the size of the log file

There is no upper limit on the size of the log file.

The following is an estimate of the log output size in normal operation:

Log output size in normal operation (one week's)

The output size of the log for one day x 7 (day)

Log output size for one day

= Log output size per 1 sample^{#1} x scrapes per day^{#2} x samples collected from every Exporter by a scrape^{#3}

#1

Indicates the output size of the log output by writing trend data.

For JP1/IM - Agent, 50 bytes are assumed.

#2

For JP1/IM - Agent, calculate based on scrape interval specified in Prometheus configuration file (`jpc_prometheus_server.yml`) `scrape_interval`. For details, see the description of `scrape_interval` in *Prometheus configuration file (jpc_prometheus_server.yml)* in *Chapter 2. Definition Files in the JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

If the specified scrape interval is 1 m (1 minute), it will be 1440 times (60 minutes x 24 hours).

#3

Indicates the sum of the number of metrics specified in the metric definition file for each Exporter targeted by the monitoring agent.

For details about metric definition file of each Exporters supported by JP1/IM - Agent, see the description of metric definition file of each Exporters in *Chapter 2. Definition Files in the JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

In the case of Linux, you can reduce the disk space of log files by creating the following script (compressing or deleting logs for a certain period of time) [#] and running it regularly (once per day).

Place it in the `/etc/cron.daily` directory.

Example of a shell script that compresses logs on a daily basis and deletes them on a 30-day basis:

```
#!/usr/bin/bash
LOGDIR=/var/opt/jplimm/database/imgndb/log
LOGSAVE=/var/opt/jplimm/log/imgndb
COMPRESS_DAY=1
REMOVE_DAY=30
COMPRESS_CMD=gzip

COMPRESS_MTIME=`expr $COMPRESS_DAY - 1`
#Search for ".log" files whose modification date is "$COMPRESS_MTIME" or later
COMPRESS_FILE=`find $LOGDIR -name '*.log' -daystart -type f -mtime +$COMPRESS_MTIME`

#Add the date to the end of the file to be compressed and compress it.
if [ "$COMPRESS_FILE" != "" ]
then
  for i in $COMPRESS_FILE
  do
    if [ -f ${i} ]
    then
      mv ${i} ${i}.\`date '+%Y%m%d'\`
      $COMPRESS_CMD ${i}.\`date '+%Y%m%d'\`
    fi
  fi
```

```

done
fi

#Search for ".gz" files
MV_FILE=`find $LOGDIR -name '*.gz'`

#Move compressed logfiles to "$LOGSAVE"
if [ "$MV_FILE" != "" ]
then
for i in $MV_FILE
do
if [ -f ${i} ]
then
mv ${i} $LOGSAVE
fi
done
fi

REMOVE_TIME=`expr $REMOVE_DAY - 1`
#Search for ".gz" files whose modification date is "$REMOVE_TIME " or later
REMOVE_FILE=`find $LOGSAVE -name 'postgresql-*.gz' -daystart -type f -mtime +$REMOVE_TIME`

#Delete the file to be deleted
if [ "$REMOVE_FILE" != "" ]
then
for i in $REMOVE_FILE
do
if [ -f ${i} ]
then
rm -f ${i}
fi
done
fi
fi

```

When the above script is executed and operated, the estimated disk space of the log file will be approximately 20GB# when the number of monitored items is 500.

#

The sum of the sizes of each of the following log files:

- The size of the log file of the day: about 4GB
- Size of the log file of the previous day (before compression): about 4GB
- The size of the log file after compression (400MB) x 30 days: about 12GB

Intelligent Integrated Management Database log is extremely large, so the data collection tool# cannot collect it. If your case corresponds to the case described in " 12.3.1(1)(b) JP1 information" or " 12.3.1(2)(b) JP1 information", it must be collected individually by hand.

#

For details, see *jim_log.bat* (Windows only) and *jim_log.sh* (UNIX only) in Chapter 1. Commands in the JP1/Integrated Management 3 - Manager Command, Definition File and API Reference.

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 [12. 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 [6.1 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 JP1/Integrated Management 3 - Manager Command, Definition File and API 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 *4.2.7(5) Information included in a common exclusion history file* and *4.2.7(6) Information included in a common exclusion-conditions definition history file* of the *JP1/Integrated Management 3 - 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.

- 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 (Intelligent Integrated Management Base)

During migration of the Intelligent Integrated Management Base to another host, the definition files are the only definitions that can be migrated.

The definition files for the Intelligent Integrated Management Base must be edited on the host at the migration destination.

(2) 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.

(3) 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.

(4) 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 [9.7.3 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.

(5) JP1/IM - View

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

(6) 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](#).

(7) 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*.

(8) Intelligent Integrated Management Database

You can migrate only the trend data and integrated agent host data stored in Intelligent Integrated Management Database (only Trend data Management Database and integrated agent host managed DB are migrated).

You must make a backup on the source host and restore on the destination host where you set up Intelligent Integrated Management Database. The migration procedure is shown below.

1. Install JP1/IM - Manager on the destination host.
2. Back up the definition file on the source host.

Back up the following definition files:

- For physical hosts

Definition file name	File Path
Intelligent Integrated Management Database setup information file	<ul style="list-style-type: none">• For Windows <i>Manager-path</i>\imgndb\setup\jimgnbdbsetupinfo.conf• For Linux /etc/opt/jplimm/conf/imgndb/setup/jimgnbdbsetupinfo.conf
postgresql.conf	<ul style="list-style-type: none">• For Windows <i>Manager-path</i>\conf\imgndb\postgresql.conf• For Linux /etc/opt/jplimm/conf/imgndb/postgresql.conf

- For logical hosts

Definition file name	File Path
Cluster Environment Intelligent Integrated Management Database setup information file	<ul style="list-style-type: none">• For Windows <i>Manager-path</i>\imgndb\setup\jimgnbdbclustersetupinfo.conf• For Linux /etc/opt/jplimm/conf/imgndb/setup/jimgnbdbclustersetupinfo.conf
postgresql.conf	<ul style="list-style-type: none">• For Windows <i>Shared-folder</i>\jplimm\conf\imgndb\postgresql.conf• For Linux <i>Shared-directory</i>/jplimm/conf/imgndb/postgresql.conf

3. Back up Intelligent Integrated Management Database data files.

Use the following procedure.

Step 1: Stop JP1/IM - Manager services.

For details about how to shut down, see [3.2 Stopping JP1/IM - Manager](#).

Step 2: Stop servicing Intelligent Integrated Management Database.

For Windows

To stop Intelligent Integrated Management Database service and trend data management service, select [Control Panel]-[Management tools]-[Service] and then stop the trend data management service and Intelligent Integrated Management Database service.

For Linux

As JP1/IM - Manager goes down, Intelligent Integrated Management Database, and Trend Data Management services are also stopped. For details, see [3.2.2 In UNIX](#).

Step 3: Back up Intelligent Integrated Management Database for migration using `jimgndbbackup` command-with TRANSF in the parameter -m.

For details and examples of executing the `jimgndbbackup` command, see `jimgndbbackup` in *Chapter 1. Commands* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

Step 4: Start Intelligent Integrated Management Database servicing.

For Windows

To start Intelligent Integrated Management Database service, start Intelligent Integrated Management Database service and Trend Data Management Service in order from [Control Panel]-[Management tools]-[Service] (There is a dependency. When you start the Trend Data Management Service, Intelligent Integrated Management Database service starts automatically.)

For Linux

As JP1/IM - Manager starts, Intelligent Integrated Management Database, and Trend Data Management Services are also started. For details, see [3.1.2 In UNIX](#).

Step 5: Start JP1/IM - Manager services.

For details about how to start JP1/IM - Manager services, see [3.1 Starting JP1/IM - Manager](#).

4. Perform Intelligent Integrated Management Base migration.

For details about migrating Intelligent Integrated Management Base, see [1.5.1\(1\) JP1/IM - Manager \(Intelligent Integrated Management Base\)](#).

5. Copy Intelligent Integrated Management Database setup information file that you backed up from the source (or cluster environment Intelligent Integrated Management Database setup information file for logical hosts) to the destination host.

6. Set up the Intelligent Integrated Management Database according to the contents of the Intelligent Integrated Management Database Setup File (in the case of a logical host, the Cluster Environment Intelligent Integrated Management Database Setup File) copied in step 5.

For details about how to setup, see `jimgndbsetup` in *Chapter 1. Commands* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

7. Reflect the parameters that have been changed from the default in the `postgresql.conf` file backed up from the source to the `postgresql.conf` file in destination host.

8. Restore Intelligent Integrated Management Database data files that you backed up at the source.

Use the following procedure.

Step 1: Verify that JP1/IM - Manager is out of service.

For details about how to stop a when it is not stopped, see [3.2 Stopping JP1/IM - Manager](#).

Step 2: Verify that Intelligent Integrated Management Database is Out of Service.

The following shows how to stop the equipment when it is not stopped.

For Windows

To stop Intelligent Integrated Management Database service and trend data management service, select [Control Panel]-[Management tools]-[Service] and then stop the trend data management service and Intelligent Integrated Management Database service.

For Linux

As JP1/IM - Manager goes down, Intelligent Integrated Management Database, and Trend Data Management services are also stopped. For details, see [3.2.2 In UNIX](#).

Step 3: Restore Intelligent Integrated Management Database for migration using `jimgndbrestore` command-specifying TRANSF in the parameter `-m`.

For details and examples of executing the `jimgndbrestore` command, see *jimgndbrestore* in *Chapter 1. Commands* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

Step 4: Start Intelligent Integrated Management Database servicing.

For Windows

To start Intelligent Integrated Management Database service, start Intelligent Integrated Management Database service and Trend Data Management Service in order from [Control Panel]-[Management tools]-[Service] (There is a dependency. When you start the Trend Data Management Service, Intelligent Integrated Management Database service starts automatically.)

For Linux

As JP1/IM - Manager starts, Intelligent Integrated Management Database, and Trend Data Management Services are also started. For details, see [3.1.2 In UNIX](#).

Step 5: Start JP1/IM - Manager services.

For details about how to start JP1/IM - Manager services, see [3.1 Starting JP1/IM - Manager](#).

Step 6: Run `jddupdatetree` command in New/Rebuild mode.

For details about the `jddupdatetree` command, see *jddupdatetree* in *Chapter 1. Commands* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

(9) Migrating JP1/IM - Agent of integrated agent host

(a) Data migration between hosts

You can migrate an integrated agent host to a host with the same hostname. You can migrate performance data, JP1 event data, and definitions.

If you are migrating to a host with the same hostname, follow the steps in [1.1.2 Backing Up and Recovering of JP1/IM - Agent](#).

If you are migrating to a host with a different host name, follow the steps in [1.1.2 Backing Up and Recovering of JP1/IM - Agent](#), migrating to a host with the same host name, and then follow the steps in [2.2.1\(3\) Tasks when agent hostname is changed](#).

Note that if you change the hostname to a different one, performance data and JP1 events retrieved up to that point cannot be viewed.

(b) Referencing between JP1 Users

Performance data collected by JP1/IM - Agent and stored in JP1/IM - Manager (Intelligent Integrated Management Base) can be viewed by anyone in your JP1/IM - Manager's integrated operation viewer if you are a JP1 user accessible to IM management node to which the performance data is associated.

Since the JP1/IM - Agent does not store data that depends on JP1 users, there is no migration of data between JP1 users who log in to the Integrated Operations Viewer.

(c) Migrating Web Scenario Files to another host

When using the Web scenario monitoring function, when migrating the Web scenario file to another host, the following settings must be made so that the destination host can access the monitored website.

■ Editing the Playwright configuration file

If the item "proxy" is set in the playwright configuration file (`jpc_playwright.config.ts`), edit the definition file according to the network settings of the destination host.

For details of the Playwright configuration file, see *Playwright configuration file (jpc_playwright.config.ts)* in *Chapter 2. Definition File* in the manual *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

For details on how to edit the configuration file, see *To edit the configuration files (for Windows)* in *1.19.3(1)(a) Common way to setup* in the *JP1/Integrated Management 3 - Manager Configuration Guide*.

■ Browser settings

Follow the steps described in *Browser Settings* in *1.21.2(13)(b) JP1/IM - Agent Setup* in the *JP1/Integrated Management 3 - Manager Configuration Guide*.

■ Configuring Authentication

Execute the steps described in *Authentication Settings* in *1.21.2(13)(b) JP1/IM - Agent Setup* in the *JP1/Integrated Management 3 - Manager Configuration Guide*.

(d) About Migrating Existing JP1/PFM from other products

JP1/IM - Agent is a new product that collects performance data using a protocol that differs from JP1/PFM products that already exist. As a result, there is no way to migrate from JP1/PFM.

(10) Migrating an Integration Manager Host JP1/IM - Agent

(a) Migrating to Other Hosts

The procedure for migrating to another host is as follows:

1. Migrate the definition file.
Copy to the destination of the definition file of the source host.
2. Change hostname and IP address following in *2.2.1(2)(i) Hostname given in the server certificate used in JP1/IM - Agent* and *2.3.1(2)(d) IP address listed in the server certificate used by JP1/IM - Agent*.
Perform destination host-specific settings, such as those related to host name.
3. Change to the target manager host according to *1.21.2(2)(a) Change Integrated manager to connect to (for Windows) (optional)* and *2.19.2(2)(a) Change Integrated manager to connect to (for Linux) (optional)* in the *JP1/Integrated Management 3 - Manager Configuration Guide*.

Update the connection information on the Unified Agent host side (the information connected to the source host) with the information on the destination host.

(b) Migrating to Other Hosts in a Cluster System

The procedure for migrating to another host is as follows:

After copying the source host's definition file to the destination and performing the destination host-specific settings (such as settings related to the host name), integrated agent host's connection information (the information that was connected to the source host) is updated to the destination host's information.

1. Migrate the definition file.

Copy to the destination of the definition file of the source host.

2. Change hostname and IP address following *Changing the hostname of the Integration Manager host in a cluster system" of 2.2.1(2)(i) Hostname given in the server certificate used in JP1/IM - Agent* and *Changing IP address of the Integration Manager Host in a Cluster System of 2.3.1(2)(d) IP address listed in the server certificate used by JP1/IM - Agent*.

Perform destination host-specific settings, such as those related to host name.

3. Change to the target manager host according to *1.21.2(2)(a) Change Integrated manager to connect to (for Windows) (optional)* and *2.19.2(2)(a) Change Integrated manager to connect to (for Linux) (optional)* in the *JP1/Integrated Management 3 - Manager Configuration Guide*.

Updates the connection information on integrated agent host (the information that was connected to the source host) to the information on the destination host.

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 *9.4.2 Changing configured certificates* in the *JP1/Integrated Management 3 - 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 `openssl` command, see the official website of OpenSSL.

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 *9.4.4(3) Keystores for JP1/IM - Manager* in the *JP1/Integrated Management 3 - 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 3 - Manager Overview and System Design Guide*. For details about how to carry out setting tasks, see the *JP1/Integrated Management 3 - Manager Configuration Guide* and the *JP1/Base User's Guide*.

2.1.1 Changing the JP1/IM - Agent settings with integrated agent host

(1) Change to IP binding method (optional)

If you want to change to IP binding method, change the following settings:

- Configuring JP1/IM agent control base
- Configuring Prometheus server
- Configuring Alertmanager
- Configuring Node exporter
- Configuring Windows exporter
- Configuring Blackbox exporter
- Configuring Yet another cloudwatch exporter

For details about how to change the settings, see the physical host settings in *Change to IP binding method* in 7.3.6 *Newly installing JP1/IM - Agent with integrated agent host (for Windows)* and 8.3.6 *Newly installing JP1/IM - Agent with integrated agent host (for UNIX)* of the *JP1/Integrated Management 3 - Manager Configuration Guide*.

(2) Configuration changes on container systems

If you need to change the settings, it is recommended that you recreate Docker image or Podman image.

If you make configuration changes after you start a container, note the following:

- Delete function and update function of definition file by the definition file operation facility is not available. Updating or deleting using the definition file operation facility in a container environment will result in a KNBC00019-E error.
- If you want to edit a file in a container, you must run the following command to connect to the container after you launch the container:

- For Docker

```
# docker exec-it container name /bin/bash
```

- For Podman

```
# podman exec-it container name /bin/bash
```

- The steps for editing unit definition file are to edit the service-management program definition file in the container. For example, for supervisor, edit supervisor definition file (supervisor.conf).

(3) Change the setting of Web scenario-monitoring function

(a) Changing Browser Settings on agent host

When you add or change the language used to display a browser, you must make the appropriate language available to the browser.

Check whether the language to be used has been added in the setting window of the browser to be used. If not, add the language to be used because Codegen run and monitoring by Playwright may not work properly.

(b) Changing authentication Settings

If you change the settings for the client authentication or HTTP authentication (Basic authentication) when Playwright accesses the monitored Web application, you need to review the settings for certificates, passwords, etc.

For the required settings, see *Authentication settings* in 1.21.2(13)(b) *JP1/IM - Agent Setup* in the *JP1/Integrated Management 3 - Manager Configuration Guide*.

(c) Modify Web scenario file

The behavior when modifying Web scenarios generated using Codegen is not supported.

For the codes recorded by Codegen operation, see *Browser operations and operations that can be recorded and measured as Web scenarios* described in *Web scenario creation function (playwright codegen)* in 3.15.1(1)(m) *Web scenario monitoring function* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

If you want to change Web scenario file, perform the following steps:

1. Remove Web scenario file.

See 2.1.1(3)(d) *Removing a Web scenario file*.

2. Create a new Web scenario file.

See *Creating a New Web Scenario File* in 1.21.2(13)(b) *Setting up JP1/IM - Agent* in the *JP1/Integrated Management 3 - Manager Configuration Guide*.

(d) Removing a Web scenario file

Here are the steps to remove a Web scenario file:

1. Shut down Web exporter.

Stops Web exporter running Web scenario file to be deleted.

2. Remove Web scenario file.

You remove Web scenario file that you have created.

For details about Web scenario file, see *Web scenario file (any name.spec.ts)* in *Chapter 2. Definition Files* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

For details on how to remove configuration file, see 1.21.2(1)(a) *Edit the configuration files (for Windows)* in the *JP1/Integrated Management 3-Manager Configuration Guide*.

3. Change Playwright configuration file.

From Playwright configuration file, remove the definition that runs Web scenario file that you want to remove.

For details about Playwright configuration file, see *Playwright configuration file (jpc_playwright.config.ts)* in *Chapter 2. Definition Files* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

For details on configuration file editing procedure, see *To edit the configuration files (for Windows)* in *1.19.3(1)(a) Common way to setup* in the *JP1/Integrated Management 3-Manager Configuration Guide*.

4. Change Web exporter discovery configuration file.

From Web exporter discovery configuration file, remove the definition that runs Web scenario file that you want to remove.

For details about Web exporter discovery configuration file, see *Web exporter discovery configuration file (jpc_file_sd_config_web.yml)* in *Chapter 2. Definition Files* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

For details on configuration file editing procedure, see *To edit the configuration files (for Windows)* in *1.19.3(1)(a) Common way to setup* in the *JP1/Integrated Management 3-Manager Configuration Guide*.

5. Start Web exporter.

(e) Changing Web exporter operation settings

Editing Playwright configuration file (jpc_playwright.config.ts) is performed in the following cases:

- When you create a new Web scenario file
See *Setting up Playwright configuration file* in *1.21.2(13)(b) Setting up JP1/IM - Agent* in the *JP1/Integrated Management 3 - Manager Configuration Guide*.
- When Web scenario file is removed
See the procedure *Change Playwright configuration file.* in *2.1.1(3)(d) Removing a Web scenario file.*
- Changing the runtime configuration of Web scenario file

For details about Playwright configuration file, see *Playwright configuration file (jpc_playwright.config.ts)* in *Chapter 2. Definition Files* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

For details on configuration file editing procedure, see *To edit the configuration files (for Windows)* in *1.19.3(1)(a) Common way to setup* in the *JP1/Integrated Management 3-Manager Configuration Guide*.

(f) Change Web exporter settings that Prometheus server will scrape

Editing Web exporter discovery configuration file (jpc_file_sd_config_web.yml) is performed in the following cases:

- When you create a new Web scenario file
See *Setting up Web exporter discovery configuration file* in *1.21.2(13)(b) Setting up JP1/IM - Agent* in the *JP1/Integrated Management 3 - Manager Configuration Guide*.
- When Web scenario file is removed
See the procedure *Change Web exporter discovery configuration file.* in *2.1.1(3)(d) Removing a Web scenario file.*
- To change the settings of other Web scenario-monitoring functions

For details about Web exporter discovery configuration file, see *Web exporter discovery configuration file (jpc_file_sd_config_web.yml)* in *Chapter 2. Definition Files* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

For details on configuration file editing procedure, see *To edit the configuration files (for Windows)* in *1.19.3(1)(a) Common way to setup* in the *JP1/Integrated Management 3-Manager Configuration Guide*.

2.1.2 Changing the Integration Manager Host JP1/IM - Agent settings

(1) Updating initial secret (optional)

1. Log in to integrated operation viewer.

2. Perform an initial secret refresh.

Select **Issue initial secret** in the **Option** menu of the integrated operation viewer to open the Show Initial Secret window.

For details, see *2.2 Windows related to Option* in the *JP1/Integrated Management 3 - Manager GUI Reference* for the relevant menus and screen descriptions.

3. Get the new initial secret displayed in integrated operation viewer.

When you build an integrated agent in the future, you must specify a new initial secret.

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. Since JP1/IM - Manager assumes JP1/Base, please see the chapter on changing the settings during JP1/Base operation of the *JP1/Base User's Guide* and perform the necessary work to change the host name of JP1/Base.

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.

Stop JP1/Base of the manager or agent whose name is to be changed before starting the tasks.

2.2.1 When you are using JP1/IM - Agent as agent

(1) Tasks necessary what you need to do immediately after you change the host name of the manager.

Description about the tasks necessary what you need to do immediately after you change the host name of the manager.

(a) Tasks necessary in JP1/Base

In JP1/Base of the manager who changed the host name, change the host name of the authentication server. For details such as procedures, see the description of the effects and follow-up tasks when changing the host names in the chapter on modifying settings during JP1/Base operation of the *JP1/Base User's Guide*.

After that, you must exit JP1/Base of the manager whose hostname has been changed, and then restart.

(b) Necessary tasks related to 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) Tasks when you change the manager hostname

(a) 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.

(b) 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 `jccachange` command.

(c) 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 [2.2.2\(3\) Procedure for re-distributing the system configuration when the host name of a manager or JP1/Base is changed](#).

(d) 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.

(e) 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.

(f) 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.

(g) 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 [9.4.2 Changing configured certificates](#) in the *JP1/Integrated Management 3 - Manager Configuration Guide*.

(h) Hostname of the host that Intelligent Integrated Management Base runs on

After you change the host name of the host on which the Intelligent Integrated Management Base runs, you will need to restart JP1/IM - Manager. For details about how to start JP1/IM - Manager, see [3.1 Starting JP1/IM - Manager](#).

In addition, 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 [9.4.2 Changing configured certificates](#) in the *JP1/Integrated Management 3 - Manager Configuration Guide*.

If the host name of the host serving as the IM management node needs to be changed, you need to recollect the IM management node. For details about how to recollect an IM management node, see [3.5.6 Changes in IM management nodes](#) in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

(i) Hostname given in the server certificate used in JP1/IM - Agent

■ Changing the hostname of the Integration Manager Host

1. Shut down JP1/IM - Manager.
2. Update with a server certificate that reflects the host name change.
For details on updating certificates, see *Setup the certificate* in [1.19.3\(1\)\(b\) Change settings of JP1/IM agent management base \(for Windows\)](#) of *JP1/Integrated Management 3 - Manager Configuration Guide*.
Note that this step is not necessary if the certificate does not contain the host name before the change.
3. Start JP1/IM - Manager.

■ Changing the hostname of the Integration Manager host in a cluster system

1. Shut down JP1/IM agent management base.
2. Update with a server certificate that reflects changes in the logical host name.
For details on updating the certificate, see *Setup the certificate* in [7.3.3\(9\)\(a\) Setup changes for JP1/IM agent management base](#) and [8.3.3\(9\)\(a\) Setting changes for JP1/IM agent management base](#) of *JP1/Integrated Management 3 - Manager Configuration Guide*.
Note that this step is not necessary if the certificate does not contain the host name before the change.
3. Start JP1/IM agent management base.

(3) Tasks when agent hostname is changed

(a) Hostname of agent

1. Log in to agent host.
2. Shut down JP1/IM - Agent servicing.
3. For all JP1/IM - Agent definition files, change the location where the old host name is listed to the new host name.
For details about JP1/IM - Agent definition file, see *Chapter 2. Definition Files* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.
4. Start JP1/IM - Agent servicing.
5. Reflects IM management node tree.

See 1.21.2(18) *Creation and import of IM management node tree data (for Windows) (required)* and 2.19.2(18) *Creating and importing IM management node tree data (for Linux) (required)* in the *JP1/Integrated Management 3 - Manager Configuration Guide*.

If you are using the event-forwarding relay function, see 1.21.2(2)(g) *Configuring the event-forwarding relay function (for Windows) (optional)* in the *JP1/Integrated Management 3 - Manager Configuration Guide*. Review the event-forwarding settings of JP1/Base, the event-forwarding relay source.

Important

The following notes apply to modifying definition files:

If you start a JP1/IM - Agent service without editing some of the definition files, or if you change the hostname to a previously used hostname (that is, a hostname with trend data left in Trend data Management Database), several configuration SID are mapped to a single tree SID. In such cases, IM management node tree file output by `jddcreatetree` command must be edited. For details about editing IM management node tree file, see 1.19.3(2)(c) *Creation and import of IM management node tree data (for Windows) (required)* in the *JP1/Integrated Management 3 - Manager Configuration Guide*.

If you reflect the tree information without editing IM management node tree file, the display of the trend data may fail in the **Trends** tab of the integrated operation viewer.

(b) Hostname to monitor for Blackbox exporter

Change the monitoring target of Blackbox exporter.

See 1.21.2(6)(c) *Add, change, or Delete the monitoring target (for Windows) (required)* and 2.19.2(7)(c) *Add, Modify, or Delete a monitoring target (for Linux) (required)* in the *JP1/Integrated Management 3 - Manager Configuration Guide*.

(c) Hostname of the host that Intelligent Integrated Management Base runs on

After you change the host name of the host on which the Intelligent Integrated Management Base runs, you will need to restart JP1/IM - Manager. For details about how to start JP1/IM - Manager, see 3.1 *Starting JP1/IM - Manager*.

In addition, 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 9.4.2 *Changing configured certificates* in the *JP1/Integrated Management 3 - Manager Configuration Guide*.

If the host name of the host serving as the IM management node needs to be changed, you need to recollect the IM management node. For details about how to recollect an IM management node, see 3.5.6 *Changes in IM management nodes* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

(d) Logical host name of the cluster system

■ For Windows

1. Shut down JP1/IM - Agent for a logical host.
Stop the service from the cluster software
2. Remove the logical-host service from Windows.
For the service used by the logical host, release the service for the logical host from Windows on both the running server and the standby server.

Run the following command to remove the logical host service:

```
Agent-path\tools\jpc_service -off service-key -h logical-host-name
```

The following shows a sample procedure for deactivating Alertmanager servicing.

```
Agent-path\tools\jpc_service -off jpc_alertmanager -h logical-host-name
```

3. Update the logical host name described in the definition file.

For files located in the *shared-folder\jplima\conf* and *Agent-path\bin*, search for the old logical host name and change all applicable locations to the new logical host name.

Agent-path\bin is executed on both the running server and the standby server because they exist on both servers.

4. Update the logical host name contained in the file name.

Change to the new logical host name because the file that exists in *Agent-path\bin* contains the logical host name.

Agent-path\bin is executed on both the running server and the standby server because they exist on both servers.

5. Registers a logical-host service with Windows.

For the service used by the logical host, register the service for the logical host in Windows on both the running server and the standby server.

Run the following command to register services on the logical host:

```
Agent-path\tools\jpc_service -on service-key -h logical-host-name
```

The following shows an example of registering a Alertmanager service.

```
Agent-path\tools\jpc_service -on jpc_alertmanager -h logical-host-name
```

6. Start all JP1/IM - Agent services for the logical host.

Start the service from the cluster software.

7. Reflects IM management node tree.

For details, see *1.21.2(18) Creation and import of IM management node tree data (for Windows) (required)* and *2.19.2(18) Creating and importing IM management node tree data (for Linux) (required)* in the *JP1/Integrated Management 3 - Manager Configuration Guide*.

■ For Linux

1. Shut down JP1/IM - Agent for a logical host.

Stop the service from the cluster software.

2. Remove the logical-host service from systemd.

For a service used by a logical host, the service for the logical host is released from systemd on both the running system and the standby system.

Run the following command to remove the logical host service:

```
/opt/jplima/tools/jpc_service-off service-key -h logical-host-name
```

The following shows a sample procedure for deactivating Alertmanager servicing.

```
/opt/jplima/tools/jpc_service -off jpc_alertmanager -h logical-host-name
```

3. Update the logical host name described in the definition file.

For files that exist in the *shared-directory*/jplima/conf and /usr/lib/systemd/system, search for the old logical host name and change all applicable locations to the new logical host name.

Because /usr/lib/systemd/system exists on both the running server and the standby server, it is executed on both servers.

4. Update the logical host name contained in the file name.

Change to the new logical host name because the file that exists in /usr/lib/systemd/system contains the logical host name.

Because /usr/lib/systemd/system exists on both the running server and the standby server, it is executed on both servers.

5. Registers a logical-host service with systemd.

For a service used by a logical host, the service for the logical host is registered in systemd on both the running system and the standby system.

Run the following command to register services on the logical host:

```
/opt/jplima/tools/jpc_service -on service-key -h logical-host-name
```

The following shows an example of registering a Alertmanager service.

```
/opt/jplima/tools/jpc_service -on jpc_alertmanager -h logical-host-name
```

6. Start all JP1/IM - Agent services for the logical host.

Start the service from the cluster software.

7. Reflects IM management node tree.

For details, see *1.21.2(18) Creation and import of IM management node tree data (for Windows) (required)* and *2.19.2(18) Creating and importing IM management node tree data (for Linux) (required)* in the *JP1/Integrated Management 3 - Manager Configuration Guide*.

! Important

If you are using the event-forwarding relay function, see *1.21.2(2)(g) Configuring the event-forwarding relay function (for Windows) (optional)* in the *JP1/Integrated Management 3 - Manager Configuration Guide*. Review the event-forwarding settings of JP1/Base, the event-forwarding relay source.

(e) Host name of the container

You cannot change the hostname of a container. Therefore, create a new container and delete any containers that you no longer need.

For details on how to create a container, see *1.22.1(3) How to Create Docker and Podman Containers* and *1.22.1(4) How to delete Docker and Podman Containers* in the *JP1/Integrated Management 3 - Manager Configuration Guide*.

2.2.2 When you are using JP1/Base as agent

(1) Tasks necessary what you need to do immediately after you change the host name of the manager or JP1/Base

Describes the tasks required immediately after changing the host name of a manager or JP1/Base.

(a) Tasks necessary in JP1/Base

In JP1/Base of the manager who changed the host name, change the host name of the authentication server. For details such as procedures, see the description of the effects and follow-up tasks when changing the host names in the chapter on modifying settings during JP1/Base operation of the *JP1/Base User's Guide*.

After that, JP1/Base of the manager or agent whose host name was changed must be terminated and restarted.

(b) 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) What to do if you change the host name of a manager or JP1/Base

(a) 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.

(b) 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 `j cachange` command.

(c) 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 *2.2.2(3) Procedure for re-distributing the system configuration when the host name of a manager or JP1/Base is changed*.

(d) 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 `j coegschange` command.

(e) 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_spmd_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.

(f) 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_spmd_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.

(g) 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 *9.4.2 Changing configured certificates* in the *JP1/Integrated Management 3 - Manager Configuration Guide*.

(h) Host name of the host that Intelligent Integrated Management Base runs on

After you change the host name of the host on which the Intelligent Integrated Management Base runs, you will need to restart JP1/IM - Manager. For details about how to start JP1/IM - Manager, see *3.1 Starting JP1/IM - Manager*.

In addition, 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 *9.4.2 Changing configured certificates* in the *JP1/Integrated Management 3 - Manager Configuration Guide*.

If the host name of the host serving as the IM management node needs to be changed, you need to recollect the IM management node. For details about how to recollect an IM management node, see *3.5.6 Changes in IM management nodes* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

(3) Procedure for re-distributing the system configuration when the host name of a manager or JP1/Base is changed

If the host name of a manager or JP1/Base 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 *1.9 Setting the system hierarchy (when IM Configuration Management is used) (for Windows)*, *1.10 Setting the system hierarchy (when IM Configuration Management is not used) (for Windows)*, or *2.9 Setting the system hierarchy (when IM Configuration Management is not used) (for UNIX)* in the *JP1/Integrated Management 3 - Manager Configuration Guide*.

2.2.3 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.

2.2.4 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 *7.7.1 Deleting logical hosts (for Windows)* in the *JP1/Integrated Management 3 - 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 Windows)* or *7.6 Upgrade installation and setup of logical hosts (for Windows)* in the *JP1/Integrated Management 3 - Manager Configuration Guide*.

In UNIX:

For details about how to delete a logical host, see *8.7.1 Deleting logical hosts (for UNIX)* in the *JP1/Integrated Management 3 - Manager Configuration Guide*. For details about how to set up a logical host, see *8.3 Installing and setting up logical hosts (new installation and setup) (for UNIX)* or *8.6 Upgrade installation and setup of logical hosts (for UNIX)* in the *JP1/Integrated Management 3 - 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.

Stop JP1/Base of the manager or agent whose name is to be changed before starting the tasks.

2.3.1 When JP1/IM - Agent is used as agent

(1) Work needed right after changing manager IP address

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

(a) Necessary tasks in JP1/Base

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

(b) 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) Tasks to be performed when the IP address of a manager is changed

(a) 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.

After setting the IP address, restart the system. For details, see [2.3.2\(3\) How to restart the system if you change the IP address of the manager or JP1/Base](#).

(b) Using IM Configuration Management

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

(c) IP address of the host where Intelligent Integrated Management Base runs

After you change the IP address of the host on which the Intelligent Integrated Management Base runs, you need to restart JP1/IM - Manager. In addition, if you are using a plug-in customized by the user, handle the situation according to the specification of the plug-in. For details about how to start JP1/IM - Manager, see [3.1 Starting JP1/IM - Manager](#).

Note that after you change the IP address of the host serving as the IM management node, you do not have to do anything.

(d) IP address listed in the server certificate used by JP1/IM - Agent

■ Changing the Integration Manager Host IP address

1. Shut down JP1/IM - Manager.

2. Changing the Configuration of JP1/IM

2. Updating with a server certificate that reflects changes in IP addressing.

For details on updating the certificate, see *Setup the certificate in 1.19.3(1)(b) Change settings of JP1/IM agent management base (for Windows)* of the *JP1/Integrated Management 3 - Manager Configuration Guide* manual.

Note that this step is not required if the certificate does not contain the old IP address.

3. Start JP1/IM - Manager.

■ Changing IP address of the Integration Manager Host in a Cluster System

1. Shut down JP1/IM agent management base.

2. Updating with a server certificate that reflects changes in logical IP address.

For details on updating the certificate, see *Setup the certificate in 7.3.3(9)(a) Setup changes for JP1/IM agent management base* and *8.3.3(9)(a) Setting changes for JP1/IM agent management base* of the *JP1/Integrated Management 3 - Manager Configuration Guide*.

Note that this step is not required if the certificate does not contain the old IP address.

3. Start JP1/IM agent management base.

(3) Tasks to be performed when IP address for agent is changed

(a) IP addressing for agent

You do not need to change the settings if any of the following conditions is true: If applicable, it is affected by agent's IP address changes, so a configuration change is required.

- When the listen address is set with IP address

This is affected if the listen address of JP1/IM - Agent process is specified with IP address.

Check the procedure for changing the port of each process, and if the listen address is set, set it again.

- If the certificate contains IP addressing data

You must reposition the modified certificate to the new IP address.

Important

If you are using the event-forwarding relay function, see *1.21.2(2)(g) Configuring the event-forwarding relay function (for Windows) (optional)* in the *JP1/Integrated Management 3 - Manager Configuration Guide*. Review the event-forwarding settings of JP1/Base, the event-forwarding relay source.

(b) IP addresses monitored by Blackbox exporter

Blackbox exporter target is specified by the hostname.

Changing IP address does not require any configuration changes in agent.

(c) IP addresses of the host where Intelligent Integrated Management Base runs

After you change the IP address of the host on which the Intelligent Integrated Management Base runs, you need to restart JP1/IM - Manager. In addition, if you are using a plug-in customized by the user, handle the situation according to the specification of the plug-in. For details about how to start JP1/IM - Manager, see *3.1 Starting JP1/IM - Manager*.

Note that after you change the IP address of the host serving as the IM management node, you do not have to do anything.

(d) Cluster system IP address

This is the same as [2.3.1\(3\)\(a\) IP addressing for agent](#).

However, note the following:

- To start or stop integrated agent services, use the cluster software.
- Perform the modification on both the active server and the standby server.
- You must restart integrated agent service after changing IP addressing.

(e) IP addressing for containers

No configuration changes are required.

2.3.2 When JP1/Base is used as agent

(1) Tasks to be performed when the IP address of a manager or JP1/Base is changed

This subsection explains the tasks you must perform immediately after the IP address of a manager or JP1/Base is changed.

(a) 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.

(b) 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) Work when you change IP address of the manager or JP1/Base

(a) 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.

After setting the IP address, restart the system. For details, see [2.3.2\(3\) How to restart the system if you change the IP address of the manager or JP1/Base](#).

(b) Using IM Configuration Management

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

(c) IP address of the host where Intelligent Integrated Management Base runs

After you change the IP address of the host on which the Intelligent Integrated Management Base runs, you need to restart JP1/IM - Manager. In addition, if you are using a plug-in customized by the user, handle the situation according to the specification of the plug-in. For details about how to start JP1/IM - Manager, see [3.1 Starting JP1/IM - Manager](#).

Note that after you change the IP address of the host serving as the IM management node, you do not have to do anything.

(3) How to restart the system if you change the IP address of the manager or JP1/Base

If you change the IP address of the manager or JP1/Base, you will need to restart JP1/IM - Manager and JP1/IM - View. Here are the steps:

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.

2.3.3 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 [2.6 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, and JP1/IM - Agent 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/IM3-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	<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>
Command execution log file	All files under <code>/var/opt/jplbase/log/COMMAND/</code>
	All files under <code>shared-directory/jplbase/log/COMMAND/</code>
Event database	IMEvent*.* files under <code>/var/opt/jplbase/sys/event/servers/default/#</code>
	IMEvent*.* files under <code>shared-directory/jplbase/event/#</code>

#: 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. When you are using the Intelligent Integrated Management Base, delete the file shown in the table below.

OS	Files to delete
Windows	<code>Manager-path\data\imdd\actevent.ser</code>
	<code>Manager-path\data\imdd\imdd_nodeStatus.ser</code>
	<code>Manager-path\data\imdd\jddactseq.ser</code>
	<code>shared-folder\data\imdd\actevent.ser</code>
	<code>shared-folder\data\imdd\imdd_nodeStatus.ser</code>
	<code>shared-folder\data\imdd\jddactseq.ser</code>
UNIX	<code>/var/opt/jplimm/data/imdd/actevent.ser</code>
	<code>/var/opt/jplimm/data/imdd/imdd_nodeStatus.ser</code>
	<code>/var/opt/jplimm/data/imdd/jddactseq.ser</code>
	<code>shared-directory/jplimm/data/imdd/actevent.ser</code>
	<code>shared-directory/jplimm/data/imdd/imdd_nodeStatus.ser</code>
	<code>shared-directory/jplimm/data/imdd/jddactseq.ser</code>

8. Start JP1/Base.

9. 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

(a) When JP1/IM - Agent is used as agent

To restore agent date and time, you must make configuration changes to JP1/IM - Agent on the host. For details such as procedures, see the description in [2.5 Required steps to change integrated agent host system date and time](#).

(b) When JP1/Base is used as agent

When you reset the agent's date/time to the original date/time, you must modify the settings for JP1/Base on the applicable host. 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 Required steps to change integrated agent host system date and time

2.5.1 Changing integrated agent host system date and time

You do not need to do anything if the time is corrected in a few seconds.

To change the system date and time, perform the following steps:

1. Shut down JP1/IM - Agent servicing.
2. Change the system date and time.
3. Empty the following directory:
 - For Windows
Agent-path\data\alertmanager
Agent-path\data\prometheus
Agent-path\data\fluentd
 - For Linux
/opt/jplima/data/alertmanager
/opt/jplima/data/prometheus
/opt/jplima/data/fluentd
4. Start JP1/IM - Agent servicing.

2.5.2 Changing the system date and time on a cluster system

You do not need to do anything if the time is corrected in a few seconds.

To change the system date and time, perform the following steps:

1. Shut down JP1/IM - Agent from the cluster software.
2. If the physical host is also running, JP1/IM - Agent of the physical host is also serviced.
3. Change the system date and time on both the running and standby servers.
4. Empty the following directory:
 - For Windows
Agent-path\data\alertmanager#
Agent-path\data\prometheus#
Agent-path\data\fluentd#
Shared-folder\jplima\data\alertmanager
Shared-folder\jplima\data\prometheus
Shared-folder\jplima\data\fluentd
#: Note that both the active server and the standby server exist.
 - For Linux (note that /opt/jplima is for both the active system and the standby system.)

```
/opt/jplima/data/alertmanager#  
/opt/jplima/data/prometheus#  
/opt/jplima/data/fluentd#  
Shared-directory/jplima/data/alertmanager  
Shared-directory/jplima/data/prometheus  
Shared-directory/jplima/data/fluentd
```

#

Note that it exists on both the active server and the standby server.

5. Start all JP1/IM - Agent services from the cluster software.
6. If the physical host is also running, start JP1/IM - Agent process on the physical host.

2.5.3 Changing the system date and time in a container

You do not need to do anything if the time is corrected in a few seconds.

If you want to change the system date and time, delete the container, change the system date and time, and then re-create the container.

2.6 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.

2.6.1 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.

2.6.2 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.

2.7 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 3 - Manager Configuration Guide*.

For details about the Remote Monitoring Settings window and the System Common Settings window, see the following sections in the *JP1/Integrated Management 3 - Manager GUI Reference*.

- *5.7 Remote Monitoring Settings window*
- *5.20 System Common Settings window*

2.8 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 *8.6 Managing remotely monitored hosts* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

2.8.1 Notes on JP1/Base 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).

2.8.2 Notes on JP1/Base 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).

2.9 Tasks necessary when an Port number is changed

When you change the setting of port number to accept HTTP request on the Intelligent Integrated Management Base service, follow the procedure described below.

1. Stop the JP1/IM - Manager service.
2. Chang server.port of the Intelligent Integrated Management Base definition file (`imdd.properties`).
3. Start the JP1/IM - Manager service.

For details about the Intelligent Integrated Management Base definition file (`imdd.properties`), see *Intelligent Integrated Management Base definition file (`imdd.properties`)* in *Chapter 2. Definition Files* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

2.10 Tasks to be performed when changing the locale of integrated agent host

2.10.1 Changing the locale of integrated agent host

(1) For Windows

Use the following steps to change Windows language.

1. Shut down JP1/IM - Agent servicing.
2. Change Windows linguistic settings.

Windows linguistic settings must be consistent as follows:

Setting	Setting point	How to check
System locale ^{#1}	Control Panel - the Region window - Administration tab	Programming languages that do not support Unicode
Language and local format	Control Panel - the Region window - Format tab	Format
	Control Panel - the Region window - Location tab ^{#2}	Main use place
Country or Region	Settings - the Time and Language window - Region and Language tab ^{#2}	Country or Region
	Settings - the Time and Language window - Region tab ^{#3}	Country or Region Regional Settings
Language	Settings - the Time and Language window - Region and Language tab ^{#2}	Language
	Settings - the Time and Language window - Language tab ^{#3}	Language displayed on Windows Preferred Language
Set the region and language for the system account and welcome screen	Control Panel - the Region window - Administration tab - Copy settings button - the Welcome screen and New user account settings window	Current User Welcome screen

^{#1} Use of Unicode UTF-8 in worldwide languages is not supported.

^{#2} This applies to Windows Server 2016.

^{#3} This applies to Windows Server 2019 and Windows Server 2022.

3. Start integrated agent.

(2) For Linux

For the setting of the environment variable LANG supported by Linux environment, see *3.15.11(1) Language Settings for integrated agent* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

The configuration of LANG for running processes is described in unit definition file in the following format:

```
Environment=LANG=ja_JP.UTF-8
```

For details on how to edit unit definition file, see *2.19.2(1)(b) Changing unit definition file (for Linux only)* in the *JP1/Integrated Management 3 - Manager Configuration Guide*.

2.10.2 Changing the locale on a cluster system

This is the same as the steps in *2.10.1 Changing the locale of integrated agent host*.

However, note the following for Windows deployments:

- To start or stop integrated agent services, use the cluster software.
- Perform the modification on both the active server and the standby server.

2.10.3 Changing the locale in a container

This is the same as the steps in *2.10.1 Changing the locale of integrated agent host*.

2.11 Tasks necessary when configuration of event-forwarding relay source for integrated agent host is changed

If you change the IM configuration of the JP1/IM - Manager that is the event-forwarding relay source while using the event-forwarding relay function, follow the procedure below:

1. Restart JP1/IM - Agent.
2. Refresh Intelligent Integrated Management Base tree in JP1/IM - Manager.
If event-forwarding relay source IM management node is not displayed when the tree is refreshed, check `jima_message.log` of imagent from which the event was relayed is not erroneous.

2.12 Duplicate an integrated agent host

2.12.1 Replicating physical hosts

1. Prevent all JP1/IM - Agent services from starting automatically.

For details on disabling automatic startup, see [1.21.1\(2\) Enable and Disable of Auto-start](#) and [2.19.1\(2\) Enable and Disable of Auto-start](#) in the *JP1/Integrated Management 3 - Manager Configuration Guide*.

2. Duplicate the host and boot the replicated host.

3. Set the new host name for the replicated host.

4. Reconfigure initial secret on the replicated host.

Sets initial secret (secret for first-time connectivity) for accessing the Integration Manager.

Check initial secret in integrated operation viewer of the Integration Manager host. For details on displaying initial secret, see [2.2.3 Show Initial Secret window](#) in the *JP1/Integrated Management 3 - Manager GUI Reference*.

Reconfigure initial secret with the Secret Manager command.

```
jmimsecret -add -key immgr.initial_secret -s "initial-secret"
```

5. Deletes the individual secret registered in the replicated host.

Use the secret management command to delete an individual secret.

```
jmimsecret -rm -key immgr.client_secret
```

6. Perform the steps to change the hostname of JP1/IM - Agent.

For details about how to change the host name, see [2.2.1\(3\) Tasks when agent hostname is changed](#).

7. Restore the automatic startup setting of JP1/IM - Agent services that was changed so as not to start automatically in step 1.

For details on enabling automatic startup, see [1.21.1\(2\) Enable and Disable of Auto-start](#) and [2.19.1\(2\) Enable and Disable of Auto-start](#) in the *JP1/Integrated Management 3 - Manager Configuration Guide*.

2.12.2 Duplicate AWS/EC2 instance after operation starts

1. Prevent all JP1/IM - Agent services from starting automatically.

For details on disabling automatic startup, see [1.21.1\(2\) Enable and Disable of Auto-start](#) and [2.19.1\(2\) Enable and Disable of Auto-start](#) in the *JP1/Integrated Management 3 - Manager Configuration Guide*.

2. Create an AMI for AWS/EC2 instance.

3. Boot a new host from AMI.

4. Set the new host name to the new host.

5. Reconfigure the secret for the initial connection to the new host.

Sets initial secret (secret for first-time connectivity) for accessing the Integration Manager.

Check initial secret in integrated operation viewer of the Integration Manager host. For details on displaying initial secret, see *2.2.3 Show Initial Secret window* in the *JP1/Integrated Management 3 - Manager GUI Reference*.

Reconfigure initial secret with the Secret Manager command.

```
jimasecret -add -key immgr.initial_secret -s "initial-secret"
```

6. Deletes the individual secret registered in the replicated host.

Use the secret management command to delete an individual secret.

```
jimasecret -rm -key immgr.client_secret
```

7. Perform the steps to change the hostname of JP1/IM - Agent.

For details about how to change the host name, see *2.2.1(3) Tasks when agent hostname is changed*.

8. Restore the automatic startup setting of the process that was changed so as not to start automatically in step 1.

For details on enabling automatic startup, see *1.21.1(2) Enable and Disable of Auto-start* and *2.19.1(2) Enable and Disable of Auto-start* in the *JP1/Integrated Management 3 - Manager Configuration Guide*.

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.

1. Start the IM database (if you are using IM database).
Start the JP1/IM3-Manager DB Server service.
2. Start Intelligent Integrated Management Database (if you are using Intelligent Integrated Management Database)
Start JP1/IM3-Manager Trend Data Management Service service.
JP1/IM3-Manager Intelligent Integrated DB Server service is started automatically in conjunction.
3. Start JP1/IM - Manager.
Start the JP1/IM3-Manager Trend Data Management Service service.

To start the IM database, Intelligent Integrated Management 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 to "manual".

- JP1/IM3-Manager DB Server service (when using IM database)
- JP1/IM3-Manager Intelligent Integrated DB Server service and JP1/IM3-Manager Trend Data Management Service service (when using Intelligent Integrated Management Database)
- JP1/IM3-Manager service

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/IM3-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 Intelligent Integrated Management Database

By default, Intelligent Integrated Management Database is set not to start with JP1/Base boot control feature.

To start without using the boot control feature, start JP1/IM3-Manager Intelligent Integrated DB Server service and JP1/IM3-Manager Trend Data Management Service service from **Control Panel - Administrative Tools - Services**.

To start using the boot control feature, add the following lines to the section between [Jp1IM-Manager DB] and [Jp1IM-Manager] in JP1/Base boot order definition file.

```
[Jp1IM-GN DB]
Name=JP1/IM-Manager Intelligent Integrated DB Server
ServiceName=JP1_IMGNDDB_Service
StopCommand=Manager-path\bin\imgndb\jimngndbstop.exe
[Jp1IM-Trend Data Management]
Name=JP1/IM-Manager Trend Data Management Service
ServiceName=promscale
```

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/IM3-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).

At system startup, the autostart script runs and starts in the following order:

1. JP1/Base
2. JP1/IM - Manager
3. IM database (if you are using IM database)
4. Intelligent Integrated Management Database (if you are using Intelligent Integrated Management Database)
5. JP1/IM agent management base (if you are using a JP1/IM - Agent)

Note that the `pdprcd` process is started during system startup whether or not the automatic startup script is enabled.

For details about how to set the automatic startup script, see *2.18.2 Setting automatic startup and automatic stop (for UNIX)* in the *JP1/Integrated Management 3 - Manager Configuration Guide*. For details about the automatic startup script, see *jco_start (UNIX only)* in *Chapter 1. Commands* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API 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. Also, start the following databases when JP1/IM - Manager starts:

- IM database (if you are using IM database)
- Intelligent Integrated Management Database (if you are using Intelligent Integrated Management Database)

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_spmc_status` command. When the IM database is used, you can use the `jimdbstatus` command to check the operating status of the IM database. If you are using Intelligent Integrated Management Database, you can use `jimgndbstatus` command to check Intelligent Integrated Management Database operating status.

- 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
```

(2) Setting of integrated agent management base to use JP1/IM - Agent

The following shows how to start JP1/IM - Agent service of Integrated Manager host (UNIX).

Conditions		Operation
Physical host	When to Use integrated agent	1. Run the <code>jco_start</code> command.

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 *7.5 Registering into the cluster software during new installation and setup (for Windows)* or *8.5 Registering into the cluster software during new installation and setup (for UNIX)* in the *JP1/Integrated Management 3 - 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. IM database (if using IM database)
 - Start JP1/IM3-Manager DB Cluster Service_logical-host-name.
3. Intelligent Integrated Management Database (if using Intelligent Integrated Management Database)

Start JP1/IM3-Manager Intelligent Integrated DB Server_ *logical-host-name* and JP1/IM3-Manager Trend Data Management Service_ *logical-host-name*.

4. JP1/IM - Manager

Start JP1/IM3-Manager service.

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. You must also terminate the following databases when you terminate JP1/IM - Manager:

- IM database (if you are using IM database)
- Intelligent Integrated Management Database (if you are using Intelligent Integrated Management Database)

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

3.2.1 In Windows

Terminate in the following order.

1. JP1/IM3-Manager service
2. JP1/IM3-Manager Trend Data Management Service (if you are using Intelligent Integrated Management Database)
3. JP1/IM3-Manager Intelligent Integrated DB Server Services (if you are using Intelligent Integrated Management Database)
4. JP1/IM3-Manager DB Server Services (if you are using IM database)
5. JP1/Base

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/IM3-Manager service from **Services**.

3.2.2 In UNIX

When the automatic termination script is set, the system terminates continuously in the following order.

1. JP1/IM - Manager
2. Intelligent Integrated Management Database (if you are using Intelligent Integrated Management Database)
3. IM database (if you are using IM database)
4. JP1/Base

Although the `pdprcd` process continues running even when JP1/IM - Manager, Intelligent Integrated Management Database, and the IM database have stopped, it is not necessary to stop it.

For details about how to set the automatic startup script, see 2.18.2 *Setting automatic startup and automatic stop (for UNIX)* in the *JP1/Integrated Management 3 - Manager Configuration Guide*. For details about the automatic termination script, see `jco_stop (UNIX only)` in *Chapter 1. Commands* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

To stop JP1/IM - Manager without setting up the automatic termination script, execute the `/etc/opt/jp1cons/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_spmd_status` command. When the IM database is used, you can use the `jimdbstatus` command to check the operating status of the IM database. If you are using Intelligent Integrated Management Database, you can use `jimgndbstatus` command to check Intelligent Integrated Management Database operating status.

- To stop JP1/IM - Manager:

Physical hosts:

```
systemctl stop jp1_cons.service
```

Logical hosts:

```
systemctl stop jp1_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 jp1_cons.service
```

Logical hosts:

```
systemctl is-active jp1_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

Stop JP1/IM3-Manager_ *logical-host-name*.

2. Intelligent Integrated Management Database (if using Intelligent Integrated Management Database)

Stop JP1/IM3-Manager Intelligent Integrated DB Server_ *logical-host-name* and JP1/IM3-Manager Trend Data ManagementService_ *logical-host-name*.

3. IM database (if using IM database)

Stop JP1/IM3-Manager DB Cluster Service_ *logical-host-name*.

4. 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 Linux)

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

Storage destination: `/usr/lib/systemd/system/jp1_cons_logical-host-name.service`

Automatic startup and automatic stop script example

```

[Unit]
Description=JP1/Integrated Management - Manager logical-host-name Service
Requires=jp1_base_logical-host-name.service
After=jp1_base_logical-host-name.service
ConditionFileIsExecutable=/etc/opt/jp1cons/jco_start.cluster
ConditionFileIsExecutable=/etc/opt/jp1cons/jco_stop.cluster

[Service]
ExecStart=/etc/opt/jp1cons/jco_start.cluster logical-host-name
ExecStop=/etc/opt/jp1cons/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.

After creating an automatic start or automatic stop script for a logical host, run the following command to set permissions.

```

chmod 644 /usr/lib/systemd/system/jp1_cons_logical-host-name.service
chgrp root /usr/lib/systemd/system/jp1_cons_logical-host-name.service
chown root /usr/lib/systemd/system/jp1_cons_logical-host-name.service

```

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

```
# systemctl --system enable jp1_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:

```
# systemctl daemon-reload
```

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 `jp1_spm_status` command. When the IM database is used, you can use the `jp1dbstatus` command to check the operating status of the IM database.

- Starting JP1/IM - Manager

Physical hosts:

```
systemctl start jp1_cons.service
```

Logical hosts:

```
systemctl start jp1_cons_logical-host-name.service
```

- Stopping JP1/IM - Manager

Physical hosts:

```
systemctl stop jp1_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
```

3.3.3 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
<code>/etc/rc.d/rc3.d/S99_JP1_20_CONS</code>	<code>/etc/rc.d/rc0.d/K01_JP1_80_CONS</code>
<code>/etc/rc.d/rc5.d/S99_JP1_20_CONS</code>	<code>/etc/rc.d/rc6.d/K01_JP1_80_CONS</code>

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).

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 2.8 *JP1/IM - Manager service* in the *JP1/Integrated Management 3 - 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/IM3-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/IM3-Manager service (in Windows) is 125 seconds. The timeout period for the `jco_start` command (in UNIX) is 300 seconds. For details about setting the timeout for the `jco_start` command, see 14.7.11 *Considering the timeout period during startup or stop of JP1/IM - Manager (in UNIX)* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

- 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.
- If you terminate hosts from JP1/Power Monitor by using the default description example given in the JP1/Base startup sequence definition file (`jp1svprm.dat`), KAVA4516-E is output to the event log in the service termination processing for the IM database.

To restrict the output of KAVA4516-E, change the definition of the startup sequence definition file as follows:

- For a physical host

(1) Create a batch file that has the following content with any file name:

```
Manager-path\bin\imdb\jimdbstop.exe  
net stop HiRDBEmbeddedEdition_JM0
```

(2) Set the startup sequence definition file in a way such as the following:

The following shows the settings to set when the name and storage destination of the batch file created in step (1) is "C:\jp1\jp1imdbstopservice.bat":

```
[Jp1IM-Manager DB]  
Name=JP1/IM-Manager DB Server  
ServiceName=HiRDBEmbeddedEdition_JM0  
StopCommand=C:\jp1\jp1imdbstopservice.bat
```

- For a logical host

(1) Create a batch file that has the following content with any file name for each logical host:

```
Manager-path\bin\imdb\jimdbstop.exe -h logical-host-name  
net stop HiRDBClusterService_JMn#
```

#: *n* is a number in the range from 1 to 9. Use the value specified for LOGICALHOSTNUMBER in the cluster setup information file.

(2) Set the startup sequence definition file in a way such as the following:

The following shows the settings to set when the name and storage destination of the batch file created in step (1) is "C:\jp1\jp1imdbstopservice.bat":

```
[Jp1IM-Manager DB]  
Name=JP1/IM-Manager DB Cluster Service_logical-host-name  
ServiceName=HiRDBClusterService_JMn#  
StopCommand=C:\jp1\jp1imdbstopservice.bat
```

#: *n* is a number in the range from 1 to 9. Use the value specified for LOGICALHOSTNUMBER in the cluster setup information file.

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 a Web browser to log in to JP1/IM - Manager (Intelligent Integrated Management Base)

To use a Web browser to log in to JP1/IM - Manager (Intelligent Integrated Management Base):

1. In WWW browser, specify URL of JP1/IM - Manager (Intelligent Integrated Management Base) to connect to and show Login window.

The format of URL is as follows:

`Http:// Intelligent Integrated Management server hostname:portnumber /login`

Note

`https` when using SSL communication.

For the port number of URL, specify the port number (defaults to 20703) of Intelligent Integrated Management Base that you configured in Intelligent Integrated Management Base definition file (`imdd.properties`).

For details, see *Intelligent Integrated Management Base definition file (imdd.properties)* in Chapter 2. *Definition Files* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

2. In the Login window, enter your user name and password.

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.

3. Click the **Log In** button.

The window for the integrated operation viewer opens.

4.1.2 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 3 - 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 *1.2.2 Login window of Central Consol and Central Scope* in the *JP1/Integrated Management 3 - 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.

(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 3 - View**, and then **Configuration Management**.

The Login window opens.

If **Configuration Management** is removed from the Windows **Start** menu, you must 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 *1.20.3 Setting up and customizing IM Configuration Management - View (for Windows)* in the *JP1/Integrated Management 3 - 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.

4.1.3 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 [4.1.2 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 *JP1/Integrated Management 3 - Manager Command, Definition File and API 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 [4.1.2 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 *JP1/Integrated Management 3 - Manager Command, Definition File and API 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 (Intelligent Integrated Management Base):

- In the Integrated Operation Viewer window, from the **File** menu, choose **Logout**.

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.

When you log out of JP1/IM - Manager (Central Console), the user profile will be updated and the user environment for the event console, such as the column widths and whether the view filter is enabled or disabled, is saved.

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.

If you exit it without logging out of it, the login information remains on the manager, ultimately leading to a potential lack of resources for the manager. Make sure that you exit it using the logout operation.

5

System Monitoring from the Intelligent Integrated Management Base

This chapter explains how to use the Intelligent Integrated Management Base to monitor your system. Note that the integrated monitoring database and the event-source-host mapping definition must be enabled to monitor the system through the Intelligent Integrated Management Base.

5.1 Viewing the system status

When you enable the event-source-host mapping function, the **Operating status** area of the integrated operation viewer window shows the status of the systems that are registered in the integrated monitoring database for the manager to which the user has logged in. If a change occurs in the system, the window is refreshed automatically to show the latest status at all times.

By viewing the status of a system through the integrated operation viewer window, you can:

- View the systems you are managing and their status at a glance.
- Detect problems during job operation to avoid serious obstacles to business.
- Identify where a failure occurred in the system and know whether a serious event occurred.
- See which managed systems are affected by a failure in order to grasp the cause of it.
- See the color of the item shown in the sunburst chart, tree chart, or node status panel on dashboard to understand how high or low the priority of handling the failure is (urgency).
- See Alert information for Various IT Resources
- See trend information of various IT resources

5.1.1 What Intelligent Integrated Management Base can monitor

Intelligent Integrated Management Base allows you to monitor "System Health", "JP1 Events", "related node", "Alerts on Various IT Resources", and "trend information on Various IT Resources".

- System Status
Sunburst and Tree can be monitored in a hierarchical structure.
On dashboard, you can monitor the nodes that you want to see only by selecting.
- JP1 Event
On the event list screen, you can narrow down by a node or by error status. The dashboard allows you to monitor the number of critical events that have occurred and the number of events for each action.
- Related node
You can view the relationship of nodes graphically.
- Alerts for Various IT Resources
The dashboard allows you to visually monitor the number of occurrences per selected node.
- Trend information for various IT resources
Trend information of the selected node can be displayed in graph on the [Trend] tabbed page. The dashboard allows you to monitor trend information of selected nodes in graphical, gauge, numeric, and ranking formats.

5.1.2 Items displayed in the sunburst chart or the tree chart

In the sunburst chart or the tree chart of the **Operating status**, the items shown in the following table are shown hierarchically.

Table 5–1: Items displayed in the sunburst chart or the tree chart

Display item	Explanation
System name	It displays the name of the system or subsystem.
Host name	It displays the name of the host in the system.
Category name	This item shows the group that the monitoring target is in.
Scheduler service name/job group name	If a link with JP1/AJS is enabled, the scheduler service name of JP1/AJS and its job group name are displayed as one component.
Root jobnet name	If a link with JP1/AJS is enabled, the name of the root jobnet in the job group is displayed.
Service name for the monitoring agent of JP1/PFM	If a link with JP1/AJS is enabled, the service name of the monitoring agent collected from JP1/PFM - Manager is displayed.
Name of the installed product	The name of the installed JP1 product (such as JP1/Base, JP1/AJS, JP1/PFM, or JP1/IM - Manager) is displayed.

The following figure shows a display example of the **Operating status** area.

Figure 5–1: Example of changing the Operating status area



The color of each item means how healthy the system is. If the system is healthy, the item is shown in *green*, which means Normal/Resolved. *Yellow* means a Warning, *orange* means an Error, and *red* indicates that an Emergency/Alert/Critical failure has occurred.

When you click an item, the information related to the item you selected is displayed in the **Details** area.

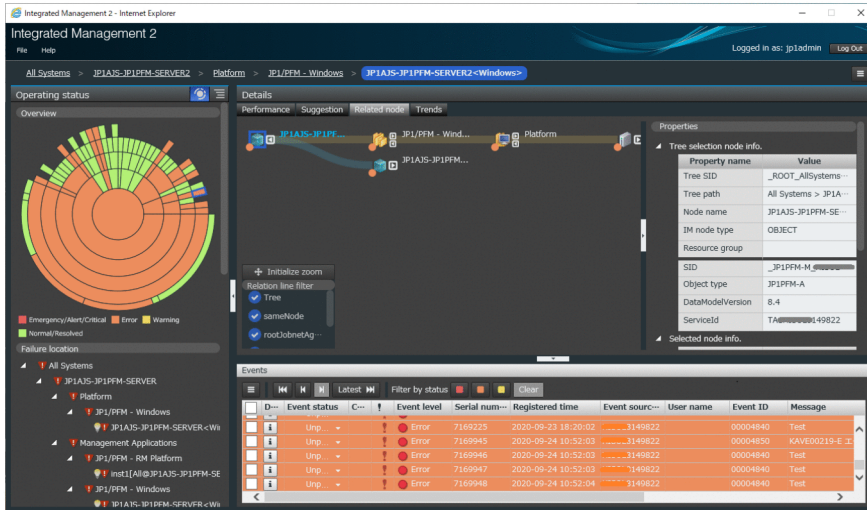
5.2 Viewing JP1 events (Events window)

By checking the attributes and response status of the system on the event window, you can operate as follows.

When you select an item in the **Operating status** area or the **Details** area of the integrated operation viewer window, ongoing JP1 events for the selected item are listed in the **Events** area.

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.

Figure 5–2: Events window display example



The following types of events are displayed in the events list:

- Event registered in the integrated monitoring database
- Event that occurs from the selected item and an event that occurs from one of all the underlying items
- Item that a logged-in user has access permissions to, if a resource group or business group is set up
- Event that passed a filter according to the event receiver filter setting, if the event receiver filter is set up

By viewing the system attributes and the event status in the Events window, you can:

- Check the status of the system where a failure occurred, because you can narrow down the events related to the system easily.
- Carefully examine the cause of the failure and how to handle it with the details of the event.
- Change an event status easily.
- For consolidation events, you can see the repeating events that have been consolidation on the repeated event list window by displaying the repeated event list window.

The repeat event List window is displayed by clicking the **Repeated event list** menu in the event list.

- If the event is a monitor started event, you can start the application window for the event and see more information about the event.









You can start the monitor from the **monitor** menu in the event list.

5.2.1 Items displayed in the events list

The events list displays the attribute items (basic attributes, common extended attributes, and program-specific extended attributes) of each event. The displayed items cannot be changed.

The following table lists the items (columns) displayed in the events list.

Table 5–2: Items displayed in the events list

Display item (column name)	Explanation
Event status	It displays the status (<i>Processed</i> , <i>Processing</i> , <i>Held</i> , and <i>Unprocessed</i>) of the JP1 event. In the case of a consolidation event, the event status of the consolidation start event is displayed. If the event status of the consolidation start event differs from the event status of a repeated event consolidated with it, an exclamation mark (!) is displayed in the Event status column of the consolidation start event.
Consolidation event	A consolidation start event displays  .
! (Severe event)	If an event is a severe event, it displays  . A consolidation start event displays  if it is a severe event. When repeated events consolidated as a severe event actually consist of not only severe events but also non-severe events, an exclamation mark (!) is displayed.
Event level	It indicates the urgency of a JP1 event. From the most urgent to the least urgent, the value can be: <i>Emergency</i> , <i>Alert</i> , <i>Critical</i> , <i>Error</i> , <i>Warning</i> , <i>Notice</i> , <i>Information</i> , and <i>Debug</i> . 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.
Serial number	Order in which the JP1 event arrived at this event server, regardless of the source.
Registered time	Time at which a JP1 event was registered in the event database of the event-issuing host.
Event source host	Name of the agent that registered the JP1 event (source event server).
User name	Name of the user that issued the JP1 event.
Event ID	Value that indicates the source program or the event that occurred.
Message	Message text that shows the content of the JP1 event.
Object type	Character strings, such as <i>JOB</i> and <i>JOBNET</i> , that indicate the type of object where the event that triggered event generation occurred.
Action	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. If a large number of events occur while the corresponding action is suppressed by the repeated event monitoring suppression function,  is displayed in the Events window. When an event is not the target of action execution due to the common exclusion-conditions,  (action-excluded event) is displayed. When the action status differs between a consolidation start event and repeated events, an exclamation mark (!) is displayed in the Action column.

Width of the item column

You can change the width of the column for the item displayed in the events list with the drag operation of the mouse. You can also drag the column itself to change the order of the columns.

Background colors for severe events

For a severe event, one of the colors shown in the following table is applied depending on the event level displayed in the **Events** area:

Table 5–3: Background colors for severe events




Event level	Event status	Background color
Warning, Notice, Information, Debug	Other than Processed	Yellow
Error		Orange
Emergency, Alert, Critical		Red
None of the above	Processed	White (no background color)

Event response status

For any event for which the JP1 event response status is specified, an event status and an icon are displayed at the leftmost column of the events list.

The table below lists the event status types and the corresponding event status icons. Choose the event status to set for each situation based on the operation.

Table 5–4: Event status types and event status icons

Event status	Event status icon
Processed	
Processing	
Held	
Unprocessed	(No icon)

The specified event status is registered in the logged-in manager's integrated monitoring database or event database. (For a JP1 event that has been forwarded from a different host, the information in the integrated monitoring database or event database of the forwarding source host is not changed.) Consequently, the event 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.

Upper limit of the number of events that can be displayed on the screen

The upper limit of JP1 events that can be displayed on the screen is 100. If the number of JP1 events exceeds the upper limit of JP1 events that can be displayed, 100 events from the latest event are displayed. You can view 101st and later events sequentially by moving to the next page.

Refresh of the Events window

The Events window refreshes automatically after the Intelligent Integrated Management server is checked for new events at regular intervals. The window is updated automatically only if the latest events are displayed. The window is not updated automatically if past events (101st and later events) are displayed. In addition, you cannot change the update interval.

Note that if you update the window manually, the latest events are displayed.

Status filtering

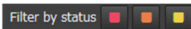
You can filter the events to be displayed in the Events window by using the  **Filter by status** button. With the colors of the buttons, the events shown in the following table can be filtered:

Table 5–5: Button color and Event to be filtered

Button color	Event to be filtered	
	Event level	Event status
Yellow	Warning, Notice, Information, Debug	Other than Processed
Orange	Error	
Red	Emergency, Alert, Critical	

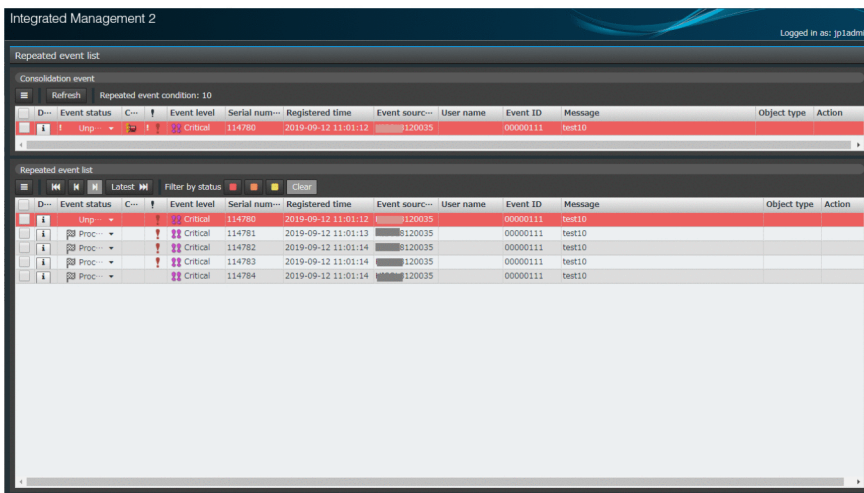
You can turn on all the buttons. If the filtering mode is changed, the latest events (100 events) are collected to refresh the events list with the settings after the change.

5.2.2 Displaying Repeated event list window

The Repeated event list window shows consolidation events and consolidated repeated events in a list. This window allows you to process the event status of all consolidation events displayed in the list.

To display the Repeated event list window, select a consolidation start event, and click the **Operation menu** button, and then **Repeated event list**.

Figure 5–3: Repeated event list window example



For details about the items displayed in the Repeated event list window, see *Chapter 2. Integrated Operation Viewer Window* in the *JP1/Integrated Management 3 - Manager GUI Reference*.

5.2.3 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 of the Events window, click **i** of the JP1 event of which you want to display the attribute. The Event Detail dialog opens in a separate window.

5.3 Add metric for Trend Viewing and Alerting

You can add metrics for JP1/IM - Agent trend viewing and alerting.

For metrics handled in trend viewing, see 3.15.6 (3) *Return metric List* and 3.15.6 (4) *Return of trend data* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*, and for metrics handled in alerting, see 3.15.1 (3) *Performance data monitoring notification function* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

The configuration steps for adding metrics are as follows:

1. Exporter Settings

If Exporter has not collected metric you want to add, configure the settings to collect them. Different Exporters are configured differently. For details, see 3.15.1(1)(i) *Blackbox exporter (Synthetic metric collector)*, 3.15.1(1)(d) *Node exporter (Linux performance data collection capability)*, 3.15.1(1)(c) *Windows exporter (Windows performance data collection capability)*, and 3.15.1(1)(g) *Yet another cloudwatch exporter (Azure Monitor performance data collection capability)* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

Restart Exporter after configuring the settings. (For Blackbox exporter, you can perform a reload instead of a reboot.)

2. Edit the Prometheus configuration file

In scrape definition of Prometheus configuration file (`jpc_prometheus_server.yml`), change the `metric_relabel_configs` settings to ensure that metric of Exporter used by PromQL expression is not removed. Specifically, `metric_relabel_configs` the new metric name to be used by the Exporter where the importer's metric names are listed in the next regex. If it has already been added, no additional is required.

Here is an example of adding the "aws_ec2_network_in_average" metric in the Yet another cloudwatch exporter (add an underline):

```
- job_name: 'jpc_cloudwatch'
...
  metric_relabel_configs:
  ...
    - source_labels: ['__name__', 'jpl_pc_nodelabel']
      regex: '(aws_ec2_network_in_average|aws_ec2_cpuutilization_average|.
..);.+${'
      action: 'keep'
```

For details about the Prometheus configuration file, see *Prometheus configuration file (jpc_prometheus_server.yml)* in *Chapter 2. Definition Files* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

3. Edit the alert configuration file (if you want to add metrics to be handled by the alert)

Add a metric to the alert definition in the alert configuration file and write a PromQL statement using the added metric in the expression of the alert.

For details about the alert configuration file, see *Alert configuration file (jpc_alerting_rules.yml)* in *Chapter 2. Definition Files* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

4. Restarting or reloading the Prometheus server service

Restart or reload the Services of the Prometheus server on the host where you edited the Prometheus configuration file and the alert configuration file.

5. Edit the metric definition file (if you want to add metrics to be handled in the trend display)

The return function of the metric list returns the metric defined in the metric definition file. The metric definition file exists for each Exporter. Check the Exporter of the IM management node to which you want to add the metric, and add the metric definition to the metric definition file for the exporter.

For details about the metric definition file, see the metric definition file for each Exporter in *Chapter 2. Definition Files* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

After editing the metric definition file, the information in the updated metric definition file is reflected when you perform one of the following operations:

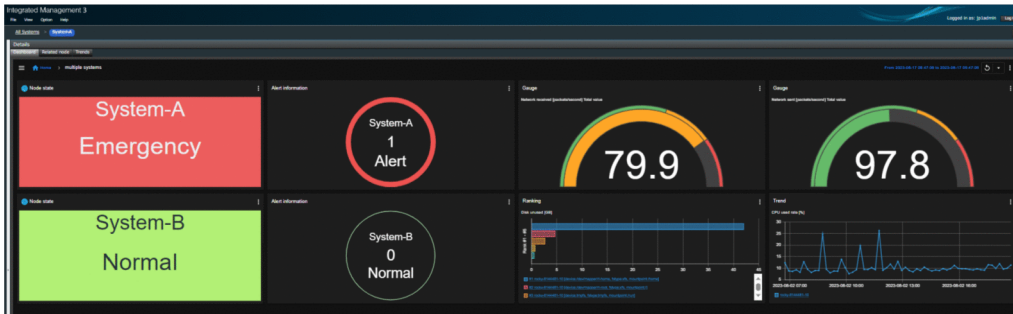
- Refresh the **Trends** tab in the Integrated Operations Viewer
- Refresh the **Dashboard** tab in the Integrated Operation Viewer
- Run the JP1/IM - Manager Metrics List Acquisition API
- Run the JP1/IM - Manager Time Series Data Acquisition API

5.4 How to look at the dashboard

In the dashboard, you can see Node Status, Alerts on Various IT Resources, trend information on Various IT Resources, and Critical Event Count. For Alerts for Miscellaneous IT Resources, trend information for Miscellaneous IT Resources, and Critical Event Counts, you can view the info for the duration specified in the dashboard.

You can create dashboards for each IM management node, so you can create dashboards that monitor the entire system, as well as for each subsystem or server. Note that you can create different dashboards for each user by customizing the auto-generated dashboards that are displayed by default for each IM management node. For the procedure for creating dashboards, see the *JPI/Integrated Management 3 - Manager Configuration Guide*.

Figure 5–5: The sample of the Dashboard window



You can monitor node-status, alert-information, and trend information for various IT resources side-by-side on a single screen.

For details about how to navigate the Dashboard, see the *JPI/Integrated Management 3 - Manager GUI Reference*.

5.4.1 For viewing dashboards

(1) Display in the Dashboard tab

When the Integrated Operation Viewer window is displayed, the **Dashboard** tabbed page is displayed in **Details** area. This tab shows the dashboard corresponding to IM management node selected in the **Operating status** area. By default, the auto-generated dashboard is displayed.

(2) Open the Dashboard List dialog box

If you have customized the auto-generated dashboard or created a new dashboard, select **View** and then **Dashboard List** from the Integrated Operation Viewer window menu. The Dashboard List dialog box is displayed. Click a title in the list to display the selected dashboard.

(3) Display in full screen

You can view the dashboard in full screen by clicking **Full screen display** in the operation menu of the dashboard displayed in a tab. To cancel full screen, press **Esc** key or the [x] button displayed by mouse-over to the upper part of the display.

(4) Open in a separate window in Web browser

You can display the Dashboard window in another window of Web browser by clicking **Open in another window** in the operation menu of the dashboard displayed in a tab.

(5) View in another Web browser tab/in Web browser of another device

You can open the Dashboard window by accessing URL of the dashboard from another tab in Web browser or from Web browser of another device.

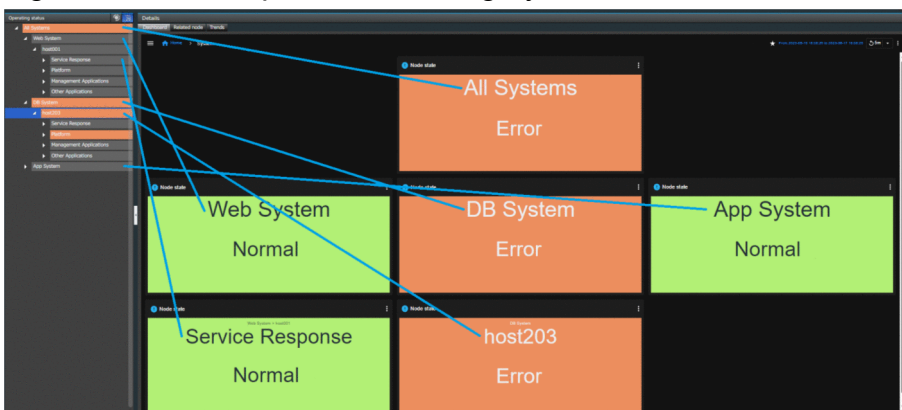
Here's how to get URL for a dashboard:

1. In the integrated operation viewer, view the dashboard of interest.
2. Select **Copy dashboard URL** menu from the operation menu of the displayed dashboard.
3. In the Copy dashboard URL dialog box, click the **Copy to clipboard** button.

5.4.2 IM management node status monitoring

In the dashboard, you can select only IM management node that you want to monitor in the tree and monitor them side by side in the dashboard.

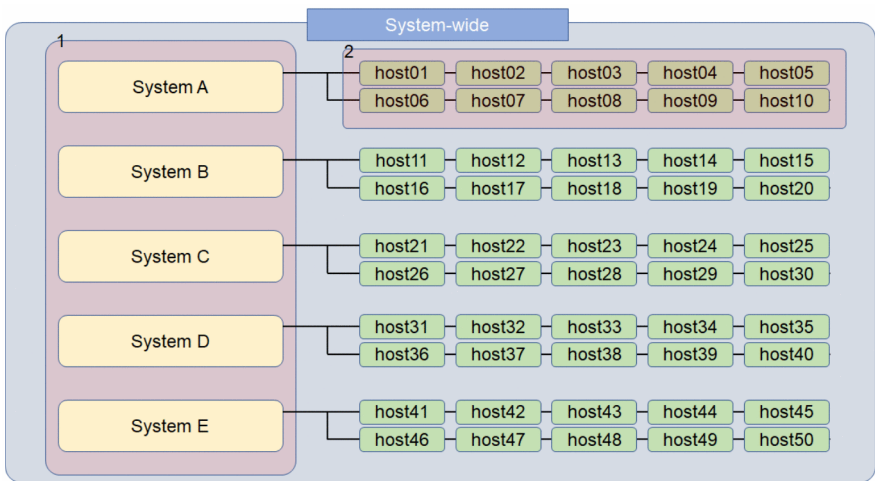
Figure 5–6: Example of monitoring by IM node state



(1) Monitoring with the Node Status Panel

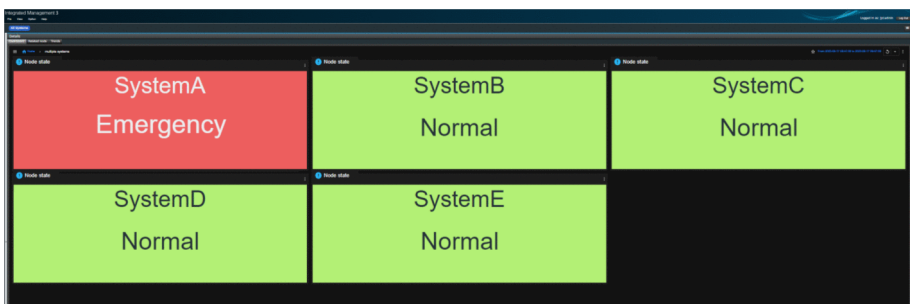
The following shows an example of monitoring "(1) Whole system" and an example of monitoring "(2) System A" of a part of the system in the following system configurations.

Figure 5–7: System configuration example



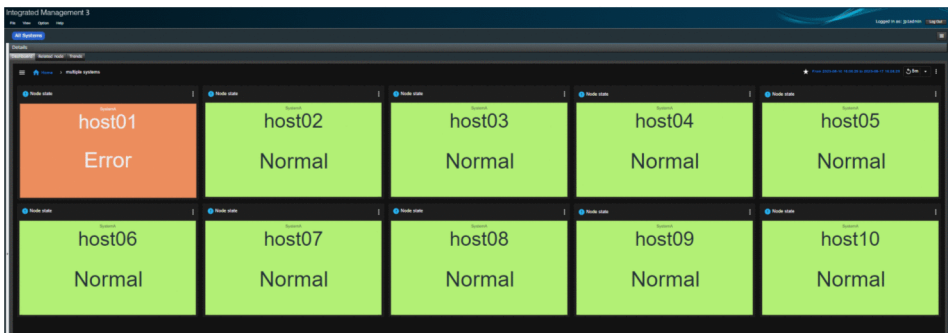
Monitor the whole system.

Specify node state monitoring per system in the dashboard, and define the panels that monitor the nodes of "System A", "System B", "System C", "System D", and "System E" to understand the overall system status.



Monitor system A

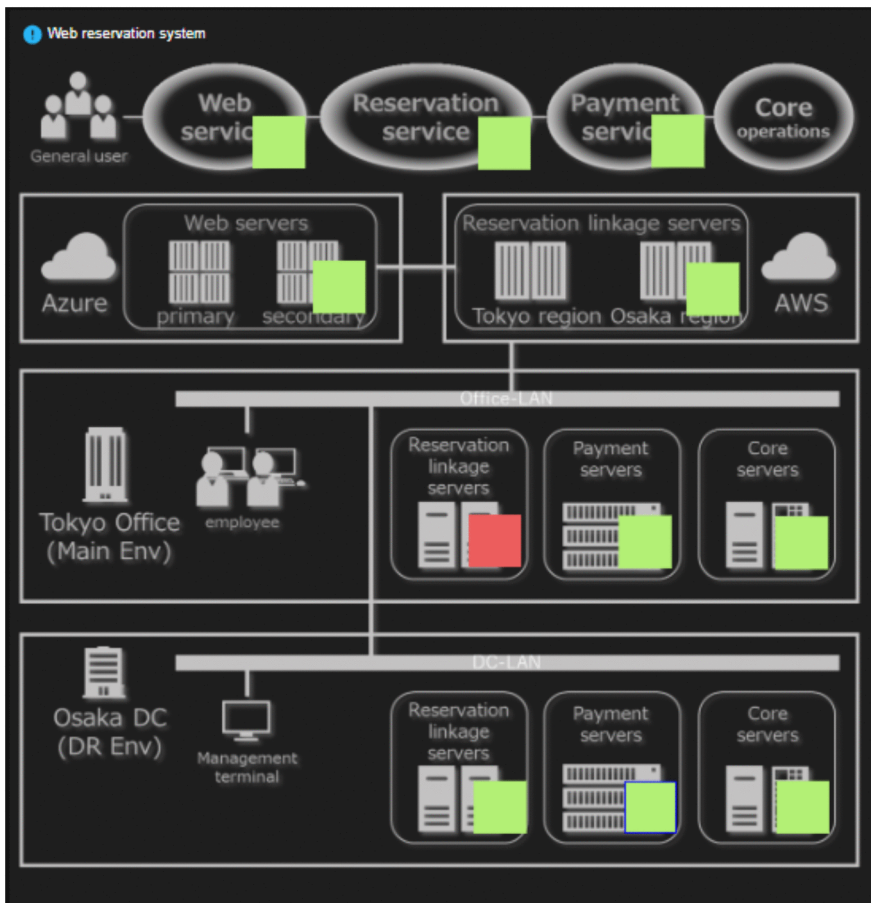
You can understand the status of System A by specifying node status monitoring per host in the dashboard and defining panels that monitors nodes from "host01" to "host10".



(2) Monitoring with Node state map

With Node state map monitoring, you can specify a background image to show the status of the node on the background image. In the following example, you can see the status of a node with small green or red square status icon.

Figure 5–8: Example of monitoring with Node state map

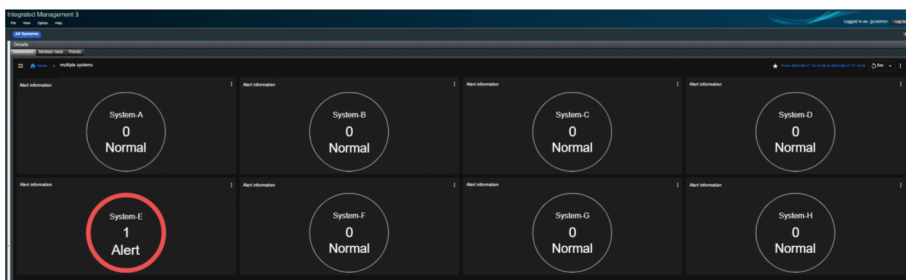


5.4.3 Monitoring with alert information

JP1/IM - Agent provides threshold monitoring for various IT resource performance data. The dashboard allows you to view as alert info the number of times the threshold is exceeded, and the alert notification is in "firing" status. If more than one alert occurs, the number is added and displayed.

In the [Alert Info] pane of the dashboard, you can check the number of alerts occurring under any IM management node.

Figure 5–9: Example of alert monitoring

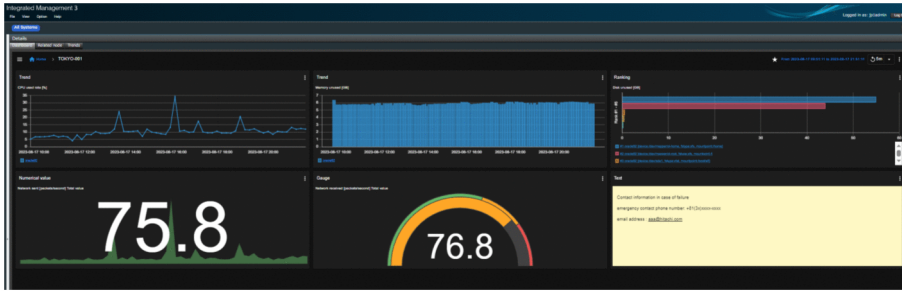


5.4.4 Checking various IT resources

You can see the properties of the various IT resources visually.

You can choose from line charts, bar charts, numbers, gauges, and ranking formats.

Figure 5–10: Example of displaying various IT resources



Select the display format according to the characteristics and visibility of the data. Target metric is the number of metric and JP1 events (number of critical events) collected by JP1/IM - Agent performance monitoring, including OS performance information, external monitoring information on URL and ICMP, cloud monitoring information, and container monitoring information.

If an error is detected in IT resource, you can check the various IT resource information of the target host and check the status before and after the occurrence time.in dashboard.

In addition to the most recent situation, you can also display the past situation side by side, so you can also check whether it suddenly became abnormal or gradually approached abnormal from the previous day.

Figure 5–11: Example of displaying a graph of the past status on the right



5.4.5 Flow of Problem Investigation and Response Based on Dashboard

This section explains the operation workflow from monitoring to investigation when using dashboards.

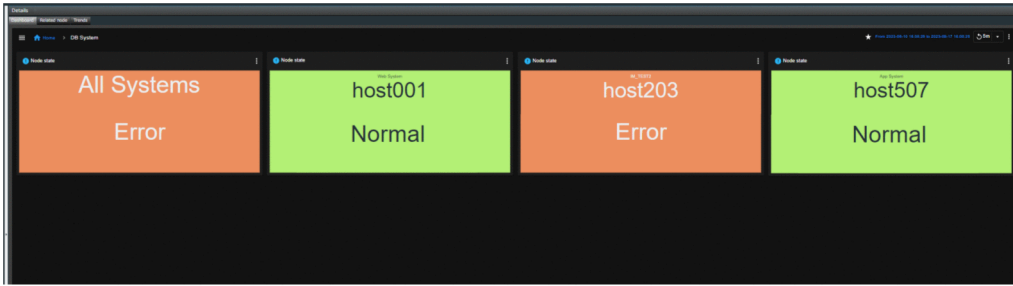
(1) Sequence of actions from IM management node status monitoring

The [Node Status] pane can be monitored in units of IM management node.

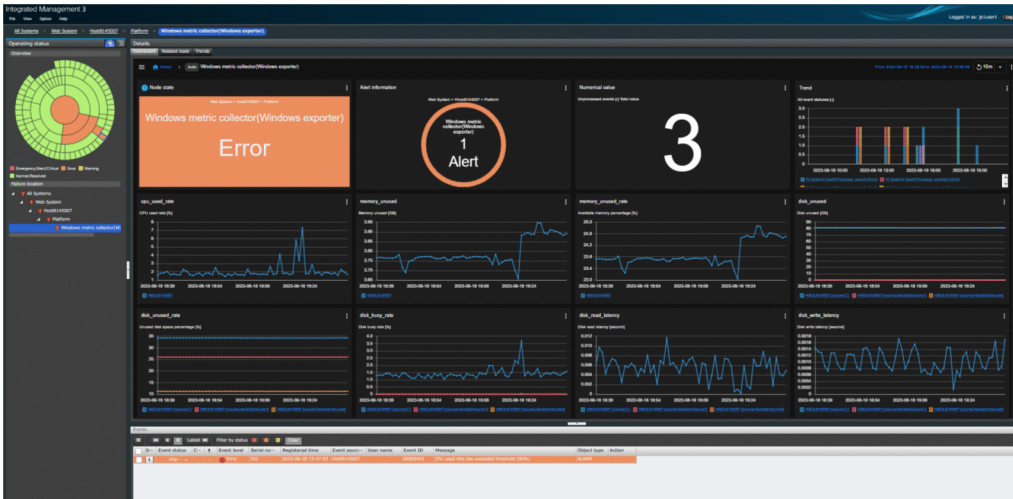
For example, if the entire system consists of eight systems, you can define eight node state monitors per system in the dashboard to monitor the entire system.

The procedure for monitoring is as follows.

1. Start monitoring.
2. When an error occurs, the color of the corresponding system panel changes.



3. Clicking the corresponding colored panel changes IM management node in the tree to the selected state.



4. In the [Event List] window, only events under the corresponding IM management node are filtered.

5. In the event list, check the "Event Detail" message of the relevant event, identify the cause, and investigate.

Attribute name	Attribute value
Serial number	292
Event ID	00000403
Process ID	0
Registered time	2023-08-18 15:47:03
Arrived time	2023-08-18 15:47:03
User ID	-1
Group ID	-1
User name	root
Group name	
Event source host	Host8145007
Source event server name	Rocky-8145007
Source IP address	10.164.205.232
Source serial number	292
Event level	Error
Product name	/HITACHI/JP1/JPCCS2
Object type	ALARM
Object name	cpu_used_rate(Windows exporter)
Occurrence	NOTICE
Date and time of alert firing	2023-08-18 15:46:58
Hostname of monitoring agent	Host8145007
Scrape job	jpc_windows
jp1_pc_nodelabel	Windows metric collector(Windows exporter)
Exporter name	JPC Windows exporter
metric name	windows_logical_disk_free_bytes
Component name	/HITACHI/JP1/JPCCS/CONFINFO
Message	CPU used rate has exceeded threshold (90%)

6. If the cause is related to OS resources or process performance, use dashboard to trend parse OS resources and investigate the cause.



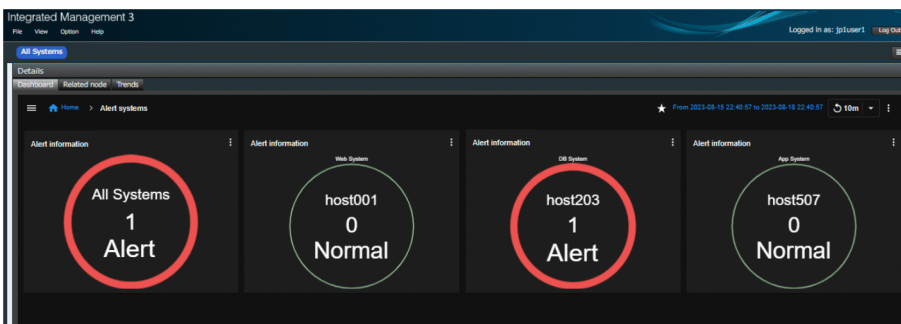
(2) Series of operations from alert information monitoring

Alert-information can be monitored on a system-by-system or host-by-host basis, for example, in IM management node.

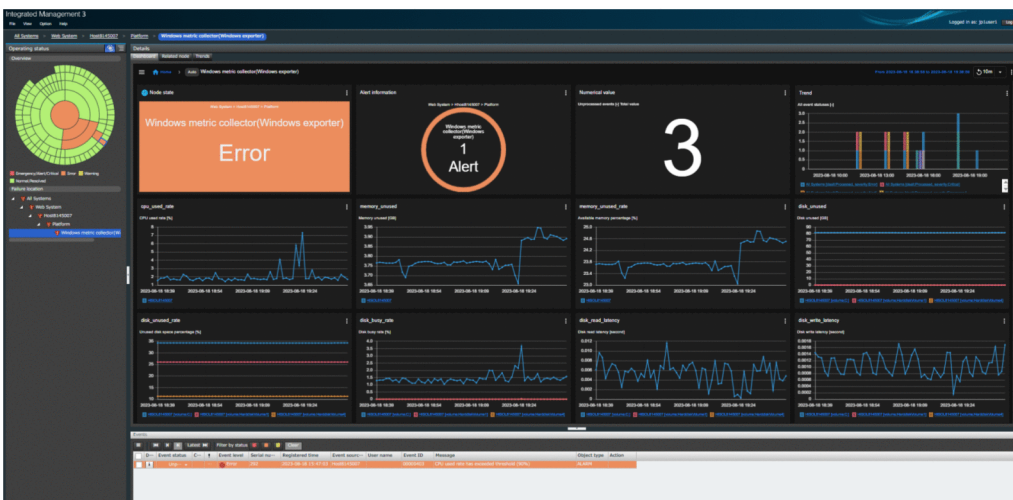
For example, if a system consists of 16 hosts, you can monitor alert information for the system by defining alert information monitoring on a per-host basis in the dashboard.

The procedure for monitoring is as follows.

1. Start monitoring.
2. When an alert occurs, the color of the Alerts panel for that host changes and displays the number of alerts occurring.



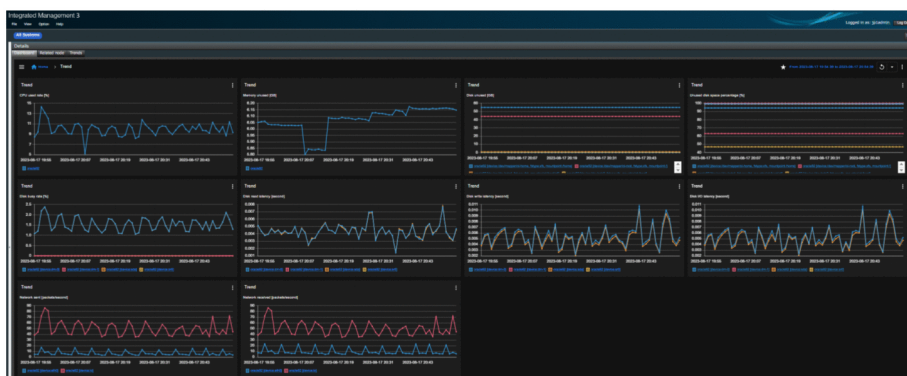
3. Clicking on the corresponding coloured pane displays a list of IM management node and the alerts that have occurred, and you can also see the time of occurrence. Clicking the displayed IM management node changes to the tree selection.



4. In the [Event List] window, only events under the corresponding IM management node are filtered.
5. From the event list, check the "Event Detail" message of the relevant event judging from the alert occurrence time, identify the cause, and investigate.

Attribute name	Attribute value
Serial number	292
Event ID	00000403
Process ID	0
Registered time	2023-08-18 15:47:03
Arrived time	2023-08-18 15:47:03
User ID	-1
Group ID	-1
User name	root
Group name	
Event source host	Host8145007
Source event server name	Rocky-8145007
Source IP address	10.164.205.232
Source serial number	292
Event level	Error
Product name	/HITACHI/JP1/JPCCS2
Object type	ALARM
Object name	cpu_used_rate(Windows exporter)
Occurrence	NOTICE
Date and time of alert firing	2023-08-18 15:46:58
Hostname of monitoring agent	Host8145007
Scrape job	jpc_windows
jp1_pc_nodelabel	Windows metric collector(Windows exporter)
Exporter name	JPC Windows exporter
metric name	windows_logical_disk_free_bytes
Component name	/HITACHI/JP1/JPCCS/CONFINFO
Message	CPU used rate has exceeded threshold (90%)

6. If the cause is related to OS resources or process performance, use the dashboard to trend parse OS resources and investigate the cause.



5.4.6 Notes

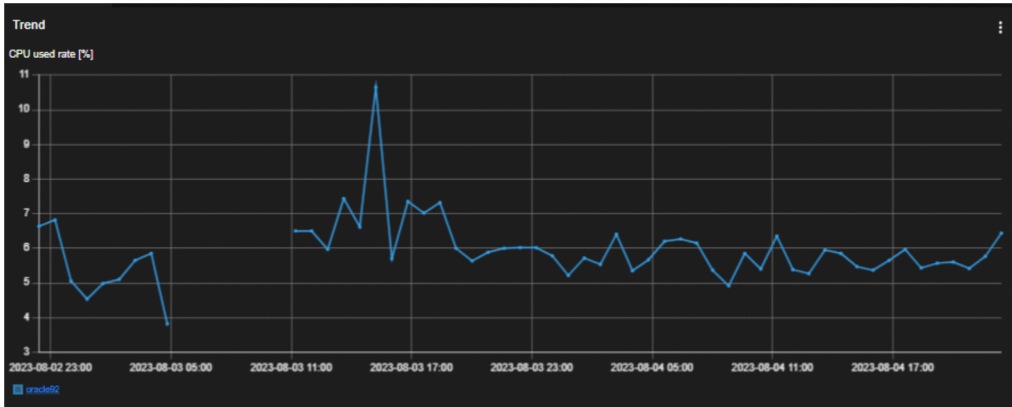
- If you want to delete a JP1 user, please delete the dashboard created by the JP1 user in advance. Deleting a JP1 user does not automatically delete the dashboard. If the JP1 user does not already exist, create the JP1 user again and delete the dashboard created by the JP1 user.
- The vertical axis of the graph in the Trend panel of the dashboard dynamically changes the minimum and maximum values depending on the contents of the data in the range to be displayed. Note that the minimum and maximum values of the vertical axis change even when continuously monitored.

If you want to fix the minimum and maximum values, set the Minimum and Maximum values when setting the panel.

In particular, care should be paid to the difference between the minimum and maximum values of the vertical axis of the two graphs compared to the past. If you want to compare on the same scale, specify the same minimum and maximum values for both.

The period of metric data that can be displayed in the dashboard is the period stored in the trend data management DB.

- If there is no data for the metric, "NO DATA" is displayed in the panel.
- If performance data cannot be collected temporarily due to a monitored outage, the lines in the graph are displayed in a broken state, as follows:



5.5 Viewing links with other products

In the Intelligent Integrated Management Base, you can monitor data from other linked products with the integrated operation viewer.

5.5.1 Using signs to avoid failures (link with JP1/AJS)

To see the sign of an operational failure, such as a higher load on JP1/AJS, in the event notification and avoid the failure:

1. In the Events window, click the **Detail** button for the event of which a sign is notified.
The Event Detail dialog box is displayed.
2. Check the event guide information and **Message**.
3. Check the operating status of the scheduler service in the **Trends** tab.
A graph of the trend information for the selected event is displayed.
4. Click the **[+] Add node** button to select a node with performance data of the host where the job is executed.
A graph of the performance data of the host where the job is executed is displayed.
5. Compare the graph shown in step 3 with the one shown in step 4.
Compare the trends to determine how extensive the failure is and isolate the cause of it.
6. Based on the resulting isolated cause of the failure, give instructions to the person in charge to avoid it.

5.5.2 Understanding how extensive a problem that occurred during operation of a job is and handling it (link with JP1/AJS)

To understand the cause of a problem that occurred during operation of a job and how extensive it is:

1. Click the location where a problem occurred in the **Operating status** area.
You can see the location in red, orange, or yellow on the sunburst chart or the tree chart.
2. The following information of the root jobnet you clicked is displayed in the **Job flow** tab.
 - Relation with the preceding and following root jobnets
 - Whether it affects the following root jobnets
 - List of ongoing events
3. Click the icon shown before the node to open the Linked unit dialog box.
Check the following unit to be affected and its expected start date and time.
4. Click the link of the following unit to open a monitor window of JP1/Web Console.
Deal with the following unit to be affected.

5.5.3 Understanding in advance which root jobnets are affected before the definition or content of a job is changed (link with JP1/AJS)

To understand potentially affected root jobnets in advance before changing the definition or content of a job:

1. Click the root jobnet you are going to change.
2. Check the **Job flow** tab or **Related node** tab.
The nodes related to the root jobnet you are going to change are displayed.
3. Refer to the displayed root jobnet name and the information in **Properties** to understand whether the change will have an effect and how extensive the effect is.


5.5.4 Checking performance data and handling the problem (link with JP1/PFM)

To check the status of a related infrastructure to determine whether it caused a job to terminate abnormally:

1. Click the location where a problem occurred in the **Operating status** area.
You can see the location in red, orange, or yellow on the sunburst chart or the tree chart.
2. Check the target agent of the job in the **Related node** tab.
Expand the layer of the related node and check the target agent of the job.
3. Add the node for the target agent in the **Trends** tab to show the graph of performance data.
Check events on the target agent.
4. Open the **Performance** tab.
Select a report related to the applicable metric, identify a process with high usage of resources, and handle the problem.
For details about the Custom UI window of JP1/PFM, see the descriptions on JP1/PFM - Web Console in JP1/PFM manuals of version 12-10 or later.

5.5.5 Handling errors by viewing suggestions

To use the suggestion function to handle errors in your system:

1. Identify the location where a problem occurred in the **Operating status** area.
You can see the location in red, orange, or yellow on the sunburst chart or the tree chart.
2. Click the IM management node for which the  icon is displayed.
A list of suggestions appears in the **Suggestion** tab.
3. Click the **Suggestion** button.
The suggestion bars are activated, which you can use to handle the problem.
4. Click one of the suggestion bars to check the description of the suggestion and the previous execution history in the **Suggestion details** area.

To check the details of the criteria, click the **Show the case details** button. The Case details window appears, where you can see the activation criteria of the suggestion.

5. Click the **Execute** button.

The response action is taken. The name of the button turns into **Running**.

6. Check that the response action is complete.

The name of the button turns into **Execute**. You can also check the completion of the response action through an email notification sent by an automated action of an event.

- If you click the **Suggestion** button again after the response action is taken, the list of activated suggestions now appears in a deactivated state because the system status has been changed due to the execution of the action.
- If a response action to change the status of the event to *Processed* when the system returns to normal is defined in the suggestion definition file, the applicable suggestion is activated.
- If you execute the suggestion for which the response action to change the status of the event to *Processed* is defined, changing the status of the event to *Processed* will change the status of the node to `Normal`. Clicking the **Suggestion** button again shows the list of deactivated suggestions.

Important

- Response actions for the same IM management node and same suggestion ID cannot be executed simultaneously.
- If the `jddupdatesuggestion` command or the `jddupdatetree` command is executed while a response action is being executed, the response action will not terminate midway. Therefore, response actions that reference the IM management node or suggestion definitions may fail.
- If a JP1 user is deleted or JP1 user permissions are changed or deleted while a response action is being executed, command executions using JP1 user information, plug-in common methods, and the REST API may fail, causing the response action to fail.
- If the JP1/IM - Manager service is stopped while a response action is being executed, the JP1/IM - Manager service will not stop until the response action terminates, meaning it may take some time for the service to stop. If the REST API or commands that take time are executed with the response action, it is necessary to carry out processing asynchronously.
- If the JP1/IM - Manager service is stopped directly after the execution of a response action began, response actions of the following types may fail:
 - `plugin` (if using common methods related to JP1 events)
 - `eventStatus`Furthermore, if the REST API of JP1/IM is executed while the service is stopped, the status code of 500 is returned. As a result of this, the response action may fail.

5.5.6 Logging in to the system with single sign-on through linkage with external products using OIDC authentication

The following shows procedures when single sign-on is enabled for linking external products that use OIDC authentication.

(1) Opening the Web console window of another service

1. Log in to the Intelligent Integrated Management Base through authentication provided by an OpenID provider. The Integrated Operation Viewer window appears.
2. Click an event managed by the service in the **Events** area.
3. The Web console window of the service appears without the authentication window of the OpenID provider.

(2) Opening the Integrated Operation Viewer window from another service

1. Log in to another service through authentication provided by an OpenID provider.
2. Start the Integrated Operation Viewer window from the service.
3. The Integrated Operation Viewer window appears without the login window of the Intelligent Integrated Management Base.

(3) Issuing the REST API of JP1/IM with authentication information authenticated by an OpenID provider attached to it from another service

1. Log in to another service through authentication provided by an OpenID provider.
2. Issue the REST API to which authentication information at the time of login is attached.

5.5.7 Sharing information using a direct access URL

This subsection describes how to share information on a specific node with other users, using an example of sending an email notification about a URL for viewing the Event detail dialog box in the Integrated Operation Viewer window, to the person in charge (`userA`) via an automated action.

1. Define an email to be sent via an automated action.[#]

The definition of the email is as follows:

From: `admin@xxxxxx.com`

To: `userA@xxxxxx.com`

Email subject: Check the impact on your business

Email body: `http://host-name-of-the-Intelligent-Integrated-Management-server:20703/index?seqno=73&tab=job&eou=1`

2. An error occurs in the system, causing the automated action to send an email to the person in charge (`userA`).
3. The person in charge (`userA`) clicks the direct access URL in the email body.
Access the Integrated Operation Viewer window through the URL in the email that contains a serial number.
4. The Integrated Operation Viewer window appears with the Event detail dialog box open.

#

If you have changed the port number on which HTTP communication is received in the Intelligent Integrated Management Base service, change the port number 20703 in the email definition example to the changed one. In addition, if you use the communication encryption function of JP1/IM - Manager (encrypt communications between your web browser and the Intelligent Integrated Management Base with HTTPS), change `http` to `https`.

5.6 Notes on operating the Intelligent Integrated Management Base

This section provides notes on operating the Intelligent Integrated Management Base.

5.6.1 Notes on when there is a link with JP1/AJS

- Execute the `jddcreatetree` command while the JP1/AJS3 - Manager host is not running any job. If the `jddcreatetree` command is executed while a job is running, both command and job processes impose a load on the system, causing them to potentially be delayed.

If jobs are always running, then execute the `jddcreatetree` command when the number of executed jobs is small, so that the command execution causes less impact on business operations. In addition, verify the execution in your development environment sufficiently to make sure there is no problem with each of the processes.

- The `jddcreatetree` command can collect information from JP1/AJS3 - Manager hosts for a maximum of 60 minutes. A timeout occurs when 60 minutes is reached and the command can no longer collect the information. If it takes 60 minutes or more to collect the information and then a timeout occurs, the `IMDDAdapter_HITACHI_JP1_AJS3` adapter command process, which is responsible for information collection, might be kept running on the JP1/AJS3 - Manager host. As two adapter commands cannot be executed at once, you need to terminate the `IMDDAdapter_HITACHI_JP1_AJS3` process by using the following method on the JP1/AJS3 - Manager host, if you collect the information again:

In Windows

Use Task Manager to terminate the process.

In UNIX

Use the `kill` command to terminate the process.

Then, adjust how your units are configured and the number of jobnets registered for execution so that the collection time is less than or equal to 60 minutes, and re-execute the `jddcreatetree` command.

- The `jddcreatetree` command does not collect unit information from:
 - Manager job group
 - Manager jobnet
 - Recovery manager jobnet
 - Remote jobnet and its underlying units
 - Recovery remote jobnet and its underlying units
 - JP1 event sending job in which *queueless* is specified for its execution service, and units with wait conditions
 - JP1 event reception monitoring job and JP1 event sending job that are defined in the same level as a root jobnet
 - Root jobnet not registered for execution and its underlying units
- Execution of an adapter command running on a JP1/AJS3 - Manager host cannot be cancelled from a JP1/IM - Manager host. To cancel it, on the JP1/AJS3 - Manager host, use the following method to terminate the `IMDDAdapter_HITACHI_JP1_AJS3` process:

In Windows

Use Task Manager to terminate the process.

In UNIX

Use the `kill` command to terminate the process.

- A single JP1/AJS3 - Manager host can collect information from up to 400,000 units. If the number of units exceeds 400,000, the `jddcreatetree` command fails with message `KAJY04260-E` and the configuration management tree is not updated. You can estimate the number of units by executing the following commands on the JP1/AJS3 - Manager host:

In Windows

Total number of rows obtained by executing the following commands:

```
ajpname -F scheduler-service-name -R -E "/"
ajpname -F scheduler-service-name -R -G "/"
```

In UNIX

Total number of rows obtained by executing the following commands:

```
/opt/jp1ajs2/bin/ajpname -F scheduler-service-name -R -E "/"
/opt/jp1ajs2/bin/ajpname -F scheduler-service-name -R -G "/"
```

- If environment settings parameter `ADMACLIMIT` is set to `yes` on the JP1/AJS3 - Manager host, the `jddcreatetree` command might fail to collect information. Use the following corrective action to make a configuration so that the information can be collected before operation:

In Windows

Set environment settings parameter `ADMACLIMIT` to `no` or remove the parameter to disable the function.

On the JP1/AJS3 - Manager host, register a JP1 user named `system` and add one of the following JP1 permission levels to the user:

Or, on the JP1/AJS3 - Manager host, register a JP1 user named `SYSTEM` and add one of the following JP1 permission levels to the user:

- JP1_AJS_Admin permission
- JP1_AJS_Manager permission
- JP1_AJS_Editor permission
- JP1_AJS_Operator permission
- JP1_AJS_Guest permission

In UNIX

Set environment settings parameter `ADMACLIMIT` to `no` or remove the parameter to disable the function.

Or, on the JP1/AJS3 - Manager host, register a superuser as a JP1 user and add one of the following JP1 permission levels to the user:

- JP1_AJS_Admin permission
- JP1_AJS_Manager permission
- JP1_AJS_Editor permission
- JP1_AJS_Operator permission
- JP1_AJS_Guest permission

- If information, such as a unit name, unit definition, execution agent name, or JP1 resource group name, collected by the `jddcreatetree` command contains a control character, the command might fail to collect the information. Avoid using any control character in the information if it is to be collected.
- If the system time on the JP1/AJS3 manager host of the trend information acquisition destination is set back[#], and the time recorded in duplicate in the performance log files due to the system time change overlaps with the specified start or end time for the trend information display period, only part of the duplicate record in the performance log file might be displayed. If so, it might be possible to avoid this issue by one of the following methods.
 - Wait before displaying again
 - Change the periods before displaying again

- If you perform the above workarounds but the record in the performance log files is not output correctly, perform the following methods.
- Execute the `ajsreport` command on the JP1/AJS3 manager host of the trend information acquisition destination. For details on trend information metrics and the item list that is output in the performance reports by `ajsreport` command, see *2.7.1 Metrics that can be retrieved from JP1/AJS in the JP1/Integrated Management 3 - Manager GUI Reference*.
- Consider deleting the performance log files. To delete the performance log files, you will need to stop the scheduler service of the JP1/AJS3 manager host of the trend information acquisition destination. For details, see the JP1/Automatic Job Management System 3 manual.
This applies if the prerequisites for the trend information display function are not met, or if the system time is set back while the JP1/AJS3 services on the JP1/AJS3 manager host of the trend information acquisition destination are stopped. To set back the system time while the JP1/AJS3 services are stopped, see the *JP1/Automatic Job Management System 3 Administration Guide*, and delete the performance log files.
- If the `jddcreatetree` command is used to obtain information from a target JP1/AJS3 - Manager host of version 12-50 or later, make sure that the JP1/AJS3 - Manager host as the information acquisition target can resolve the agent host name as the job execution destination, before you execute the `jddcreatetree` command.

5.6.2 Notes on using event receiver filters

It may take time to get events for displaying the events list if you do one of the following operations in the integrated operation viewer window when setting up an event receiver filter:

- If you select an IM management node
- If you use a button on the toolbar in the **Events** area to update the events list

In these cases, event acquisition is interrupted after a certain number of searches and the events acquired before the interruption are displayed in the **Events** area.

You can change the upper limit for the number of searches before event acquisition is interrupted in the `jp1.imdd.gui.settings.eventSearchCount` property of the Intelligent Integrated Management Base definition file (`imdd.properties`). If you want to shorten the time before event acquisition is interrupted, decrease the upper limit for the number of searches. If you want to lengthen the time before event acquisition is interrupted, increase the upper limit for the number of searches. If you do not want to interrupt event acquisition, set the upper limit for the number of searches to 0.

We recommend you use a system node definition file (`imdd_systemnode.conf`) or a business group, not an event receiver filter, for the limit of events that can be referred to or worked with in the Intelligent Integrated Management Base.

For details about the `jp1.imdd.gui.settings.eventSearchCount` property, see *Intelligent Integrated Management Base definition file (imdd.properties)* in *Chapter 2. Definition Files of the JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*, and for details about the system node definition file (`imdd_systemnode.conf`), see *System node definition file (imdd_systemnode.conf)* in *Chapter 2. Definition Files*.

6

System Monitoring from Central Console

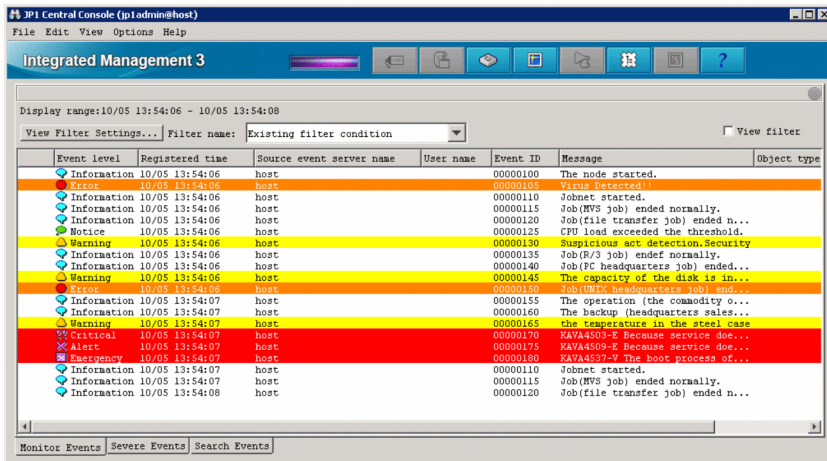
This chapter explains how to use JP1/IM - View to monitor JP1 events.

6.1 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 6–1: Event Console window (Monitor Events page) display example



The screenshot shows the 'JP1 Central Console (jp1admin@host)' window. The title bar includes 'File Edit View Options Help'. Below the title bar is a toolbar with icons for back, forward, home, search, and help. The main area displays a table of events with the following columns: Event level, Registered time, Source event server name, User name, Event ID, Message, and Object type. The events are listed in descending order of time, with the most recent at the bottom. The events include Information, Warning, and Error levels, with messages such as 'The node started.', 'Jobnet started.', 'Job(MVS job) ended normally.', 'CPU load exceeded the threshold.', 'Suspicious act detection.Security', 'Job(R/3 job) ended normally.', 'Job(PC headquarters job) ended...', 'The capacity of the disk is in...', 'Job(UNIX headquarters job) end...', 'The operation (the commodity o...', 'The backup (headquarters sales...', 'The temperature in the steel case', 'KAWA4503-E Because service doe...', 'KAWA4503-E Because service doe...', 'KAWA4537-V The boot process of...', 'Jobnet started.', 'Job(MVS job) ended normally.', and 'Job(file transfer job) ended n...'. At the bottom of the window, there are tabs for 'Monitor Events', 'Severe Events', and 'Search Events'.

Event level	Registered time	Source event server name	User name	Event ID	Message	Object type
Information	10/05 13:54:06	host		0000100	The node started.	
Information	10/05 13:54:06	host		0000105	View(PC-headq...	
Information	10/05 13:54:06	host		0000110	Jobnet started.	
Information	10/05 13:54:06	host		0000115	Job(MVS job) ended normally.	
Information	10/05 13:54:06	host		0000120	Job(file transfer job) ended n...	
Notice	10/05 13:54:06	host		0000125	CPU load exceeded the threshold.	
Warning	10/05 13:54:06	host		0000130	Suspicious act detection.Security	
Information	10/05 13:54:06	host		0000135	Job(R/3 job) ended normally.	
Information	10/05 13:54:06	host		0000140	Job(PC headquarters job) ended...	
Warning	10/05 13:54:06	host		0000145	The capacity of the disk is in...	
Error	10/05 13:54:06	host		0000150	Job(UNIX headquarters job) end...	
Information	10/05 13:54:07	host		0000155	The operation (the commodity o...	
Information	10/05 13:54:07	host		0000160	The backup (headquarters sales...	
Warning	10/05 13:54:07	host		0000165	The temperature in the steel case	
Critical	10/05 13:54:07	host		0000170	KAWA4503-E Because service doe...	
Alert	10/05 13:54:07	host		0000175	KAWA4503-E Because service doe...	
Emergency	10/05 13:54:07	host		0000180	KAWA4537-V The boot process of...	
Information	10/05 13:54:07	host		0000110	Jobnet started.	
Information	10/05 13:54:07	host		0000115	Job(MVS job) ended normally.	
Information	10/05 13:54:08	host		0000120	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 *4.15.3 Copying JP1 event information and action execution results to the clipboard* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

6.1.1 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 3 - Manager Configuration Guide*.

For details about how to set up the severity changing function, see *5.13 Setting the severity changing function* in the *JP1/Integrated Management 3 - 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 *3.24 Preferences window* in the *JP1/Integrated Management 3 - 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 *3.24 Preferences window* in the *JP1/Integrated Management 3 - 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 6–1: 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 (source 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.
Object type	Character strings, such as JOB and JOBNET, that indicate the type of object where the event that triggered event generation occurred.

Attribute	Explanation
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) 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	<p>When the severity level is changed, the icon  is displayed.</p> <p>This attribute is displayed when the integrated monitoring database is used and the severity changing function is enabled.</p>
Changed display message	Displays a message after the change.

Attribute	Explanation
	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.
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.
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.
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.

(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 [6.9.2 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 [6.3.1 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.

6.1.2 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 [6.1.2\(1\) Displaying consolidated events in the events list](#).
- Correlation events
The icon  or  is displayed in **Type**.
For details about displaying correlation events, see [6.1.2\(2\) 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 3 - 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 [6.8 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:

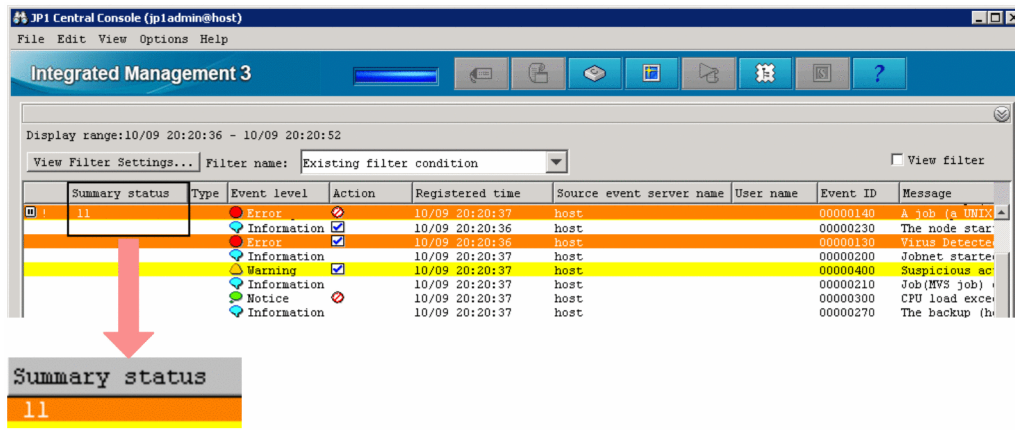
The events list is updated at a user-specified updating interval, and displays the latest JP1 events. However, if automatic updating is not set up, the latest JP1 events are not displayed even when the screen is started. To display the latest JP1 events in such a case, from the **View** menu, choose **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 6–2: 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.

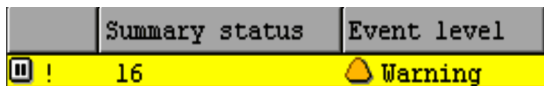
If you are using the repeated event monitoring suppression function, deleting a repeated event does not reduce the number of repetitions of consolidated events.

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 6–2: 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 3.24 *Preferences window* in the *JP1/Integrated Management 3 - Manager GUI Reference*.

6.1.3 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 [6.5.1 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 [5.16 Setting JP1/IM - View for each login user](#) in the *JP1/Integrated Management 3 - 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 [6.5.2 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 [6.5.3 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 [6.5.4 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 [5.2 Setting JP1 event filtering](#) in the *JP1/Integrated Management 3 - Manager Configuration Guide*.

6.2 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 [6.4.1\(1\) 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 6–3: 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): <i>Emergency, Alert, Critical, Error, Warning, Notice, Information, and Debug</i> .
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.
Common exclude conditions group target-for-exclusion	Exclusion target of the common exclusion-conditions. <i>action</i> appears when the JP1 event is excluded from automated-action execution.

Display name#1	Description
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 KAVB1588-I 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.


6.2.1 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 3 - Manager Configuration Guide*.

For details about how to enable the memo entry startup function, see *5.7 Setting memo entries* in the *JP1/Integrated Management 3 - 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.

6.3 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.

6.3.1 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 6–4: 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.

6.3.2 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 3 - Manager Command, Definition File and API Reference*.

6.3.3 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.

6.4 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 *JP1/Integrated Management 3 - Manager GUI Reference*:

- *3.8 Related Events (Summary) window*
- *3.9 Related Events (Correlation) window*

6.4.1 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 [6.8 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 [6.3.1 Settings for JP1 event response statuses](#).

6.4.2 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 6–5: 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 [6.1.2\(1\) 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 [6.4.2\(1\) 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 [6.4.2\(1\) 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.

6.5 Applying a JP1/IM filter

This subsection explains how to apply a JP1/IM filter from JP1/IM - View.

6.5.1 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 *5.2.1 Settings for view filters* in the *JP1/Integrated Management 3 - 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.

6.5.2 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 *6.3.2 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 3 - 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 JPI/Integrated Management 3 - Manager Command, Definition File and API Reference*.

6.5.3 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 JPI/IM uses when it acquires JPI events from JPI/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 JPI 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 JPI 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 JPI/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 JPI_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 JPI resource group and JPI permissions level. For details, see *4.1.4(2) Assigning a JPI resource group and permission level to a JPI user* in the *JPI/Integrated Management 3 - Manager Overview and System Design Guide*.

For details about the events that are generated when an event acquisition filter is switched, see *4.2.2 Event acquisition filter* in the *JPI/Integrated Management 3 - 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 *5.2.4 Settings for event acquisition filters* in the *JP1/Integrated Management 3 - 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 *JP1/Integrated Management 3 - Manager Command, Definition File and API 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 6–3: 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 *JPI/Integrated Management 3 - Manager Command, Definition File and API 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 JPI/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
```

6.5.4 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 *5.2.4(3)(a) Switching between common exclusion-conditions basic mode and extended mode* in the *JPI/Integrated Management 3 - 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 *JPI/Integrated Management 3 - Manager Command, Definition File and API 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.

6.6 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 3 - Manager Configuration Guide*. For details about the display range when specifying an event display start-time, see *3.2 Monitor Events page* in the *JP1/Integrated Management 3 - 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 3-4 Monitor Events page with the event display start-time specification area displayed* in *3.2 Monitor Events page* in the *JP1/Integrated Management 3 - 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.

6.7 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 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 *4.18 Specifying the event display period* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

6.8 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 *4.6 Searching for events* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*. For details about the window used to search for events, see *3.25 Event Search Conditions window* in the *JP1/Integrated Management 3 - Manager GUI Reference*.

6.8.1 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 *JP1/Integrated Management 3 - 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 *6.8.1(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, program-specific extended attribute, memo^{#2}, new severity level^{#3}, original severity level^{#3}, new display message^{#4}, changed display message^{#4}, repeated events^{#5}, and suppressed event ID^{#5}.

#1: You can specify this item if source host mapping is enabled.

#2: You can specify this item if the memo function is enabled.

#3: You can specify this item if the severity changing function is enabled.

#4: You can specify this item if the display message change function is enabled.

#5: 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 [6.8.1\(3\) 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 [6.8.2 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*.

6.8.2 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 *3.24 Preferences window* in the *JP1/Integrated Management 3 - 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 6–4: 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 6–5: 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 6–6: 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 6–7: 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 6–8: 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	} Added
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	

6.9 Customizing JP1 event information by operation

You can customize JP1 event information according to different operations.

6.9.1 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 *5.11 Setting the display and specification of program-specific extended attributes* in the *JP1/Integrated Management 3 - 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:

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.

6.9.2 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 6–6: 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 6–7: 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 *4.1.4(2) Assigning a JP1 resource group and permission level to a JP1 user in the JP1/Integrated Management 3 - 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 4,102,444,799 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 *4.14 Displaying user-defined event attributes* in the *JP1/Integrated Management 3 - 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 *JP1/Integrated Management 3 - Manager Command, Definition File and API 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.

6.9.3 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 *4.12 Adding program-specific attributes* in the *JP1/Integrated Management 3 - 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*.

6.9.4 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 3 - Manager Configuration Guide*.

For details about how to set up the severity changing function, see *5.13 Setting the severity changing function* in the *JP1/Integrated Management 3 - 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* in *Chapter 1. Commands* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API 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* in *Chapter 1. Commands of the JP1/Integrated Management 3 - Manager Command, Definition File and API 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 JP1/Integrated Management 3 - Manager Command, Definition File and API 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_spmd_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_spmd_reload` command, see *jco_spmd_reload* in *Chapter 1. Commands of the JP1/Integrated Management 3 - Manager Command, Definition File and API 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.

6.9.5 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_spmc_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 3 - Manager Configuration Guide*.

For details about how to configure the display message change function, see *5.14 Setting the display message change function* in the *JP1/Integrated Management 3 - 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 JP1/Integrated Management 3 - Manager Command, Definition File and API 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 JP1/Integrated Management 3 - Manager Command, Definition File and API 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 JP1/Integrated Management 3 - Manager Command, Definition File and API 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 JP1/Integrated Management 3 - Manager Command, Definition File and API 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 JP1/Integrated Management 3 - Manager Command, Definition File and API 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 *JP1/Integrated Management 3 - Manager Command, Definition File and API 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.

6.10 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 *4.5.1 Mechanism of the suppression of monitoring of a large number of events* in the *JP1/Integrated Management 3 - 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 *13.1.2 Considerations for forwarding JP1 events to managers* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*. For details about the settings for event filtering on the manager, see *13.1.3 Considerations for filtering JP1 events* in the *JP1/Integrated Management 3 - 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 *5.3 Setting monitoring of repeated events to be prevented* in the *JP1/Integrated Management 3 - Manager Configuration Guide*.

6.10.1 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 6–9: General procedure for handling detection of a large number of events

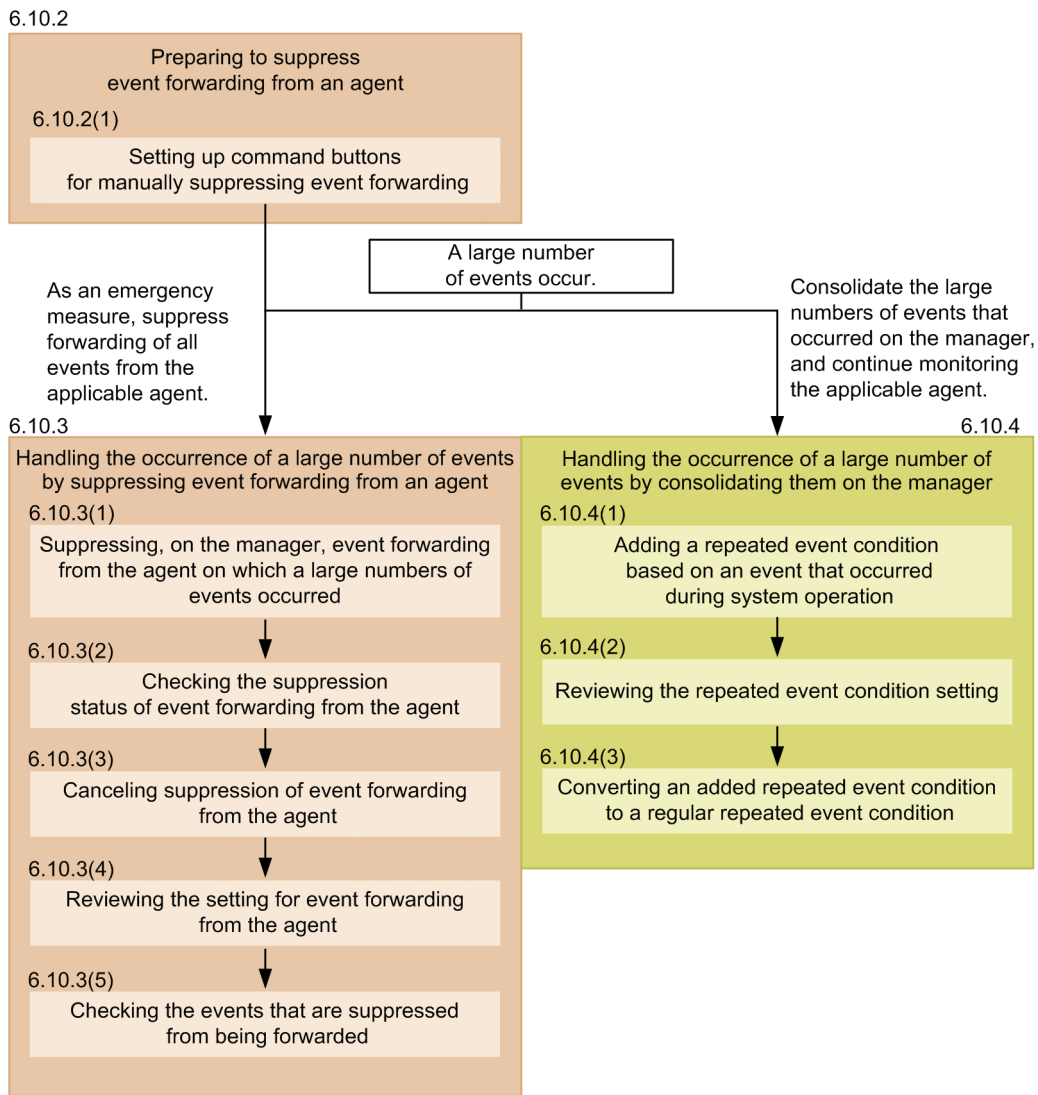
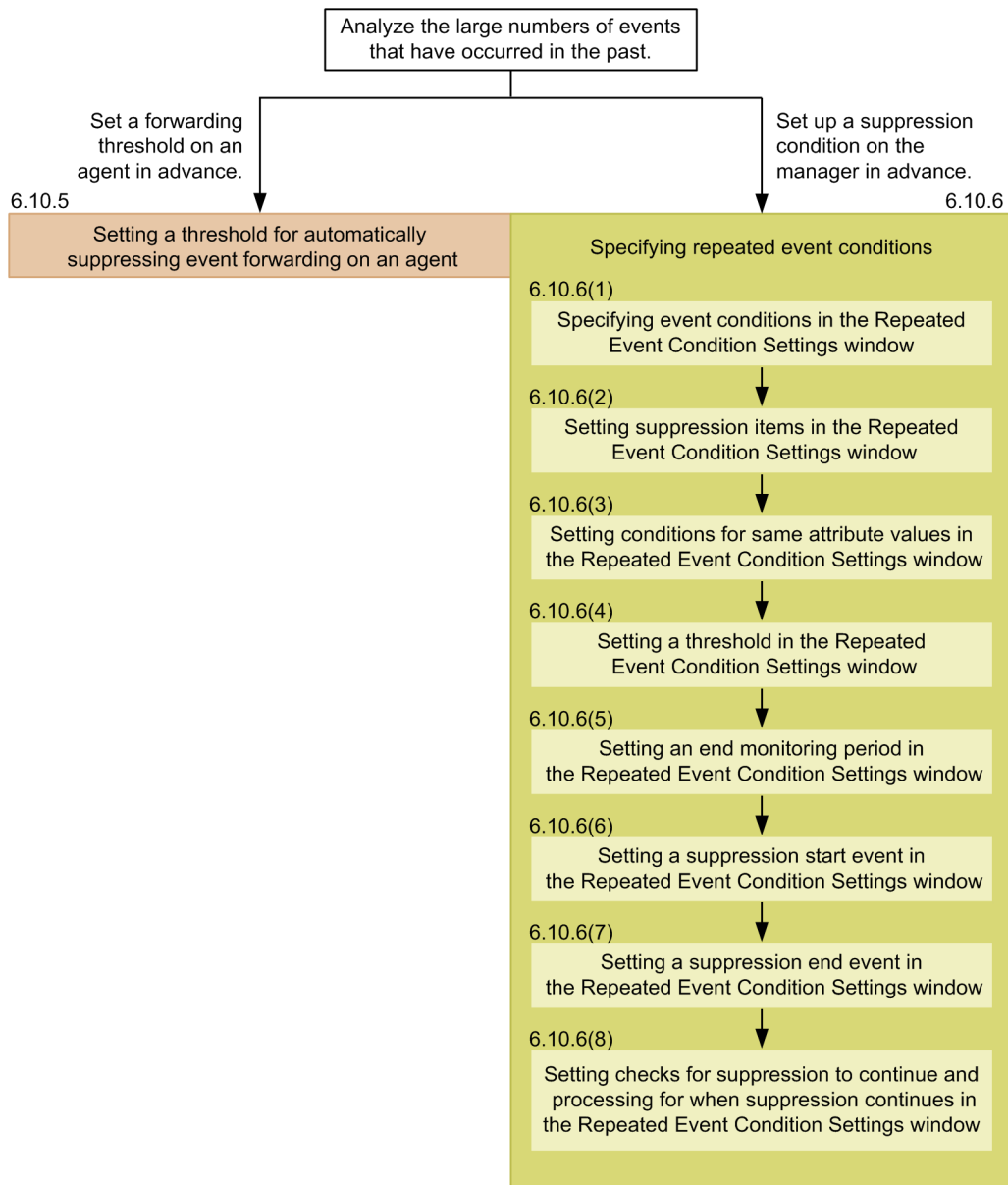


Figure 6–10: General procedure when a large number of events have occurred in the past or are expected to occur again



6.10.2 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 *1.16 Setting up a command execution environment (for Windows)* or *2.15 Setting up a command execution environment (for UNIX)* in the *JP1/Integrated Management 3 - 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

```

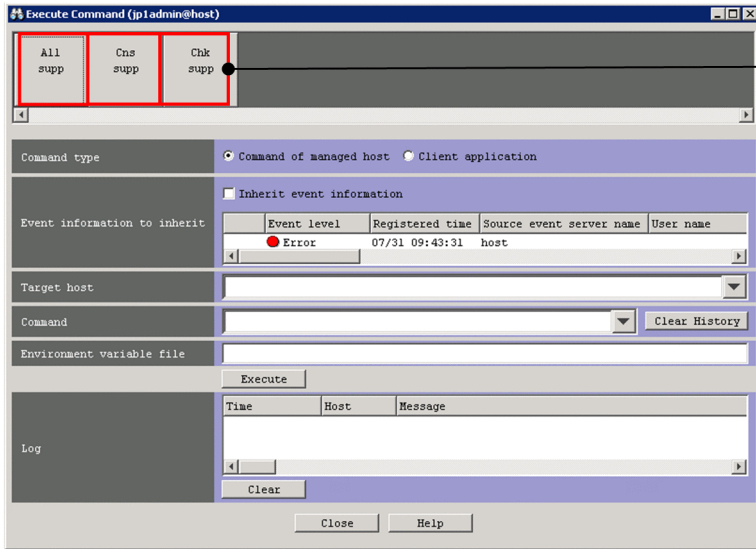
For \$EVHOST in the definition example, the event-issuing host name of the event selected in the Console window of JP1/IM - View is assigned.

For UNIX, replace *Base-path*\bin\jevagtfw.exe with /opt/jp1base/bin/jevagtfw.

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.

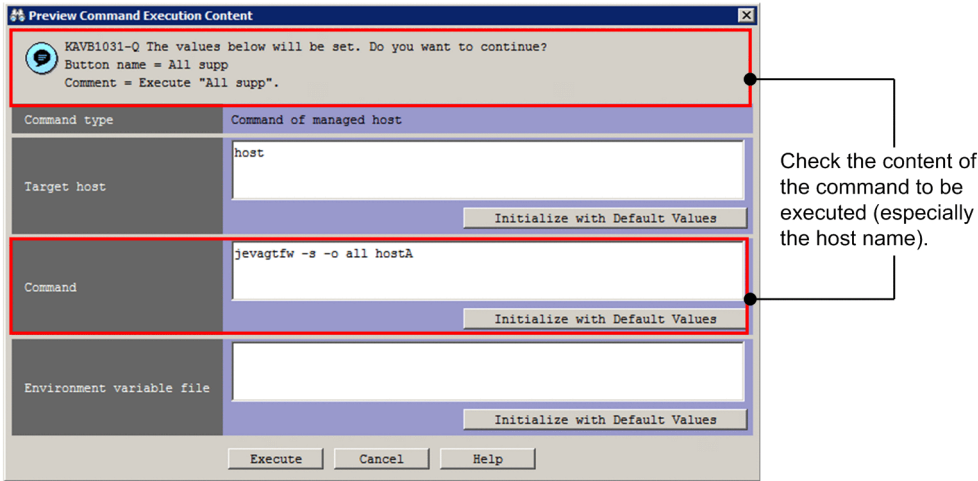
6.10.3 Handling the occurrence of a large number of events by suppressing event forwarding from an agent

This subsection explains how to use the command buttons that you set up in [6.10.2 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.

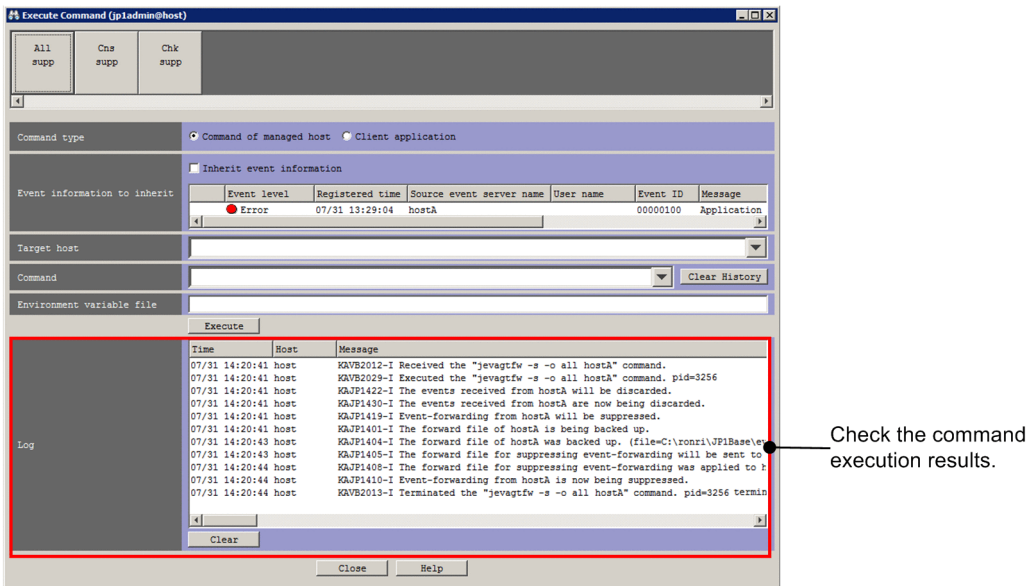
(1) Suppressing, on the manager, event forwarding from the agent on which a large numbers of events occurred

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 [6.10.2 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 `jevagt fw` 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.

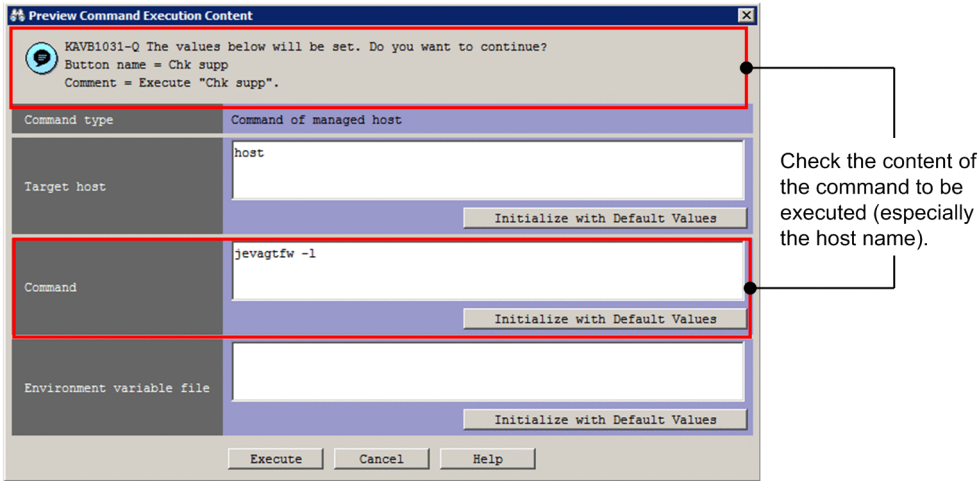


6. Identify the reason why a large number of events are occurring, and then solve the problem. While event forwarding is suppressed, investigate the agent that is outputting the events, and then solve the problem.

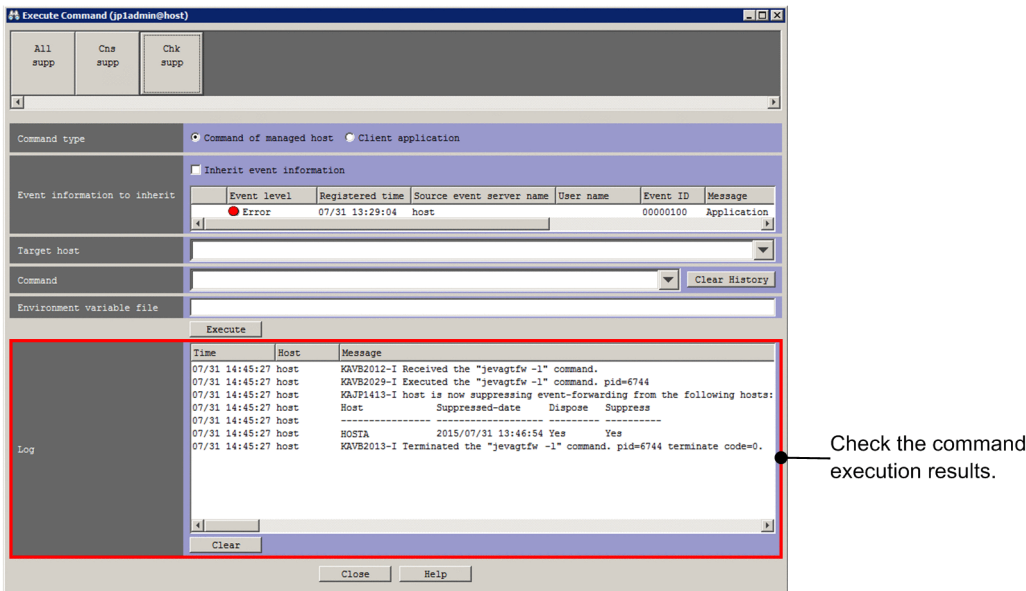
(2) Checking the suppression status of event forwarding from the agent

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 *6.10.2 Preparing to suppress event forwarding from an agent*.
The Preview Command Execution Content window opens. Check the content of the command to be executed.



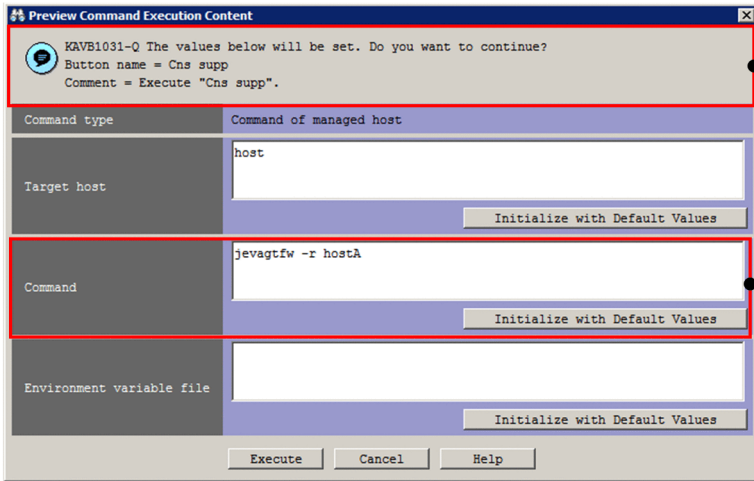
3. In the Preview Command Execution Content window, click the **Execute** button to execute the `jevagt fw` command. In the **Log** area of the Execute Command window, check the suppression status. You can check the execution result of the command in the **Log** area of the Execute Command window.



(3) Canceling suppression of event forwarding from the agent

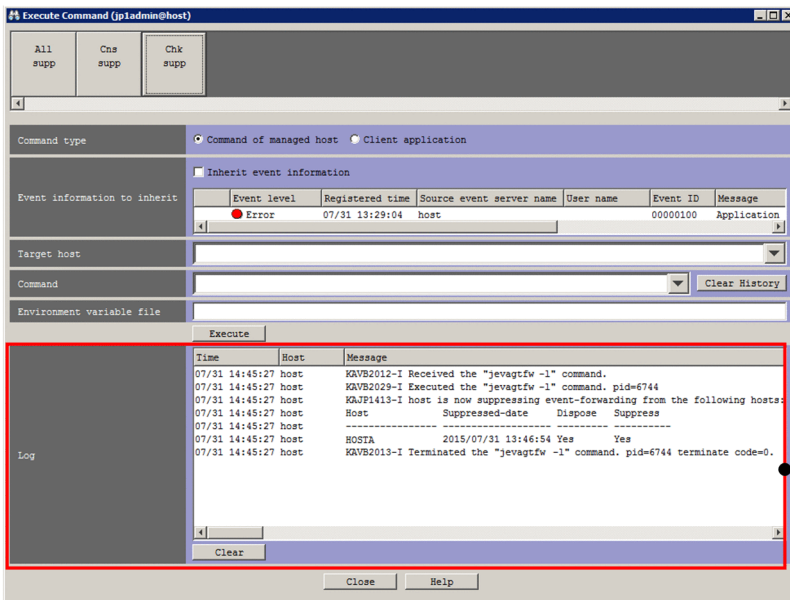
Using a command button that was set up, you can, on the manager, cancel suppression of event forwarding from an agent.

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 *6.10.2 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).



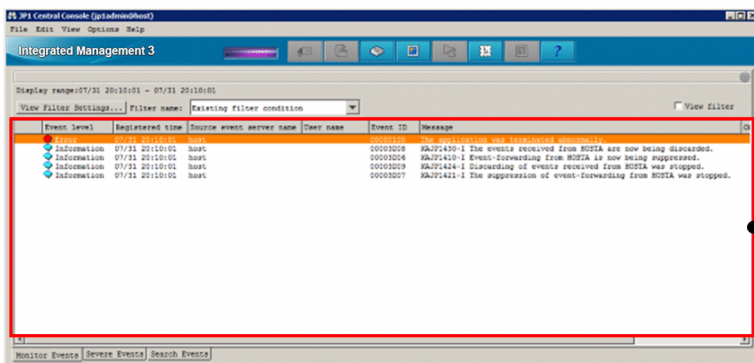
Check the content of the command to be executed (especially the host name).

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.



Check the command execution results.

5. Also in the Event Console window, confirm that suppression has been canceled and that events are being forwarded from the specified agent.



Check the notifications about suppression cancellation and events from the applicable 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 [6.10.5 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 [6.8 Searching for JP1 events](#).

6.10.4 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 JPI/Integrated Management 3 - Manager Command, Definition File and API 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 *4.5.4 When the suppression of monitoring of a large number of events starts* in the *JPI/Integrated Management 3 - Manager Overview and System Design Guide*.

(2) Reviewing the repeated event condition setting

Review the repeated event condition that is specified. For details, see *6.10.6 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.

6.10.5 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 JPI/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.

6.10.6 Specifying repeated event conditions

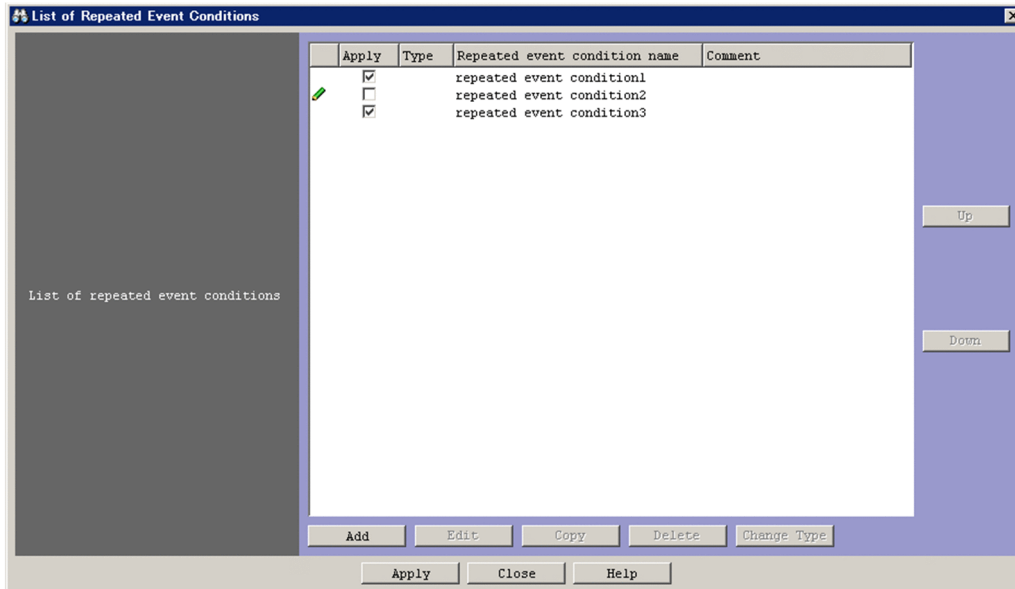
By specifying repeated event conditions, you can consolidate events that meet the specified conditions on the manager, display them in the events list, and suppress automatic action execution.

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 *3.17 Repeated Event Condition Settings window* and *3.19 List of Repeated Event Conditions window* in the *JP1/Integrated Management 3 - Manager GUI Reference*.

To specify repeated event conditions, the JP1 user who performs operations from JP1/IM - View must have `JP1_Console_Admin` permissions.

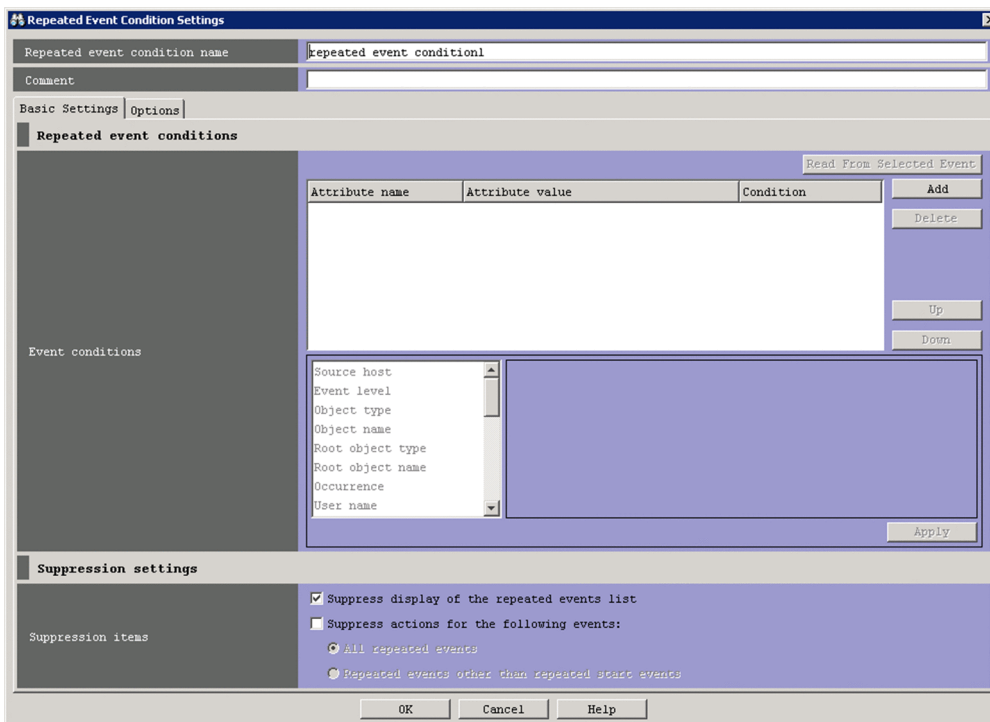
To specify repeated event conditions:

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 [6.10.6\(1\) 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 [6.10.6\(2\) 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).

For details about the specification procedure, see [6.10.6\(3\) 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 [6.10.6\(4\) 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 [6.10.6\(5\) 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 [6.10.6\(6\) 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 [6.10.6\(7\) 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 *6.10.6(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 [6.10.6\(4\) 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 *4.4.7 Issuing notifications when the suppression of repeated-event display continues* in the *JP1/Integrated Management 3 - 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.

6.10.7 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 *8.5 Profile management* in the *JP1/Integrated Management 3 - 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 3 - 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 *5.15 Setting event source host mapping* in the *JP1/Integrated Management 3 - 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.

6.10.8 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 *4.4.10 Suppressing repeated-event display by the consolidated display of repeated events* in the *JP1/Integrated Management 3 - 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 *6.10.4 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.

6.11 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.

6.11.1 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 *10.1.1 Enabling calling the JP1/Service Support window* in the *JP1/Integrated Management 3 - 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 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 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 opens and displays the Select the process work board as the registration target window of JP1/Service Support.

6.11.2 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 *10.2 Linking to JP1/Navigation Platform* in the *JP1/Integrated Management 3 - 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 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.

6.11.3 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.

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 *5.17 Setting monitor startup for linked products* in the *JP1/Integrated Management 3 - 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_pfmgr_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

6.11.4 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.

6.12 Notes for Central Console

- Delay monitoring of the automated action monitors the delay of execution of the automated action at a set interval. Therefore, it may not be able to detect the delay exactly as you specified in [Delay monitoring] of [Action Parameter Detailed Definitions] window. Furthermore, if the automated action causes the delay monitoring to terminate, for example, when the automated action terminates soon after [Delay monitoring] has passed, a delay may not be detected.
- JP1/IM - Manager operates in a WOW64 environment. For this reason, a 64-bit program might not run through automated action in the above OSs. In such cases, execute the following command through automated action, and execute the program from the 64-bit cmd.exe:

```
%WinDir%\Sysnative\cmd.exe execution-command
```

- In the following cases, the maximum length of a URL that can be set in a web browser is 2,046 characters:
 - When a link to an HTML event guide is clicked
 - When an incident is registered in JP1/IM - Service Support
 - When a report is displayed by the event-source-host performance report display function

By entering the following common definition information to any file, and by applying it with the `jbssetcnf` command, you can reset this limit (same as 09-10 or earlier), or change the limit value:

```
[logical-host-name\JP1CONSOLEMANAGER]  
"GUIDE_URLLIMIT"="value"  
"URLLIMIT_CHAR_NUM"=dword:value
```

In the case of a physical host, set the above *logical-host-name* as `JP1_DEFAULT`.

In the case of a logical host, set it to the actual name of the logical host.

Enter [*logical-host-name*\JP1CONSOLEMANAGER] at the beginning of the file.

`GUIDE_URLLIMIT`: You can limit, or not limit, the URL length of hyperlinks of HTML event guides.

- When limiting the length of the URL: Specify "1".
- When not limiting the length of the URL: Specify "0".

`URLLIMIT_CHAR_NUM`: The following cases can specify the maximum length of the URL to be set for a web browser:

- When a link to an HTML event guide is clicked
- When an incident is registered in JP1/IM - Service Support
- When a report is displayed by the event-source-host performance report display function

Enter the maximum length as a hexadecimal number. The unit is the number of characters.

If you disable this restriction or change the maximum length, make sure that the length of the URL does not exceed the maximum length allowed by the web browser.

- Do not specify an extended attribute whose attribute name begins with "E.JP1_" for a JP1 event. If JP1/IM - Manager receives a JP1 event that has an extended attribute whose name begins with "E.JP1_", JP1/IM - Manager might not operate properly.

6.13 Notes on using the Central Console - View

- The event response status only shows the current status and does not check the validity of the response status transition. Even if you have changed the response status of an event to "responded" using the `jcochstat` command, by acting when a trouble ticket is closed in such a system as Problem Management System, you can still change the response status of that event to "not responded" from the window. Be careful when you change the response status from a window if the system works in conjunction with another system.
- If you attempt to start JP1/IM - View by executing the `jcoview` command with an incorrect argument specified, the login window appears after either of the following messages is output:
 - KAVB0104-E Failed to authenticate the user.
 - KAVB1210-E A communication error occurred while establishing a connection. Cannot convert the host name into an IP address. Confirm the host name. Host name: *host-name*, Port number: *port-number* Details: *detailed-information*

In the login window displayed in this status, you may be unable to select the input fields even with the mouse to enter information in them. If this problem occurs, click the taskbar button for a program other than JP1/IM - View, and then click the login window.

- The time required for searching an event is proportional to the size of the event DB. If the capacity of the event DB reaches the maximum size, more than 30 minutes may be required for searching an event. By specifying [Arrived timeframe] as an event search condition, you may be able to shorten the time required for searching the event.
- If it takes a long time to start the event console service due to such reasons as system load, and if the limits are exceeded in terms of the number of retries and interval of retries when connecting the Event Flow Control Service and the Event Console Service, the past events are no longer displayed in [Monitor Events] page and [Severe Events] page when JP1/IM - View is connected. Restart the Event Console Service, and ensure that "KAVB4754-1 Event Console Server was connected." has been output to the integrated trace log, and then restart JP1/IM - View.
- If UAC (User Account Control) is enabled, when an administrator or standard user starts and uses JP1/IM - View to save displayed events, UAC redirects the file containing the data to a user-dependent virtual folder. The destination folders are as follows:
 - When redirected to `%ProgramFiles%`

```
%LocalAppData%\VirtualStore\Program Files
```

(The default folder is `system-drive:\Users\OS-user-name\AppData\Local\VirtualStore\Program Files`)

- When redirected to `%WINDIR%`

```
%LocalAppData%\VirtualStore\Windows
```

(The default folder is `system-drive:\Users\OS-user-name\AppData\Local\VirtualStore\Windows`)

When the displayed events are saved, the reply message (KAVB0321-Q or KAVB0322-Q) that appears contains the file name path that was specified before the redirection was performed.

- Windows 10(x64), On Windows Server 2016 , Windows Server 2019, Windows Server 2022 or Windows 11 access and command execution for files under the `%WINDIR%\System32` folder may fail because WOW64 redirection function redirects files under the `%WINDIR%\SysWow64` folder. Do not specify a command less than or equal to the `%WINDIR%\System32` in JP1/IM - View [Execute Command] or definition file for executing applications command.

7

System Monitoring from Central Scope

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

7.1 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.

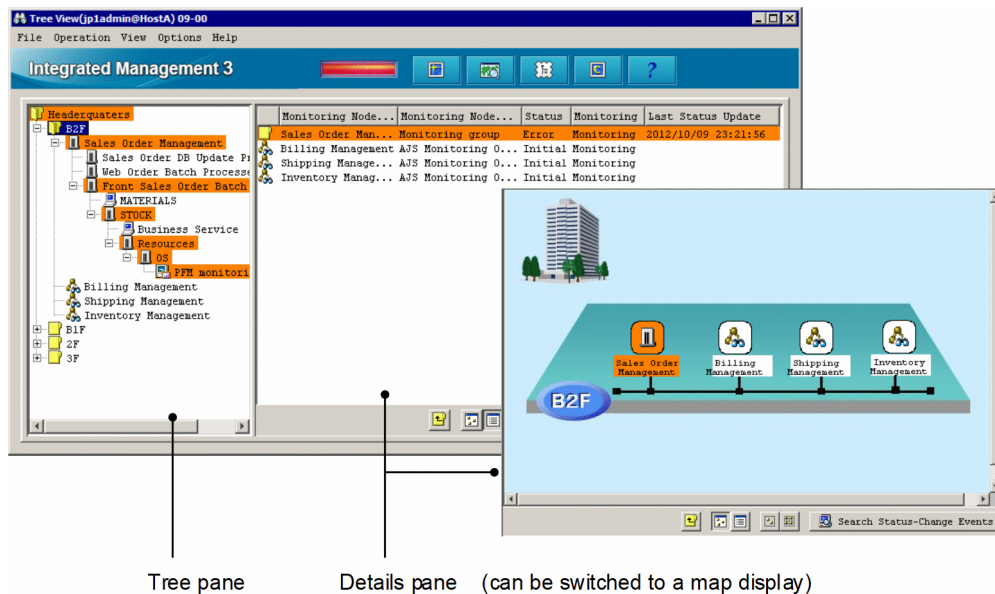
When the monitoring range settings of the monitoring tree are enabled, the monitoring tree displays only the monitoring nodes that are set for the JP1 resource group of the logged-in JP1 user. In this case, a virtual root node is displayed as the highest-order node. If there is no monitoring node that 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 7–1: Monitoring Tree window display example



7.1.1 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 5.2.2 *Statuses of monitoring nodes* in the *JP1/Integrated Management 3 - 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**.

7.1.2 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 5.2.2 *Statuses of monitoring nodes* in the *JP1/Integrated Management 3 - 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.

7.1.3 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.

7.1.4 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.

7.1.5 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`.

7.1.6 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 5.8 *Guide function* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.
- About editing the guide information file:
See 6.6 *Editing guide information* in the *JP1/Integrated Management 3 - 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 *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

7.1.7 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**.

7.1.8 Displaying a login user list

To display a list of JP1 users that have logged in to JP1/IM - Manager (Central Scope):

1. In the menu bar, choose **Options** and then **Login User List**.

7.1.9 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.

7.2 Monitoring from the Visual Monitoring window

You can monitor the statuses of monitored objects from the Visual Monitoring window.

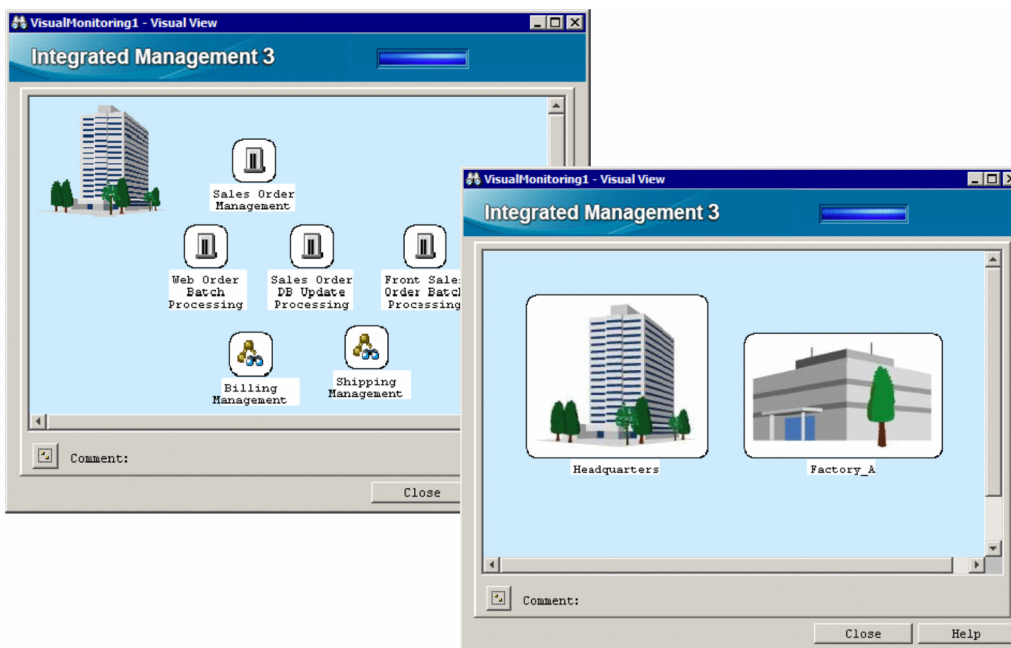
When the monitoring range settings of the monitoring tree are enabled, the Visual Monitoring window displays only the monitoring nodes that are set for the JP1 resource group of the logged-in JP1 user. However, if the JP1 resource group is JP1_Console and if the user has logged in as a JP1 user with 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 7–2: Visual Monitoring window display example



7.2.1 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.

7.2.2 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 *5.2.2 Statuses of monitoring nodes* in the *JP1/Integrated Management 3 - 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**.

7.2.3 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 *5.2.2 Statuses of monitoring nodes* in the *JP1/Integrated Management 3 - 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.

7.2.4 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.

7.2.5 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.

7.2.6 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`.

7.2.7 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 *5.8 Guide function* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.
- About editing the guide information file:

See 6.6 *Editing guide information* in the *JP1/Integrated Management 3 - 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 *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

7.3 Cautions on integrated scope

- Do not stop the service while updating the tree. Inconsistencies may occur with the database contents.
If inconsistencies occur with the database, 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, <code>)" are displayed.
If this occurs, restore the backup of the database, or recreate the database by `jcsdbsetup` command. For details about the procedure for recovering the monitored object database, see [1.2.2\(2\) Monitored object database backup and recovery procedures](#), and [1.2.2\(3\) Host information database backup and recovery procedures](#).
- If the central scope service abnormally terminates or is forcibly terminated, the database used by the central scope service may become corrupted. For this reason, back up the database on a regular basis. For details about the procedure for backing up the monitored object database, see [1.2.2\(2\) Monitored object database backup and recovery procedures](#), and [1.2.2\(3\) Host information database backup and recovery procedures](#).
- When you reinstall JP1/IM - Manager after uninstalling it, or if you connect JP1/IM - View after executing `jcsdbsetup` command, the [Monitoring tree] window may display the monitoring tree that existed before JP1/IM - Manager was reinstalled or the monitoring tree that existed before the `jcsdbsetup` command was executed. If that happens, stop the JP1/IM - View that is running, and delete the following folder before starting JP1/IM - View. The folder to be deleted:
`View-path\log\output`
- If you deleted the event DB for JP1/Base, follow these procedures:
 - Start the [Monitoring Tree (being edited)] window of JP1/IM - View.
 - Select [File], and then [Obtain tree from server], to obtain the monitoring tree from the server.If you don't perform the above procedures, the following phenomenon occurs.
 - In the [Status Change Event Search] of the [Monitoring Tree] window, a wrong event is displayed.
 - In the guide function, another guide is displayed.
- If the host name defined in the system configuration definition of JP1/IM and the host name included in the information collected by the automatic generation function are different, a monitoring object that is identical to the one included in the existing monitoring tree is output as a difference.
For example, if the host name written in FQDN format in the system configuration definition of JP1/IM is defined in a format other than FQDN on the job execution host of JP1/AJS2, a jobnet monitoring object is output as a difference. If it is not necessary, manually delete the monitoring object that has been output as a difference.
- If you start the [Monitoring Tree] window of Jp1/IM - View soon after you started JP1/IM - Manager or while the tree is being updated, a message "KAVB7240-W JP1/IM - CS was temporarily unable to perform the operation request (monitoring tree acquisition) from JP1/IM - View (Cause: The database is being used by another user) is displayed, and the [Monitoring Tree] window is not displayed. If that happens, wait for a while and then restart the [Monitoring Tree] window.
- When you monitor an event in JP1/SES format, you are not allowed to specify a message and detailed information of a basic attribute as a status change condition for an individual condition or a common condition.
- Regarding the message, detailed information and extended attribute of JP1 events, the character codes supported in status change conditions of the monitoring node are C (English code).
- If the status of the monitoring group is other than the initial status, and basic attributes or extended attributes of JP1 event are included in the guide viewing conditions for the guide information displayed in the monitoring group, the guide information will not change unless the status of the applicable monitoring group changes to the initial status. For example, consider a situation where a monitoring object with an error status and a monitoring object with a warning status exist directly under a monitoring group.

In this situation, it is assumed that the monitoring group has the error status, and a guide, whose viewing condition is a JP1 event that meets a status change condition for a monitoring object with the error status, is displayed in the monitoring group.

In this situation, changing the status of the monitoring object from error to initial, therefore changing the status of the monitoring group to warning, will not change the guide information displayed in the monitoring group.

Changing the status of the monitoring object from warning to initial, therefore changing the status of the monitoring group to initial, will change or hide the guide information. We recommend that you specify only the monitoring node ID for a viewing guide condition that is displayed in the monitoring group, and provide a definition that does not include basic attributes or extended attributes of a JP1 event. Providing a definition like this allows you to always display the same guide, when you display guide in a monitoring group, regardless of the status of the monitoring group. Furthermore, be sure to provide a definition for a guide in which you specified only a monitoring node ID as a guide viewing condition, before providing a definition for a guide that includes basic attributes or extended attributes of a JP1 event as its viewing condition.

- The default setting for updating data to a monitoring object DB on a server is asynchronous writing.
- The following settings in a cluster configuration enables synchronous writing when the data is updated to the server.
 - (a) Stop all the JP1/IM - Managers in physical host and logical host environments.
 - (b) Create a text file with the following contents. (Fill in the name of the logical host to be configured, for "Logical host name" below).

```
[Logical-host-name\JP1SCOPE\BMS]
```

```
"DB_ACC_MODE_SYNC"=dword:00000000
```

- (c) Specify the text file you created in (b) for the argument, and execute the following command on the active server and on the standby server.

```
jbssetcnf <The name of the file created>
```

If you configure settings to enable synchronous writing to a monitoring object DB, the performance of updating data to the server decreases. However, because this makes it less likely that a monitoring object DB will be damaged at the time of logical host failover, the above configuration is recommended for a cluster environment.

- To change the configuration from synchronous writing back to asynchronous writing, use the following procedures:
 - (a) Stop all the JP1/IM - Manager in physical host and logical host environments.
 - (b) Create a text file with the following contents. (Fill in the name of the logical host to be configured, for "Logical host name" below).

```
[Logical-host-name\JP1SCOPE\BMS]
```

```
"DB_ACC_MODE_SYNC"=dword:00000001
```

- (c) Specify the text file you created in (b) for the argument, and execute the following command on the active server and on the standby server.

```
jbssetcnf <The name of the file created>
```

- Specify one of the following names for the host name to be specified as the status change condition for the monitoring object. If you don't specify one of the following host names, the status of the monitoring object may not change even if a JP1 event occurs.

- (a) The host name returned by hostname command.
- (b) The host name you registered with the host information DB.

For details on how to configure (b), see *jcshostsimport command* in *Chapter 1. Commands* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

- Specify the following host name for a managed host and a manager host of JP1/IM - Manager. If you don't specify the following host name, the monitoring node of the applicable host may not be displayed when using the automatic generation function of the monitoring tree.
 - (a) The host name returned by hostname command

For details on how to configure a managed host and a manager host of JP1/IM - Manager, see the description of the configuration definition file (`jbs_route.conf`) in the *JP1/Base User's Guide*.

- If you automatically generate a large number of monitoring nodes using the automatic generation function of the monitoring tree, the automatic generation of the monitoring tree may time out. If that happens, execute the setup command for the automatic generation on the managed host and disable the automatic generation to decrease the number of the monitoring nodes that are going to be generated with the automatic generation function.

Furthermore, if there is more than one managed host of JP1/IM - Manager where JP1/Base has not been started, the automatic generation of the monitoring tree may time out. If that happens, start JP1/Base, or exclude the hosts where JP1/Base has not been started from the managed hosts of JP1/IM - Manager.

- If you automatically generate the monitoring tree using the "business-oriented tree" template, monitoring objects for JP1/PFM placed under the monitoring group named <AJS2 host name> are generated to correspond to resources or applications monitored by JP1/PFM on the <AJS2 Host name> host. Manually delete the monitoring objects for resources and applications that are not related to the jobnet represented by the monitoring group named <jobnet name> to which <AJS2 host name> belongs.

Similarly, with regard to the monitoring objects for JP1/PFM placed under the monitoring group named <Cosminexus operation management agent host name>, manually delete the monitoring objects for resources and applications that are not related to J2EE application represented by the monitoring group for <Cosminexus business operation>.

- If you edit the filter definition file (`snmpfilter.conf`) for the SNMP trap conversion function of JP1/Base, in order to monitor JP1/Cm2/NNM, add only definitions regarding the SNMP trap to be monitored in your environment from the definitions in the sample file (`snmpfilter_im_sample.conf`) to the filter definition file. Configure the size of the definition within 900 bytes in the filter definition file, by using the following formula.

$$((a1+1) + (a2+1) + (a3+1) + (a4+1) \dots (an+1)) + 34 < 900 \text{ bytes}$$

- an: The OID length of the SNMP trap defined in `snmpfilter.conf` (If OID is [1.2.3.4.5], an is 10 bytes.)
 - If general traps are defined in `snmpfilter.conf`, the filter size is the [Result of the above calculation + (Number of general traps * 2)].
 - For the filter, based on what is defined in the filter file (`snmpfilter.conf`), the applicable object ID (OID) is obtained from `trapd.conf` of NNM.
- In the list of common conditions in the Common Condition Settings window, the following items are displayed but are not used in an English environment:
 - Common conditions related to JP1/Cm2/SSO, such as a System Alert Event (SSO) or an Application Alert Event (SSO)
 - Common conditions related to SCIM, such as a System Error Event (SCIM) or a System Warning Event (SCIM)
 - Common conditions related to System Manager, such as a Physical Host Emergency Event (System Manager)
 - In the list of monitoring node types in the Create New Monitoring Node window, the following items are displayed but are not used in an English environment:
 - Monitoring objects related to JP1/Cm2/SSO, such as a System Alert Event (SSO) or Category Monitoring (SSO)
 - Monitoring objects related to SCIM, such as a System Error Event (SCIM) or a System Warning Event (SCIM)
 - Monitoring objects related to System Manager, such as a Physical Host Emergency Event (System Manager)
 - In the list of generation trees in the Auto-generation - Select Configuration window the following item is displayed but is not used in an English environment:
 - System Configuration Tree
 - Tuning to improve performance of JP1 event reception of central scope

When JP1/IM - Manager receives a JP1 event, the received JP1 event is compared by central scope with the state change conditions of each monitored object in the monitoring tree. If the number of monitored objects increases, the

number of comparisons also increases. This deteriorates the performance of not only central scope, but also JP1/IM - Manager as a whole.

Tuning to prevent performance deterioration, and to enhance the JP1 event reception performance of central scope, is described below.

(a) By validating the definition file for on-memory mode of status change conditions, JP1 event reception performance can be expected to improve because the number of times the disk is accessed for central scope processing when a JP1 event is received can be reduced.

(b) To reduce the state change conditions that are compared, central scope performs filter processing when a JP1 event is received by using the following state change conditions:

- Common conditions
- Host name as an individual condition (the individual condition that set host name comparison as the comparison method)

By setting the items described above in the state change conditions of the monitored object, JP1 event reception performance can be expected to improve because of the number of state change conditions for comparison can be reduced.

- When the system monitoring object [NNMi Monitor] or [Node Monitor (NNMi)] is used, please set the extended attribute NNMI_FAMILY_UK for the JP1 event, which is issued by JP1/IM-EG and converted to an NNMi incident (This is not set by default).

When the extended attribute NNMI_FAMILY_UK is not set, the system monitoring object [NNMi Monitor] or [Node Monitor (NNMi)] cannot be monitored. For details on how to set up the extended attribute NNMI_FAMILY_UK, see the *JP1/Integrated Management 2 - Event Gateway for Network Node Manager i*.

8

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 3. Event Console Window* and *Chapter 4. Monitoring Tree Window* in the *JP1/Integrated Management 3 - Manager GUI Reference*.

8.1 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.

8.1.1 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 *1.16 Setting up a command execution environment (for Windows)* or *2.15 Setting up a command execution environment (for UNIX)* in the *JP1/Integrated Management 3 - 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 *4.1.4(3) How to specify business groups* in the *JP1/Integrated Management 3 - 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)
- JP1/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 *3.41 Preview Command Execution Content window* in the *JP1/Integrated Management 3 - 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.

8.1.2 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
1.16 Setting up a command execution environment (for Windows) in the JP1/Integrated Management 3 - Manager Configuration Guide
- For UNIX
2.15 Setting up a command execution environment (for UNIX) in the JP1/Integrated Management 3 - 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 3.41 *Preview Command Execution Content window* in the *JP1/Integrated Management 3 - 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.

8.1.3 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*.

8.1.4 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*.

8.2 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 *3.32 Action Parameter Definitions window* in the *JP1/Integrated Management 3 - 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 *JP1/Integrated Management 3 - Manager Command, Definition File and API 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.

8.2.1 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 *3.32 Action Parameter Definitions window* in the *JP1/Integrated Management 3 - Manager GUI Reference*.
See *3.33.1 Action Parameter Detailed Definitions window* in the *JP1/Integrated Management 3 - 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 *JP1/Integrated Management 3 - Manager Command, Definition File and API 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 *JP1/Integrated Management 3 - Manager Command, Definition File and API 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 *4.1.4(2) Assigning a JP1 resource group and permission level to a JP1 user* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

To check the execution status of an automated action:

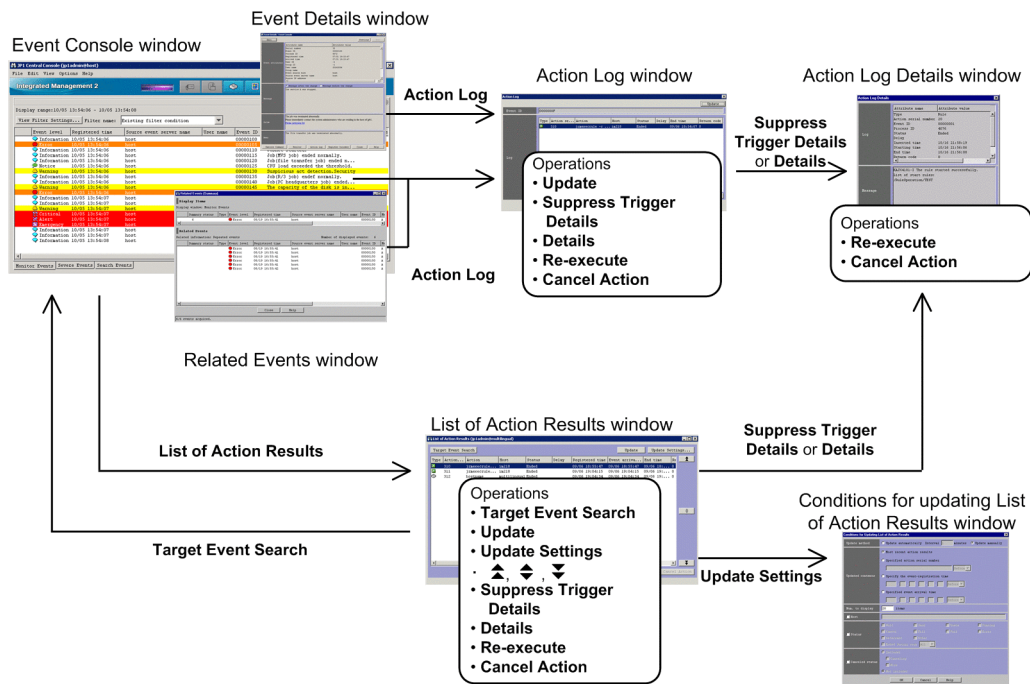
1. In the Event Console window, check the execution status of the automated action. Alternatively, check whether a notification command has reported that an error occurred.
If generation of a JP1 event was set, a JP1 event with event ID 2010 or 2011 is displayed in the events list. If execution of a 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 *8.2.2 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.

8.2.2 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 8–1: 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 *3.37 Action Log Details window* in the *JP1/Integrated Management 3 - 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 *3.39 Conditions for Updating List of Action Results window* in the *JP1/Integrated Management 3 - 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 *3.37 Action Log Details window* in the *JP1/Integrated Management 3 - 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 *JP1/Integrated Management 3 - Manager Command, Definition File and API 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 *4.1.4(2) Assigning a JP1 resource group and permission level to a JP1 user* in the *JP1/Integrated Management 3 - 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 *8.2.2(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 [8.2.2\(1\) 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 [8.2.2\(1\) 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 *JP1/Integrated Management 3 - Manager Command, Definition File and API 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 [4.1.4\(2\) Assigning a JP1 resource group and permission level to a JP1 user](#) in the *JP1/Integrated Management 3 - 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 *8.2.2(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 *8.2.2(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.

8.2.3 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 `jcastatus` command to check the operating status of the automated action function.

When the `jcastatus` 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 `jchange` 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 `jcastatus` command and the display format

See *jcastatus* (in *Chapter 1. Commands*) in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

For the `jcachange` command and the display format

See *jcachange* (in *Chapter 1. Commands*) in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

For details about how to start and stop JP1/IM - Manager:

See *Chapter 3. Starting and Stopping JP1/IM - Manager*.

8.3 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

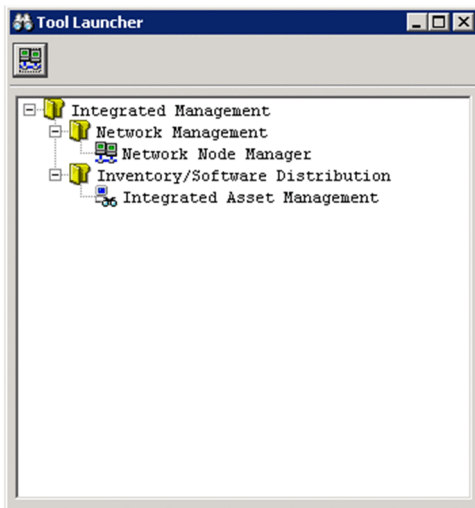
When an application on the system provides a Web page, you can display that Web page. When you select a program from the Tool Launcher, a Web browser starts and displays the Web page.

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 *JP1/Integrated Management 3 - Manager Command, Definition File and API 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 8–2: 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 [8.3.2 Functions that can be operated from the Tool Launcher window](#).

8.3.1 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 JP1/Integrated Management 3 - Manager Command, Definition File and API 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 8–1: 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.

8.3.2 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 8–2: 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

9

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 5. IM Configuration Management Window* in the *JP1/Integrated Management 3 - Manager GUI Reference*.

9.1 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 3 - 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 3 - 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 3 - 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 3 - 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 3 - 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 3 - Manager Configuration Guide*.

9.2 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 3 - 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 3 - 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 3 - 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 3 - 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 3 - 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 3 - Manager Configuration Guide*.

9.3 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 8.3 *Virtualization configuration management* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

9.3.1 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 3 - Manager Configuration Guide*.

9.3.2 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.

9.3.3 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.

9.4 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 *JPI/Integrated Management 3 - 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 *JPI/Integrated Management 3 - 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 *JPI/Integrated Management 3 - 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 *JPI/Integrated Management 3 - Manager Configuration Guide*.

9.5 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 3 - 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 3 - 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 3 - 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 3 - 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 3 - Manager Configuration Guide*.

9.6 Managing service operation status

This chapter explains how to use IM Configuration Management - View to manage the status of service operations on each host.

9.6.1 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 *8.7.2 Collecting service activity information* in the *JP1/Integrated Management 3 - 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 *8.7.2 Collecting service activity information* in the *JP1/Integrated Management 3 - 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.

9.6.2 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 [9.6.1 Collecting service operation information](#).

The information on services in the IM Configuration Management window displays the following types of operation information:

Table 9–1: 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 9–2: Commands that collect information about individual services

Service name	Collection command
JP1/Base	jbs_spm�_status
Event Service	jevstat
Log file trap	jevlogstat ALL
JP1/IM - Manager	jco_spm�_status
Log file trap (remote)	jcfallogstat#
Event log trap (remote)	jcfaleltstat#

#: Information corresponding to the collection command is output.

9.7 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.

9.7.1 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 *JP1/Integrated Management 3 - Manager Command, Definition File and API 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 *JP1/Integrated Management 3 - Manager Command, Definition File and API 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 *JP1/Integrated Management 3 - Manager Command, Definition File and API 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 9–3: 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 9–4: 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 9–5: 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>jvlog_start.conf</code>
Event log-trap action definition file	<code>ntevent.conf</code>
Local action execution definition file	<code>jbslact.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 (*al*) 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 9–6: 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>ntevent.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 9–7: Exported business 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 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 2-85 Character encoding of files in Host input information file (host_input_data.csv) in Chapter 2. Definition Files of the JP1/Integrated Management 3 - Manager Command, Definition File and API 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 9–8: 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 <code>LANG</code> environment variable of the manager. For details, see <i>Table 2-85 Character encoding of files in Host input information file (host_input_data.csv) in Chapter 2. Definition Files of the JP1/Integrated Management 3 - Manager Command, Definition File and API 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"
```

9.7.2 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 [9.7.3 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 JPI/Integrated Management 3 - Manager Command, Definition File and API 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 9–9: 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}	This item can be used for remote monitoring. You can input one of the following: <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 the virtual management former host name.	

Host type	Virtual manager type	Configuration information corresponding to virtual manager type	Required/Optional	Remarks
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 9–10: 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 9–11: 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	ntevent.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 9–12: 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 entire string in double quotation marks.	Optional	Blank
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 9-9 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 9–13: 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 in double quotation marks. Do not use environment-dependent characters for monitoring group names. Such characters can cause character corruption in the definition.	Required	--
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 Table 9-9 Host	Optional	Blank

Item	Input range	Required/Optional	Default
	<i>information that is imported (manually-entered information).</i>		

Legend:

--: There is no default value.

9.7.3 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 `jcimport` 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 3 - 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 3 - Manager Configuration Guide*.

9.8 Cautions on the IM configuration

- If you perform unsetup of the IM configuration management database, set it up again, and then connect to the IM configuration management viewer, the host icon might not appear in the system hierarchy in the IM configuration tab. If this problem occurs, then the system hierarchy will display the configuration from before you performed unsetup of the database. To update the system hierarchy, from the menu bar select [Operations], and then [IM configuration collection].
- In the information of JP1/Integrated Management - Manager, which is displayed in [Product Information] on the [Hosts List] page, the version of the following items might differ:
 - JP1/Integrated Management - Central Scope
 - JP1/Integrated Management - Central Console

For details on the version of JP1/Integrated Management - Manager, see the JP1/Integrated Management - Manager items.

- When using the following functionality in IM Configuration Management, use JP1/Base 09-50-01 or higher:
 - When using references or limiting the operation of a business group (when specifying the `-bizmonmode` option in `jcoimdef`)
 - When you want to apply an IM configuration without deleting the system hierarchy (when specifying `"APPLY_CONFIG_TYPE"=dword:00000001` to the IM configuration reflecting method settings file `[jp1cf_applyconfig.conf]`)
- In the list of virtual Manager types in [Virtual Manager Settings] window, although [JP1/SC/CM] will be displayed, it will not be used in an English environment.

10

Starting and Stopping JP1/IM - Agent

This section provides instructions for starting and stopping JP1/IM - Agent.

10.1 Service of JP1/IM - Agent

You can use the following commands to operate JP1/IM - Agent services:

Command name	Function
<code>jpc_service</code>	Sets whether to enable or disable the enrollment of services on systemd of Windows or Linux.
<code>jpc_service_start</code>	Start the service.
<code>jpc_service_stop</code>	Stop the service.
<code>jpc_service_autostart</code>	Set whether to start the service automatically when OS starts.

The service key specified in the above command is shown below.

Table 10–1: Service key of JP1/IM - Agent in Windows

Display name	Service key
JP1/IM3-Agent	<code>jpc_imagent</code>
JP1/IM3-Agent proxy	<code>jpc_imagentproxy</code>
JP1/IM3-Agent action	<code>jpc_imagentaction</code>
JP1/IM3-Agent Metric forwarder	<code>jpc_prometheus_server</code>
JP1/IM3-Agent Alert forwarder	<code>jpc_alertmanager</code>
JP1/IM3-Agent Windows metric collector	<code>jpc_windows_exporter</code>
JP1/IM3-Agent Synthetic metric collector	<code>jpc_blackbox_exporter</code>
JP1/IM3-Agent Log trapper	<code>jpc_fluentd</code>
JPC YA Cloudwatch exporter	<code>jpc_ya_cloudwatch_exporter</code>
JPC Promitor Scraper	<code>jpc_promitor</code>
JPC Promitor Resource Discovery	
JPC Script exporter	<code>jpc_script_exporter</code>
JP1/IM3-Agent Synthetic web metric collector	<code>jpc_web_exporter</code>
JP1/IM3-Agent VMware metric collector	<code>jpc_vmware_exporter</code>

Table 10–2: Service key of JP1/IM - Agent in Linux

Unit definition file Name	Service key
<code>jpc_imagent.service</code>	<code>jpc_imagent</code>
<code>jpc_imagentproxy.service</code>	<code>jpc_imagentproxy</code>
<code>jpc_imagentaction.service</code>	<code>jpc_imagentaction</code>
<code>jpc_prometheus_server.service</code>	<code>jpc_prometheus_server</code>
<code>jpc_alertmanager.service</code>	<code>jpc_alertmanager</code>
<code>jpc_node_exporter.service</code>	<code>jpc_node_exporter</code>
<code>jpc_blackbox_exporter.service</code>	<code>jpc_blackbox_exporter</code>

Unit definition file Name	Service key
<code>jpc_ya_cloudwatch_exporter.service</code>	<code>jpc_ya_cloudwatch_exporter</code>
<code>jpc_fluentd.service</code>	<code>jpc_fluentd</code>
<code>jpc_process_exporter.service</code>	<code>jpc_process_exporter</code>
<code>jpc_promitor_scraper.service</code>	<code>jpc_promitor</code>
<code>jpc_promitor_resource_discovery.service</code>	
<code>jpc_script_exporter.service</code>	<code>jpc_script_exporter</code>
<code>jpc_vmware_exporter.service</code>	<code>jpc_vmware_exporter</code>

For details on enabling or disabling add-on program for JP1/IM - Agent, see *1.21.1(1) Enable or disable add-on program in the JP1/Integrated Management 3 - Manager Configuration Guide*.

10.2 Starting the Service

Run the following command to start JP1/IM - Agent services:

```
jpc_service_start -s service-key
```

If you specify `all` as the *service-key*, all services in JP1/IM - Agent are started.

For details on the auto start setting, see *1.21.1(2) Enable and Disable of Auto-start* in the *JP1/Integrated Management 3 - Manager Configuration Guide*.

10.3 Stopping the service

Stop JP1/IM - Agent service by running the following command:

```
jpc_service_stop -s service-key [-f]
```

If you specify `all` as the *service-key*, all services in JP1/IM - Agent are stopped.

If `-f` is specified, the service is terminated forcibly.

For details about automatic shutdown during OS shutdown, see *1.21.1(2) Enable and Disable of Auto-start* in the *JP1/Integrated Management 3 - Manager Configuration Guide*.

10.4 Optional Functions in JP1/IM - Agent

10.4.1 Servicing OracleDB exporter

(1) Windows

(a) Service name and display name

The service name and display name of OracleDB exporter service (Windows service) are shown below.

Service operating environment	Service name	Display name
Physical host	<i>Oracledb_exporter_instance-name</i>	OracleDB Exporter <i>instance-name</i>
Logical host	<i>Oracledb_exporter_instance-name_logical-host-name</i>	OracleDB Exporter <i>instance-name logical-host-name</i>

(b) Starting the Service

Start OracleDB exporter in one of the following ways:

- Start on Windows management tools service-screen.
- Start by sc command or net command.

(c) Stopping the service

Shut down OracleDB exporter in one of the following ways:

- Shut down on Windows management tools service-screen.
- It is stopped by sc command or net command.

(d) Auto start setting

In Windows management tools Services window, set the startup type in OracleDB exporter to automatic startup.

(2) Linux

(a) Unit name and Description

The following table shows the unit names and Description for OracleDB exporter servicing in a Linux.

Service operating environment	Unit name	Description
Physical host	<i>Oracledb_exporter_instance-name</i>	OracleDB Exporter <i>instance-name</i>
Logical host	<i>Oracledb_exporter_instance-name_logical-host-name</i>	OracleDB Exporter <i>instance-name logical-host-name</i>

(b) Starting the Service

Start the service with the following command:

```
$ systemctl start unit-name
```

(c) Stopping the service

Stop the service with the following command:

```
$ systemctl stop unit-name
```

(d) Auto start setting

- Enabling Automatic Startup

Enable automatic startup of the service with the following command:

```
$ systemctl enable unit-name
```

- Disabling automatic startup

Disable automatic startup of services with the following command:

```
$ systemctl disable unit-name
```

(e) Alive monitoring

Check the operating status of the service with the following command.

```
$ systemctl is-active unit-name
```

10.4.2 Servicing Node exporter for AIX

Node exporter for AIX services are operated on the monitored AIX hosts.

(1) Enabling registering services

Enable service registration with the following command:

- For physical host operation

```
mkssys -p /bin/sh -s jpc_node_exporter_aix -u root -S -f 9 -n 15 -a "-c \  
'"Node-exporter-for-AIX-destination-directory/jplima/bin/node_exporter_aix  
' -CcADmdiabf -p 20730 2>&1 | logger\''"
```

- For logical host operation

```
mkssys -p /bin/sh -s jpc_node_exporter_aix__logical-host-name# -u root -S  
-f 9 -n 15 -a "-c \  
'"Node-exporter-for-AIX-destination-directory/jplima/bi  
n/node_exporter_aix' -CcADmdiabf -p 20730 2>&1 | logger\''"
```


 If the logical hostname is 8 bytes or more, specify `-s` option by appending "jpc_node_exporter_aix_" followed by any character string up to 7 characters. The character string specified in `-s` option must be unique within Subsystem of `lssrc -a` command.

The following is a description of the above `node_exporer_aix` command-options:

- Node_exporer_aix Command-Option

Item name	Description	Chang eab ility	What you set in JP1/IM-Agent	JP1/IM - Agent Default value
-C#	Specifies that metrics are to be collected for linux node exporter.	Y	--	--
-c#	Specifies that metrics are to be collected for CPU.	Y	--	--
-A#	Specifies that metrics are to be collected for the disk adapter.	Y	--	--
-D#	Specifies that metrics are to be collected for the disk path.	Y	--	--
-m#	Specifies that metrics are to be collected for memory.	Y	--	--
-d#	Specifies that metrics are to be collected for the disk.	Y	--	--
-i#	Specifies that metrics are to be collected for a network interface.	Y	--	--
-a#	Specifies that metrics are to be collected for the net adapter.	Y	--	--
-b#	Specifies that metrics are to be collected for the net buffer.	Y	--	--
-f#	Specifies that metrics are to be collected for the file system.	Y	--	--
-p	Specify the listen port.	Y	Specify this option if you want to change the port.	-p 20730

Legend

Y: Changeable --: Not applicable

 If all options other than `-p` are not specified, the command is enabled.

(2) Disable registering service

Disable service registration with the following command:

- For physical host operation

```
rmssys -s jpc_node_exporter_aix
```

- For logical host operation

```
rmssys -s jpc_node_exporter_aix_logical-host-name#
```

#

If the logical host name is 8 bytes or more, add any character string of up to 7 characters specified in [10.4.2\(1\) Enabling registering services](#) or [10.4.2\(3\) Registering the service changed](#) to the end of "jpc_node_exporter_aix_" and specify it in -s option.

(3) Registering the service changed

If you want to change Node exporter for AIX port number, use the following command to change the service-registration:

- For physical host operation

```
chssys -p /bin/sh -s jpc_node_exporter_aix -u root -S -f 9 -n 15 -a "-c \
'"Node-exporter-for-AIX-destination-directory/jplima/bin/node_exporter_aix
' -CcADmdiabf -p new-port-number 2>&1 | logger\""
```

- For logical host operation

```
chssys -p /bin/sh -s jpc_node_exporter_aix_logical-host-name# -u root -S
-f 9 -n 15 -a "-c \'"Node-exporter-for-AIX-destination-directory/jplima/bi
n/node_exporter_aix' -CcADmdiabf -p new-port-number 2>&1 | logger\""
```

#

If the logical hostname is 8 bytes or more, specify -s option by appending "jpc_node_exporter_aix_" followed by any character string up to 7 characters. The character string specified in -s option must be unique within Subsystem of lssrc -a command.

(4) Checking the status of services

Check the status of the service with the following command:

- For physical host operation

```
lssrc -s jpc_node_exporter_aix
```

- For logical host operation

```
lssrc -s jpc_node_exporter_aix_logical-host-name#
```

#

If the logical host name is 8 bytes or more, add any character string of up to 7 characters specified in [10.4.2\(1\) Enabling registering services](#) or [10.4.2\(3\) Registering the service changed](#) to the end of "jpc_node_exporter_aix_" and specify it in -s option.

(5) Confirmation of service registration details

Confirm the registered contents of the service with the following command.

- For physical host operation

```
lssrc -S -s jpc_node_exporter_aix
```

- For logical host operation


```
lssrc -S -s jpc_node_exporter_aix_logical-host-name#
```

#

If the logical host name is 8 bytes or more, add any character string of up to 7 characters specified in [10.4.2\(1\) Enabling registering services](#) or [10.4.2\(3\) Registering the service changed](#) to the end of "jpc_node_exporter_aix_" and specify it in -s option.

(6) Starting the Service

1. Start the service.

Start the service with the following command:

- For physical host operation

```
startsrc -s jpc_node_exporter_aix
```

- For logical host operation

```
startsrc -s jpc_node_exporter_aix_logical-host-name#
```

#

If the logical host name is 8 bytes or more, add any character string of up to 7 characters specified in [10.4.2\(1\) Enabling registering services](#) or [10.4.2\(3\) Registering the service changed](#) to the end of "jpc_node_exporter_aix_" and specify it in -s option.

2. Confirm the start of the service.

Execute [10.4.2\(4\) Checking the status of services](#) and confirm that the service has started.

(7) Stopping the service

1. Stop the service.

Stop the service with the following command:

- For physical host operation

```
Node-exporter-for-AIX-destination-directory/jplima/bin/jpc_stop_node_exporter_aix
```

- For logical host operation

```
ode-exporter-for-AIX-destination-directory/jplima/bin/jpc_stop_node_exporter_aix -h logical-host-name#
```

#

If the logical host name is 8 bytes or more, add any character string of up to 7 characters specified in [10.4.2\(1\) Enabling registering services](#) or [10.4.2\(3\) Registering the service changed](#) to the end of "jpc_node_exporter_aix_" and specify it in -s option.

2. Confirm that the service is stopped.

Execute [10.4.2\(4\) Checking the status of services](#) to confirm that the service has stopped.

3. Confirm that the node_exporter_aix process is stopped.

Execute ps command. Confirm that the node_exporter_aix process is stopped.

(8) Forced Stop of Service

1. Stop the service forcibly.

Stop the service forcibly with the following command:

- For physical host operation

```
Node-exporter-for-AIX-destination-directory/jplima/bin/jpc_stop_node_exporter_aix -f
```

- For logical host operation

```
Node-exporter-for-AIX-destination-directory/jplima/bin/jpc_stop_node_exporter_aix -f -h logical-host-name#
```

#

If the logical host name is 8 bytes or more, add any character string of up to 7 characters specified in [10.4.2\(1\) Enabling registering services](#) or [10.4.2\(3\) Registering the service changed](#) to the end of "jpc_node_exporter_aix_" and specify it in `-s` option.

2. Confirm that the service is stopped.

Execute [10.4.2\(4\) Checking the status of services](#) to confirm that the service has stopped.

3. Confirm that the `node_exporter_aix` process is stopped.

Execute `ps` command. Confirm that the `node_exporter_aix` process is stopped.

(9) Enabling Automatic Startup

1. Set the auto-launch setting

Enable autostart with the following command:

- For physical host operation

```
mkitab "jpcaixexporter:2:wait:startsrc -s jpc_node_exporter_aix"
```

- For logical host operation

```
mkitab "jpcaixexporter:2:wait:startsrc -s jpc_node_exporter_aix_logical-host-name#"
```

#

If the logical host name is 8 bytes or more, add any character string of up to 7 characters specified in [10.4.2\(1\) Enabling registering services](#) or [10.4.2\(3\) Registering the service changed](#) to the end of "jpc_node_exporter_aix_" and specify it in `-s` option.

2. Check settings

Check the settings with the following command.

```
lsitab -a
```

(Example of execution result)

```
init:2:initdefault:
brc::sysinit:/sbin/rc.boot 3 >/dev/console 2>&1 # Phase 3 of system boot
...
jpcaixexporter:2:wait:startsrc -s jpc_node_exporter_aix
```

(10) Disabling automatic startup

1. Set the auto-launch setting

Disable autostart with the following command:

- For physical host operation

```
rmitab "jpcaixexporter"
```

- For logical host operation

```
rmitab "jpcaixexporter"
```

2. Check settings

Use the following command to confirm that the item specified in step 1 has been deleted.

```
lsitab -a
```

(11) Enabling Automatic Stop

1. Open /etc/rc.shutdown file in a text editor and add the following Node exporter for AIX description:

- For physical host operation

```
Node-exporter-for-AIX-destination-directory/jplima/bin/jpc_stop_node_exporter_aix
```

- For logical host operation

```
Node-exporter-for-AIX-destination-directory/jplima/bin/jpc_stop_node_exporter_aix -h logical-host-name#
```

#

If the logical host name is 8 bytes or more, add any character string of up to 7 characters specified in [10.4.2\(1\) Enabling registering services](#) or [10.4.2\(3\) Registering the service changed](#) to the end of "jpc_node_exporter_aix_" and specify it in -s option.

2. At the end of /etc/rc.shutdown file add one line:

```
exit 0
```

If the exit code of the last command executed is other than "0", /etc/rc.shutdown script recognizes it as an error and aborts the shutdown process.

(12) Disabling Automatic Stop

1. Open /etc/rc.shutdown file in a text editor and remove the following Node exporter for AIX descriptions:

- For physical host operation

```
Node-exporter-for-AIX-destination-directory/jplima/bin/jpc_stop_node_exporter_aix
```

- For logical host operation

```
Node-exporter-for-AIX-destination-directory/jplima/bin/jpc_stop_node_exporter_aix -h logical-host-name#
```

#

If the logical host name is 8 bytes or more, add any character string of up to 7 characters specified in [10.4.2\(1\) Enabling registering services](#) or [10.4.2\(3\) Registering the service changed](#) to the end of "jpc_node_exporter_aix_" and specify it in -s option.

2. At the end of /etc/rc.shutdown file add one line:

```
exit 0
```

If the exit code of the last command executed is other than "0", /etc/rc.shutdown script recognizes it as an error and aborts the shutdown process.

10.5 When operating in a cluster system

10.5.1 Starting the Service

Start from the cluster software.

10.5.2 Stopping the service

Stop from the cluster software.

10.5.3 Settings of auto start

Because it is controlled by the cluster software, the service auto start at OS startup is not set.

10.5.4 Auto-Stop at OS Shutdown

Because it is controlled by the cluster software, the service auto stop at OS shutdown is not set.

11

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.

11.1 Overview of BJEX and JP1/AS linkage

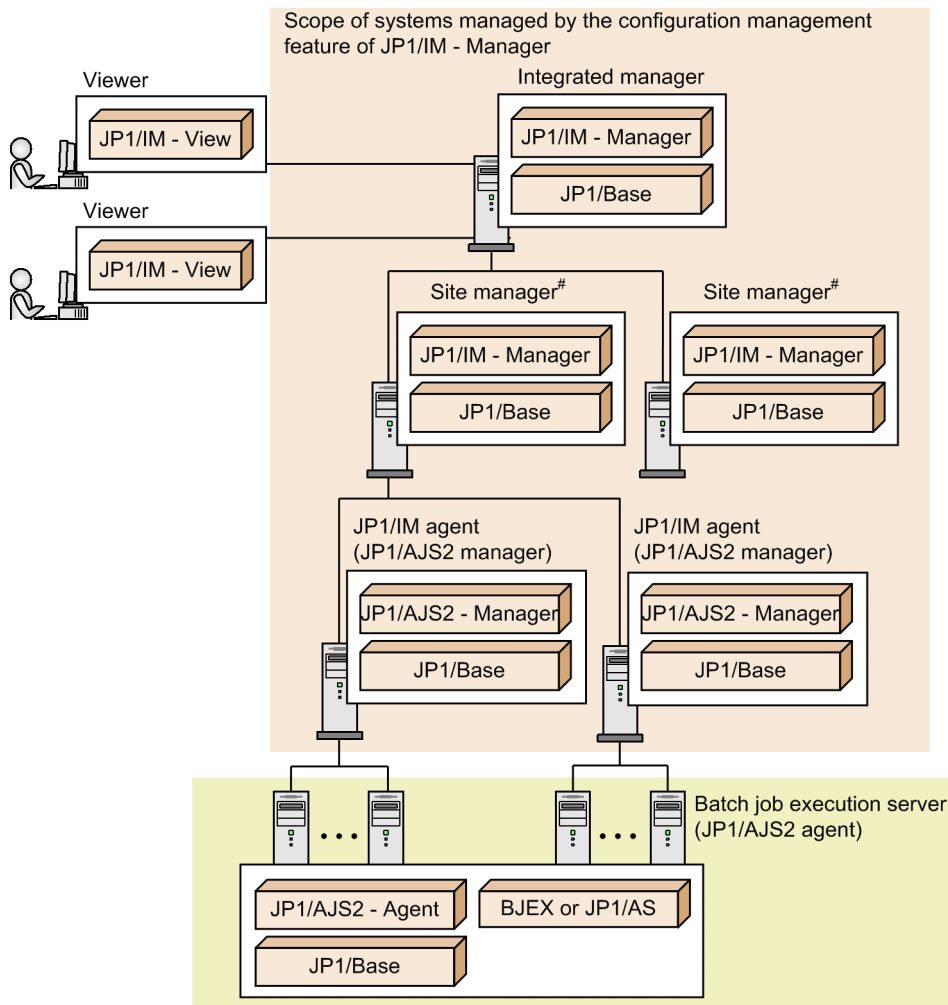
BJEX is a product that realizes mainframe-like job management in an open system. JP1/AS is a system used to create and execute shell scripts that serve as batch jobs. A job management system that links with JP1/AJS to control batch jobs (jobs that execute batch processing) is called a *batch job execution 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.

11.1.1 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 11–1: 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

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 [11.3 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

11.2 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.

11.2.1 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

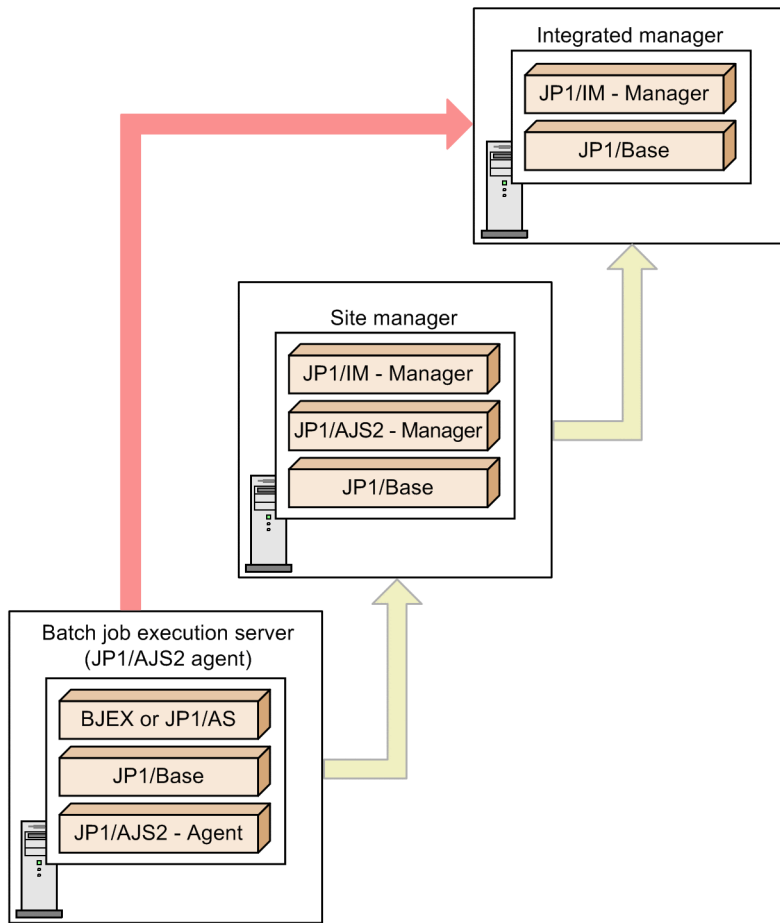
BJEX and JP1/AS issue response-waiting events directly to the integrated manager, not by the usual forwarding paths provided by JP1/Base. To have BJEX issue all response-waiting events directly to the integrated manager, specify the JP1/IM - Manager host name in the `JP1IM_MANAGER_HOST` parameter of 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 11–2: 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 [11.3 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.

11.2.2 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.

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:

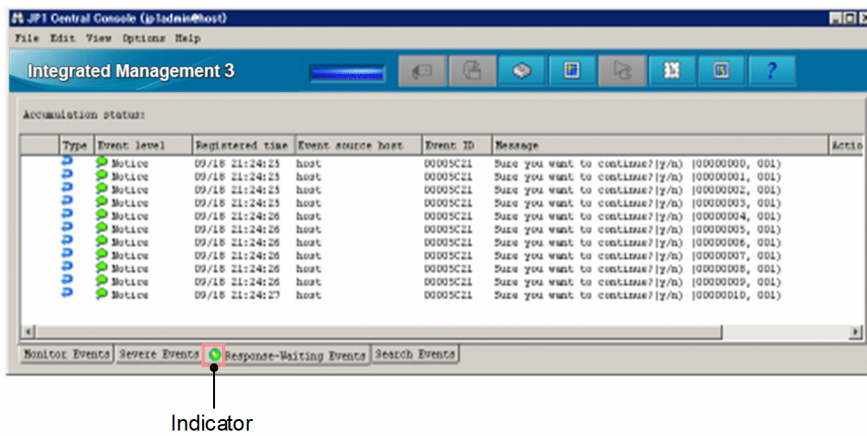
- Display detailed information about a response-waiting event
- Open the monitors of linked products
- Display execution results of automated actions
- Change display items for JP1 events
- Set the background color for JP1 events
- Set the response status for response-waiting events
- Specify the event display period

For details about these features, see *4.1 Centralized monitoring using JP1 events* in the *JP1/Integrated Management 3 - 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 11–3: 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 [11.2.3 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 [3.44.8 Filter condition definition windows](#) in the *JP1/Integrated Management 3 - 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 [11.2.3 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 [3.44.7 Event Search Conditions window](#) in the *JP1/Integrated Management 3 - 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 11–1: 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 *1.20.2 Customizing operation of JP1/IM - View (Central Console viewer and Central Scope viewer) (for Windows)* in the *JP1/Integrated Management 3 - Manager Configuration Guide*.

11.2.3 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:

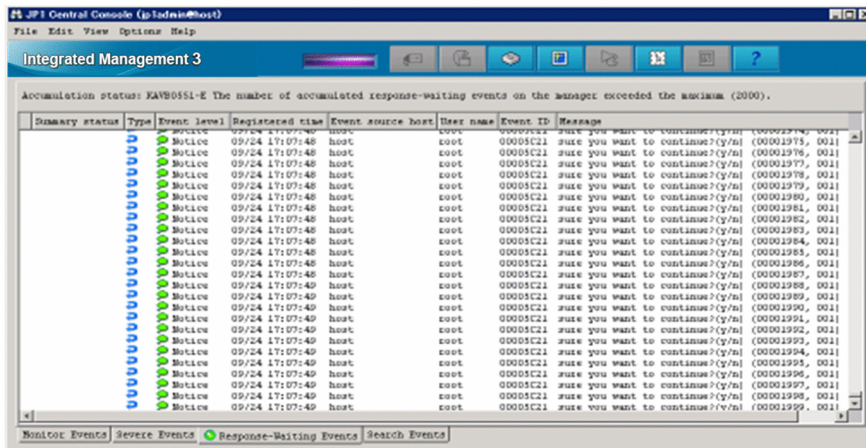
- An operator successfully responds to a response-waiting event
- The response-waiting event is canceled in BJEX or JP1/AS
- An operator manually releases the event from the hold-and-accumulate state
- There are more than 2,000 response-waiting events
In this case, accumulated response-waiting events 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 11-4: 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 [11.4.4 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*.

11.2.4 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 `yes` 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.

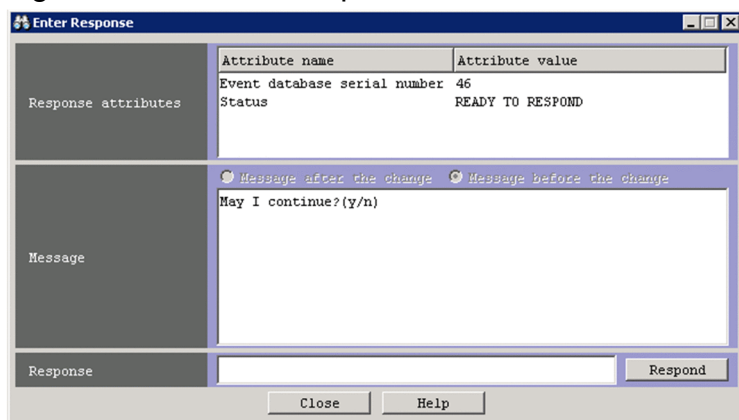
- Related Events window

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 11–5: Enter Response window



The following table lists the statuses that appear as the value of the **Status** attribute in the **Response attributes** area:

Table 11–2: 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 [11.3.4\(1\) 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.

(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*.

11.2.5 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 cancelation 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.

11.3 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.

11.3.1 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_spm�_reload` command.

For details about the `-resevent` option of the `jcoimdef` command, see [11.5.1 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_spm�_reload` command or restart JP1/IM - Manager.

For details about the `jcoimdef` command, see *jcoimdef* in *Chapter 1. Commands of the JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

For details about the `jco_spm�_reload` command, see *jco_spm�_reload* in *Chapter 1. Commands of the JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

11.3.2 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 *3.44.6 Preferences window* in the *JP1/Integrated Management 3 - 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 *5.2.2 Settings for event receiver filters* in the *JP1/Integrated Management 3 - Manager Configuration Guide*.

For details about the Detailed Settings for Event Receiver Filter window, see *3.44.8 Filter condition definition windows* in the *JP1/Integrated Management 3 - Manager GUI Reference*.

11.3.3 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*.

11.3.4 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 3 - Manager Command, Definition File and API 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 11–3: Port numbers used for communication between BJEX or JP1/AS and JP1/IM - Manager

Service	Port	Traffic direction
jplbsplugin	20306/tcp	JP1/IM - Manager -> BJEX or JP1/AS
jplimevt	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 3 - Manager Overview and System Design Guide*

11.3.5 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*.

11.4 Working with response-waiting events

This section describes the operations you can perform on response-waiting events.

11.4.1 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

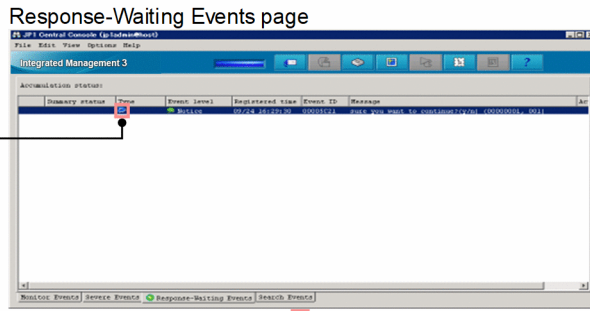
The following figure shows an overview of how to monitor and respond to response-waiting events in Central Console:

Figure 11–6: Monitoring and responding to response-waiting events in Central Console

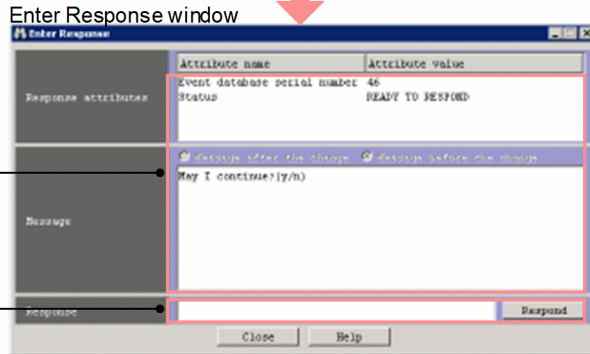
1. A response-waiting event appears on the Response-Waiting Events page.



Icon indicating a response-waiting event



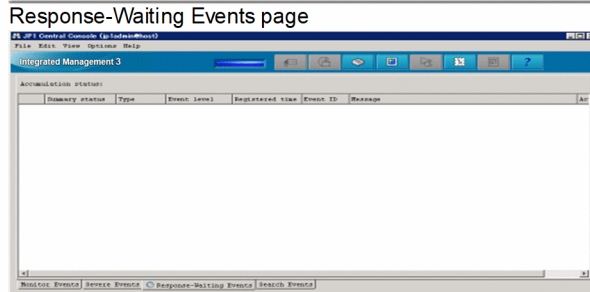
2. Display the Enter Response window.



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**.

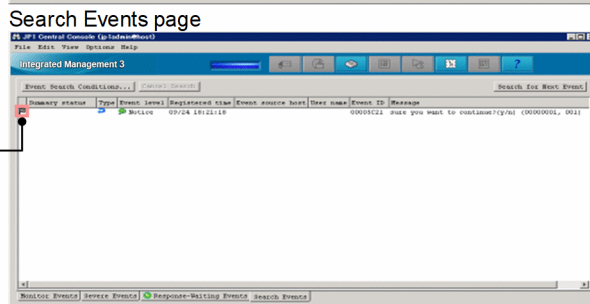
5. If the response is successful, the response-waiting event disappears from the Response-Waiting Events page.



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

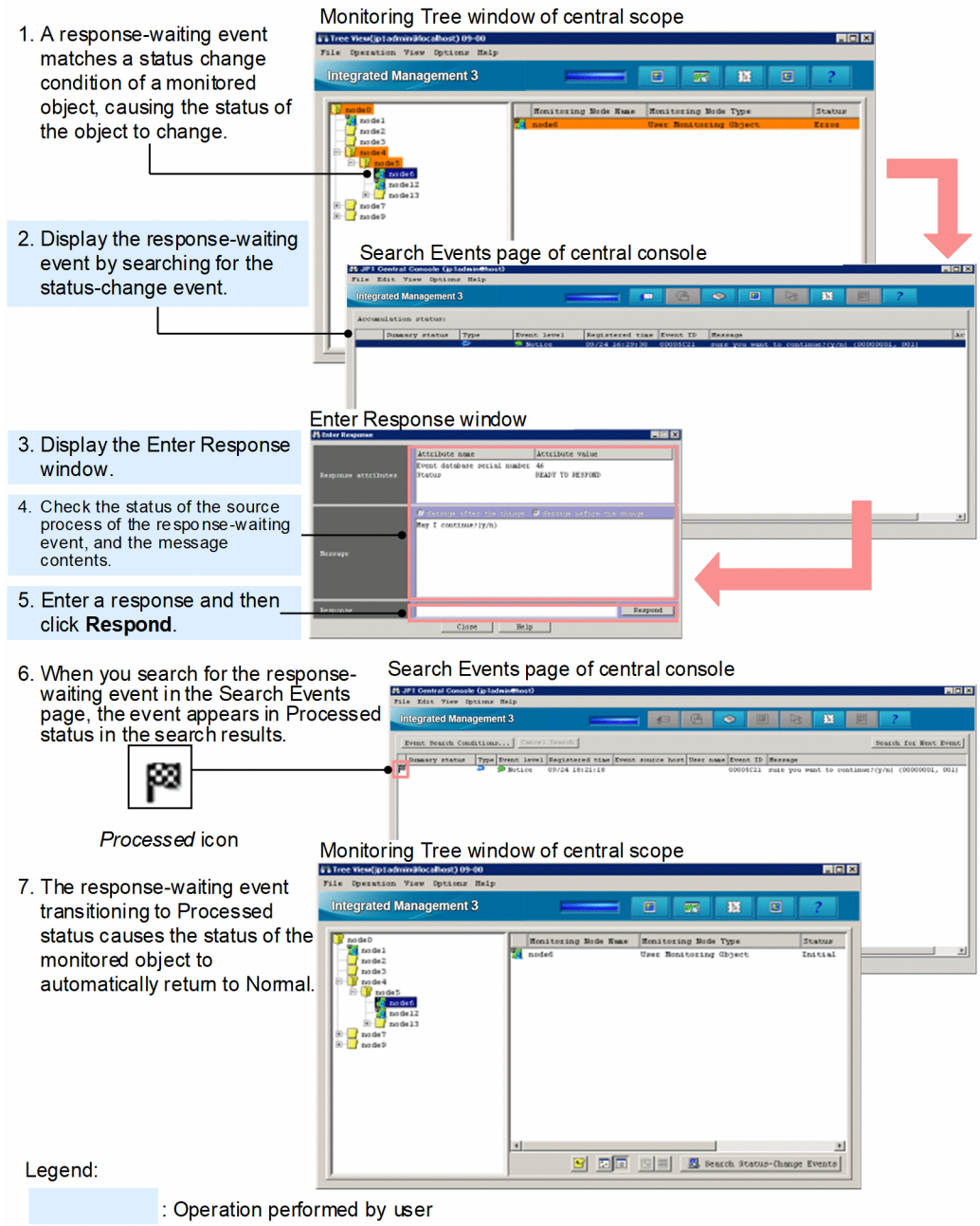
The numbers in the figures correspond to the steps below:

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 11–7: Monitoring and responding to response-waiting events in Central Scope



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.

11.4.2 Responding to response-waiting events

The conditions under which you can respond to a response-waiting event are described in [11.2.4\(2\) 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*.

11.4.3 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.

11.4.4 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 [11.2.3\(2\) 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.

11.5 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 3 - Manager Command, Definition File and API Reference*. Note that the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference* does not describe the options for linking with BJEX.

11.5.1 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 3 - Manager Command, Definition File and API Reference*.

11.5.2 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 3 - Manager Command, Definition File and API Reference*.

11.5.3 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/jplcons/log/response`

Internal directory for primary data on logical hosts

`./shared-disk/jplcons/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 3 - Manager Command, Definition File and API Reference*.

12

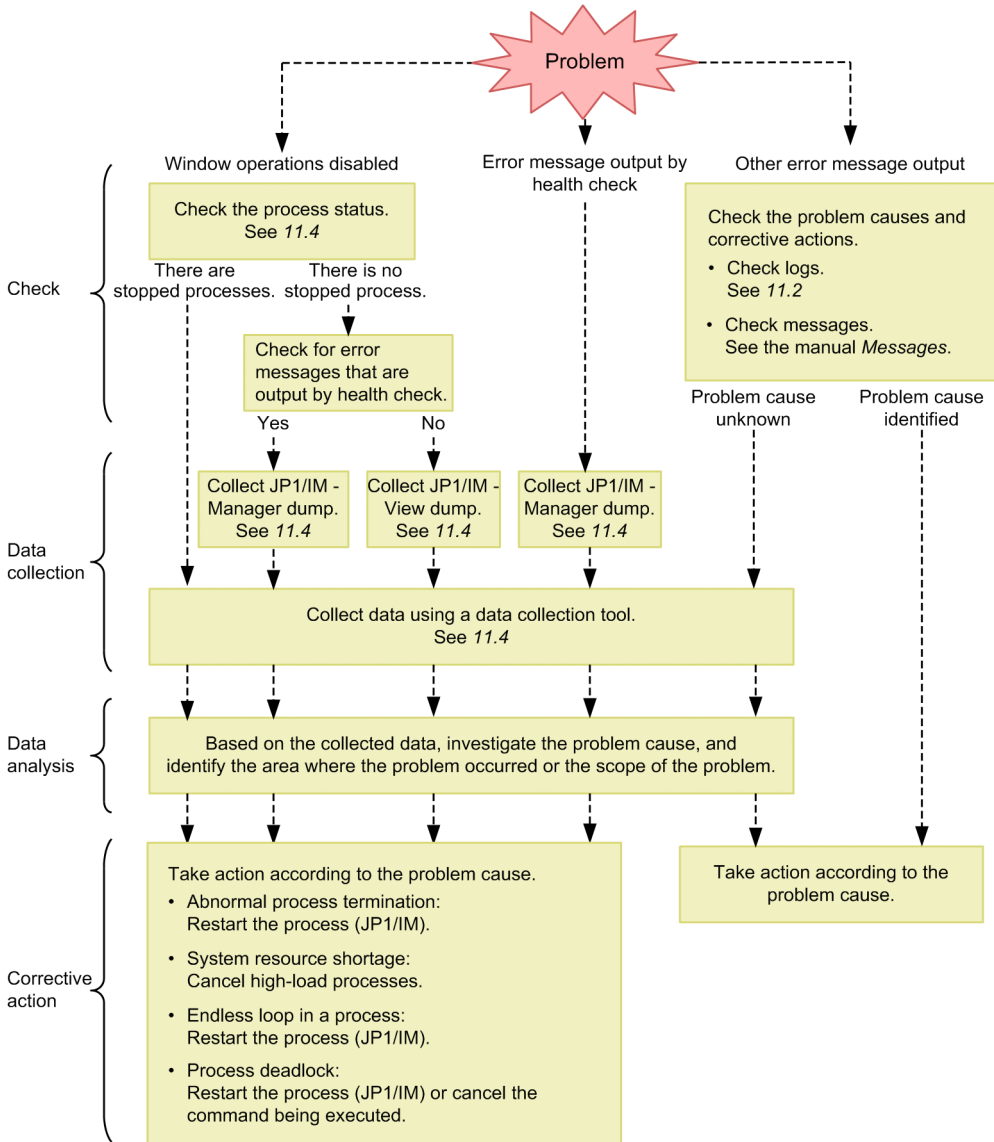
Troubleshooting

This chapter explains how to handle problems if they occur in JP1/IM. It also explains items that tend to cause problems.

12.1 Troubleshooting procedure

The figure below shows the procedure to follow when a problem occurs in JP1/IM.

Figure 12–1: Troubleshooting procedure



12.2 Log information types

This section explains the log information that is output when JP1/IM is operating.

12.2.1 JP1/IM - Manager log information

(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 SUSE Linux 15 or later, the common message log is not output to syslog by default. Instead, the common message log is output to a log file called a *journal*. In this manual, read *syslog* as *journal*.

In UNIX, the common message log is output to the following files:

- /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.

(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.

Product plugin log for JP1/IM - Agent is written to JP1/IM - Manager integrated trace log.

The default output destination of the integrated trace log is as follows:

In Windows (32 bit):

`system-drive\Program Files\Hitachi\HNTRLib2\spool\hntr2{1|2|3|4}.log`

In Windows (64 bit):

`system-drive\Program Files\Hitachi\HNTRLib2\spool\hntr2{1|2|3|4}.log`

or

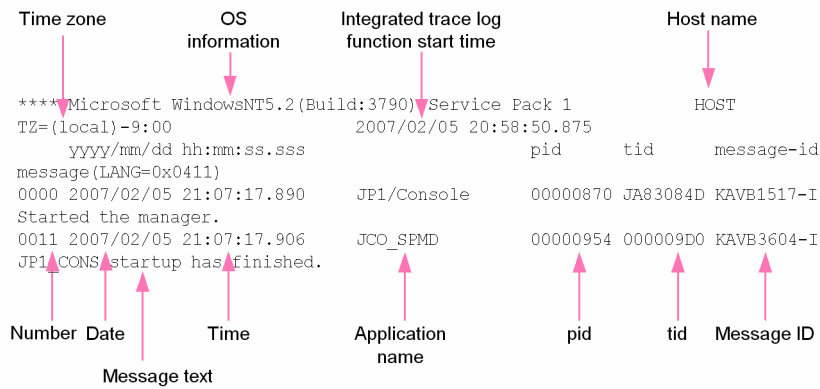
`system-drive\Program Files(x86)\Hitachi\HNTRLib2\spool\hntr2{1|2|3|4}.log`

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 12–2: 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 12–1: 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 12–2: 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 jcain • Intelligent Integrated Management Base Service jddmain • Event Generation Service evgen • Central Scope Service jcsmain

Output items	Explanation
	<ul style="list-style-type: none"> IM Configuration Management Service jcfmain 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.

(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 3 - Manager Overview and System Design Guide*.

(4) Individual log

For authentication results using the secrets listed in initial secret and IM client secret, print the success or failure of authentication and its time in the secret authentication log file in the following format: Regarding initial secret and IM client secret, refer to *3.7 Initial secret and IM client secret* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*. The file has UTF-8 (no BOMs) character encoding, and the maximum file size is 60MB.

Time Message type Message

Output Item	Description
Time	Print the time in "yyyy/MM/dd/hh:mm:ss.SSS" format.
Message type	Outputs one of the following message types:

Output Item	Description
	<ul style="list-style-type: none"> • INFO: Notification • WARN: Alert • ERROR: Failed
Message	<p>Outputs one of the following messages:</p> <ul style="list-style-type: none"> • KAJY68010-I • KAJY68011-E • KAJY68019-E <p>For details about messages, see Chapter 2. <i>List of Messages</i> in the <i>JP1/Integrated Management 3 - Manager Messages</i>.</p>

The maximum number of characters that can be output in a single line is 4096 bytes. If it exceeds 4096 bytes, it will be wrapped and output. If the 4096th byte is in the middle of a multibyte character, the character is wrapped.

Also, the destination for the secret authentication log file is as follows:

For Windows

For physical host: *Manager-path*\log\secretAuth\jddSecretAuth.log{.1|2|3}

For logical host: *Shared-folder*\jplimm\log\secretAuth\jddSecretAuth.log{.1|2|3}

For UNIX

For physical host: /var/opt/jplimm/log/secretAuth/jddSecretAuth.log{.1|2|3}

For logical host: *Shared-Directory*/jplimm/log/secretAuth/jddSecretAuth.log{.1|2|3}

(5) 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.

(a) 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 12–3: 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 ^{#3}	<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)* in *Chapter 2. Definition Files* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API 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 *Appendix K.2 Storage format of operation log output* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

#3: 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 12–4: 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 ^{#9}	<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 ^{#9}	<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 ^{#9}	<i>Console-path</i> \log\jplhassetup.{log log.old}	2,000 KB	1,000 KB
Setup log ^{#9}	<i>Console-path</i> \log\command\comdef[_old].log	512 KB	256 KB
Event console log ^{#9}	<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}
	<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}

Log type	Default file name and folder name	Maximum disk usage	File-switching timing
	<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 ^{#9}	<i>Console-path</i> \log\action\JCAMAIN{1 2 3 4 5}.log	25,600 KB ^{#2}	5,120 KB

Log type	Default file name and folder name	Maximum disk usage	File-switching timing
	<i>shared-folder\jp1cons\log\action\JCAMAIN{1 2 3 4 5}.log</i>	25,600 KB ^{#2}	5,120 KB
Product information log ^{#9}	<i>Console-path\log\hliclib\hliclibtrc{1 2 3 4 5}.log</i>	5 MB	1 MB
	<i>Console-path\log\hliclib\hlicliberr{1 2 3 4 5}.log</i>	5 MB	1 MB
	<i>Console-path\log\hliclib\hliclibmgrtrc{1 2 3 4 5}.log</i>	5 MB	1 MB
	<i>Console-path\log\hliclib\hliclibmgrerr{1 2 3 4 5}.log</i>	5 MB	1 MB
	<i>shared-folder\jp1cons\log\hliclib\hliclibtrc{1 2 3 4 5}.log</i>	5 MB	1 MB
	<i>shared-folder\jp1cons\log\hliclib\hlicliberr{1 2 3 4 5}.log</i>	5 MB	1 MB
	<i>shared-folder\jp1cons\log\hliclib\hliclibmgrtrc{1 2 3 4 5}.log</i>	5 MB	1 MB
	<i>shared-folder\jp1cons\log\hliclib\hliclibmgrerr{1 2 3 4 5}.log</i>	5 MB	1 MB
Action information file ^{#9}	<i>Console-path\log\action\actinf.log</i>	626 KB ^{#3}	No switching
	<i>shared-folder\jp1cons\log\action\actinf.log</i>	626 KB ^{#3}	No switching
Action host name file ^{#9}	<i>Console-path\log\action\acttxt{1 2}.log</i>	48.9 MB ^{#4}	When the action information file wraps around
	<i>shared-folder\jp1cons\log\action\acttxt{1 2}.log</i>	48.9 MB ^{#4}	When the action information file wraps around
Action re-execution file	<i>Console-path\log\action\actreaction</i>	300 MB	When the service is started
	<i>shared-folder\jp1cons\log\action\actreaction</i>	300 MB	When the service is started
jcochstat, and jcoevtreport command trace logs ^{#5#9}	<i>Console-path\log\command\CMD{1 2 3}.log</i>	3,072 KB	1,024 KB
	<i>Console-path\log\command\jp1cons_cmd{1 2}.log</i>	12,288 KB	6,144 KB
	<i>Console-path\log\command\jp1consM_cmd{1 2}.log</i>	12,288 KB	6,144 KB
	<i>Console-path\log\command\jplexattrnameDef_cmd{1 2 3 4 5}.log</i>	25 MB	5 MB

Log type	Default file name and folder name	Maximum disk usage	File-switching timing
Plug-in log ^{#9}	<i>Console-path</i> \log\command\jcoplugin{1 2 3}.log	3 MB	1 MB
Reporting status storage file ^{#9}	<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 ^{#9}	<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 ^{#9}	<i>Console-path</i> \log\evflow\EVFLOW{1 2 3 4 5 6 7 8 9 10}.log	100 MB	10 MB
	<i>Console-path</i> \log\evflow\jplevflowM{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\jplevflowM{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

Log type	Default file name and folder name	Maximum disk usage	File-switching timing
Matching information file ^{#9}	<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 ^{#9}	<i>Console-path</i> \log\evflow\jpl-evflow{1 2 3 4 5 6 7 8}.log	40,960 KB	5,120 KB
	<i>shared-folder</i> \jplcons\log\evflow\jpl-evflow{1 2 3 4 5 6 7 8}.log	40,960 KB	5,120 KB
Event base stack trace ^{#9}	<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 ^{#9}	<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}
	<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 ^{#9}	<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

Log type	Default file name and folder name	Maximum disk usage	File-switching timing
Correlation event generation individual log ^{#9}	<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) ^{#9}	<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 ^{#9}	<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 ^{#9}	<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 ^{#9}	<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#9}	<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
Backup file for accumulated response-waiting events ^{#9}	<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 ^{#9}	<i>Base-path</i> \log\COMMAND\	See the <i>JPI/Base User's Guide</i> .	
	<i>shared-folder</i> \jplbase\log\COMMAND\		
Remote command log ^{#9}	<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		

Log type	Default file name and folder name	Maximum disk usage	File-switching timing
	<i>Base-path</i> \log\JCOCMD\jocmdcom{1 2 3}.log		
	<i>Base-path</i> \log\JCOCMD\jocmdcom_trace{1 2 3}.log		
	<i>Base-path</i> \log\JCOCMD\jocmdexe{1 2 3}.log		
	<i>Base-path</i> \log\JCOCMD\jocmdexe_trace{1 2 3}.log		
	<i>Base-path</i> \log\JCOCMD\jocmdrouter{1 2 3}.log		
	<i>Base-path</i> \log\JCOCMD\jocmdrouter_trace{1 2 3}.log		
	<i>Base-path</i> \log\JCOCMD\JCOCMDCMD{1 2 3}.log		
	<i>shared-folder</i> \jp1base\log\JCOCMD\jocmd_result{1 2 3}.log		
	<i>shared-folder</i> \jp1base\log\JCOCMD\jocmdapi{1 2 3}.log		
	<i>shared-folder</i> \jp1base\log\JCOCMD\jocmdapi_trace{1 2 3}.log		
	<i>shared-folder</i> \jp1base\log\JCOCMD\jocmdcom{1 2 3}.log		
	<i>shared-folder</i> \jp1base\log\JCOCMD\jocmdcom_trace{1 2 3}.log		
	<i>shared-folder</i> \jp1base\log\JCOCMD\jocmdexe{1 2 3}.log		
	<i>shared-folder</i> \jp1base\log\JCOCMD\jocmdexe_trace{1 2 3}.log		
	<i>shared-folder</i> \jp1base\log\JCOCMD\jocmdrouter{1 2 3}.log		
	<i>shared-folder</i> \jp1base\log\JCOCMD\jocmdrouter_trace{1 2 3}.log		
	<i>shared-folder</i> \jp1base\log\JCOCMD\JCOCMDCMD{1 2 3}.log		
Configuration management log ^{#9}	<i>Base-path</i> \log\route\JBSRT{1 2 3}.log		

Log type	Default file name and folder name	Maximum disk usage	File-switching timing
	<i>shared-folder</i> \jplbase\log\route\JBSRT{1 2 3}.log		
Trace log file#9	<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#9	<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#9	<i>Console-path</i> \log\evflow\EVFLOW_CFDBAPI{1 2 3}.log	30 MB	10 MB
	<i>Console-path</i> \log\console\EVCONS_CFDBAPI{1 2 3}.log	30 MB	10 MB
	<i>Console-path</i> \log\command\CMD_CFDBAPI{1 2 3}.log	30 MB	10 MB
	<i>shared-folder</i> \jplcons\log\evflow\EVFLOW_CFDBAPI{1 2 3}.log	30 MB	10 MB
	<i>shared-folder</i> \jplcons\log\console\EVCONS_CFDBAPI{1 2 3}.log	30 MB	10 MB
jcodbsetup command log#9	<i>Console-path</i> \log\imdb\jcodbsetup{1 2}.log	512 KB	256 KB
jcodbunsetup command log#9	<i>Console-path</i> \log\imdb\jcodbunsetup{1 2}.log	512 KB	256 KB
jimmail command log#9	<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
jimmailpasswd command log#9	Console- path\log\mail\jimmailpasswd_cmd{1 2 3}.log	768 KB	256 KB
	Console- path\log\mail\jimmailpasswd_cmdM{1 2 3}.log	768 KB	256 KB
	Console-path\log\mail\JIMMAILPASSWD{1 2 3}.log	768 KB	256 KB
	Console- path\log\mail\jimmailpasswd_exe{1 2 3}.log	768 KB	256 KB

#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 *JP1/Integrated Management 3 - Manager Command, Definition File and API 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 *JP1/Integrated Management 3 - Manager Command, Definition File and API 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 *JP1/Integrated Management 3 - Manager Command, Definition File and API 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.

#9: 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 12–5: 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	Scope-path\log\jcsmain{1 2 3}.log	6 MB	2 MB
	Scope-path\log\jcsmain_trace{1 2 3}.log	6 MB	2 MB
	shared-folder\JP1Scope\log\jcsmain{1 2 3}.log	6 MB	2 MB
	shared- folder\JP1Scope\log\jcsmain_trace{1 2 3}.log	6 MB	2 MB
Communication trace log	Scope-path\log\jcsmain_trace_com{1 2 3}.log	6 MB	2 MB
	shared- folder\JP1Scope\log\jcsmain_trace_com{1 2 3}.log	6 MB	2 MB
	Scope-path\log\jcsmain_trace_ping{1 2 3}.log	6 MB	2 MB

Log type	Default file name and folder name	Maximum disk usage	File-switching timing
	<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
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
jcldbsetup command log	<i>Scope-path</i> \log\jcldbsetup{1 2 3}.log	6 MB	2 MB
	<i>shared-folder</i> \JP1Scope\log\jcldbsetup{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
jcldbexport command log	<i>Scope-path</i> \log\jcldbexport{1 2 3}.log	6 MB	2 MB
	<i>shared-folder</i> \JP1Scope\log\jcldbexport{1 2 3}.log	6 MB	2 MB
jcldbimport command log	<i>Scope-path</i> \log\jcldbimport{1 2 3}.log	6 MB	2 MB
	<i>shared-folder</i> \JP1Scope\log\jcldbimport{1 2 3}.log	6 MB	2 MB
jcldbconvert command log	<i>Scope-path</i> \log\jcldbconvert{1 2 3}.log	6 MB	2 MB
	<i>shared-folder</i> \JP1Scope\log\jcldbconvert{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

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 12–6: 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
	<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

Log type	Default file name and folder name	Maximum disk usage	File-switching timing
	<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\jplhassetup.{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
	<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

Log type	Default file name and folder name	Maximum disk usage	File-switching timing
	<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
	<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

Log type	Default file name and folder name	Maximum disk usage	File-switching timing
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
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

Log type	Default file name and folder name	Maximum disk usage	File-switching timing
jcfcolumhcsn command log	<i>Manager-path</i> \log\imcf\jcfcolumhcsn_trace{1 2 3}.log	3 MB	1 MB
jcfeexport command log	<i>Manager-path</i> \log\imcf\jcfeexport_VM_trace{1 2 3}.log	3 MB	1 MB
	<i>shared-folder</i> \JP1IMM\log\imcf\jcfeexport_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 12–7: Intelligent Integrated Management Base log files and folders

Log type	Default file name and folder name	Maximum disk usage	File-switching timing
Intelligent Integrated Management Base service individual log	<i>Manager-path</i> \log\imdd\jddmain\jddmain.log{.1-7}	1 GB	128 MB
	<i>shared-folder</i> \jp1imm\log\imdd\jddmain\jddmain.log{.1-7}		
Definition file ^{#1} , node file history log	<i>Manager-path</i> \log\imdd\jddmain\jimddDef.log{.1-10}	80 MB	8 MB
	<i>shared-folder</i> \jp1imm\log\imdd\jddmain\jimddDef.log{.1-10}		
	<i>Manager-path</i> \log\imdd\jddmain\jimddMaster.log{.1-30}	240 MB	8 MB
	<i>shared-folder</i> \jp1imm\log\imdd\jddmain\jimddMaster.log{.1-30}		
jddsetaccessuser command trace log	<i>Manager-path</i> \log\imdd\jddsetaccessuser\jddsetaccessuser.log{.1-6}	70 MB	10 MB

Log type	Default file name and folder name	Maximum disk usage	File-switching timing
	<i>shared-folder</i> \jplimm\log\imdd\jddsetaccessuser\jddsetaccessuser.log{.1-6}		
	<i>Manager-path</i> \log\imdd\jddsetaccessuser\jddsetaccessuser_exe{1 2 3}.log	768 KB	256 KB
	<i>shared-folder</i> \jplimm\log\imdd\jddsetaccessuser\jddsetaccessuser_exe{1 2 3}.log		
	<i>Manager-path</i> \log\imdd\jddsetaccessuser\javalog0{1 2 3 4}.log	1,024 KB	At startup or 256 KB
	<i>shared-folder</i> \jplimm\log\imdd\jddsetaccessuser\javalog0{1 2 3 4}.log		
jddcreatetree command trace log	<i>Manager-path</i> \log\imdd\jddcreatetree\jddcreatetree.log{.1-6}	70 MB	10 MB
	<i>shared-folder</i> \jplimm\log\imdd\jddcreatetree\jddcreatetree.log{.1-6}		
	<i>Manager-path</i> \log\imdd\jddcreatetree\jddcreatetree_exe{1 2 3}.log	768 KB	256 KB
	<i>shared-folder</i> \jplimm\log\imdd\jddcreatetree\jddcreatetree_exe{1 2 3}.log		
	<i>Manager-path</i> \log\imdd\jddcreatetree\javalog0{1 2 3 4}.log	1,024 KB	At startup or 256 KB
	<i>shared-folder</i> \jplimm\log\imdd\jddcreatetree\javalog0{1 2 3 4}.log		
jddupdatetree command trace log	<i>Manager-path</i> \log\imdd\jddupdatetree\jddupdatetree.log{.1-6}	70 MB	10 MB
	<i>shared-folder</i> \jplimm\log\imdd\jddupdatetree\jddupdatetree.log{.1-6}		
	<i>Manager-path</i> \log\imdd\jddupdatetree\jddupdatetree_exe{1 2 3}.log	768 KB	256 KB
	<i>shared-folder</i> \jplimm\log\imdd\jddupdatetree\jddupdatetree_exe{1 2 3}.log		
	<i>Manager-path</i> \log\imdd\jddupdatetree\javalog0{1 2 3 4}.log	1,024 KB	256 KB

Log type	Default file name and folder name	Maximum disk usage	File-switching timing
	<i>shared-folder</i> \jplimm\log\imdd\jddupdatetree\java\valog0{1 2 3 4}.log		
jddsetproxyuser command trace log	<i>Manager-path</i> \log\imdd\jddsetproxyuser\jddsetproxyuser.log{.1-6}	70 MB	10 MB
	<i>shared-folder</i> \jplimm\log\imdd\jddsetproxyuser\jddsetproxyuser.log{.1-6}		
	<i>Manager-path</i> \log\imdd\jddsetproxyuser\jddsetproxyuser_exe{1 2 3}.log	768 KB	256 KB
	<i>shared-folder</i> \log\imdd\jddsetproxyuser\jddsetproxyuser_exe{1 2 3}.log		
	<i>Manager-path</i> \log\imdd\jddsetproxyuser\javalog0{1 2 3 4}.log	1,024 KB	256 KB
	<i>shared-folder</i> \log\imdd\jddsetproxyuser\javalog0{1 2 3 4}.log		
jddupdatesuggestion command trace log	<i>Manager-path</i> \log\imdd\jddupdatesuggestion\jddupdatesuggestion.log{.1-6}	70MB	10MB
	<i>shared-folder</i> \jplimm\log\jddupdatesuggestion\jddupdatesuggestion.log{.1-6}		
	<i>Manager-path</i> \log\imdd\jddupdatesuggestion\jddupdatesuggestion_exe{1 2 3}.log	768KB	256KB
	<i>shared-folder</i> \log\imdd\jddupdatesuggestion\jddupdatesuggestion_exe{1 2 3}.log		
	<i>Manager-path</i> \log\imdd\jddupdatesuggestion\javalog0{1 2 3 4}.log	1,024KB	256KB
	<i>shared-folder</i> \log\imdd\jddupdatesuggestion\javalog0{1 2 3 4}.log		
jddsetopinfo command trace log	<i>Manager-path</i> \log\imdd\jddsetopinfo\jddsetopinfo.log{.1-6}	70MB	10MB
	<i>shared-folder</i> \jplimm\log\jddsetopinfo\jddsetopinfo.log{.1-6}		
	<i>Manager-path</i> \log\imdd\jddsetopinfo\jddsetopinfo_exe{1 2 3}.log	768KB	256KB

Log type	Default file name and folder name	Maximum disk usage	File-switching timing
	<i>shared-folder</i> \log\imdd\jddsetopinfo\jddsetopinfo_exe{1 2 3}.log		
	<i>Manager-path</i> \log\imdd\jddsetopinfo\javalog0{1 2 3 4}.log	1,024KB	256KB
	<i>shared-folder</i> \log\imdd\jddsetopinfo\javalog0{1 2 3 4}.log		
jddupdatessomap command trace log	<i>Manager-path</i> \log\imdd\jddupdatessomap\jddupdatessomap.log{.1-6}	70MB	10MB
	<i>shared-folder</i> \jplimm\log\jddupdatessomap\jddupdatessomap.log{.1-6}		
	<i>Manager-path</i> \log\imdd\jddupdatessomap\jddupdatessomap_exe{1 2 3}.log	768KB	256KB
	<i>shared-folder</i> \log\imdd\jddupdatessomap\jddupdatessomap_exe{1 2 3}.log		
	<i>Manager-path</i> \log\imdd\jddupdatessomap\javalog0{1 2 3 4}.log	1,024KB	256KB
	<i>shared-folder</i> \log\imdd\jddupdatessomap\javalog0{1 2 3 4}.log		
jimgndbsetup command trace log	<i>Manager-path</i> \log\imgndb\jimgndbsetup{1 2}.log	512KB	256KB
jimgndbunsetup command trace log	<i>Manager-path</i> \log\imgndb\jimgndbunsetup{1 2}.log	512KB	256KB
jimgndbstop command trace log	<i>Manager-path</i> \log\imgndb\jimgndbstop{1-10}.log	51,200KB	5,120KB
	<i>shared-folder</i> \jplimm\log\imgndb\jimgndbstop{1-10}.log		
jimgndbstatus command trace log	<i>Manager-path</i> \log\imgndb\jimgndbstatus{1-10}.log	51,200KB	5,120KB
	<i>shared-folder</i> \jplimm\log\imgndb\jimgndbstatus{1-10}.log		
Logs of the response action execution history file #4	<i>Manager-path</i> \log\suggestion\jddSuggestionHistory.log{.1-3}	240MB	60MB

Log type	Default file name and folder name	Maximum disk usage	File-switching timing
	shared-folder\jplimm\log\suggestion\jddSuggestionHistory.log{.1-3}		
Secret authentication logfile	Manager-path\log\secretAuth\jddSecretAuth.log{.1-3}	240MB	60MB
	shared-folder\jplimm\log\secretAuth\jddSecretAuth.log{.1-3}		
User-created plug-ins	Manager-path\log\imdd\user-created-plug-in-name\user-created-plug-in.log{1-21} ^{#3}	220MB	10MB
	shared-folder\JP1IMM\log\imdd\user-created-plug-in-name\user-created-plug-in.log{1-21} ^{#3}		
Other logs	Manager-path\log\imdd\jddmain\jddmain_exe{1 2 3}.log	768 KB	256 KB
	shared-folder\jplimm\log\imdd\jddmain\jddmain_exe{1 2 3}.log		
	Manager-path\log\imdd\jddmain\javalog0{1 2 3 4}.log	1,024 KB	At startup or 256 KB
	shared-folder\jplimm\log\imdd\jddmain\javalog0{1 2 3 4}.log		
	Manager-path\log\imdd\jcoapi{1-50}.log	500 MB	10 MB
	shared-folder\jplimm\log\imdd\jddmain\jcoapi{1-50}.log		
	Manager-path\log\imdd\jcoapiM{1-50}.log	500 MB	10 MB
	shared-folder\jplimm\log\imdd\jddmain\jcoapiM{1-50}.log		
	Manager-path\log\imdd\component-name ^{#2} \component-name ^{#2} {1-21}.log	220 MB	10 MB
shared-folder\log\imdd\component-name ^{#2} \component-name ^{#2} {1-21}.log			

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 logs for the following definition files are output to the definition file log for the Intelligent Integrated Management Base:

System node definition file, category name definition file for IM management nodes, host name definition file, target host definition file for configuration collection, IM management node link definition file, IM management node link file, IM management node tree file, IM management node file

#2

One of the following is displayed as the component name:

- jplajs
- jplpfm
- jplim

#3

{1-21} indicates the file count. You can view the log files in a text editor of your choice.

#4

The log is created when a response action is taken. Users can check the logs of response actions by themselves in order to examine the causes of failures, for example.

Table 12–8: 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}
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
	<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\jpl\jpl_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.

Table 12–9: 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\jpl\jpl_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.

(b) 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 12–10: 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	<code>/var/opt/jplimm/log/operationlog/imm_operation{none 1 2... 16}.log^{#1}</code>	55 MB ^{#1}	5 MB ^{#1#2}
jimnodecount command log ^{#3}	<code>/var/opt/jplimm/log/nodecount/jimnodecount_cmd{1 2}.log</code>	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)* in *Chapter 2. Definition Files in the JP1/Integrated Management 3 - Manager Command, Definition File and API 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 *Appendix K.2 Storage format of operation log output* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

#3: 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 12–11: 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}	<code>/var/opt/jplcons/log/JCO_SPMD{1 2 3}.log</code>	384 KB	128 KB
	<code>/var/opt/jplcons/log/JCO_SPMD_COMMAND{1 2 3}.log</code>	384 KB	128 KB
	<code>shared-directory/jplcons/log/JCO_SPMD{1 2 3}.log</code>	384 KB	128 KB

Log type	Default file name and directory name	Maximum disk usage	File-switching timing
	<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 ^{#1}	/var/opt/jplcons/log/ JCO_SETUP/jco_setup.log	100 KB	During installation
	/var/opt/jplcons/log/ JCO_SETUP/jco_inst.log	100 KB	During installation
	/var/opt/jplcons/log/jco_setup/logical-host-name/ jco_setup.log	100 KB	During installation
	/var/opt/jplcons/log/jco_setup/logical-host-name/ reg.txt	100 KB	During installation
	/var/opt/jplcons/log/jco_setup/logical-host-name/ reg_def.txt	100 KB	During installation
	/var/opt/jplcons/log/ command/comdef[_old].log	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

Log type	Default file name and directory name	Maximum disk usage	File-switching timing
	/var/opt/jplcons/log/console/jplexattrnameDef{1 2 3 4 5}.log	25 MB	5 MB
	shared-directory/jplcons/log/console/EVCONS{1 2 3}.log	30,720 KB	10,240 KB
	shared-directory/jplcons/log/console/jplcons{1 2 3 4 5 6 7 8}.log	40,960 KB	5,120 KB ^{#3}
	shared-directory/jplcons/log/console/JCOAPI{1 2 3}.log	96 KB	32 KB
	shared-directory/jplcons/log/console/jplconsM{1 2... 60}.log	300 MB	5 MB ^{#3}
	shared-directory/jplcons/log/console/jpleventStormDef{1 2 3 4 5}.log	100 MB	20 MB
	shared-directory/jplcons/log/console/jplfilterDef{1 2 3 4 5}.log	100 MB	20 MB
	shared-directory/jplcons/log/console/jplbizGroupDef{1 2}.log	10 MB	5 MB
	shared-directory/jplcons/log/console/evtcon_exe{1 2 3}.log	256 KB × 3	256 KB
	shared-directory/jplcons/log/console/jplcmdButtonDef{1 2 3 4 5}.log	25 MB	5 MB
	shared-directory/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
	shared-directory/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
	shared-directory/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
	shared-directory/jplcons/log/action/acttxt{1 2}.log	48.9 MB ^{#6}	When the action information file wraps around
Action re-execution file	/var/opt/jplcons/log/action/actreaction	300 MB	When the service is started
	shared-directory/jplcons/log/action/actreaction	300 MB	When the service is started
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

Log type	Default file name and directory name	Maximum disk usage	File-switching timing
	/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
	/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
	<i>shared-directory</i> /jplcons/log/evflow/EVFLOW{1 2 3 4 5 6 7 8 9 10}.log	100 MB	10 MB
	<i>shared-directory</i> /jplcons/log/evflow/jplevflowM{1 2... 60}.log	300 MB	5 MB
	<i>shared-directory</i> /jplcons/log/evflow/jplactDef{1 2 3 4 5}.log	25 MB	5 MB
	<i>shared-directory</i> /jplcons/log/evflow/jplchsevDef{1 2 3 4 5}.log	25 MB	5 MB
	<i>shared-directory</i> /jplcons/log/evflow/jplchmsgDef{1 2 3 4 5}.log	25 MB	5 MB
	<i>shared-directory</i> /jplcons/log/evflow/jplhostmapDef{1 2 3 4 5}.log	25 MB	5 MB
	<i>shared-directory</i> /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

Log type	Default file name and directory name	Maximum disk usage	File-switching timing
	<i>shared-directory</i> /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
	<i>shared-directory</i> /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
	<i>shared-directory</i> /jplcons/log/action/jplact{1 2 3}.log	15,360 KB	5,120 KB
Correlation event generation history file	/var/opt/jplcons/operation/evgen/egs_discrim{1 2 3}.log ^{#8}	30 MB ^{#8}	10 MB ^{#8}
	<i>shared-directory</i> /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
	<i>shared-directory</i> /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
	<i>shared-directory</i> /jplcons/operation/comexclude/comexcludeDef{1 2 3 4 5}.log	100 MB	20 MB
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

Log type	Default file name and directory name	Maximum disk usage	File-switching timing
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
	/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

Log type	Default file name and directory name	Maximum disk usage	File-switching timing
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		
	/var/opt/jplbase/log/JCOCMD/jcocmdrouter_trace{1 2 3}.log		
	/var/opt/jplbase/log/JCOCMD/JCOCMDCMD{1 2 3}.log		
	<i>shared-directory</i> /jplbase/log/JCOCMD/jcocmd_result{1 2 3}.log		
	<i>shared-directory</i> /jplbase/log/JCOCMD/jcocmdapi{1 2 3}.log		
	<i>shared-directory</i> /jplbase/log/JCOCMD/jcocmdapi_trace{1 2 3}.log		
	<i>shared-directory</i> /jplbase/log/JCOCMD/jcocmdcmc{1 2 3}.log		
	<i>shared-directory</i> /jplbase/log/JCOCMD/jcocmdcmc_trace{1 2 3}.log		
	<i>shared-directory</i> /jplbase/log/JCOCMD/jcocmdcom{1 2 3}.log		
<i>shared-directory</i> /jplbase/log/JCOCMD/jcocmdcom_trace{1 2 3}.log			
<i>shared-directory</i> /jplbase/log/JCOCMD/jcocmdexe{1 2 3}.log			
<i>shared-directory</i> /jplbase/log/JCOCMD/jcocmdexe_trace{1 2 3}.log			

Log type	Default file name and directory name	Maximum disk usage	File-switching timing
	<i>shared-directory</i> /jplbase/log/JCOCMD/jcocmdrouter{1 2 3}.log		
	<i>shared-directory</i> /jplbase/log/JCOCMD/jcocmdrouter_trace{1 2 3}.log		
	<i>shared-directory</i> /jplbase/log/JCOCMD/JCOCMDCMD{1 2 3}.log		
Configuration management log#1	/var/opt/jplbase/log/route/JBSRT{1 2 3}.log		
	<i>shared-directory</i> /jplbase/log/route/JBSRT{1 2 3}.log		
Trace log file#1	/var/opt/jplbase/sys/tmp/event/logtrap/jeallog/jeallog{1 2 3 4 5}.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: 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 *JP1/Integrated Management 3 - Manager Command, Definition File and API 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 *JP1/Integrated Management 3 - Manager Command, Definition File and API 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.

$((\text{action information file size} \div 64 \text{ bytes}) - 1) \times 5 \text{ kilobytes}$

#7: The files are output to the `jcocostat` and `jcocofmode` 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 *JP1/Integrated Management 3 - Manager Command, Definition File and API 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 12–12: 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	/var/opt/jplscope/log/jcsmain{1 2 3}.log	6 MB	2 MB
	/var/opt/jplscope/log/jcsmain_trace{1 2 3}.log	6 MB	2 MB
	<i>shared-directory</i> /jplscope/log/jcsmain{1 2 3}.log	6 MB	2 MB
	<i>shared-directory</i> /jplscope/log/jcsmain_trace{1 2 3}.log	6 MB	2 MB
Communication trace log	/var/opt/jplscope/log/jcsmain_trace_com{1 2 3}.log	6 MB	2 MB
	<i>shared-directory</i> /jplscope/log/jcsmain_trace_com{1 2 3}.log	6 MB	2 MB

Log type	Default file name and directory name	Maximum disk usage	File-switching timing
	/var/opt/jplscope/log/jcsmain_trace_ping{1 2 3}.log	6 MB	2 MB
	<i>shared-directory</i> /jplscope/log/jcsmain_trace_ping{1 2 3}.log	6 MB	2 MB
Database operation API trace log	/var/opt/jplscope/log/jcsmain_trace_db{1 2 3}.log	6 MB	2 MB
	<i>shared-directory</i> /jplscope/log/jcsmain_trace_db{1 2 3}.log	6 MB	2 MB
jcshostsexport command log	/var/opt/jplscope/log/jcshostsexport{1 2 3}.log	6 MB	2 MB
	<i>shared-directory</i> /jplscope/log/jcshostsexport{1 2 3}.log	6 MB	2 MB
jcshostsimport command log	/var/opt/jplscope/log/jcshostsimport{1 2 3}.log	6 MB	2 MB
	<i>shared-directory</i> /jplscope/log/jcshostsimport{1 2 3}.log	6 MB	2 MB
jcsdbsetup command log	/var/opt/jplscope/log/jcsdbsetup{1 2 3}.log	6 MB	2 MB
	<i>shared-directory</i> /jplscope/log/jcsdbsetup{1 2 3}.log	6 MB	2 MB
jcschstat command log	/var/opt/jplscope/log/jcschstat{1 2 3}.log	6 MB	2 MB
	<i>shared-directory</i> /jplscope/log/jcschstat{1 2 3}.log	6 MB	2 MB
jcsdbimport command log	/var/opt/jplscope/log/jcsdbimport{1 2 3}.log	6 MB	2 MB
	<i>shared-directory</i> /jplscope/log/jcsdbimport{1 2 3}.log	6 MB	2 MB
jcsdbexport command log	/var/opt/jplscope/log/jcsdbexport{1 2 3}.log	6 MB	2 MB
	<i>shared-directory</i> /jplscope/log/jcsdbexport{1 2 3}.log	6 MB	2 MB
Setup log	/var/opt/jplscope/log/JCS_SETUP/jcs_setup.log	100 KB	During installation
	/var/opt/jplscope/log/jcs_setup/ <i>logical-host-name</i> /jcs_setup.log	100 KB	During installation
	/var/opt/jplscope/log/jcs_setup/ <i>logical-host-name</i> /reg.txt	100 KB	During installation
	/var/opt/jplscope/log/jcs_setup/ <i>logical-host-name</i> /reg_def.txt	100 KB	During installation

Note: 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 12–13: 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/jplimm/log/imcf/jcfallogtrap{1 2 3 4 5 6 7 8 9 10}.log	200 MB	10 MB
	/var/opt/jplimm/log/imcf/jcfallogtrap_VM_trace{1 2 3}.log	3 MB	1 MB
	/var/opt/jplimm/log/imcf/jcfallogtrap_trace_auth{1 2 3 4 5 6 7 8 9 10}.log	20 MB	2 MB
	/var/opt/jplimm/log/imcf/jcfmain{1 2 3 4 5 6 7 8 9 10}.log	20 MB	2 MB
	/var/opt/jplimm/log/imcf/jcfmain_trace{1 2 3 4 5 6 7 8 9 10}.log	20 MB	2 MB
	/var/opt/jplimm/log/imcf/jcfmain_VM_trace{1 2 3}.log	3 MB	1 MB
	<i>shared-directory</i> /jplimm/log/imcf/jcfallogtrap{1 2 3 4 5 6 7 8 9 10}.log	200 MB	10 MB
	<i>shared-directory</i> /jplimm/log/imcf/jcfallogtrap_VM_trace{1 2 3}.log	3 MB	1 MB
	<i>shared-directory</i> /jplimm/log/imcf/jcfallogtrap_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{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
/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

Log type	Default file name and directory name	Maximum disk usage	File-switching timing
	<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
	<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

Log type	Default file name and directory name	Maximum disk usage	File-switching timing
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	/var/opt/jplimm/log/imcf/ jcfcolvmesx_trace{1 2 3}.log	3 MB	1 MB
	<i>shared-directory</i> /jplimm/log/imcf/ jcfcolvmesx_trace{1 2 3}.log		
jcfcolvmvirtage command log	/var/opt/jplimm/log/imcf/ jcfcolvmvirtage_trace{1 2 3}.log	3 MB	1 MB
	<i>shared-directory</i> /jplimm/log/imcf/ jcfcolvmvirtage_trace{1 2 3}.log		
jcfcolvmvc command log	/var/opt/jplimm/log/imcf/ jcfcolvmvc_trace{1 2 3}.log	3 MB	1 MB
	<i>shared-directory</i> /jplimm/log/imcf/ jcfcolvmvc_trace{1 2 3}.log		
jcfcolvmkvm command log	/var/opt/jplimm/log/imcf/ jcfcolvmkvm_trace{1 2 3}.log	3 MB	1 MB
	<i>shared-directory</i> /jplimm/log/imcf/ jcfcolvmkvm_trace{1 2 3}.log		
jcfcolvmhcsn command log	/var/opt/jplimm/log/imcf/ jcfcolvmhcsn_trace{1 2 3}.log	3 MB	1 MB
	<i>shared-directory</i> /jplimm/log/imcf/ jcfcolvmhcsn_trace{1 2 3}.log		
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
	<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.

Table 12–14: Intelligent Integrated Management Base log files and folders

Log type	Default file name and directory name	Maximum disk usage	File-switching timing
Intelligent Integrated Management Base service individual log	/var/opt/jplimm/log/imdd/jddmain/jddmain.log{.1-7}	1 GB	128 MB
	<i>shared-directory</i> /jplimm/log/imdd/jddmain/jddmain.log{.1-7}		
Definition file ^{#1} , node file history log	/var/opt/jplimm/log/imdd/jddmain/jimddDef.log{.1-10}	80 MB	8 MB
	<i>shared-directory</i> /jplimm/log/imdd/jddmain/jimddDef.log{.1-10}		
	/var/opt/jplimm/log/imdd/jddmain/jimddMaster.log{.1-30}	240 MB	8 MB
	<i>shared-directory</i> /jplimm/log/imdd/jddmain/jimddMaster.log{.1-30}		
jddsetaccessuser command trace log	/var/opt/jplimm/log/imdd/jddsetaccessuser/jddsetaccessuser.log{.1-6}	70 MB	10 MB
	<i>shared-directory</i> /jplimm/log/imdd/jddsetaccessuser/jddsetaccessuser.log{.1-6}		
	/var/opt/jplimm/log/imdd/jddsetaccessuser/jddsetaccessuser_exe{1 2 3}.log	768 KB	256 KB
	<i>shared-directory</i> /jplimm/log/imdd/jddsetaccessuser/jddsetaccessuser_exe{1 2 3}.log		
	/var/opt/jplimm/log/imdd/jddsetaccessuser/javalog0{1 2 3 4}.log	1,024 KB	At startup or 256 KB
	<i>shared-directory</i> /jplimm/log/imdd/jddsetaccessuser/javalog0{1 2 3 4}.log		
jddcreatetree command trace log	/var/opt/jplimm/log/imdd/jddcreatetree/jddcreatetree.log{.1-6}	70 MB	10 MB
	<i>shared-directory</i> /jplimm/log/imdd/jddcreatetree/jddcreatetree.log{.1-6}		
	/var/opt/jplimm/log/imdd/jddcreatetree/jddcreatetree_exe{1 2 3}.log	768 KB	256 KB
	<i>shared-directory</i> /jplimm/log/imdd/jddcreatetree/jddcreatetree_exe{1 2 3}.log		
	/var/opt/jplimm/log/imdd/jddcreatetree/javalog0{1 2 3 4}.log	1,024 KB	At startup or 256 KB
	<i>shared-directory</i> /jplimm/log/imdd/jddcreatetree/javalog0{1 2 3 4}.log		
jddupdatetree command trace log	/var/opt/jplimm/log/imdd/jddupdatetree/jddupdatetree.log{.1-6}	70 MB	10 MB
	<i>shared-directory</i> /jplimm/log/imdd/jddupdatetree/jddupdatetree.log{.1-6}		

Log type	Default file name and directory name	Maximum disk usage	File-switching timing
	/var/opt/jplimm/log/imdd/jddupdatetree/ jddupdatetree_exe{1 2 3}.log	768 KB	256 KB
	<i>shared-directory</i> /jplimm/log/imdd/jddupdatetree/ jddupdatetree_exe{1 2 3}.log		
	/var/opt/jplimm/log/imdd/jddupdatetree/ javalog0{1 2 3 4}.log	1,024 KB	256 KB
	<i>shared-directory</i> /jplimm/log/imdd/jddupdatetree/ javalog0{1 2 3 4}.log		
jddproxyuser command trace log	/var/opt/jplimm/log/imdd/ jddproxyuser/jddproxyuser.log{.1-6}	70MB	10MB
	<i>shared-directory</i> /jplimm/log/imdd/ jddproxyuser/jddproxyuser.log{.1-6}		
	/var/opt/jplimm/log/imdd/jddproxyuser/ jddproxyuser_exe{1 2 3}.log	768KB	256KB
	<i>shared-directory</i> /jplimm/log/imdd/jddproxyuser/ jddproxyuser_exe{1 2 3}.log		
	/var/opt/jplimm/log/imdd/jddproxyuser/ javalog0{1 2 3 4}.log	1,024KB	256KB
	<i>shared-directory</i> /jplimm/log/imdd/jddproxyuser/ javalog0{1 2 3 4}.log		
jimgndbsetup command trace log	/var/opt/jplimm/log/imgndb/ jimgndbsetup{1 2}.log	512KB	256KB
jimgndbunsetup command trace log	/var/opt/jplimm/log/imgndb/ jimgndbunsetup{1 2}.log	512KB	256KB
jimgndbstop command trace log	/var/opt/jplimm/log/ imgndb/jimgndbstop{1-10}.log	51,200KB	5,120KB
	<i>shared- directory</i> /jplimm/log/ imgndb/jimgndbstop{1-10}.log		
jimgndbstatus command trace log	/var/opt/jplimm/log/ imgndb/jimgndbstatus{1-10}.log	51,200KB	5,120KB
	<i>shared- directory</i> /jplimm/log/ imgndb/jimgndbstatus{1-10}.log		
Logs of the response action execution history file ^{#4}	/var/opt/jplimm/log/ suggestion/jddSuggestionHistory.log{.1-3}	240MB	60MB
	<i>shared-directory</i> /jplimm/log/ suggestion/jddSuggestionHistory.log{.1-3}		
Secret authentication logfile	var/opt/jplimm/log/ secretAuth/jddSecretAuth.log{.1-3}	240MB	60MB
	<i>shared-directory</i> /jplimm/log/ secretAuth/jddSecretAuth.log{.1-3}		
User-created plug-ins	/var/opt/jplimm/log/imdd/ <i>user-created-plug-in- name</i> / <i>user-created-plug-in</i> .log{1-21} ^{#3}	220MB	10MB
	<i>shared-directory</i> /jplimm/log/imdd/ <i>user-created-plug-in- name</i> / <i>user-created-plug-in</i> .log{1-21} ^{#3}		

Log type	Default file name and directory name	Maximum disk usage	File-switching timing
Other logs	/var/opt/jp1imm/log/imdd/jddmain/ jddmain_exe{1 2 3}.log	768 KB	256 KB
	<i>shared-directory</i> /jp1imm/log/imdd/jddmain/ jddmain_exe{1 2 3}.log		
	/var/opt/jp1imm/log/imdd/jddmain/javalog0{1 2 3 4}.log	1,024 KB	At startup or 256 KB
	<i>shared-directory</i> /jp1imm/log/imdd/jddmain/ javalog0{1 2 3 4}.log		
	/var/opt/jp1imm/log/imdd/jcoapi{1-50}.log	500 MB	10 MB
	<i>shared-directory</i> /jp1imm/log/imdd/ jddmain/jcoapi{1-50}.log		
	/var/opt/jp1imm/log/imdd/jcoapiM{1-50}.log	500 MB	10 MB
	<i>shared-directory</i> /jp1imm/log/imdd/ jddmain/jcoapiM{1-50}.log		
	/var/opt/jp1imm/log/imdd/ <i>component- name</i> ^{#2} / <i>component-name</i> ^{#2} {1-21}.log	220MB	10MB
	<i>shared-directory</i> /jp1imm/log/imdd/ <i>component- name</i> ^{#2} / <i>component-name</i> ^{#2} {1-21}.log		

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 logs for the following definition files are output to the definition file log for the Intelligent Integrated Management Base:

System node definition file, category name definition file for IM management nodes, host name definition file, target host definition file for configuration collection, IM management node link definition file, IM management node link file, IM management node tree file, IM management node file

#2: One of the following is displayed as the component name:

- jp1ajs
- jp1pfm
- jp1im

#3: {1-21} indicates the file count. You can view the log files in a text editor of your choice.

#4: The log is created when a response action is taken. Users can check the logs of response actions by themselves in order to examine the causes of failures, for example.

(6) Log of JP1/IM - Agent (JP1/IM agent management base)

(a) Public log

JP1/IM agent management base log for publishing is output.

Upper limit of log size and number of planes

It is specified in JP1/IM agent management base definition file.

Output destination

- For Windows

Manager-path[#]\log\imdd\imagent\imbase\

Manager-path[#]\log\imdd\imagent\imbaseproxy\

#: For a cluster, replace it with "*shared-folder\jplimm*"

- For Linux

/var/opt#/jplimm/log/imdd/imagent/ibase/

/var/opt#/jplimm/log/imdd/imagent/ibaseproxy/

#: For a cluster, replace it with "*shared-directory*".

File name

jima_message.log^{#1}

jima_message-YYYY-MM-DDThh-mm-ss.sss.log^{#2}

#1

When the log reaches the specified size, "*-YYYY-MM-DDThh-mm-ss.sss.log*" is added to the log filename and the log is rotated.

#2

Rename the output destination log file name to a new date and delete the oldest log file.

Output format

Datetime PID Job-Identifier Message-ID Message

Note

When the command is executed in response action, the contents of the standard output and standard error output of executed command is output to the public log of imagent. Therefore, when execution of command that outputs message is expected in response action, expand logging sectors and max. file size of public log as needed. Logging sectors and max. file size of public log can be specified in *log.message.num* and *log.message.size* in imagent configuration file.

(b) Log of setting values at start up

The setting values read by JP1/IM agent management base at startup are output.

Upper limit of log size and number of planes

The log size and number of planes are fixed in the system. It cannot be changed by a user.

Output destination

- For Windows

Manager-path#\log\imdd\imagent\ibase

Manager-path#\log\imdd\imagent\ibaseproxy

#: For a cluster, replace it with "*shared-folder\jplimm*"

- For Linux

/var/opt#/jplimm/log/imdd/imagent/ibase/

/var/opt#/jplimm/log/imdd/imagent/ibaseproxy/

#: For a cluster, replace it with "*shared-directory*".

File name

jima_setting.log^{#1}

jima_setting-YYYY-MM-DDThh-mm-ss.sss.log^{#2}

#1

When the log reaches the specified size, "*-YYYY-MM-DDThh-mm-ss.sss.log*" is added to the log filename and the log is rotated.

#2

Rename the output destination log file name to a new date and delete the oldest log file.

Output format

Outputs a log that shows the date and time and the set value.

12.2.2 JP1/IM - Agent log information

(1) Prometheus server log

Prometheus server log is output.

Upper limit of log size and number of planes

- For Windows
Specify in service definition file.
- For Linux
Specify in unit definition file.

For details on the specification procedure, see *Service definition file (jpc_program-name_service.xml)* and *Unit definition file (jpc_program-name.service)* in *Chapter 2. Definition Files* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

Output destination

- For Windows
`Agent-path#\logs\prometheus_server\jpc_prometheus_server_service.
(err|out).log`
#: For a cluster, replace it with "*shared-folder\jplima*".
- For Linux
`/opt#/jplima/logs/prometheus_server/prometheus_service`
#: For a cluster, replace it with "*shared-directory*".

Output format

Prometheus server outputs text data that is output to stdout or stderr during operation.

(2) Alertmanager log

Alertmanager log is output.

Upper limit of log size and number of planes

- For Windows
Specify in service definition file.
- For Linux
Specify in unit definition file.

For details on the specification procedure, see *Service definition file (jpc_program-name_service.xml)* and *Unit definition file (jpc_program-name.service)* in *Chapter 2. Definition Files* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

Output destination

- For Windows

Agent-path[#]\logs\alertmanager\jpc_alertmanager_service.(err|out).log

#: For a cluster, replace it with "*shared-folder*\jplima".

- For Linux

/opt[#]/jplima/logs/alertmanager/alertmanager_service

#: For a cluster, replace it with "*shared-directory*".

Output format

Alertmanager outputs text data output to standard output or standard error output while running.

(3) Exporter Logs

Exporter logs will be output.

Upper limit of log size and number of planes

- For Windows

Specify in service definition file.

- For Linux

Specify in unit definition file.

For details on the specification procedure, see *Service definition file (jpc_program-name_service.xml)* and *Unit definition file (jpc_program-name.service)* in Chapter 2. *Definition Files in the JPI/Integrated Management 3 - Manager Command, Definition File and API Reference.*

Output destination

- For Windows

Agent-path[#]\logs*Exporter-name*\jpc_*Exporter-name*_service.(err|out).log

#: For a cluster, replace it with "*shared-folder*\jplima".

- For Linux

/opt[#]/jplima/logs/*Exporter-name*/*Exporter-name*_service

#: For a cluster, replace it with "*shared-directory*".

Output format

Exporter outputs text data output to standard output or standard error output while running.

(4) Service Control Log

- For Windows

Log is output when the service is started or stopped.

- For Linux

No log is output.

Upper limit of log size and number of planes

Rotate when the log reaches a certain size. You cannot specify the maximum log size and the number of planes.

Output destination

- For Windows

`Agent-path#\logs\prometheus\jpc_prometheus_server_service.wrapper.log`
`Agent-path#\logs>alertmanager\jpc_alertmanager_service.wrapper.log`
`Agent-path#\logs\Exporter-name\jpc_Exporter-name_service.wrapper.log`
`Agent-path#\logs\fluentd\jpc_fluentd_service.wrapper.log`
`Agent-path#\logs\imagent\jpc_imagent_service.wrapper.log`
`Agent-path#\logs\imagentproxy\jpc_imagentproxy_service.wrapper.log`
`Agent-path#\logs\imagentaction\jpc_imagentaction_service.wrapper.log`
 #: For a cluster, replace it with "*shared-folder\jplima*".

Output format

The text data output by Windows service program is output.

Timing and size of output

The following table summarizes the timing and size of the output to the service control log.

Opportunity	A measure of size (bytes)	Output example
Starting the Service	750	2021-11-22 14:18:48,135 DEBUG - Starting WinSW in service mode 2021-11-22 14:18:48,394 INFO - Starting prometheus.exe --config.file="jpc_prometheus_server.yml" --web.read-timeout=5m --web.max-connections=10 --web.enable-lifecycle --storage.tsdb.path="data/" --storage.tsdb.retention.time=0d --storage.remote.flush-deadline=2m --rules.alert.for-outage-tolerance=1h --rules.alert.for-grace-period=10m --rules.alert.resend-delay=1m --alertmanager.notification-queue-capacity=10000 --log.level=info --log.format=logfmt 2021-11-22 14:18:50,805 INFO - Started process 17384 2021-11-22 14:18:50,826 DEBUG - Forwarding logs of the process System.Diagnostics.Process (prometheus) to WinSW.SizeBasedRollingLogAppender
Stopping the Service	300	2021-11-22 14:12:04,083 INFO - Stopping jpc_prometheus 2021-11-22 14:12:04,084 DEBUG - ProcessKill 16492 2021-11-22 14:12:04,108 DEBUG - Stopping process 16492... 2021-11-22 14:12:04,141 DEBUG - Process 16492 canceled with code 0. 2021-11-22 14:12:04,176 INFO - Finished jpc_prometheus

How to delete

Move or rename the log file and save it. After saving, the program creates a log file when the user performs an operation to output the log. There is no need to stop the service when saving log files.

The saved file is deleted manually when it is judged to be unnecessary.

(5) Fluentd log

Fluentd log is output.

Upper limit of log size and number of planes

- For Windows
Specify in service definition file.
- For Linux

Specify in unit definition file.

For details on the specification procedure, see *Service definition file (jpc_program-name_service.xml)* and *Unit definition file (jpc_program-name.service)* in Chapter 2. *Definition Files* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

Output destination

- For Windows

Agent-path[#]\logs\fluentd\jpc_fluentd_service.(err|out).log

#: For a cluster, replace it with "*shared-folder*\jplima."

- For Linux

/opt[#]/jplima/logs/fluentd/fluentd_server

#: For a cluster, replace it with "*shared-directory*".

Output format

Fluentd outputs text data that is output to stdout or stderr during operation.

(6) Command log

The command log is output.

Upper limit of log size and number of planes

The maximum log size and the number of planes are determined for each command, cannot be changed.

Output destination

- For Windows

Agent-path[#]\logs\tools\command-name.*

#

For clusters, there are commands that output to physical disks and commands that output to shared disks. If the command is to be exported to a shared disk, replace it with "*shared-folder*\jplima".

- For Linux

/opt[#]/jplima/logs/tools\command-name.*

#

For clusters, there are commands that output to physical disks and commands that output to shared disks. If the command is output to a shared disk, replace it with "*shared-directory*".

Output format

Date log-contents

(7) JP1/IM agent control base log

(a) Public log

JP1/IM agent control base log for publishing is output.

Upper limit of log size and number of planes

It is specified in JP1/IM agent control base definition file.

Output destination

- For Windows

Agent-path#\logs\imagent\
Agent-path#\logs\imagentproxy\
Agent-path#\logs\imagentaction\
#: For a cluster, replace it with "*shared-folder*\jplima"

- For Linux

/opt#/*jplima*/logs/imagent/
/opt#/*jplima*/logs/imagentproxy/
/opt#/*jplima*/logs/imagentaction/
#: For a cluster, replace it with "*shared-directory*".

File name

jima_message.log#1
jima_message-YYYY-MM-DDThh-mm-ss.sss.log#2

#1

When the log reaches the specified size, "*-YYYY-MM-DDThh-mm-ss.sss.log*" is added to the log filename and the log is rotated.

#2

Rename the output destination log file name to a new date and delete the oldest log file.

Output format

Datetime PID Job-Identifier Message-ID Message

(b) Log of setting values at start up

The setting values read by JP1/IM agent control base at startup are output.

Upper limit of log size and number of planes

The log size and number of planes are fixed in the system. It cannot be changed by a user.

Output destination

- For Windows

Agent-path#\logs\imagent\
Agent-path#\logs\imagentproxy\
Agent-path#\logs\imagentaction\
#: For a cluster, replace it with "*shared-folder*\jplima"

- For Linux

/opt#/*jplima*/logs/imagent/
/opt#/*jplima*/logs/imagentproxy/
/opt#/*jplima*/logs/imagentaction/
#: For a cluster, replace it with "*shared-directory*".

File name

jima_setting.log#1
jima_setting-YYYY-MM-DDThh-mm-ss.sss.log#2

#1

When the log reaches the specified size, "-YYYY-MM-DDThh-mm-ss.sss.log" is added to the log filename and the log is rotated.

#2

Rename the output destination log file name to a new date and delete the oldest log file.

Output format

Outputs a log that shows the date and time and the set value.

12.3 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.

12.3.1 Information about JP1/IM - Manager

(1) In Windows

(a) 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 12–15: 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

Information type	Collected data	File name ^{#1}	View
Startup service list	net start execution result	netstart.log	Y
Network statistical information	netstat -nao execution result	netstat.log	Y
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\HITACHI\jplcommon\	Copies of the files indicated at left	Y
JP1/IM - Manager installation information	<i>system-drive</i> : Program Files\InstallShield Installation Information\setup.ini	imm_setup.ini	Δ
JP1/IM - Manager installation log file	<i>system-drive</i> : Program Files\InstallShield Installation Information\setup.ilg	imm_setup.ilg	Δ
JP1/Base installation information	<i>system-drive</i> : Program Files\InstallShield Installation Information\setup.ini	base_setup.ini	Δ
JP1/Base installation log file	<i>system-drive</i> : Program Files\InstallShield Installation Information\setup.ilg	base_setup.ilg	Δ
JP1/IM - View installation information	<i>system-drive</i> : Program Files\InstallShield Installation Information\setup.ini	imv_setup.ini	Y
JP1/IM - View installation log file	<i>system-drive</i> : Program Files\InstallShield Installation Information\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_jplbase_log_COMMAND.log	Δ
	cacls <i>shared-folder</i> \JP1Base\log\COMMAND execution result#2	cacls_jplbase_log_COMMAND.log	--
JP1/Base access permission information (event database folder)	cacls <i>Base-path</i> \sys execution result	cacls_jplbase_sys.log	Δ
JP1/Base access permission information (event database folder)	cacls <i>Base-path</i> \sys\event execution result	cacls_jplbase_sys_event.log	Δ
	cacls <i>shared-folder</i> \JP1Base\event execution result#2	cacls_jplbase_event.log	--
JP1/Base access permission information (event database folder)	cacls <i>Base-path</i> \sys\event\servers execution result	cacls_jplbase_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_jplbase_sys_event_servers_default.log	Δ
JP1/IM - Manager (Central Console) access permission information (installation folder)	cacls <i>Console-path</i> execution result	cacls_jplcons.log	Δ
	cacls <i>shared-folder</i> \JP1Cons execution result#2	cacls_jplcons.log	--
JP1/IM - Manager (Central Console) access permission information (log folder)	cacls <i>Console-path</i> \log execution result	cacls_jplcons_log.log	Δ
	cacls <i>shared-folder</i> \JP1Cons\log execution result#2	cacls_jplcons_log.log	--
JP1/IM - Manager (Central Console) access permission information (correlation history folder)	cacls <i>Console-path</i> \operation execution result	cacls_jplcons_operation.log	Δ
	cacls <i>shared-folder</i> \JP1Cons\operation execution result#2	cacls_jplcons_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_jplcons_operation_evgen.log	Δ
	cacls <i>shared-folder</i> \JP1Cons\operation\evgen execution result#2	cacls_jplcons_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_jplcons_operation_comexclude.log	Δ
JP1/IM - View access permission information (installation folder)	cacls <i>View-path</i> execution result	cacls_jplcoview.log	Y
JP1/IM - View access permission information (log folder)	cacls <i>system-drive</i> :\ProgramData\Hitachi\jpl\jpl_default\JP1CoView\log execution result	cacls_programdata_jplcoview_log.log	Y

Information type	Collected data	File name#1	View
JP1/IM - Manager access permission information (installation folder)	cacls <i>Manager-path</i> execution result	cacls_jp1imm.log	Δ
JP1/IM - Manager access permission information (log folder)	cacls <i>Manager-path</i> \log execution result	cacls_jp1imm_log.log	Δ
JP1/IM - Manager (Central Scope) access permission information (installation folder)	cacls <i>Scope-path</i> execution result	cacls_jp1scope.log	Δ
	cacls <i>shared-folder</i> \JP1Scope execution result#2	cacls_jp1scope.log	--
JP1/IM - Manager (Central Scope) access permission information (log folder)	cacls <i>Scope-path</i> \log execution result	cacls_jp1scope_log.log	Δ
	cacls <i>shared-folder</i> \JP1Scope\log execution result#2	cacls_jp1scope_log.log	--
JP1/IM - Manager (Central Scope) access permission information (database folder)	cacls <i>Scope-path</i> \database execution result	cacls_jp1scope_database.log	Δ
	cacls <i>shared-folder</i> \JP1Scope\database execution result#2	cacls_jp1scope_database.log	--
JP1/IM - Manager (Central Scope) access permission information (database folder)	cacls <i>Scope-path</i> \database\event execution result	cacls_jp1scope_database_event.log	Δ
	cacls <i>shared-folder</i> \JP1Scope\database\event execution result#2	cacls_jp1scope_database_event.log	--
JP1/IM - Manager (Central Scope) access permission information (database folder)	cacls <i>Scope-path</i> \database\jcsdb execution result	cacls_jp1scope_database_jcsdb.log	Δ
	cacls <i>shared-folder</i> \JP1Scope\database\jcsdb execution result#2	cacls_jp1scope_database_jcsdb.log	--
JP1/IM - Manager (Central Scope) access permission information (database folder)	cacls <i>Scope-path</i> \database\jcsdb\event execution result	cacls_jp1scope_database_jcsdb_event.log	Δ
	cacls <i>shared-folder</i> \JP1Scope\database\jcsdb\event execution result#2	cacls_jp1scope_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_jp1scope_database_jcsdb_pw.log	Δ
	cacls <i>shared-folder</i> \JP1Scope\database\jcsdb\pw execution result#2	cacls_jp1scope_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_jp1scope_database_jcsdb_tree.log	Δ
	cacls <i>shared-folder</i> \JP1Scope\database\jcsdb\tree execution result#2	cacls_jp1scope_database_jcsdb_tree.log	--

Information type	Collected data	File name#1	View
JP1/IM - Manager (Central Scope) access permission information (database folder)	cacls <i>Scope-path</i> \database\jcshosts execution result	cacls_jplscope_database_jcshosts.log	Δ
	cacls <i>shared-folder</i> \JP1Scope\database\jcshosts execution result#2	cacls_jplscope_database_jcshosts.log	--
JP1/IM - Manager (Intelligent Integrated Management Base) access permission information (log folder)	cacls <i>Manager-path</i> \log\imdd execution result	cacls_jplimm_log_imdd.log	--
	cacls <i>shared-folder</i> \log\imdd execution result#2	cacls_jplimm_log_imdd.log	--
JP1/IM - Manager (Intelligent Integrated Management Base) access permission information (response action execution history folder)	cacls <i>Manager-path</i> \log\suggestion execution result	cacls_jplimm_log_suggestion.log	--
	cacls <i>shared-folder</i> \log\suggestion execution result#2	cacls_jplimm_log_suggestion.log	--
Access permission information for the operation log file output destination	cacls <i>operation-log-output-destination</i> execution result <i>operation-log-output-destination</i> indicates the folder specified in the following common definition: [JP1_DEFAULT\JP1IMM\OPERATION] "LOGFILEDIR"	cacls_jplimm_operationlog.log	Δ
	cacls <i>operation-log-output-destination</i> execution result <i>operation-log-output-destination</i> indicates the folder specified in the following common definition: [<i>logical-host-name</i> \JP1IMM\OPERATION] "LOGFILEDIR"	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

Information type	Collected data	File name#1	View
	dir <i>shared-folder</i> \JP1Scope /s execution result#2	dir_ <i>logical-host-name</i> _jp1scope.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: [<i>logical-host-name</i> \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) jbsgethostbyname_err.log (standard error) 	Δ
	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#3	<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,#3	<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

Information type	Collected data	File name#1	View
	<code>jcastatus -h logical-host-name</code> execution result#2	<ul style="list-style-type: none"> • <code>jcastatus.log</code> (standard output) • <code>jcastatus_err.log</code> (standard error) 	--
Automated action definition file content	<code>jcastatus -d</code> execution result	<ul style="list-style-type: none"> • <code>jcastatus_d.log</code> (standard output) • <code>jcastatus_d_err.log</code> (standard error) 	Δ
	<code>jcastatus -d -h logical-host-name</code> execution result#2	<ul style="list-style-type: none"> • <code>jcastatus_d.log</code> (standard output) • <code>jcastatus_d_err.log</code> (standard error) 	--
Event Generation Service status	<code>jcoegsstatus</code> execution result	<ul style="list-style-type: none"> • <code>jcoegsstatus.log</code> (standard output) • <code>jcoegsstatus_err.log</code> (standard error) 	Δ
	<code>jcoegsstatus -h logical-host-name</code> execution result#2	<ul style="list-style-type: none"> • <code>jcoegsstatus.log</code> (standard output) • <code>jcoegsstatus_err.log</code> (standard error) 	--
Process operation status	<code>jco_spm�_status</code> execution result	<ul style="list-style-type: none"> • <code>jco_spm�_status.log</code> (standard output) • <code>jco_spm�_status_err.log</code> (standard error) 	Δ
	<code>jco_spm�_status -h logical-host-name</code> execution result#2	<ul style="list-style-type: none"> • <code>jco_spm�_status.log</code> (standard output) • <code>jco_spm�_status_err.log</code> (standard error) 	--
Results of executing the data collection tool	<code>jim_log.bat</code> command execution result	<code>jim_log_result.log</code>	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"> • <code>hlicliberr{n}.log</code> • <code>hliclibmgrerr{n}.log</code> • <code>hliclibtrc{n}.log</code> • <code>hliclibmgrtrc{n}.log</code> 	--
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"> • <code>hlicliberr{n}.log</code> • <code>hliclibmgrerr{n}.log</code> • <code>hliclibtrc{n}.log</code> • <code>hliclibmgrtrc{n}.log</code> 	--
Windows event log	<ul style="list-style-type: none"> • Application: <code>system-root-folder\system32\config\AppEvent.Evt</code> • System: <code>system-root-folder\system32\config\SysEvent.Evt</code> 	<ul style="list-style-type: none"> • <code>AppEvent (Backup).evt</code> • <code>AppEvent (Backup).txt</code> • <code>SysEvent (Backup).evt</code> • <code>SysEvent (Backup).txt</code> 	Y
jplhosts2 information registered on the host	<code>jbshosts2export</code> execution result	<ul style="list-style-type: none"> • <code>jbshosts2export.log</code> (standard output) • <code>jbshosts2export_err.log</code> (standard error) 	Δ
	<code>jbshosts2export -h logical-host-name</code> execution result	<ul style="list-style-type: none"> • <code>jbshosts2export.log</code> (standard output) • <code>jbshosts2export_err.log</code> (standard error) 	--
Media sense functionality's ON/OFF information	Content of the registry <code>HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\DisableDHCPMediaSense</code> displayed by the <code>reg</code> command	<code>DisableDHCPMediaSense_reg.txt</code>	--

Information type	Collected data	File name#1	View
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) 	--
Intelligent Integrated Management Database Files List	<ul style="list-style-type: none"> dir <i>Intelligent-Integrated-Management-Database-install-destination-folder</i>#4 /s execution result Result of executing dir <i>Intelligent-Integrated-Management-Database-data-storage-folder</i>#5 /s execution result 	<ul style="list-style-type: none"> dir_jplimgndb_env.log dir_jplimgndb_data.log 	--

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 JP1/Integrated Management 3 - Manager Command, Definition File and API Reference
- jcoview_log.bat* (Windows only) in Chapter 1. Commands in the JP1/Integrated Management 3 - Manager Command, Definition File and API Reference

#2: Can be collected when data in a logical host (cluster) environment is being collected.

#3: Can be collected only when `Console-path\log\action\action-information-file-name` exists.

#4: The default is `Manager-path\dbms`.

#5: The default is `Manager-path\database`.

(b) 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 12–16: JP1 information (Windows)

Information type	Collected data	File name#1	View	
Common to JP1/IM and JP1/Base	Integrated trace log	<code>system-drive:Program Files\Hitachi\HNTRLib2\spool</code>	The following files in the default mode: <code>hntr2[1 2 3 4].log</code>	Y
JP1/IM - Manager (common to components)	Patch information	<code>Manager-path\PATCHLOG.TXT</code>	<code>Patchlog_jplimm.txt</code>	--

Information type		Collected data	File name ^{#1}	View
	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	--
		Files under the folder specified in the following common definition: [<i>logical-host</i> \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	--
		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	--

Information type		Collected data	File name#1	View
		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 (Intelligent Integrated Management Base)	Settings and definition file	Files under <i>Manager-path</i> \conf\imdd\	Copies of the files indicated at left	--
		Files under <i>shared-folder</i> \jplimm\conf\imdd\#2	Copies of the files indicated at left	--
	Log file	Files under <i>Manager-path</i> \log\imdd\	Copies of the files indicated at left	--
		Files under <i>shared-folder</i> \jplimm\log\imdd\#2	Copies of the files indicated at left	--
	Plug-in file	Files under <i>Manager-path</i> \plugin\	Copies of the files indicated at left	--
		Files under <i>shared-folder</i> \plugin\#2	Copies of the files indicated at left	--
	Response action execution history file	Files under <i>Manager-path</i> \log\suggestion\	Copies of the files indicated at left	--
		Files under <i>shared-folder</i> \log\suggestion\#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 - Manager (Intelligent Integrated Management Database)#4	Configuration and definition files	Files under <i>Manager-path</i> \conf\imgndb\	Copy file of the file on the left	--
		Files under <i>Shared-folder</i> \jplimm\conf\imgndb\#2	Copy file of the file on the left	--

Information type		Collected data	File name#1	View
		Files under <i>Physical-host-Intelligent-Integrated-Management-Database-data-storage-folder</i> \imgndb\ <ul style="list-style-type: none"> • postgresql.conf • pg_hba.conf • pg_ident.conf • postmaster.pid • postmaster.opts • PG_VERSION 	Copy file of the file on the left	--
		Files under <i>Logical-host-Intelligent-Integrated-Management-Database-data-storage-folder</i> \imgndblogical-host-number\ <ul style="list-style-type: none"> • postgresql.conf • pg_hba.conf • pg_ident.conf • postmaster.pid • postmaster.opts • PG_VERSION 	Copy file of the file on the left	--
		Files under <i>Physical-host-Intelligent-Integrated-Management-Database-installation-folder</i> \imgndbbin\promscale\ <ul style="list-style-type: none"> • promsrv.xml 	Copy file of the file on the left	--
		Files under <i>Logical-host-Intelligent-Integrated-Management-Database-Installation-folder</i> \imgndbbinlogical-host-number\promscale\ <ul style="list-style-type: none"> • promsrv.xml 	Copy file of the file on the left	--
	Log Files	Files under <i>Manager-path</i> \log\imgndb\ 	Copy file of the file on the left	--
		Files under <i>Shared-folder</i> \jplimm\log\imgndb\ 	Copy file of the file on the left	--
	State of the database	Result of executing the following commands on the physical host (jimgndb_status.txt) <ul style="list-style-type: none"> • Jimgndbstatus • Jimgndbstauts -ri#5 • Jimgndbstatus -rs#5 	Copy file of the file on the left	--
		Result of executing the following command on the logical host (jimgndb_status.txt) <ul style="list-style-type: none"> • Jimgndbstatus -h logical hostname • Jimgndbstauts -h logical hostname -ri#5 • Jimgndbstatus -h logical hostname -rs#5 	Copy file of the file on the left	--
	JP1/IM - Agent (JP1/IM agent management base)	Definition file	Files that need to be collected under <i>Manager-path</i> \conf\imdd\plugin\jplpccs\ <ul style="list-style-type: none"> • AWS definition file (aws_settings.conf) 	--

Information type		Collected data	File name#1	View
			<ul style="list-style-type: none"> • Property display name definition file (property_labels.conf) • Node exporter metric definition file (metrics_node_exporter.conf) • Windows exporter metric definition file (metrics_windows_exporter.conf) • Windows exporter (process monitoring) metric definition file (metrics_windows_exporter_process.conf) • Blackbox exporter metric definition file (metrics_blackbox_exporter.conf) • Yet another cloudwatch exporter metric definition file (metrics_ya_cloudwatch_exporter.conf) • Container Monitor (kubelet) metric Definition Files (metrics_kubelet.conf) • Fluentd metric definition file (metrics_fluentd.conf) • User-defined Exporter's metric definition-file (metrics_any Prometheus of trend name.conf) • Process exporter metric definition file (metrics_process_exporter.conf) • Promitor metric definition file (metrics_promitor.conf) • Script exporter metric definition file (metrics_script_exporter.conf) • Web exporter metric definition file (metrics_web_exporter.conf) • VMware exporter metric definition file for host (metrics_vmware_exporter_host.conf) • VMware exporter metric definition file for VM (metrics_vmware_exporter_vm.conf) 	

Information type		Collected data	File name#1	View	
		Files that need to be collected under <i>Manager-path</i> \conf\imdd\plugin\jplpccs\user\	User-defined Exporter's metric definition-file (metrics_any Prometheus trend name.conf)	--	
		Files that need to be collected under <i>Manager-path</i> \conf\imdd\imagent\	<ul style="list-style-type: none"> Imbase configuration file (jpc_imbase.json) Imbaseproxy configuration file (jpc_imbaseproxy.json) JP1/IM agent management base Server Certificate Files 	--	
	Log Files	Files that need to be collected under <i>Manager-path</i> \conf\imdd\imagent\imbase\	JP1/IM agent management base (imbase) log	--	
		Files that need to be collected under <i>Manager-path</i> \conf\imdd\imagent\imbaseproxy\	JP1/IM agent management base (imbaseproxy) log	--	
		Files that need to be collected under <i>Manager-path</i> \conf\imdd\imagent\tools\	Logs such as commands	--	
		Files that need to be collected under <i>Manager-path</i> \conf\imdd\jplpccs\	Product plugin Log	--	
	JP1/IM - View	Patch information	<i>View-path</i> \Patchlog.txt	Patchlog_jplcoview.txt	Y
		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\jpl\jpl_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\jpl\jpl_default\JP1CoView\log\	Copies of the files indicated at left	Y	
JP1/Base	Patch information	<i>Base-path</i> \PatchLog.txt	Patchlog_jplbase.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	--	

Information type		Collected data	File name#1	View
		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	--
	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 *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*
- *jcoview_log.bat (Windows only)* in *Chapter 1. Commands* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API 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 *11.5.2 jim_log.bat (Windows only)*.

#4: Intelligent Integrated Management Database log is not subject to data collection tool. For more information about Intelligent Integrated Management Database log, see *1.3.2(1) Checking the log output by Intelligent Integrated Management Database*. If you are using Intelligent Integrated Management Database and matches the following cases, collect them manually separately:

- When an error message related to Intelligent Integrated Management Database is output and the action taken by the operator for that message is described to log Intelligent Integrated Management Database
- When storing or retrieving trend data for Intelligent Integrated Management Database issues an error message that begins with "KAJY6200" and the problem cannot be resolved by the corrective action for that message

Collect the log file of Intelligent Integrated Management Database immediately after collecting other materials with the data collection tool. (The log will be wrapped when only one-week is left until the log file is collected.)

Note that Intelligent Integrated Management Database log files are included in the backup target of Intelligent Integrated Management Database, so if there is enough disk space, you can make a backup and collect it. For the backup procedure, see *1.2.2(7) Backup and recovery procedure of Intelligent Integrated Management Database*.

5 `-ri` and `-rs` option-attached execution results can be retrieved only when the database is running.

(c) 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

(d) 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)

(e) User dump (only for Windows)

If a JP1/IM - View process stops due to an application error in Windows, collect a user dump.

(f) 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 [12.4.1\(1\)\(g\) Collecting RAS information](#).

(g) IM management node-related files

If the Intelligent Integrated Management Base is used, collect the following information:

- Files under the folder specified by the `-o` option of the `jddcreatetree` command
- Files under the folder specified by the `-i` option of the `jddupdatetree` command

(2) In UNIX

(a) 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 12–17: OS system information (UNIX)

Information type	Collected data	File name#1
Installed Hitachi product information	<code>/etc/.hitachi/pplistd/pplistd</code>	<ul style="list-style-type: none">• <code>jp1_default_imm_1st.tar.{Z gz}</code>• <code>pplistd</code>
Information about products installed by Hitachi PP Installer	Output based on <code>/etc/.hitachi/bin/SHOWPP</code>	<ul style="list-style-type: none">• <code>jp1_default_imm_1st.tar.{Z gz}</code>• <code>SHOWPP</code>
Hitachi PP Installer installation log file	<code>/etc/.hitachi/.install.log*</code>	<ul style="list-style-type: none">• <code>jp1_default_imm_1st.tar.{Z gz}</code>• <code>.install.log*</code>
Hitachi PP Installer uninstallation log file	<code>/etc/.hitachi/.uninstall.log*</code>	<ul style="list-style-type: none">• <code>jp1_default_imm_1st.tar.{Z gz}</code>

Information type	Collected data	File name#1
		<ul style="list-style-type: none"> • .uninstall.log*
Common definition information	Files under /opt/jp1/hcclibcnf/	<ul style="list-style-type: none"> • jp1_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/jp1cons	<ul style="list-style-type: none"> • jp1_default_imm_1st.tar.{Z gz} • core_module-name.log
	Analysis result from seraph shared-directory/jp1cons/log#2	<ul style="list-style-type: none"> • logical-host-name_imm_1st.tar.{Z gz} • core_module-name.log
JP1/IM - Manager (Central Scope) core analysis information (back trace)#6	Analysis result from seraph /var/opt/jp1scope	<ul style="list-style-type: none"> • jp1_default_imm_1st.tar.{Z gz} • core_module-name.log
	Analysis result from seraph shared-directory/jp1scope/log#2	<ul style="list-style-type: none"> • logical-host-name_imm_1st.tar.{Z gz} • core_module-name.log
JP1/IM - Manager (Intelligent Integrated Management Base) core analysis information (back trace)#6	Analysis result from seraph /var/opt/jp1imm/log	<ul style="list-style-type: none"> • jp1_default_imm_1st.tar.{Z gz} • core_module-name.log
	Analysis result from seraph shared-directory/jp1imm/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 • SUSE Linux /etc/SuSE-release
JP1/Base installation log file	/tmp/HITACHI_JP1_INST_LOG/ jp1base_inst{1 2 3 4 5}.log	<ul style="list-style-type: none"> • jp1_default_imm_1st.tar.{Z gz} • jp1base_inst{1 2 3 4 5}.log
JP1/IM - Manager installation log file	/tmp/HITACHI_JP1_INST_LOG/ jp1imm_inst{1 2 3 4 5}.log	<ul style="list-style-type: none"> • jp1_default_imm_1st.tar.{Z gz} • jp1imm_inst{1 2 3 4 5}.log
File list	<ul style="list-style-type: none"> • ls -lRa /opt/jp1imm execution result • ls -lRa /var/opt/jp1imm execution result • ls -lRa /opt/jp1cons execution result • ls -lRa /etc/opt/jp1cons execution result • ls -lRa /var/opt/jp1cons execution result • ls -lRa /opt/jp1scope execution result • ls -lRa /etc/opt/jp1scope execution result • ls -lRa /var/opt/jp1scope execution result • ls -lRa /opt/jp1base execution result • ls -lRa /etc/opt/jp1base execution result • ls -lRa /var/opt/jp1base execution result 	<ul style="list-style-type: none"> • jp1_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 user-specified -IMDBENVDIR-value-in-setup-information-file</code> execution result • <code>ls -lRa user-specified -IMDBDIR-value-in-setup-information-file</code> execution result • <code>ls -lRa /etc/opt/jplimm</code> execution result • <code>ls -lRa /tmp/HITACHI_JP1_INST_LOG</code> execution result • <code>ls -lRa /etc/.hitachi</code> execution result • <code>ls -lRa /etc/opt/.hlic</code> execution result • <code>ls -lRa operation-log-output-destination</code> execution result#4 • <code>ls -lRa Intelligent-Integrated-Management-Database-install-destination-directory</code> execution result • <code>ls -lRa Intelligent-Integrated-Management-Database-data-storage-directory</code> execution result 	
	<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 • <code>ls -lRa Intelligent-Integrated-Management-Database-install-destination-directory</code> execution result • <code>ls -lRa Intelligent-Integrated-Management-Database-data-storage-directory</code> execution result 	<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 	<ul style="list-style-type: none"> • <code>jpl_default_imm_1st.tar.{Z gz}</code> • <code>inst_dir_lRaL.log</code>

Information type	Collected data	File name#1
	<ul style="list-style-type: none"> • <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 -IMBDDIR-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 • <code>ls -lRaL Intelligent-Integrated-Management-Database-install-destingation-directory</code> execution result • <code>ls -lRaL Intelligent-Integrated-Management-Database-data-storage-directory</code> execution result 	
	<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 • <code>ls -lRaL shared-directory/event</code> execution result • <code>ls -lRaL operation-log-output-destination</code> execution result#5 • <code>ls -lRaL Intelligent-Integrated-Management-Database-install-destingation-directory</code> execution result • <code>ls -lRaL Intelligent-Integrated-Management-Database-data-storage-directory</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>
Data collection date/time	date execution result	<ul style="list-style-type: none"> • <code>jpl_default_imm_1st.tar.{Z gz}</code> • <code>jpl_default_imm_2nd.tar.{Z gz}</code>

Information type	Collected data	File name#1
		<ul style="list-style-type: none"> • <i>logical-host-name_imm_1st.tar.{Z gz}</i> • <i>logical-host-name_imm_2nd.tar.{Z gz}</i> • <i>date.log</i>
Disk information	df -k execution result	<ul style="list-style-type: none"> • <i>jp1_default_imm_1st.tar.{Z gz}</i> • <i>df.log</i>
btrfs file system information	Only when btrfs is installed in Linux <ul style="list-style-type: none"> • <i>btrfs filesystem show --all-device result</i> 	<ul style="list-style-type: none"> • <i>Linux:jp1_default_imm_1st.tar.gz</i> • <i>df.log</i>
Information about process operation based on the automated startup service (systemd)	Only when systemd is installed in Linux systemctl --all, systemctl list-unit-files, systemctl status jp1_base, systemctl status jp1_cons, systemctl status /usr/lib/systemd/system/2248-*start.service result	<ul style="list-style-type: none"> • <i>jp1_default_imm_1st.tar.gz</i> • <i>systemctl.log</i>
Machine's environment variable	env execution result	<ul style="list-style-type: none"> • <i>jp1_default_imm_1st.tar.{Z gz}</i> • <i>env.log</i>
Host name settings that are set in the machine	/etc/hosts(Linux)	<ul style="list-style-type: none"> • <i>jp1_default_imm_1st.tar.{Z gz}</i> • <i>hosts</i>
Status of shared memory for inter-process communication	ipcs -ma execution result	<ul style="list-style-type: none"> • <i>jp1_default_imm_1st.tar.{Z gz}</i> • <i>ipcs.log</i>
Host name for resolving network address	jbsgethostbyname execution result	<ul style="list-style-type: none"> • <i>jp1_default_imm_1st.tar.{Z gz}</i> • <i>jbsgethostbyname.log (standard output)</i> • <i>jbsgethostbyname_err.log (standard error)</i>
	jbsgethostbyname <i>logical-host-name</i> execution result#2	<ul style="list-style-type: none"> • <i>logical-host-name_imm_1st.tar.{Z gz}</i> • <i>jbsgethostbyname_logical-host-name.log</i>
Health check	jbshcstatus -debug -a execution result	<ul style="list-style-type: none"> • <i>jp1_default_imm_1st.tar.{Z gz}</i> • <i>jbshcstatus.log (standard output)</i> • <i>jbshcstatus_err.log (standard error)</i>
	jbshcstatus -debug -a -h <i>logical-host-name</i> execution result#2	<ul style="list-style-type: none"> • <i>logical-host-name_imm_1st.tar.{Z gz}</i> • <i>jbshcstatus.log (standard output)</i> • <i>jbshcstatus_err.log (standard error)</i>
Process operation status of Event Service	jevstat execution result	<ul style="list-style-type: none"> • <i>jp1_default_imm_1st.tar.{Z gz}</i> • <i>jevstat.log (standard output)</i> • <i>jevstat_err.log (standard error)</i>
	jevstat <i>logical-host-name</i> execution result	<ul style="list-style-type: none"> • <i>logical-host-name_imm_1st.tar.{Z gz}</i> • <i>jevstat.log (standard output)</i> • <i>jevstat_err.log (standard error)</i>
Process operation status of items other than Event Service	jbs_spmd_status execution result	<ul style="list-style-type: none"> • <i>jp1_default_imm_1st.tar.{Z gz}</i> • <i>jbs_spmd_status.log (standard output)</i> • <i>jbs_spmd_status_err.log (standard error)</i>

Information type	Collected data	File name#1
	jbs_spmd_status -h <i>logical-host-name</i> execution result#2	<ul style="list-style-type: none"> • <i>logical-host-name_imm_1st.tar</i>.{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"> • jpl_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_imm_1st.tar</i>.{Z gz} • jcashowa.log (standard output) • jcashowa_err.log (standard error)
Automated action function status	jcastatus execution result	<ul style="list-style-type: none"> • jpl_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_imm_1st.tar</i>.{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"> • jpl_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_imm_1st.tar</i>.{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"> • jpl_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_imm_1st.tar</i>.{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"> • jpl_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_imm_1st.tar</i>.{Z gz} • jco_spmd_status.log (standard output) • jco_spmd_status_err.log (standard error)
Results of executing the data collection tool	jim_log.sh command execution result	<ul style="list-style-type: none"> • jpl_default_imm_1st.tar.{Z gz} • jim_log_result.log
IP address acquisition	ifconfig -a	<ul style="list-style-type: none"> • jpl_default_imm_1st.tar.{Z gz} • ifconfig.log
	ip addr show	<ul style="list-style-type: none"> • jpl_default_imm_1st.tar.gz • ip_addr_show.log
NIC installation status	netstat -ai execution result	<ul style="list-style-type: none"> • jpl_default_imm_1st.tar.{Z gz} • netstat_ai.log
	ip -s link	<ul style="list-style-type: none"> • jpl_default_imm_1st.tar.gz

Information type	Collected data	File name#1
		<ul style="list-style-type: none"> ip_s_link.log
Network statistical information	netstat -nap execution result	<ul style="list-style-type: none"> jpl_default_imm_1st.tar.{Z gz} netstat_na.log
	ss -nap	<ul style="list-style-type: none"> jpl_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"> jpl_default_imm_1st.tar.{Z gz} passwd
Process list	ps -elfa execution result	<ul style="list-style-type: none"> jpl_default_imm_1st.tar.{Z gz} ps.log
Service port settings that are set in the machine	/etc/services	jpl_default_imm_1st.tar.{Z gz} services
Memory information	cat /proc/meminfo	jpl_default_imm_1st.tar.{Z gz} swapinfo.log
System diagnostic information	dmesg execution result	jpl_default_imm_1st.tar.{Z gz} sys_info.log
Syslog (syslog)	/var/log/messages	<ul style="list-style-type: none"> jpl_default_imm_1st.tar.{Z gz} syslog.log
journal	journalctl -l --no-pager execution result Obtained in SUSE Linux 15 or later	journal.log
JP1/IM - Manager (Central Console) core analysis information (back trace) output by the jccogencore command#6	Analysis result from seraph /var/opt/jplcons	<ul style="list-style-type: none"> jpl_default_imm_1st.tar.{Z gz} trace_<i>module-name</i>.log
	Analysis result from seraph <i>shared-directory</i> /jplcons/log (core output by jccogencore)#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"> jpl_default_imm_1st.tar.{Z gz} uname_a.log
Kernel parameter information	<ul style="list-style-type: none"> sysctl -a execution result ulimit -a execution result 	<ul style="list-style-type: none"> jpl_default_imm_1st.tar.{Z gz} sysctl.log ulimit.log
Page size information	Nothing (Linux)	<ul style="list-style-type: none"> jpl_default_imm_1st.tar.{Z gz} pagesize.log
OS patch application information	rpm -qa execution result	<ul style="list-style-type: none"> jpl_default_imm_1st.tar.{Z gz} rpm.log
Distribution information	/etc/*-release	*-release
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"> jpl_default_imm_1st.tar.{Z gz} hlicliberr{n}.log hliclibmgrerr{n}.log hliclibtrc{n}.log hliclibmgrtrc{n}.log
Process startup information used by the init daemon	<ul style="list-style-type: none"> Files under /etc/init 	<ul style="list-style-type: none"> jpl_default_imm_1st.tar.{Z gz}

Information type	Collected data	File name#1
	In Linux, this information is collected only in Linux 6.	<ul style="list-style-type: none"> For left files under the <code>init</code> directory
Disk mounting information	<code>/etc/fstab</code>	<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 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 *JP1/Integrated Management 3 - Manager Command, Definition File and API 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 *2.18.10 Specifying settings for handling JP1/IM - Manager failures (for UNIX)* in the *JP1/Integrated Management 3 - Manager Configuration Guide*.

(b) 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 12–18: JP1 information (UNIX)

Information type	Collected data	File name#1
Common to JP1/IM and JP1/Base	All files under <code>/var/opt/hitachi/HNTRLib2/spool/</code>	<ul style="list-style-type: none"> <code>jp1_default_imm_1st.tar.{Z gz}</code> The following files in the default mode: <code>hntr2[1 2 3 4].log</code>

Information type		Collected data	File name ^{#1}
JP1/IM - Manager (common to components)	Patch application history	/opt/jp1imm/patch_history	<ul style="list-style-type: none"> • jp1_default_imm_1st.tar. {Z gz} • patch_history
	Patch log information	/opt/jp1imm/update.log	<ul style="list-style-type: none"> • jp1_default_imm_1st.tar. {Z gz} • update.log
	License type and expiration date	/var/opt/ jp1imm/log/ProductInfo	<ul style="list-style-type: none"> • jp1_default_imm_1st.tar. {Z gz} • ProductInfo
	Managed-node count log file	/var/opt/ jp1imm/log/nodecount	<ul style="list-style-type: none"> • jp1_default_imm_1st.tar. {Z gz} • jimnodecount_cmd{1 2}.log
	Operation log file	Files under the directory specified in the following common definition: [JP1_DEFAULT\JP1IMM\OPERATI ON] "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: [<i>logical-host- name</i> \JP1IMM\OPERATION] "LOGFILEDIR"		<ul style="list-style-type: none"> • <i>logical-host-name</i>_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 gz} • Copies of the files indicated at left
	Settings and defintion 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"> • <i>logical-host-name</i>_imm_1st.tar. {Z gz} • Copies of the files indicated at left
	Common definition information	Files under /etc/opt/ jp1cons/default/	<ul style="list-style-type: none"> • jp1_default_imm_1st.tar. {Z gz} • Copies of the files indicated at left
	Log file	Files under /var/opt/ jp1cons/log/	<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/log/#2	<ul style="list-style-type: none"> • <i>logical-host-name</i>_imm_1st.tar. {Z gz} • Copies of the files indicated at left
	File for accumulated response- waiting events ^{#3}	Files under /var/opt/ jp1cons/log/response/	<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/log/response/		<ul style="list-style-type: none"> • jp1_default_imm_1st.tar. {Z gz} • Copies of the files indicated at left 	

Information type		Collected data	File name ^{#1}	
	Core analysis information (CAR file) output by the jcoengcore command	car command result /var/opt/jp1cons/log (core output by jcoengcore)	<ul style="list-style-type: none"> • jp1_default_imm_2nd.tar.{Z gz} • car_module-name.tar[.Z] 	
		car command result shared-directory/jp1cons/log (core output by jcoengcore) ^{#2}	<ul style="list-style-type: none"> • logical-host-name_imm_2nd.tar.{Z gz} • car_module-name.tar[.Z] 	
	Core analysis information (CAR file)	car command result /var/opt/jp1cons/log	<ul style="list-style-type: none"> • jp1_default_imm_2nd.tar.{Z gz} • core_module-name_car.tar[.Z] 	
		car command result shared-directory/jp1cons/log ^{#2}	<ul style="list-style-type: none"> • logical-host-name_imm_2nd.tar.{Z gz} • core_module-name_car.tar[.Z] 	
	Correlation event generation history file	Files under /var/opt/jp1cons/operation/evgen/	<ul style="list-style-type: none"> • jp1_default_imm_2nd.tar.{Z gz} • Copies of the files indicated at left 	
		shared-directory/jp1cons/operation/evgen ^{#2}	<ul style="list-style-type: none"> • logical-host-name_imm_2nd.tar.{Z gz} • Copies of the files indicated at left 	
	Common exclusion history file, and common exclusion-conditions definition history file	Files under /var/opt/jp1cons/operation/comexclude/	<ul style="list-style-type: none"> • jp1_default_imm_2nd.tar.{Z gz} • Copies of the files indicated at left 	
		shared-directory/jp1cons/operation/comexclude ^{#2}	<ul style="list-style-type: none"> • logical-host-name_imm_2nd.tar.{Z gz} • Copies of the files indicated at left 	
	JP1/IM - Manager (Central Scope) ^{#4}	Settings and definition file	Files under /etc/opt/jp1scope/conf/	<ul style="list-style-type: none"> • jp1_default_imm_1st.tar.{Z gz} • Copies of the files indicated at left
			Files under shared-directory/jp1scope/conf/ ^{#2}	<ul style="list-style-type: none"> • logical-host-name_imm_1st.tar.{Z gz} • Copies of the files indicated at left
Common definition information		Files under /etc/opt/jp1scope/default/	<ul style="list-style-type: none"> • jp1_default_imm_1st.tar.{Z gz} • Copies of the files indicated at left 	
Log file		Files under /var/opt/jp1scope/log/	<ul style="list-style-type: none"> • jp1_default_imm_1st.tar.{Z gz} • Copies of the files indicated at left 	
		Files under shared-directory/jp1scope/log/ ^{#2}	<ul style="list-style-type: none"> • logical-host-name_imm_1st.tar.{Z gz} • Copies of the files indicated at left 	
Core analysis information (CAR file)		car command result /var/opt/jp1scope/log	<ul style="list-style-type: none"> • jp1_default_imm_2nd.tar.{Z gz} • core_module-name_car.tar[.Z] 	
		car command result shared-directory/jp1scope/log ^{#2}	<ul style="list-style-type: none"> • logical-host-name_imm_2nd.tar.{Z gz} • core_module-name_car.tar[.Z] 	

Information type		Collected data	File name ^{#1}
	Database information	Files under <code>/var/opt/jplscope/database/</code>	<ul style="list-style-type: none"> • <code>jpl_default_imm_2nd.tar.{Z gz}</code> • Copies of the files indicated at left
		Files under <i>shared-directory</i> / <code>/jplscope/database/#2</code>	<ul style="list-style-type: none"> • <i>logical-host-name_imm_2nd.tar.{Z gz}</i> • Copies of the files indicated at left
JP1/IM - Manager (Intelligent Integrated Management Base) ^{#4}	Settings and definition file	Files under <code>/etc/opt/jplimm/conf/imdd</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 <i>shared-directory</i> / <code>/jplimm/conf/imdd</code>	<ul style="list-style-type: none"> • <i>logical-host-name_imm_2nd.tar.{Z gz}</i> • Copies of the files indicated at left
	Log file	Files under <code>/var/opt/jplimm/log/imdd</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 <i>shared-directory</i> / <code>/jplimm/log/imdd</code>	<ul style="list-style-type: none"> • <i>logical-host-name_imm_2nd.tar.{Z gz}</i> • Copies of the files indicated at left
	Plug-in file	Files under <code>/etc/opt/jplimm/plugin</code>	<ul style="list-style-type: none"> • <code>jpl_default_imm_1st.tar.gz</code> • Copies of the files indicated at left
		Files under <i>shared-directory</i> / <code>/jplimm/plugin</code>	<ul style="list-style-type: none"> • <i>logical-host-name_imm_1st.tar.gz</i> • Copies of the files indicated at left
	Response action execution history file	Files under <code>/var/opt/jplimm/log/suggestion</code>	<ul style="list-style-type: none"> • <code>jpl_default_imm_1st.tar.gz</code> • Copies of the files indicated at left
		Files under <i>shared-directory</i> / <code>/jplimm/log/suggestion</code>	<ul style="list-style-type: none"> • <i>logical-host-name_imm_1st.tar.gz</i> • Copies of the files indicated at left
	Core analysis information (CAR file)	<code>car command result</code> <code>/var/opt/jplimm/log/imdd</code>	<ul style="list-style-type: none"> • <code>jpl_default_imm_2nd.tar.{Z gz}</code> • <code>core_module-name_car.tar[.Z]</code>
		<code>car command result</code> <i>shared-directory</i> / <code>/jplimm/log/imdd#2</code>	<ul style="list-style-type: none"> • <i>logical-host-name_imm_2nd.tar.{Z gz}</i> • <code>core_module-name_car.tar[.Z]</code>
JP1/IM - Manager (IM Configuration Management) ^{#4}	Settings and definition files	Files under <code>/etc/opt/jplimm/conf/imcf/</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 <i>shared-directory</i> / <code>/jplimm/conf/imcf/#2</code>	<ul style="list-style-type: none"> • <i>logical-host-name_imm_1st.tar.{Z gz}</i> • 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>jpl_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>jpl_default_imm_1st.tar.{Z gz}</code> • Copies of the files indicated at left

Information type	Collected data	File name ^{#1}	
	Files under <i>shared-directory</i> / jplimm/log/imcf/ ^{#2}	<ul style="list-style-type: none"> • <i>logical-host-name_imm_1st.tar</i>.{Z gz} • Copies of the files indicated at left 	
	Core analysis information (CAR file) car command result /var/opt/jplimm/log	<ul style="list-style-type: none"> • <i>jpl_default_imm_2nd.tar</i>.{Z gz} • <i>./var/opt/jplimm/log/_jpl_default/core/core_module-name_car.tar</i> [.Z] 	
	car command result <i>shared-directory</i> /jplimm/log ^{#2}	<ul style="list-style-type: none"> • <i>logical-host-name_imm_2nd.tar</i>.{Z gz} • <i>./var/opt/jplimm/log/_logical-host-name/core/core_module-name_car.tar</i> [.Z] 	
JP1/IM - Manager (Intelligent Integrated Management Database) ^{#5}	Settings and defintion file Files under /etc/opt/jplimm/ conf/imgndb/	<ul style="list-style-type: none"> • <i>jpl_default_imm_1st.tar.gz</i> • Copies of the files indicated at left 	
	Files under <i>shared-directory</i> /jplimm/ conf/imgndb/	<ul style="list-style-type: none"> • <i>logical-host-name_imm_2nd.tar.gz</i> • Copies of the files indicated at left 	
	Files under <i>Physical-host-Intelligent-Integration-Management-Database-data-storage-directory</i> /imgndb/ <ul style="list-style-type: none"> • postgresql.conf • pg_hba.conf • pg_ident.conf • postmaster.pid • postmaster.opts • PG_VERSION 	<ul style="list-style-type: none"> • <i>jpl_default_imm_1st.tar.gz</i> • Copies of the files indicated at left 	
	Files under <i>Logical-host-Intelligent-Integration-Management-Database-data-storage-directory</i> /imgndb/ <ul style="list-style-type: none"> • postgresql.conf • pg_hba.conf • pg_ident.conf • postmaster.pid • postmaster.opts • PG_VERSION 	<ul style="list-style-type: none"> • <i>logical-host-name_imm_1st.tar.gz</i> • Copies of the files indicated at left 	
	Log file	Files under /var/opt/ jplimm/log/imgndb/	<ul style="list-style-type: none"> • <i>jpl_default_imm_1st.tar.gz</i> • Copies of the files indicated at left
		Files under <i>shared-directory</i> / jplimm/log/imgndb/	<ul style="list-style-type: none"> • <i>logical-host-name_imm_2nd.tar.gz</i> • Copies of the files indicated at left
	Status of the database	Results of the following command on the physical host (<i>jimgndb_status.txt</i>): <ul style="list-style-type: none"> • <i>jimgndbstatus</i> • <i>jimgndbstauts -ri</i>^{#6} • <i>jimgndbstatus -rs</i>^{#6} 	<ul style="list-style-type: none"> • <i>jpl_default_imm_1st.tar.gz</i> • Copies of the files indicated at left

Information type		Collected data	File name ^{#1}
		<p>Results of the following command on the logical host (jimgndb_status.txt):</p> <ul style="list-style-type: none"> • jimgndbstatus • jimgndbstauts -ri^{#6} • jimgndbstatus -rs^{#6} 	<ul style="list-style-type: none"> • <i>logical-host-name</i>_imm_2nd.tar.gz • Copies of the files indicated at lef
JP1/IM - Agent (JP1/IM agent management base)	Defintion file	Files that need to be collected under /etc/opt/jplimm/conf/imdd/plugin/jplpccs/	<ul style="list-style-type: none"> • AWS definition file (aws_settings.conf) • Property display name definition file (property_labels.conf) • Node exporter metric definition file (metrics_node_exporter.conf) • Windows exporter metric definition file (metrics_windows_exporter.conf) • Windows exporter (process monitoring) metric definition file (metrics_windows_exporter_process.conf) • Blackbox exporter metric definition file (metrics_blackbox_exporter.conf) • Yet another cloudwatch exporter metric definition file (metrics_ya_cloudwatch_exporter.conf) • Container monitoring metric definition file (metrics_kubernetes.conf) • Container Monitoring (kubelet) metric Definition Files (metrics_kubelet.conf) • Fluentd metric definition file (metrics_fluentd.conf) • User-defined Exporter's metric definition file (metrics_ any Prometheus trend name.conf) • Process exporter metric definition file (metrics_process_exporter.conf) • Promitor metric definition file (metrics_promitor.conf) • Script exporter metric definition file (metrics_script_exporter.conf) • Web exporter metric definition file (metrics_web_exporter.conf) • VMware exporter metric definition file for host (metrics_vmware_exporter_host.conf) • VMware exporter metric definition file for VM (metrics_vmware_exporter_vm.conf)
		Files that need to be collected under /etc/opt/jplimm/conf/imdd/plugin/jplpccs/user/	User-defined Exporter's metric definition-file (metrics_ any Prometheus of trend name.conf)
		Files that need to be collected under /etc/opt/jplimm/conf/imdd/imagent/	<ul style="list-style-type: none"> • Imbase configuration file (jpc_imbase.json) • Imbaseproxy configuration file (jpc_imbaseproxy.json) • JP1/IM agent management base Server Certificate Files
	Log file	Files that need to be collected under /var/opt/jplimm/conf/imdd/imagent/imbase/	JP1/IM agent management base (imbase) log

Information type		Collected data	File name ^{#1}
		Files that need to be collected under /var/opt/jplimm/conf/imdd/imagent/ibaseproxy/	JP1/IM agent management base (ibaseproxy) log
		Files that need to be collected under /var/opt/jplimm/conf/imdd/imagent/tools/	Logs such as commands
		Files that need to be collected under /var/opt/jplimm/conf/imdd/jplpccs/	Product plugin Log
JP1/Base	Automatic startup and automatic termination script	Files under /etc/opt/jplbase/	<ul style="list-style-type: none"> • jpl_default_imm_1st.tar.{Z gz} • Copies of the files indicated at left
	Settings and definition file	Files under /etc/opt/jplbase/conf/	<ul style="list-style-type: none"> • jpl_default_imm_1st.tar.{Z gz} • Copies of the files indicated at left
		Files under <i>shared-directory</i> /jplbase/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/jplbase/default/	<ul style="list-style-type: none"> • jpl_default_imm_1st.tar.{Z gz} • Copies of the files indicated at left
	Plug-in service settings file	Files under /opt/jplbase/conf/plugin/	<ul style="list-style-type: none"> • jpl_default_imm_1st.tar.{Z gz} • Copies of the files indicated at left
	Patch application history	/opt/jplbase/PatchInfo	<ul style="list-style-type: none"> • jpl_default_imm_1st.tar.{Z gz} • PatchInfo
	Patch log information	/opt/jplbase/PatchLog	<ul style="list-style-type: none"> • jpl_default_imm_1st.tar.{Z gz} • PatchLog
	Log file	/var/opt/jplbase/log	<ul style="list-style-type: none"> • jpl_default_imm_1st.tar.{Z gz} • All files under the directory indicated at left, except COMMAND
		<i>shared-directory</i> /jplbase/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/jplbase/sys/tmp/	<ul style="list-style-type: none"> • jpl_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/jpl_ses 	<ul style="list-style-type: none"> • jpl_default_imm_2nd.tar.{Z gz} • Copies of the files indicated at left 	

Information type		Collected data	File name ^{#1}
		<ul style="list-style-type: none"> • /usr/lib/jpl_ses/log • /usr/lib/jpl_ses/sys • /usr/bin/jpl_ses/jp* • /var/opt/jpl_ses 	
	Command execution history file	Files under /var/opt/jplbase/log/COMMAND/	<ul style="list-style-type: none"> • jpl_default_imm_2nd.tar.{Z gz} • Copies of the files indicated at left
		Files under <i>shared-directory</i> /jplbase /log/COMMAND/ ^{#2}	<ul style="list-style-type: none"> • <i>logical-host-name_imm_2nd.tar.</i>{Z gz} • Copies of the files indicated at left
	Event database	Files under /var/opt/jplbase/sys/event/servers/default/	<ul style="list-style-type: none"> • jpl_default_imm_2nd.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_imm_2nd.tar.</i>{Z gz} • IMEvent*.*

#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.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 *JP1/Integrated Management 3 - Manager Command, Definition File and API 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 *11.5.3 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 *2.18.10 Specifying settings for handling JP1/IM - Manager failures (for UNIX)* in the *JP1/Integrated Management 3 - Manager Configuration Guide*.

#5: Intelligent Integrated Management Database log is not subject to data collection tool. For more information about Intelligent Integrated Management Database log, see *1.3.2(1) Checking the log output by Intelligent Integrated Management Database*. If you are using Intelligent Integrated Management Database and matches the following cases, collect them manually separately:

- When an error message related to Intelligent Integrated Management Database is output and the action taken by the operator for that message is described to log Intelligent Integrated Management Database
- When storing or retrieving trend data for Intelligent Integrated Management Database issues an error message that begins with "KAJY6200" and the problem cannot be resolved by the corrective action for that message

Collect the log file of Intelligent Integrated Management Database immediately after collecting other materials with the data collection tool. (The log will wrap when only one week is left until the log file is collected.)

Note that Intelligent Integrated Management Database log files are included in the backup target of Intelligent Integrated Management Database, so if there is enough disk space, you can make a backup and collect it. For the backup procedure, see *1.2.2(7) Backup and recovery procedure of Intelligent Integrated Management Database*.

#6 -ri and -rs option-attached execution results can be retrieved only when the database is running.

(c) 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

(d) Error information on the screen

Collect a hard copy of the following:

- Error dialog box

(e) 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 [12.4.1\(2\)\(f\) Collecting RAS information](#).

(f) IM management node-related files

If the Intelligent Integrated Management Base is used, collect the following information:

- Files under the directory specified by the `-o` option of the `jddcreatetree` command
- Files under the directory specified by the `-i` option of the `jddupdatetree` command

12.3.2 Data about JP1/IM - Agent

Collect the following documents manually:

- System log
- OS info
- Communication status
- Process information
- Configuration of silence
- Product information
- Configuration of Automatic Start and Stop
- Container information
- File list
- Installation documentation
- Secret key

The following explains how to collect each document.

(1) For Windows

See [12.4.2\(1\)\(a\) Integrated agent host](#), [12.4.2\(1\)\(b\) Integrated agent host on Cluster System](#), and [12.4.2\(1\)\(c\) Integrated agent host in Containers](#).

(2) For UNIX

See [12.4.2\(2\)\(a\) Integrated agent host](#), [12.4.2\(2\)\(b\) Integrated agent host on Cluster System](#), and [12.4.2\(2\)\(c\) Integrated agent host in Containers](#).

12.4 Collecting data

This section explains how to collect data when a problem occurs.

12.4.1 How to collect JP1/IM - Manager data

(1) In Windows

(a) 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.

■ JP1/IM - Manager

For details about JP1/IM - Manager processes, see *Appendix B.1 (1) JP1/IM - Manager* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

■ JP1/IM - View

For details about JP1/IM - View processes, see *Appendix B.1 (1) JP1/IM - Manager* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

■ 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 12–19: JP1/IM - IM Configuration Management - View processes

Parent process name	Function	Child process name	Function
jcfview.exe (3)	Controls the JP1/IM - IM Configuration Management - View window.	jcfview_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.

(b) Outputting a thread dump for JP1/IM

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

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

(c) 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.

Important

- If you are using Microsoft(R) Office Outlook(R), the following message box may appear when using the data collection tool.

The program is trying to access an email address stored within Outlook. Would you like to proceed? This is caused by the behavior of the machine configuration information collection program (MSINFO32), which is running within the data collection tool. Because email addresses are not collected by the data collection tool, press **No** button in the message box. Note that there are no problems with data collection for JP1/IM - Manager and the operation of Microsoft(R) Outlook(R).

- Do not run multiple instances of the data collection tool.
- Depending on the environment where the data collection tool is executed, it may take a while to collect data.
- When you collect JP1/IM - Manager data, some information is obtained by executing JP1/Base and JP1/IM - Manager commands. Some of these commands cannot be executed simultaneously with the same command, or with a different command. Avoid executing JP1/Base and JP1/IM - Manager commands when collecting data.
- If there are no operation records, at the time of data collection execution, "KAVB4153-E Failed to open Action Information File (action-information-file-name). : system-error-message" is output to the event log and the integrated trace log. This is output because the action information file did not exist when the data collection tool was executed. However, because the action information file is generated by operations, even if this message is output, no problems will occur with data collection if there are no operation records. Note that even if you specify a logical host, the data of the physical host is collected. Therefore, even if this message is output, there will be no problems with data collection if there are no operation records on the physical host.
- If there is a Windows event in the Windows event log in which the message format provided by the event log-issuing product and the number of padded characters do not match, an application error might occur during execution of the data collection tool. This is not a problem because the data is collected even in such cases.

When this problem occurs, a dialog box is displayed, and execution of the data collection tool might stop (the tool restarts when you respond to the dialog box). If you want to disable the display of the dialog box, execute the following procedure:

1. Click the **Start** menu and enter `gpedit.msc` in **Search programs and files** or **Run**.
 2. The Local Group Policy Editor appears. Select **Local Computer Policy**, **Computer Configuration**, **Administrative Templates**, **Windows Components**, and then **Windows Error Reporting** in the tree on the left-hand side.
 3. In **Setting** on the right-hand side, select **Effective** in **Prevent display of the user interface for critical errors**, and click the **OK** button.
- If you execute the data collection tool, the system information on the machine may not have been collected when execution of the data collection tool is completed. This is because the process that internally collects the OS information has not been completed, even though execution of the data collection tool has been completed.

After ensuring that execution of `msinfo32.exe` has been completed from the **Processes** tab or the **Details** tab, by starting the Task Manager, perform operations such as compressing the collected data by using a compression tool, or moving or deleting the collected data.

(d) 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)

(e) 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.

(f) 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.

(g) 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 *8.6.2 Collectable log information and connection methods for remote monitoring* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

The following describes how to collect information when the OS on the manager host is Windows.

Table 12–20: 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 (Windows)	<i>Table 12-21 Collecting data on the Windows manager host (for WMI connection)</i>
	Monitored host (Windows)	<i>Table 12-22 Collecting data on the Windows monitored host (for WMI connection)</i>
NetBIOS connection	Manager host (Windows)	<i>Table 12-23 Collecting data on the Windows manager host (for NetBIOS connection)</i>
	Monitored host (Windows)	<i>Table 12-24 Collecting data on the Windows monitored host (for NetBIOS connection)</i>
SSH connection	Manager host (Windows)	<i>Table 12-25 Collecting data on the Windows manager host (for SSH connection)</i>
	Monitored host (UNIX)	<i>Table 12-28 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 *8.6.2 Collectable log information and connection methods for remote monitoring* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

When collecting container information, in addition to the information to be collected on the monitored host as described in *8.6.2 Collectable log information and connection methods for remote monitoring* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*, also collect the following information:

For Podman:

- Result of running the `podman ps` command

For Docker:

- Result of running the `docker ps` command

■ For WMI connection

The following table describes how to collect data on the manager host (Windows) if a problem occurs in WMI connection.

Table 12–21: 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 monitored-host-name</code> • <code>netsh advfirewall firewall show rule name=all</code> • <code>netsh advfirewall show allprofiles</code> • <code>tasklist monitored-host-name</code> • <code>systeminfo</code> • <code>wmic qfe</code> • <code>reg export HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\ CurrentVersion\Policies\System output-file</code> • <code>reg export HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Ole output-file</code> • <code>reg export HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\System output-file</code> • <code>wmic /node:"monitored-host-name" /user:user-name /password:password port (user-specified WMI command)</code>

No.	Procedure
	<ul style="list-style-type: none"> Commands to be executed on the manager host: date /t time /t Command to be executed on the monitored host connected via WMI: wmic /node:"<i>monitored-host-name</i>" /user:<i>user-name</i> /password:<i>password</i> path Win32_LocalTime
2	Collect the authentication information for WMI connection. <ul style="list-style-type: none"> For physical hosts: <i>Manager-path</i>\conf\agtless\targets\wmi.ini For logical hosts: <i>shared-folder</i>\JP1IMM\conf\agtless\targets\wmi.ini
3	Collect the WMI connection log. <ul style="list-style-type: none"> Log file under the directory specified in HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\CIMOM\Logging Directory#
4	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. 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.
5	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> .
6	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.
7	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: <ul style="list-style-type: none"> Select * From Win32_NTLogEvent Where (Logfile='System' Or Logfile='Application') After the query is performed, obtain a screenshot of the query results indicated in the Query Result widow.

#: 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 12–22: Collecting data on the Windows monitored host (for WMI 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 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>

No.	Procedure
	<ul style="list-style-type: none"> 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	Collect the WMI connection log. <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	Collect the data indicating that the event log is correctly created on the monitored host. <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.

■ For NetBIOS connection

The following table describes how to collect data on the manager host (Windows) if a problem occurs in NetBIOS connection.

Table 12–23: Collecting data on the Windows manager host (for NetBIOS connection)

No.	Procedure
1	From the command prompt, execute the following commands, and then collect the results: <ul style="list-style-type: none"> whoami nslookup <i>monitored-host-name</i> 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 \\ <i>remotely-monitored-host-name</i> 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 12–24: Collecting data on the Windows monitored host (for NetBIOS 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 • 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	<p>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.</p>
3	<p>Collect the monitored file.</p>

#: 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.

■ For SSH connection

The following table describes how to collect data on the manager host (Windows) if a problem occurs in SSH connection.

Table 12–25: 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"> • whoami • nslookup <i>monitored-host-name</i> • netsh advfirewall firewall show rule name=all • netsh advfirewall show allprofiles • systeminfo • wmic qfe • Commands to be executed on the manager host: date /t time /t • Commands to be executed on the monitored host connected via SSH: date • dir /A <i>directory-containing-the-private-key</i>
2	<p>Collect the authentication information for SSH connection.</p> <ul style="list-style-type: none"> • For physical hosts:

No.	Procedure
	<p><i>Manager-path</i>\conf\agtless\targets\ssh.ini</p> <ul style="list-style-type: none"> For logical hosts: <i>shared-folder</i>\JP1IMM\conf\agtless\targets\ssh.ini
3	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.

For details about how to collect data on a monitored host (UNIX) if a problem occurs in SSH connection, see [Table 12-28 Collecting data on the UNIX monitored host \(for SSH connection\)](#).

(2) In UNIX

(a) 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.

■ JP1/IM - Manager

For details about JP1/IM - Manager processes, see [Appendix B.2 \(1\) JP1/IM - Manager](#) in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

(b) Outputting a dump file for JP1/IM

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

(c) 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.

(d) 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)

(e) 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.

(f) 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 8.6.2 *Collectable log information and connection methods for remote monitoring* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

The following describes how to collect information when the OS on the manager host is UNIX.

Table 12–26: 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 12-27 Collecting data on the UNIX manager host (for SSH connection)</i>
	Monitored host (UNIX)	<i>Table 12-28 Collecting data on the UNIX monitored host (for SSH connection)</i>

■ For SSH connection

The following table describes how to collect data on the manager host (UNIX) if a problem occurs in SSH connection.

Table 12–27: 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>

No.	Procedure
	<ul style="list-style-type: none"> • Command to be executed on the monitored host connected via SSH: Date • <code>ls -al <i>directory-containing-the-private-key</i></code>
2	Collect the authentication information for SSH connection. <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	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.

The following table describes how to collect data on the monitored host (UNIX) if a problem occurs in SSH connection.

Table 12–28: Collecting data on the UNIX monitored host (for SSH connection)

No.	Procedure
1	Log in to the monitored host as the monitored user, execute the following commands from the console, and then collect the results: <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 Linux: <code>dmesg</code> <code>rpm -qa</code>
2	Collect the following files: <ul style="list-style-type: none"> • <code>/etc/hosts.allow</code> • <code>/etc/hosts.deny</code> • Monitored file • In Linux: <code>/etc/nsswitch.conf</code> <code>/etc/issue</code> <code>/etc/ssh/sshd_config</code> <code>/var/log/messages</code> <code>/var/log/secure</code>

12.4.2 How to collect JP1/IM - Agent data

(1) For Windows

(a) Integrated agent host

1. Log in to integrated agent host.
2. Execute the command to collect the generated file.

- Secret key

```
jimasecret -list > secretkeys.txt
```

- System log

```
wevtutil el 2> nul 1> event_list.txt
for /f "delims=" %i in ( event_list.txt ) do echo %i 2> nul 1>> event_info
.txt& wevtutil gli "%i" 2> nul 1>> event_info.txt& echo ----- 2> nul 1>> e
vent_info.txt
wevtutil qe System /rd:true /f:text 2> nul 1> System.txt
wevtutil qe Application /rd:true /f:text 2> nul 1> Application.txt
wevtutil qe Security /rd:true /f:text 2> nul 1> Security.txt
for /f "delims=" %i in ( event_list.txt ) do echo %i 2> nul 1>> event_c
onfig_info.txt& wevtutil gl "%i" 2> nul 1>> event_config_info.txt& echo
----- 2> nul 1>> event_config_info.txt
```

- OS info

```
hostname 1> hostname.txt 2>nul
"%CommonProgramFiles%\Microsoft Shared\MSInfo\msinfo32" /report os_system.
txt /categories SystemSummary 2>nul 1>nul
set > getenv.log
```

- Communication status

```
echo --Command netsh interface ip show address -- 1>> netstat.txt 2>nul
netsh interface ip show address 1>> netstat.txt 2>nul
echo --Command netsh interface ipv6 show address -- 1>> netstat.txt 2>nul
netsh interface ipv6 show address 1>> netstat.txt 2>nul
echo -- netsh advfirewall show currentprofile -- 1> firewall.txt 2>nul
netsh advfirewall show currentprofile 1>> firewall.txt 2>nul
echo -- netsh advfirewall firewall show rule -- 1>> firewall.txt 2>nul
netsh advfirewall firewall show rule name=all verbose 1>> firewall.txt 2>n
ul
```

- Process information

```
tasklist /svc > proc_svc.list 2>&1
tasklist /v > proc_v.list 2>&1
```

- Service information

```
sc query > service.list 2>&1
```

- Configuration of silence

With Alertmanager services running, collect silence settings by executing API for acquire Alertmanager's silence list. For details about API, see 5.21.3 *Get silence list of Alertmanager* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

If you use curl command of OSS, collect the generated file by executing as shown below.

```
curl --request GET http://localhost:Alertmanager-port-number /api/v2/silences -o silence.txt
```

If silence setting contains sensitive information such as passwords, delete the corresponding definition from the definition file after collection.

- File list

```
dir /S JP1/IM-Agent-installation-folder 1>jplima_list.txt 2>nul
```

3. Manually collect the necessary files.

Manually collect the files listed in the following table.

Data to be collected	Collection object
OS info	<ul style="list-style-type: none"> • %systemroot%\system32\drivers\etc\hosts • %systemroot%\system32\drivers\etc\services
Installation documentation	<ul style="list-style-type: none"> • When installed with the provided media Files under <i>system-drive</i>\Windows\Temp\HCDINST\ • When installed with a JP1/IM - Agent package downloaded from the Integrated Operations Viewer Log files (MSI* .LOG) that was output when installing under %TEMP%#\ #: %TEMP% indicates the path specified in the environment-variable TEMP.
Product information	<p>■Files to be collected in the troubleshooting information described in <i>Appendix A.4(3) Integrated agent host (Windows)</i> in the <i>JP1/Integrated Management 3 - Manager Overview and System Design Guide</i>.</p> <p>Except for the following files:</p> <ul style="list-style-type: none"> • Files under the <i>shared folder for the logical host</i> • Files under /usr/lib/systemd/system/ <p>■If you deployed the OracleDB exporter, manually extract the following files:</p> <ul style="list-style-type: none"> • OracleDB exporter location\oracledb_exporter_windows\jplima\logs folder • Service definition file of OracleDB exporter <p>■If you have already set up the SAP system log extract command, collect the following files manually:</p> <ul style="list-style-type: none"> • Environment parameter configuration file (<i>any name.ini</i>) • Log files of SAP system log extract commands • Trace files for SAP system log extract commands • The following files-stored in the path set in WORKDIR of configuration file environment parameter <ul style="list-style-type: none"> - Log file of SAP system log extract command (<i>any name</i>) - SAP system log extract command trace file (<i>command name.log, command name.dat</i>) - Trace file (<i>dev_rfc*</i>) output by RFC library <p>If the directory where the above files are stored is changed in the environment parameter configuration file or the argument when the SAP system log extract command is executed, the changed directory must also be collected.</p>

(b) Integrated agent host on Cluster System

1. Log in to the integrated agent host of active server.
2. Collect the files generated in executing commands.

- Secret key

```
jimasecret -list -l shared-folder > secretkeys.txt
```

- Configuration of silence

With Alertmanager services running, collect silence settings by executing API for acquire Alertmanager's silence list. For details about API, see 5.21.3 *Get silence list of Alertmanager* in the *JPI/Integrated Management 3 - Manager Command, Definition File and API Reference*.

If you use curl command of OSS, collect the generated file by executing as shown below.

```
curl --request GET http://logical-host-name:logical-host-Alertmanager-port-number/api/v2/silences -o scilence_logical-host-name.txt
```

If Alertmanager is running on a physical host in the active system, execute the following procedure to collect the generated files.:

```
curl --request GET http://localhost:physical-host-Alertmanager-port-number/api/v2/silences -o scilence.txt
```

If silence setting contains sensitive information such as passwords, delete the corresponding definition from the definition file after collection.

- File list

```
dir /S JPI/IM-Agent-install-destination-directory 1>jplima_list.txt 2>nul
dir /S shared-directory 1>jplima_list_logical-host-name.txt 2>nul
```

- System log, OS info, Communication status, Processing information, and Service information

See *System log*, *OS info*, *Communication status*, *Process information*, and *Service information* in step 2 of 12.4.2 (1)(a) *Integrated agent host*.

3. Manually collect the necessary files.

Manually collect the files listed in the following table.

Data to be collected	Objects to be Collected
OS info	See <i>OS info</i> and <i>Installation documentation</i> in step 3 of 12.4.2(1)(a) <i>Integrated agent host</i> .
Installation documentation	
Product information	<p>■Files to be collected in the troubleshooting information described in <i>Appendix A.4(3) Integrated agent host (Windows)</i> in the <i>JPI/Integrated Management 3 - Manager Overview and System Design Guide</i>.</p> <p>Except for the following files:</p> <ul style="list-style-type: none"> • Files under <code>/usr/lib/systemd/system/</code> <p>■If you have already set up the SAP system log extract command, collect the following files manually:</p> <ul style="list-style-type: none"> • Environment-parameter configuration file (<i>any name.ini</i>) • RFC library allocated when the SAP system log extract command was built • CRT library allocated when the SAP system log extract command was built • The following files-stored in the path set in WORKDIR of configuration file environment parameter

Data to be collected	Objects to be Collected
	<ul style="list-style-type: none"> - Log file of SAP system log extract command (<i>any name</i>) - SAP system log extract command trace file (<i>command name.log, command name.dat</i>) - Trace file (<i>dev_rfc*</i>) output by RFC library <p>If the directory where the above files are stored is changed in the environment parameter configuration file or the argument when the SAP system log extract command is executed, the changed directory must also be collected.</p>

4. Log in to integrated agent host of the standby system.

5. collect the files generated by executing commands.

- Configuration of silence

With Alertmanager services running, collect silence settings by executing API for acquire Alertmanager's silence list. For details about API, see 5.21.3 *Get silence list of Alertmanager* in the *JPI/Integrated Management 3 - Manager Command, Definition File and API Reference*.

If Alertmanager is running on a physical host in the standby system, execute the following procedure when using curl command of OSS to collect the generated filename:

```
curl --request GET http://localhost:physical-host-Alertmanager-port-number/api/v2/silences -o scilence.txt
```

If silence setting contains sensitive information such as passwords, delete the corresponding definition from the definition file after collection.

- System log, OS info, communication status, process information, service information, file list

See *System log, OS info, Communication status, Process information, Service information, and File list* in step 2 of 12.4.2(1)(a) *Integrated agent host*.

6. Manually collect the necessary files.

Manually collect the files listed in the following table.

Data to be collected	Objects to be Collected
OS info	See <i>OS info</i> and <i>Installation documentation</i> in step 3 of 12.4.2(1)(a) <i>Integrated agent host</i> .
Installation documentation	
Product information	<p>■Files to be collected in the troubleshooting information described in <i>Appendix A.4(3) Integrated agent host (Windows)</i> in the <i>JPI/Integrated Management 3 - Manager Overview and System Design Guide</i>.</p> <p>Except for the following files:</p> <ul style="list-style-type: none"> • Files under <code>/usr/lib/systemd/system/</code> <p>■If you have already set up the SAP system log extract command, collect the following files manually:</p> <ul style="list-style-type: none"> • Environment-parameter configuration file (<i>any name.ini</i>) • RFC library allocated when the SAP system log extract command was built • CRT library allocated when the SAP system log extract command was built • The following files-stored in the path set in WORKDIR of configuration file environment parameter <ul style="list-style-type: none"> - Log file of SAP system log extract command (<i>any name</i>) - SAP system log extract command trace file (<i>command name.log, command name.dat</i>) - Trace file (<i>dev_rfc*</i>) output by RFC library <p>If the directory where the above files are stored is changed in the environment parameter configuration file or the argument when the SAP system log extract command is executed, the changed directory must also be collected.</p>

(c) Integrated agent host in Containers

Same as [12.4.2\(1\)\(a\) Integrated agent host](#).

(d) Integration Manager Host

Collect the data related to JPI/IM agent management base (imbase, imbaseproxy) with the data collection tool (jim_log.bat).

For the file to be collected, see the file folder list in [Appendix A.4 \(1\) Integrated Manager host \(Windows\)](#) in the [JPI/Integrated Management 3 - Manager Overview and System Design Guide](#).

(e) Integration Manager Host on Cluster Systems

Same as [12.4.2\(1\)\(d\) Integration Manager Host](#).

(f) Monitored AIX hosts (When Node exporter for AIX is deployed)

1. Log in to the monitored AIX host.
2. Execute the command to collect the generated file.

- OS information

```
echo "-- lslpp -l -a --" > os_inst_pp.list 2> /dev/null
lslpp -l -a >> os_inst_pp.list 2> /dev/null
echo "-- /usr/sbin/instfix -a -icv --" >> os_inst_pp.list 2> /dev/null
/usr/sbin/instfix -a -icv >> os_inst_pp.list 2> /dev/null
lsattr -E -l sys0 > kernel_param.list 2> /dev/null
hostname >> hostname.txt 2> /dev/null
echo "-- uname --" > os_system.txt 2> /dev/null
uname -a >> os_system.txt 2> /dev/null
echo "-- date --" >> os_system.txt 2>&1
date >> os_system.txt 2>&1
env > getenv.log 2> /dev/null
```

- Communication status

```
echo "--Command netstat -an --" > netstat.txt 2> /dev/null
netstat -an >> netstat.txt 2> /dev/null
echo "--Command netstat -rn --" >> netstat.txt 2> /dev/null
netstat -rn >> netstat.txt 2> /dev/null
echo "--Command ifconfig -a --" >> netstat.txt 2> /dev/null
ifconfig -a >> netstat.txt 2> /dev/null
echo "-- lsfilt --" >> firewall.txt 2>&1
lsfilt >> firewall.txt 2>&1
```

- Process information

```
ps -elfa > proc.list 2> /dev/null
```

- Autostart settings

```
lsitab -a > lsitab.txt 2> /dev/null
```

- File list

```
ls -lR Node exporter for AIX location #/jplima > jplima_list.txt 2>&1
```

In the case of logical host operation, the shared folder of the logical host is located.

3. Manually collect the necessary files.

Manually collect the files listed in the following table.

Materials to be collected	Target of collection
System log	<code>/var/adm/syslog/syslog.log#</code> # The destination of the system log is obtained by referring to the <code>"/etc/syslog.conf"</code> setting.
OS information	<ul style="list-style-type: none">• <code>/etc/hosts</code>• <code>/etc/services</code>
Automatic stop setting	<code>/etc/rc.shutdown</code>

(2) For UNIX

(a) Integrated agent host

1. Log in to integrated agent host.
2. Collect the files generated by executing commands.

- Secret key

```
jimasecret -list > secretkeys.txt
```

- OS info

```
/bin/rpm -qa > os_inst_pp.list 2> /dev/null  
/sbin/sysctl -a > kernel_param.list 2> /dev/null  
hostname >> hostname.txt 2> /dev/null  
echo "-- uname --" > os_system.txt 2> /dev/null  
uname -a >> os_system.txt 2> /dev/null  
echo "-- ls -l /boot --" >> os_system.txt 2> /dev/null  
ls -l /boot >> os_system.txt 2> /dev/null  
echo "-- cat /etc/os-release --" >> os_system.txt 2> /dev/null  
cat /etc/os-release >> os_system.txt 2> /dev/null  
echo "-- timedatectl --" >> os_system.txt 2>&1  
timedatectl >> os_system.txt 2>&1  
env > getenv.log 2> /dev/null
```

- Communication status

```
echo "--Command ss -a --" > netstat.txt 2> /dev/null  
ss -a >> netstat.txt 2> /dev/null  
echo "--Command ip route --" >> netstat.txt 2> /dev/null  
ip route >> netstat.txt 2> /dev/null  
echo "--Command ip addr --" >> netstat.txt 2> /dev/null  
ip addr >> netstat.txt 2> /dev/null  
echo "-- iptables -v -n -L --line-numbers --" >> firewall.txt 2>&1  
iptables -v -n -L --line-numbers >> firewall.txt 2>&1  
echo "-- firewall-cmd --list-all-zones --" >> firewall.txt 2>&1  
firewall-cmd --list-all-zones >> firewall.txt 2>&1
```

- Process information

```
ps -elfa > proc.list 2> /dev/null
```

- Service information

```
systemctl list-unit-files -t service > service.list 2> /dev/null
```

- Configuration of silence

See *Configuration of silence* in step 2 of *12.4.2(1)(a) Integrated agent host*.

- Settings of start and stop

For each unit definition file in JP1/IM - Agent, run the following command:

```
systemctl is-enabled unit-definition-file-name > unit-definition file-name.txt 2> /dev/null
```

- Container information

- For Docker

```
docker version > ./Docker_Verison 2>&1
docker ps -a --no-trunc > ./Docker_Process_Container_List 2>&1
docker_container_list=`docker ps -a --no-trunc -q`;for loop in $docker_container_list;do echo $loop >> Docker_Top 2>&1;docker top $loop >> Docker_Top 2>&1;echo $loop >> Docker_Inspect 2>&1;docker inspect $loop >> Docker_Inspect 2>&1;done
/bin/cat /etc/docker/daemon.json > docker_daemon.json 2>&1
/bin/cat /etc/sysconfig/docker > sysconfig_docker 2>&1
```

- For Podman

```
podman version > Podman_Verison 2>&1
podman ps --all --no-trunc --format={{.ID}} > Podman_Process_Container_List 2>&1
podman_container_list=`podman ps --all --no-trunc --format={{.ID}}`;for loop in $podman_container_list;do echo $loop >> Podman_Top 2>&1;podman top $loop hpid args >> Podman_Top 2>&1;echo $loop >> Podman_Inspect 2>&1;podman inspect $loop >> Podman_Inspect 2>&1;done
```

- File list

```
ls -lR /opt/jplima > jplima_list.txt 2>&1
ls -l /usr/lib/systemd/system/jpc* > systemd_jpc_list.txt 2>&1
getfacl -R /opt/jplima > jplima_acl_list.txt 2>&1
getfacl /usr/lib/systemd/system/jpc* > systemd_jpc_acl_list.txt 2>&1
```

3. Manually collect the necessary files.

Manually collect the files listed in the following table.

Data to be collected	Objects to be collected
System log	/var/log/messages*
OS info	<ul style="list-style-type: none"> • /etc/hosts • /etc/services
Installation documentation	<ul style="list-style-type: none"> • /etc/.hitachi/pplistd/pplistd

Data to be collected	Objects to be collected
	<ul style="list-style-type: none"> • /etc/.hitachi/.install.log* • /etc/.hitachi/.uninstall.log* • Files under /tmp/HITACHI_JP1_INST_LOG
Product information	<p>■Files to be collected in the troubleshooting information described in <i>Appendix A.4(4) Integrated agent host (Linux)</i> in the <i>JP1/Integrated Management 3 - Manager Overview and System Design Guide</i>.</p> <p>Except for the following files:</p> <ul style="list-style-type: none"> • Files under the <i>shared directory for the logical host</i> • Files for logical hosts under /usr/lib/systemd/system/ <p>■If you have placed OracleDB exporter, collect the following files manually:</p> <ul style="list-style-type: none"> • OracleDB exporter location/oracledb_exporter_linux/jplima/logs directory • Unit definition file <p>■If you have already set up the SAP system log extract command, collect the following files manually:</p> <ul style="list-style-type: none"> • Environment parameter configuration file (<i>any name.ini</i>) • RFC library allocated when the SAP system log extract command was built • CRT library allocated when the SAP system log extract command was built • The following files-stored in the path set in WORKDIR of configuration file environment parameter <ul style="list-style-type: none"> - Log file of SAP system log extract command (<i>any name</i>) - SAP system log extract command trace file (<i>command name.log, command name.dat</i>) - Trace file (<i>dev_rfc*</i>) output by RFC library <p>If the directory where the above files are stored is changed in the environment parameter configuration file or the argument when the SAP system log extract command is executed, the changed directory must also be collected.</p>

(b) Integrated agent host on Cluster System

1. Log in to the integrated agent host of active system.
2. Collect the files generated by executing commands.
 - Secret key

```
jimasecret -list -l shared-Directory > secretkeys.txt
```

- Configuration of silence

See *Configuration of silence* in step 2 of *12.4.2(1)(b)Integrated agent host on Cluster System*.

- File list

```
ls -lR /opt/jplima > jplima_list.txt 2>&1
ls -l /usr/lib/systemd/system/jpc* > systemd_jpc_list.txt 2>&1
ls -lR shared-directory > jplima_list_logical-host-name.txt 2>&1
getfacl -R /opt/jplima > jplima_acl_list.txt 2>&1
getfacl /usr/lib/systemd/system/jpc* > systemd_jpc_acl_list.txt 2>&1
getfacl -R shared-directory > jplima_acl_list_logical-host-name.txt 2>&1
```

- OS, Communication status, Process information, Service information, Settings of start and stop, and Container information
- See *OS info, Communication status, Process information, Service information, Settings of start and stop, and Container information* in step 2 of *12.4.2(2)(a)Integrated agent host*.

3. Manually collect the necessary files.

Manually collect the files listed in the following table.

Data to be collected	Objects to be collected
System log	See <i>System log</i> , <i>OS info</i> , and <i>Installation documentation</i> in step 3 of 12.4.2(2)(a) <i>Integrated agent host</i> .
OS info	
Installation documentation	
Product information	<p>■Files to be collected in the troubleshooting information described in <i>Appendix A.4(4) Integrated agent host (Linux)</i> in the <i>JP1/Integrated Management 3 - Manager Overview and System Design Guide</i>.</p> <p>■If you have already set up the SAP system log extract command, collect the following files manually:</p> <ul style="list-style-type: none"> • Environment parameter configuration file (<i>any name.ini</i>) • RFC library allocated when the SAP system log extract command was built • CRT library allocated when the SAP system log extract command was built • The following files-stored in the path set in WORKDIR of configuration file environment parameter <ul style="list-style-type: none"> - Log file of SAP system log extract command (<i>any name</i>) - SAP system log extract command trace file (<i>command name.log, command name.dat</i>) - Trace file (<i>dev_rfc*</i>) output by RFC library <p>If the directory where the above files are stored is changed in the environment parameter configuration file or the argument when the SAP system log extract command is executed, the changed directory must also be collected.</p>

4. Log in to integrated agent host of the standby system.

5. Collect the files generated by executing commands.

- Configuration of silence

See *Configuration of silence* in step 4 of 12.4.2(1)(b)*Integrated agent host on Cluster System*.

- OS info, Communication status, Process information, Service information, Settings of start and stop, Container information, File list

See *OS info*, *Communication status*, *Process information*, *Service information*, *Settings of start and stop*, *Container information*, and *File list* in step 2 of 12.4.2(1)(a)*Integrated agent host*.

6. Manually collect the necessary files.

Manually collect the files listed in the following table.

Data to be collected	Collection object
System log	See <i>System log</i> , <i>OS info</i> , and <i>Installation documentation</i> in step 3 of 12.4.2(2)(a) <i>Integrated agent host</i> .
OS info	
Installation documentation	
Product information	<p>■Files to be collected in the troubleshooting information described in <i>Appendix A.4(4) Integrated agent host (Linux)</i>" in the <i>JP1/Integrated Management 3 - Manager Overview and System Design Guide</i>.</p> <p>Except for the following files:</p> <ul style="list-style-type: none"> • Files under the <i>shared directory for the logical host</i> <p>■If you have already set up the SAP system log extract command, collect the following files manually:</p> <ul style="list-style-type: none"> • Environment parameter configuration file (<i>any name.ini</i>)

Data to be collected	Collection object
	<ul style="list-style-type: none"> • RFC library allocated when the SAP system log extract command was built • CRT library allocated when the SAP system log extract command was built • The following files-stored in the path set in WORKDIR of configuration file environment parameter <ul style="list-style-type: none"> - Log file of SAP system log extract command (<i>any name</i>) - SAP system log extract command trace file (<i>command name.log, command name.dat</i>) - Trace file (<i>dev_rfc*</i>) output by RFC library <p>If the directory where the above files are stored is changed in the environment parameter configuration file or the argument when the SAP system log extract command is executed, the changed directory must also be collected.</p>

(c) Integrated agent host in Containers

Same as [12.4.2\(2\)\(a\) Integrated agent host](#).

(d) Integrated Manager Host

Collect the data related to JP1/IM agent management base (imbase, imbaseproxy) with the data collection tool (jim_log.sh).

For the file to be collected, see the file and directory list in [Appendix A.4 \(2\) Integrated Manager host \(Linux\)](#) in the [JP1/Integrated Management 3 - Manager Overview and System Design Guide](#).

(e) Integrated Manager Host on Cluster Systems

Same as [12.4.2\(2\)\(d\) Integrated Manager Host](#).

(f) Monitored AIX hosts (When Node exporter for AIX is deployed)

Same as [12.4.2\(1\)\(f\) Monitored AIX hosts \(When Node exporter for AIX is deployed\)](#).

12.5 Troubleshooting

12.5.1 How to isolate faults

The following table lists the reasons and corrective actions for messages that are output to add-on program logs. For details about the log storage locations, see *12.2.2 JP1/IM - Agent log information*. Node exporter for AIX log is output to the system log.

(1) Prometheus server log

Message	Cause	Actions to be taken
msg="Error on ingesting samples that are too old or are too far into the future"	You have changed the system time in the past.	Wait until the time before the change.
msg="Append failed" err="out of bounds"		
msg="Appending scrape report failed" err="out of bounds"		
component=remote msg="Failed to send batch, retrying"	The JP1/IM - Manager host was unable to send performance information from Prometheus due to high load.	Check the load status of the JP1/IM - Manager host.
	The connection to the JP1/IM - Manager host was not established or was in an unstable situation.	Check the connection status with the JP1/IM - Manager host.
	The JP1/IM - Manager service was not started.	Check the startup status of the JP1/IM - Manager service.
	The JP1/IM - Manager service returned an HTTP response that indicates an error.	Check to see if there are any errors on the JP1/IM - Manager service side.
	The remote light destination specified in the Prometheus configuration file (jpc_prometheus_server.yml) was incorrect.	Review the contents of the Jpc_prometheus_server.yml configuration file (jpc_prometheus_server.yml).
msg="Skipping resharding, last successful send was beyond threshold"	Because the threshold was reached when prometheus failed to send performance information due to the load situation of the JP1/IM - Manager host, the connection status, etc., the load balancing was omitted again.	Check the load status and connection status of the JP1/IM - Manager host.
msg="Error sending alert"	Alertmanager had stopped.	Start Alertmanager.
	Alertmanager returned an HTTP response that indicates an error.	Check to see if there are any errors on the Alertmanager side.
	The alert notification destination specified in the Prometheus configuration file (jpc_prometheus_server.yml) was incorrect.	Review the specifications in the Prometheus configuration file (jpc_prometheus_server.yml).
msg="Scrape failed"	The scrape failed because the exporter is hesitation.	Launch Exporter.

Message	Cause	Actions to be taken
	Scrape failed because you specified a host name that does not exist in the discovery configuration file (file_sd_config_*.yaml).	Review the specified contents of the discovery configuration file (file_sd_config_*.yaml).
	An HTTP response indicating an error was returned from the scrape destination.	Check if there are any errors at the scrape destination.
msg="Unable to start web listener"	An invalid host name was specified on the command line Optional--web.listen-address.	Specify the correct host name.
	On the command line --web.listen-address Optional you specified a port that is already in use.	Specify a port that is not in use.
msg="Error loading config (--config.file=jpc_prometheus_server.yaml) " msg="Error reading file"	An invalid value was specified in the item that specifies the period of rometheus configuration file (jpc_prometheus_server.yaml).	Check the invalid line number or item name displayed in err and review the specified contents of the Prometheus configuration file (jpc_prometheus_server.yaml).
	The format of the Prometheus configuration file (jpc_prometheus_server.yaml) was not followed.	
	The format of the Prometheus configuration file (jpc_prometheus_server.yaml) was not followed.	

(2) Alertmanager log

Message	Cause	Action to be taken
<ul style="list-style-type: none"> msg="Notify for alerts failed" msg="Notify attempt failed, will retry later" 	Alerts could not be sent from AlertManager due to high on load of the JP1/IM - Manager host.	Check the on-load status of the JP1/IM - Manager host.
	The Connection with the JP1/IM - Manager host was not established or was unstable.	Check the status of the Connection with the JP1/IM - Manager host.
	JP1/IM - Manager service was not running.	Check the startup status of the JP1/IM - Manager's service.
	JP1/IM - Manager service returned an HTTP response indicating an error.	Check if there are any errors on the service side of the JP1/IM - Manager.
	The alert destination specified in the Alertmanager configuration file (alertmanager.yaml) was incorrect.	Review the specifications in the Alertmanager configuration file (alertmanager.yaml).
msg="Loading configuration file failed"	The specified contents of the Alertmanager configuration file (alertmanager.yaml) were invalid.	Check the contents described in err and review the specified contents of the Alertmanager configuration file (alertmanager.yaml).
msg="Listen error"	An invalid host name was specified on the command line Optional--web.listen-address.	Specify the correct host name.
	On the command line --web.listen-address Optional you specified a port that is already in use.	Specify a port that is not in use.

(3) blackbox_exporter log

In order for blackbox_exporter to collect the following logs, the log level must be set to "debug":

Message	Cause	Action to be taken
msg=" Unable to do unprivileged listen on socket, will attempt privileged " err=" socket: permission denied"	Occurs when the kernel parameter 'net.ipv4.ping_group_range' creates a socket without authority to create a ping socket. This also happens for privileged users (root).	This message can be safely ignored because ICMP sockets are created and continue with the authority of the privileged user (root) after the message is Output. It is also not recommended to Assistant to authority by setting the kernel parameter "net.ipv4.ping_group_range" only to suppress this message.
module=icmp msg="Timeout reading from socket"	The ICMP probe failed because the host to be monitored specified in the discovery configuration file (file_sd_config_blackbox_icmp.yml) of the Blackbox exporter (ICMP monitoring) is hesitation.	Review the specifications in the discovery configuration file (file_sd_config_blackbox_icmp.yml) of Blackbox exporter (ICMP monitoring).
module=icmp msg="Resolution with IP protocol failed"	The ICMP probe failed because a nonexistent host name was specified in the discovery configuration file (file_sd_config_blackbox_icmp.yml) of the Blackbox exporter (ICMP monitoring).	Review the specifications in the discovery configuration file (file_sd_config_blackbox_icmp.yml) of Blackbox exporter (ICMP monitoring).
module=http msg="Error for HTTP request"	<p>The monitored host specified in the discovery configuration file (file_sd_config_blackbox_http.yml) of Blackbox exporter (HTTP/HTTPS monitoring) was hesitation.</p> <p>The monitoring target service specified in the discovery configuration file (file_sd_config_blackbox_http.yml) of Blackbox exporter (HTTP/HTTPS monitoring) was hesitation.</p> <p>A Calipers that does not exist was specified in modules.module name .http.basic_auth.password_file) of the discovery configuration file (file_sd_config_blackbox_http.yml) of Blackbox exporter (HTTP/HTTPS monitoring).</p>	Review the specifications in the discovery configuration file (file_sd_config_blackbox_http.yml) of Blackbox exporter (HTTP/HTTPS monitoring).
module=http msg="Error resolving address"	A nonexistent host name was specified in the discovery configuration file (file_sd_config_blackbox_http.yml) of Blackbox exporter (HTTP/HTTPS monitoring).	Review the specifications in the discovery configuration file (file_sd_config_blackbox_http.yml) of Blackbox exporter (HTTP/HTTPS monitoring).
module=http msg="Failed to get decompressor for HTTP response body"	<p>The HTTP probe failed because the user name specified in modules.module name .http.basic_auth.username in the Blackbox exporter configuration file (blackbox_exporter.yml) is invalid.</p> <p>The HTTP probe failed because the Calipers word specified in modules.module name .http.basic_auth.password in the Blackbox exporter configuration file (blackbox_exporter.yml) is invalid.</p> <p>The HTTP probe failed because the modules.module name .http.basic_auth.bearer_token in the Blackbox exporter configuration file (blackbox_exporter.yml) is invalid.</p>	Review the specifications in the Blackbox exporter configuration file (blackbox_exporter.yml).

Message	Cause	Action to be taken
module=icmp msg="Error listening to socket"	An invalid IP address was specified in the modules.module name .icmp.source_ip_address of the Blackbox exporter configuration file (blackbox_exporter.yml).	Review the specifications in the Blackbox exporter configuration file (blackbox_exporter.yml).
module=http msg="Error generating HTTP client"	The HTTP probe failed because the Calipers specified in the modules.module name .http.tls_config.ca_file of the Blackbox exporter configuration file (blackbox_exporter.yml) does not exist.	Review the specifications in the Blackbox exporter configuration file (blackbox_exporter.yml).
	The HTTP probe failed because the Calipers specified in the modules.module name .http.tls_config.cert_file of the Blackbox exporter configuration file (blackbox_exporter.yml) does not exist.	
	The HTTP probe failed because the Calipers specified in the modules.module name .http.tls_config.key_file of the Blackbox exporter configuration file (blackbox_exporter.yml) does not exist.	
msg="Error loading config"	An invalid value was specified in the item that specifies the numerical value in the Blackbox exporter configuration file (blackbox_exporter.yml).	Check the incorrect line number or field name displayed in err and review the specifications in the Blackbox exporter configuration file (blackbox_exporter.yml).
	An invalid value was specified for the item that specifies the regular expression in the Blackbox exporter configuration file (blackbox_exporter.yml).	
	An invalid character string was specified in the item that specifies the value of the boolean type in the Blackbox exporter configuration file (blackbox_exporter.yml).	
module=icmp msg="Failed to set Control Message for retrieving TTL" err="not implemented on windows/amd64" (omission) module=icmp msg=" Cannot get TTL from the received packet. 'probe_icmp_reply_hop_limit' will be missing."	In a Windows environment, ICMP monitoring is performed by setting the discovery configuration file (file_sd_config_blackbox_icmp.yml) of Blackbox exporter (ICMP monitoring).	No action is required.

(4) node_exporter log

Message	Cause	Action to be taken
err="listen tcp: lookup <i>hostname</i> on <i>DNS</i> : no such host"	An invalid host name was specified on the command line Optional--web.listen-address.	Specify the correct host name.

Message	Cause	Action to be taken
err="listen tcp :port: bind: address already in use"	On the command line --web.listen-address Optional you specified a port that is already in use.	Specify a port that is not in use.
msg="Parsed flag --collector.filesystem.ption name" flag=[aaa panic: regexp: Compile(`[aaa`): error parsing regexp: missing closing]: `[aaa`"	An illegal regular expression was specified in the command line Optional.	Review the command line Optional.
msg="Parsed flag --collector.systemd.unit-include" flag=(panic: regexp: Compile(`^(?:()\$`): error parsing regexp: missing closing): `^(?:()\$`"	An invalid regular expression was specified in --collector.systemd.unit-include.	Review the specified regular expression.

(5) process_exporter logs

Message	Cause	Countermeasures
flag needs an argument: <i>command-line-option</i>	A value has not been specified in the command line option.	Review the command line option specified.
Failed to start the server: listen tcp: address <i>port</i> : missing port in address	An invalid port was specified to the command line option --web.listen-address.	Review the command line option --web.listen-address specified.
Failed to start the server: listen tcp: lookup <i>host-name</i> on DNS: <i>error-details</i>	An address that does not exist was specified to the command line option --web.listen-address.	Review the command line option --web.listen-address specified.
Failed to start the server: listen tcp : <i>port</i> : bind: address already in use	A port already in use was specified to the command line option --web.listen-address.	Specify a port that is not in use.
-config.path cannot be used with -namemapping or -procnames	Both the command line options --procnames and --config.path are specified. Both the command line options --namemapping and --config.path are specified.	Review the command line option specified.
Error parsing -namemapping argument ' <i>specified-character-string</i> ': bad namemapper: odd number of tokens	An odd number of values have been specified for the command line option --namemapping.	Review the command line option --namemapping specified.
Error parsing -namemapping argument ' <i>specified-character-string</i> ': error compiling regexp ' <i>invalid-regular-</i>	An invalid regular expression has been specified for the command line option --namemapping.	Review the command line option --namemapping specified.

Message	Cause	Countermeasures
<code>expression': error parsing regexp: error-details</code>		
error reading config file " <i>specified-path</i> ": error reading config file " <i>specified-path</i> ": open <i>specified-path</i> : no such file or directory	A path that does not exist has been specified for the command line option <code>--config.path</code> .	Review the command line option <code>--config.path</code> specified.
error reading config file " <i>specified-path</i> ": error-details	The format of the file specified to the command line option <code>--config.path</code> is invalid.	<ul style="list-style-type: none"> Review the command line option <code>--config.path</code> specified. Review the format of the Process exporter configuration file (<code>jpc_process_exporter.yml</code>).
error reading config file " <i>specified-path</i> ": error-details	The configuration file contains invalid formatting.	Review the format of the Process exporter configuration file (<code>jpc_process_exporter.yml</code>).
Error initializing: open /proc/stat: permission denied	Process exporter executed the command without access permissions for the <code>/proc</code> directory, or access permissions for the <code>/proc</code> directory were lost while Process exporter is running.	Grant read permissions to users running Process exporter for the <code>/proc</code> directory and its subdirectories. If Exporter is stopped, restart the integrated agent.
error reading procs: Error reading procs: Error reading procs: open /proc: permission denied		

(6) windows_exporter log

Message	Cause	Action to be taken
msg="cannot start windows_exporter: listen tcp: lookup <i>hostname</i> : no such host"	An invalid host name was specified in <code>--telemetry.addr</code> Optional the command line.	Review the command line Optional.
msg="cannot start windows_exporter: listen tcp : <i>port</i> : bind: Only one usage of each socket address (protocol/network address/port) is normally permitted."	On the command line, <code>--telemetry.addr</code> Optional a port that is already in use.	Review the command line Optional.
msg="Loading configuration file: windows_exporter.yml"	<p>An invalid regular expression was specified in the item for specifying a regular expression in the Windows exporter configuration file (<code>windows_exporter.yml</code>).</p> <p>An invalid value was specified for the item that specifies the numerical value of the Windows exporter configuration file (<code>windows_exporter.yml</code>).</p>	Review the specifications in the Windows exporter configuration file (<code>windows_exporter.yml</code>).
level=error msg="failed collecting service metrics:<nil> An exception occurred.	An invalid WQL of where phrase was specified in <code>services-where</code> .	Re-specify <code>services-where</code> of the <code>windows_exporter.yml</code> .

Message	Cause	Action to be taken
(Invalid query) "source="service.go:77 "		

(7) Logging node_exporter_aix

Message	Cause	Action
Error starting HTTP server: bind: Address already in use	You started the node_exporter_aix registered to the service by specifying the port number that was used for the command line option when it was started.	Review the command-line options at startup of the node_exporter_aix registered to the service.
~/node_exporter_aix: illegal option -- ~	You invoked the node_exporter_aix registered to the service with an option that is not available for the command-line options at startup.	Review the command-line options at startup of the node_exporter_aix registered to the service.
Error calling perfstat_fcstat: Invalid argument	Scrape was executed when one of the following conditions was met while FC data could not be acquired: <ul style="list-style-type: none"> • Specifying-F for Command-Line Options • You specify only-p of the command line option. 	Review the command-line options at startup of the node_exporter_aix registered to the service.

(8) ya_cloudwatch_exporter log

Message	Cause	Action to be taken
"msg": "Couldn't get account Id for role : NoCredentialProviders: ..."	Data retrieval from CloudWatch failed because ~/.aws/credentials do not exist.	Place the credentials file.
"msg": "Couldn't get account Id for role : InvalidClientTokenId: .."	Data retrieval from CloudWatch failed because the Access Key ID described in ~/.aws/credentials is invalid.	Please review the contents of the credentials file.
"msg": "Couldn't get account Id for role : SignatureDoesNotMatch: ..."	Data retrieval from CloudWatch failed because the Secret Access Key listed in ~/.aws/credentials is invalid.	Please review the contents of the credentials file.
"msg": "Couldn't describe resources for region region name:~"	You specified an AWS Region that does not exist in discovery.jobs.regions in the Yet another cloudwatch exporter configuration file (ya_cloudwatch_exporter.yml).	Review the specifications in the Yet another cloudwatch exporter configuration file (ya_cloudwatch_exporter.yml).
"msg": "Couldn't read config.yml: Discovery job [0]: Service is not in known list!: AWS service name"	In the discovery.jobs.type of Yet another cloudwatch exporter configuration file (ya_cloudwatch_exporter.yml), you specified an AWS service that does not exist.	Review the specifications in the Yet another cloudwatch exporter configuration file (ya_cloudwatch_exporter.yml).
"msg": "Couldn't read config.yml: yaml: unmarshal errors:..."	An invalid value was specified in the item that specifies the numerical value in the Yet another cloudwatch exporter configuration file (ya_cloudwatch_exporter.yml).	Check the incorrect line number or field name displayed in msg and review the specifications in the Yet another cloudwatch exporter configuration file (ya_cloudwatch_exporter.yml).

Message	Cause	Action to be taken
	<p>Yet another cloudwatch exporter configuration file (ya_cloudwatch_exporter.yml) does not follow the format.</p> <p>An invalid character string was specified in the item specifying the boolean value in the Yet another cloudwatch exporter configuration file (ya_cloudwatch_exporter.yml).</p>	
"msg": "Couldn't read config.yml: Metric [/0] in Discovery job [job name]: Name should not be empty"	You did not specify a value for the discovery.jobs.metrics.name in the Yet another cloudwatch exporter configuration file (ya_cloudwatch_exporter.yml).	Review the specifications in the Yet another cloudwatch exporter configuration file (ya_cloudwatch_exporter.yml).

(9) Promitor logs

(a) Scraper logs

Message	Cause	Countermeasures
Failed to scrape resource collection <i>discovery-group-name</i> : Connection refused (promitor.agents.resourcediscovery: <i>port</i>)	The Scraper service was started with the Resource Discovery service stopped.	Start the Resource Discovery Agent.
	The incorrect port number was specified for the resourceDiscovery.port in the Promitor Scraper runtime configuration file (runtime.yaml).	Review the specified content for the resourceDiscovery.port in the Promitor Scraper runtime configuration file (runtime.yaml).
AuthorizationFailed: The client ' <i>object-ID</i> ' with object id ' <i>object-ID</i> ' does not have authorization to perform action 'microsoft.insights/metricDefinitions/read' over scope '/subscriptions/ <i>subscription-ID</i> /resourceGroups/ <i>resource-group-name</i> / providers/ <i>resource-type</i> / <i>resource-name</i> /providers/microsoft.insights' or the scope is invalid. If access was recently granted, please refresh your credentials.	Specified an identity with insufficient permissions for the Monitoring Reader role.	Grant permissions that meet or exceed the requirements of the Monitoring Reader role.
Promitor Scraper Agent has encountered an unexpected error. Please open an issue at https://github.com/tomkerkhove/promitor/issues to let us know about it.	When the authentication.mode in the Promitor Scraper runtime configuration file (runtime.yaml) is ServicePrincipal, the Scraper was started with the incorrect value registered as the secret for connecting to Azure Monitor.	Review the content specified for the AUTH_APPKEY environment variable.

Message	Cause	Countermeasures
System.Security.Authentication.AuthenticationException: No identity secret was configured for service principle authentication		
<p>The following problems were found with the metric configuration:</p> <p><error-details></p> <p>Validation failed:</p> <p>Errors were found while deserializing the metric configuration. Promitor is not configured correctly. Please fix validation issues and re-run.</p>	The format of the Promitor Scraper configuration file (metrics-declaration.yaml) is not followed.	<p>Check <i>error-details</i> for the invalid line number and item name, and review the content specified for the Promitor Scraper configuration file (metrics-declaration.yaml).</p>
	When <code>metrics.resources</code> is not specified by any metric in the Promitor Scraper configuration file (metrics-declaration.yaml), an out-of-range value was specified for <code>azureMetadata.cloud</code> in the same file.	
	When <code>metrics.resources</code> is not specified by any metric in the Promitor Scraper configuration file (metrics-declaration.yaml), a value in an invalid format was specified for <code>metricDefault.aggregation.interval</code> .	
	When <code>metrics.resources</code> is not specified by any metric in the Promitor Scraper configuration file (metrics-declaration.yaml), an invalid value was specified for <code>metricDefault.scraping.schedule</code> .	
	An out-of-range value was specified for <code>metrics.resourceType</code> in the Promitor Scraper configuration file (metrics-declaration.yaml).	
	A value in an invalid format was specified for <code>metrics.scraping.schedule</code> in the Promitor Scraper configuration file (metrics-declaration.yaml).	
	When <code>metrics.resources</code> is not specified by any metric in the Promitor Scraper configuration file (metrics-declaration.yaml), an out-of-range value was specified for <code>metrics.azureMetricConfiguration.aggregation.type</code> .	
	When <code>metrics.resources</code> is not specified by any metric in the Promitor Scraper configuration file (metrics-declaration.yaml), a value in an invalid format was specified for <code>metrics.azureMetricConfiguration.aggregation.interval</code> .	
<p>Validation failed:</p> <p>Errors were found while deserializing the metric configuration. Promitor is not configured correctly. Please fix validation issues and re-run.</p>	The format of the Promitor Scraper configuration file (metrics-declaration.yaml) is not followed.	<p>Review the contents of the Promitor Scraper configuration file (metrics-declaration.yaml).</p>
	When <code>metrics.resources</code> is specified by a metric in the Promitor Scraper configuration file (metrics-declaration.yaml), an invalid value was specified for <code>metricDefault.aggregation.interval</code> .	

Message	Cause	Countermeasures
	When <code>metrics.resources</code> is specified by a metric in the Promitor Scraper configuration file (<code>metrics-declaration.yaml</code>), an invalid value was specified for <code>metricDefault.scraping.schedule</code> .	
	When <code>metrics.resources</code> is specified by a metric in the Promitor Scraper configuration file (<code>metrics-declaration.yaml</code>), an invalid value was specified for <code>metrics.azureMetricConfiguration.aggregation.type</code> .	
	When <code>metrics.resources</code> is specified by a metric in the Promitor Scraper configuration file (<code>metrics-declaration.yaml</code>), an invalid value was specified for <code>metrics.azureMetricConfiguration.aggregation.interval</code> .	
Promitor Scraper Agent has encountered an unexpected error. Please open an issue at https://github.com/tomkerkhove/promitor/issues to let us know about it. Unable to deserialize the configured metrics declaration. Please verify that it is a well-formed YAML specification.	The format of the Promitor Scraper configuration file (<code>metrics-declaration.yaml</code>) is not followed.	Review the specified contents of the Promitor Scraper configuration file (<code>metrics-declaration.yaml</code>).
Failed to scrape resource for metric ' <i>metric-name</i> ' AADSTS900023: Specified tenant identifier ' <i>specified-character-string</i> ' is neither a valid DNS name, nor a valid external domain.	When the <code>authentication.mode</code> is <code>ServicePrincipal</code> in the Promitor Scraper runtime configuration file (<code>runtime.yaml</code>), a value in an invalid format was specified for <code>azureMetadata.tenantId</code> in the Promitor Scraper configuration file (<code>metrics-declaration.yaml</code>).	Review the content specified for <code>azureMetadata.tenantId</code> in the Promitor Scraper configuration file (<code>metrics-declaration.yaml</code>).
Validation failed: No tenant id is configured. Promitor is not configured correctly. Please fix validation issues and re-run.	When <code>resources</code> is not specified by any metric in <code>metrics</code> in the Promitor Scraper configuration file (<code>metrics-declaration.yaml</code>), a value is not specified for <code>authentication.tenantId</code> .	Review the content specified for <code>authentication.tenantId</code> in the Promitor Scraper configuration file (<code>metrics-declaration.yaml</code>).
	When <code>resources</code> is specified by a metric in <code>metrics</code> in the Promitor Scraper runtime configuration file (<code>runtime.yaml</code>), a value is not specified for <code>authentication.tenantId</code> in the Promitor Scraper configuration file (<code>metrics-declaration.yaml</code>).	Review the content specified for <code>authentication.tenantId</code> in the Promitor Scraper configuration file (<code>metrics-declaration.yaml</code>).
Failed to scrape resource for metric ' <i>metric-name</i> '	A tenant ID that does not exist was specified for <code>azureMetadata.tenantId</code> in the Promitor Scraper configuration file (<code>metrics-declaration.yaml</code>).	Review the content specified for <code>azureMetadata.tenantId</code> in the Promitor Scraper configuration file (<code>metrics-declaration.yaml</code>).

Message	Cause	Countermeasures
<p>AADSTS90002: Tenant '<i>tenant-ID</i>' not found. Check to make sure you have the correct tenant ID and are signing into the correct cloud. Check with your subscription administrator, this may happen if there are no active subscriptions for the tenant.</p>		
<p>InvalidSubscriptionId: The provided subscription identifier '<i>specified-character-string</i>' is malformed or invalid.</p>	<p>A value in an invalid format was specified for <code>azureMetadata.subscriptionId</code> in the Promitor Scraper configuration file (<code>metrics-declaration.yaml</code>).</p>	<p>Review the content specified for <code>azureMetadata.subscriptionId</code> in the Promitor Scraper configuration file (<code>metrics-declaration.yaml</code>).</p>
	<p>A value in an invalid format was specified for <code>metrics.resources.subscriptionId</code> in the Promitor Scraper configuration file (<code>metrics-declaration.yaml</code>).</p>	<p>Review the content specified for <code>metrics.resources.subscriptionId</code> in the Promitor Scraper configuration file (<code>metrics-declaration.yaml</code>).</p>
<p>Validation failed: - No subscription id is configured Promitor is not configured correctly. Please fix validation issues and re-run.</p>	<p>When <code>metrics.resources</code> is not specified by any metric in the Promitor Scraper configuration file (<code>metrics-declaration.yaml</code>), a value is not specified for <code>azureMetadata.subscriptionId</code>.</p>	<p>Review the content specified for <code>azureMetadata.subscriptionId</code> in the Promitor Scraper configuration file (<code>metrics-declaration.yaml</code>).</p>
	<p>When <code>metrics.resources</code> is specified by a metric in the Promitor Scraper configuration file (<code>metrics-declaration.yaml</code>), a value is not specified for <code>azureMetadata.subscriptionId</code>.</p>	<p>Review the content specified for <code>azureMetadata.subscriptionId</code> in the Promitor Scraper configuration file (<code>metrics-declaration.yaml</code>).</p>
<p>SubscriptionNotFound: The subscription '<i>subscription-ID</i>' could not be found.</p>	<p>When <code>metrics.resources</code> is specified by a metric in the Promitor Scraper configuration file (<code>metrics-declaration.yaml</code>), a subscription ID that does not exist was specified for <code>azureMetadata.subscriptionId</code>.</p>	<p>Review the content specified for <code>azureMetadata.subscriptionId</code> in the Promitor Scraper configuration file (<code>metrics-declaration.yaml</code>).</p>
	<p>A subscription ID that does not exist was specified for <code>metrics.resources.subscriptionId</code> in the Promitor Scraper configuration file (<code>metrics-declaration.yaml</code>).</p>	<p>Review the content specified for <code>metrics.resources.subscriptionId</code> in the Promitor Scraper configuration file (<code>metrics-declaration.yaml</code>).</p>
<p>AuthorizationFailed: The client '<i>object-ID</i>' with object id '<i>object-ID</i>' does not have authorization to perform action <code>microsoft.insights/metricDefinitions/read</code> over scope <code>'/subscriptions/<i>subscription-ID</i>/resourceGroups/<i>specified-character-string</i>/providers/<i>resource-type</i>/<i>resource-name</i>/providers/</code></p>	<p>When the <code>authentication.mode</code> is <code>SystemAssignedManagedIdentity</code> in the Promitor Scraper runtime configuration file (<code>runtime.yaml</code>), and <code>metrics.resources</code> is specified by a metric in the Promitor Scraper configuration file (<code>metrics-declaration.yaml</code>), an invalid value was specified for <code>azureMetadata.resourceGroupName</code>.</p>	<p>Review the content specified for <code>azureMetadata.resourceGroupName</code> in the Promitor Scraper configuration file (<code>metrics-declaration.yaml</code>).</p>
	<p>An invalid value was specified for <code>metrics.resources.resourceGroupName</code> in the Promitor Scraper configuration file (<code>metrics-declaration.yaml</code>).</p>	<p>Review the content specified for <code>metrics.resources.resourceGroupName</code> in the Promitor Scraper configuration file (<code>metrics-declaration.yaml</code>).</p>

Message	Cause	Countermeasures
microsoft.insights' or the scope is invalid. If access was recently granted, please refresh your credentials.		
Validation failed: - No resource group name is not configured Promitor is not configured correctly. Please fix validation issues and re-run.	A value was not specified for <code>azureMetadata.resourceGroupName</code> in the Promitor Scraper configuration file (<code>metrics-declaration.yaml</code>).	Review the content specified for <code>azureMetadata.resourceGroupName</code> in the Promitor Scraper configuration file (<code>metrics-declaration.yaml</code>).
Microsoft.IdentityModel.Clients.ActiveDirectory.AdalServiceException: AADSTS90038: Tenant ' <i>tenant-ID</i> ' request is being redirected to the National Cloud 'MicrosoftOnline.COM'.	When <code>metrics.resources</code> is specified by a metric in the Promitor Scraper configuration file (<code>metrics-declaration.yaml</code>), an out-of-range value was specified for <code>azureMetadata.cloud</code> .	Review the content specified for <code>azureMetadata.cloud</code> in the Promitor Scraper configuration file (<code>metrics-declaration.yaml</code>).
Failed to scrape metric ' <i>metric-name</i> ' for resource ' <i>resource-name</i> '. System.NotSupportedException: Environment ' <i>cloud-name</i> ' is not supported for scraping Azure Log Analytics resource(s)	When the <code>authentication.mode</code> is <code>ServicePrincipal</code> in the Promitor Scraper runtime configuration file (<code>runtime.yaml</code>), an incorrect cloud name was specified for <code>azureMetadata.cloud</code> in the <code>metrics-declaration.yaml</code> .	Review the content specified for <code>azureMetadata.cloud</code> in the <code>metrics-declaration.yaml</code> .
Failed to scrape resource for metric ' <i>metric-name</i> ' AADSTS500011: The resource principal named <code>https://management.core.cloudapi.de/</code> was not found in the tenant named <i>tenant-ID</i> . This can happen if the application has not been installed by the administrator of the tenant or consented to by any user in the tenant. You might have sent your authentication request to the wrong tenant.	When the <code>authentication.mode</code> is <code>SystemAssignedManagedIdentity</code> or <code>UserAssignedManagedIdentity</code> in the Promitor Scraper runtime configuration file (<code>runtime.yaml</code>), an incorrect cloud name was specified for <code>azureMetadata.cloud</code> in the Promitor Scraper configuration file (<code>metrics-declaration.yaml</code>).	Review the content specified for <code>azureMetadata.cloud</code> in the Promitor Scraper configuration file (<code>metrics-declaration.yaml</code>).
Failed to scrape: Value cannot be null. (Parameter 'key')	When <code>metrics.resources</code> is specified by a metric in the Promitor Scraper configuration file (<code>metrics-declaration.yaml</code>), <code>interval</code> and <code>type</code> were not specified in <code>metricDefault.aggregation</code> and	Review the content specified for <code>interval</code> and <code>type</code> in <code>metricDefault.aggregation</code> or <code>metrics.azureMetricConfiguration.aggregation</code> in the Promitor Scraper configuration file (<code>metrics-declaration.yaml</code>).

Message	Cause	Countermeasures
	<code>metrics.azureMetricConfiguration.aggregation.</code>	
Failed to scrape resource collection <i>resource-name</i> : Value cannot be null. (Parameter 'key')	When <code>metrics.resources</code> is not specified by any metric in the Promitor Scraper configuration file (<code>metrics-declaration.yaml</code>), <code>interval</code> and <code>type</code> were not specified in <code>metricDefault.aggregation</code> and <code>metrics.azureMetricConfiguration.aggregation.</code>	Review the content specified for <code>interval</code> and <code>type</code> in <code>metricDefault.aggregation</code> or <code>metrics.azureMetricConfiguration.aggregation</code> in the Promitor Scraper configuration file (<code>metrics-declaration.yaml</code>).
Validation failed: - Limit has to be at least 1 Promitor is not configured correctly. Please fix validation issues and re-run.	A value less than 1 was specified for <code>metricDefault.limit</code> in the Promitor Scraper configuration file (<code>metrics-declaration.yaml</code>). A value less than 1 was specified for <code>metrics.azureMetricConfiguration.limit</code> in the Promitor Scraper configuration file (<code>metrics-declaration.yaml</code>).	Review the content specified for <code>metricDefault.limit</code> in the Promitor Scraper configuration file (<code>metrics-declaration.yaml</code>).
Validation failed: - No default metric scraping schedule is defined. - No metrics scraping schedule is configured Promitor is not configured correctly. Please fix validation issues and re-run.	A value was not specified for <code>metricDefault.scraping.schedule</code> in the Promitor Scraper configuration file (<code>metrics-declaration.yaml</code>).	Review the content specified for <code>metricDefault.scraping.schedule</code> in the Promitor Scraper configuration file (<code>metrics-declaration.yaml</code>).
Validation failed: - No metric name is configured Promitor is not configured correctly. Please fix validation issues and re-run.	A value was not specified for <code>metrics.name</code> in the Promitor Scraper configuration file (<code>metrics-declaration.yaml</code>).	Review the content specified for <code>metrics.name</code> in the Promitor Scraper configuration file (<code>metrics-declaration.yaml</code>).
Validation failed: - Metric name ' <i>metric-name</i> ' is declared multiple times Promitor is not configured correctly. Please fix validation issues and re-run.	The same value as another metric was specified for <code>metrics.name</code> in the Promitor Scraper configuration file (<code>metrics-declaration.yaml</code>).	Review the content specified for <code>metrics.name</code> in the Promitor Scraper configuration file (<code>metrics-declaration.yaml</code>).
Validation failed: - No metric name for Azure is configured Promitor is not configured correctly. Please fix validation issues and re-run.	A value was not specified for <code>metrics.azureMetricConfiguration.Name</code> in the Promitor Scraper configuration file (<code>metrics-declaration.yaml</code>).	Review the content specified for <code>metrics.azureMetricConfiguration.Name</code> in the Promitor Scraper configuration file (<code>metrics-declaration.yaml</code>).
Failed to scrape resource for metric ' <i>metric-name</i> '	An invalid value was specified for <code>metrics.azureMetricConfiguration.Name</code> in the Promitor Scraper configuration file (<code>metrics-declaration.yaml</code>).	Review the content specified for <code>metrics.azureMetricConfiguration.Name</code> in the Promitor Scraper configuration file (<code>metrics-declaration.yaml</code>).

Message	Cause	Countermeasures
Promitor.Integrations.AzureMonitor.Exception s.MetricNotFoundExcept ion: The metric ' <i>specified-character-string</i> ' was not found		
Validation failed: - Limit cannot be higher than <i>metricDefault.limit-value</i>	A value greater than 10000 was specified for <i>metrics.azureMetricConfiguration.limit</i> in the Promitor Scraper configuration file (<i>metrics-declaration.yaml</i>).	Review the content specified for <i>metrics.azureMetricConfiguration.limit</i> in the Promitor Scraper configuration file (<i>metrics-declaration.yaml</i>).
BadRequest: Metric: Available Memory Bytes does not support requested dimension combination: <i>specified-character-string</i> , supported ones are: , TraceId: { <i>trace-ID</i> }	An invalid value was specified for <i>metrics.azureMetricConfiguration.dimension.name</i> in the Promitor Scraper configuration file (<i>metrics-declaration.yaml</i>).	Review the content specified for <i>metrics.azureMetricConfiguration.dimension.name</i> in the Promitor Scraper configuration file (<i>metrics-declaration.yaml</i>).
Promitor Scraper Agent has encountered an unexpected error. Please open an issue at https://github.com/tomkerkhove/promitor/issues to let us know about it. [<i>resourceDiscoveryGroup</i> <i>pName</i>] cannot be Null, empty or white-space. (Parameter ' <i>resourceDiscoveryGroup</i> <i>pName</i> ')	A value was not specified for <i>metrics.resourceDiscoveryGroups.name</i> in the Promitor Scraper configuration file (<i>metrics-declaration.yaml</i>).	Review the content specified for <i>metrics.resourceDiscoveryGroups.name</i> in the Promitor Scraper configuration file (<i>metrics-declaration.yaml</i>).
Failed to scrape resource collection <i>specified-character-string</i> : Response status code does not indicate success: 404 (Not Found).	An invalid value was specified for <i>metrics.resourceDiscoveryGroups.name</i> in the Promitor Scraper configuration file (<i>metrics-declaration.yaml</i>).	Review the content specified for <i>metrics.resourceDiscoveryGroups.name</i> in the Promitor Scraper configuration file (<i>metrics-declaration.yaml</i>).
	An invalid value was specified for <i>resourceDiscoveryGroups.name</i> in the Promitor Resource Discovery configuration file (<i>resource-discovery-declaration.yaml</i>).	Review the content specified for <i>resourceDiscoveryGroups.name</i> in the Promitor Resource Discovery configuration file (<i>resource-discovery-declaration.yaml</i>).
	An invalid value was specified for <i>resourceDiscoveryGroups.type</i> in the Promitor Resource Discovery configuration file (<i>resource-discovery-declaration.yaml</i>).	Review the content specified for <i>resourceDiscoveryGroups.type</i> in the Promitor Resource Discovery configuration file (<i>resource-discovery-declaration.yaml</i>).
Validation failed: - No <i>property-name</i> is configured Promitor is not configured correctly. Please fix validation issues and re-run.	A value was not specified for <i>metrics.resources.property</i> in the Promitor Scraper configuration file (<i>metrics-declaration.yaml</i>).	Review the content specified for <i>metrics.resources.property</i> in the Promitor Scraper configuration file (<i>metrics-declaration.yaml</i>).
ResourceNotFound: The Resource ' <i>resource-type/character-string</i> ' under resource group ' <i>resource-</i>	An invalid value was specified for <i>metrics.resources.property</i> in the Promitor Scraper configuration file (<i>metrics-declaration.yaml</i>).	Review the content specified for <i>metrics.resources.property</i> in the Promitor Scraper configuration file (<i>metrics-declaration.yaml</i>).

Message	Cause	Countermeasures
<code>group-name</code> was not found. For more details please go to https://aka.ms/ARMResourceNotFoundFix		
Validation failed: - Queue & topic name are both configured while we only support one or the other. Promitor is not configured correctly. Please fix validation issues and re-run.	Both the <code>queueName</code> and <code>topicName</code> were specified in <code>metrics.resources</code> when the <code>metrics.resourceType</code> is <code>ServiceBusNamespace</code> in the Promitor Scraper configuration file (<code>metrics-declaration.yaml</code>).	Review the content specified for <code>metrics.resources</code> in the Promitor Scraper configuration file (<code>metrics-declaration.yaml</code>).
BadRequest: Metric: <i>Azure-metric-name</i> does not accept zero dimension case	A value was not specified for <code>name</code> in <code>metrics.azureMetricConfiguration.dimension</code> when the <code>metrics.resourceType</code> is <code>SqlServer</code> in the Promitor Scraper configuration file (<code>metrics-declaration.yaml</code>).	Review the content specified for <code>metrics.azureMetricConfiguration.dimension.name</code> in the Promitor Scraper configuration file (<code>metrics-declaration.yaml</code>).
BadRequest: Metric: <i>Azure-metric-name</i> does not support requested dimension combination: <i>specified-value</i> , supported ones are: <code>DatabaseResourceId</code> , <code>TraceId: { trace-ID }</code>	An invalid value was specified for <code>metrics.azureMetricConfiguration.dimension.name</code> when the <code>metrics.resourceType</code> is <code>SqlServer</code> in the Promitor Scraper configuration file (<code>metrics-declaration.yaml</code>).	Review the content specified for <code>metrics.azureMetricConfiguration.dimension.name</code> in the Promitor Scraper configuration file (<code>metrics-declaration.yaml</code>).
Failed to scrape resource collection <i>discovery-group-name</i> : Response status code does not indicate success: 501 (Not Implemented).	A value was not specified for <code>resourceDiscoveryGroups.type</code> in the Promitor Resource Discovery configuration file (<code>resource-discovery-declaration.yaml</code>).	Review the content specified for <code>resourceDiscoveryGroups.type</code> in the Promitor Resource Discovery configuration file (<code>resource-discovery-declaration.yaml</code>).
Promitor Scraper Agent has encountered an unexpected error. Please open an issue at https://github.com/tomkerkhove/promitor/issues to let us know about it. Failed to convert configuration value at ' <code>authentication:Mode</code> ' to type ' <code>Promitor.Integrations.Azure.Authentication.AuthenticationMode</code> '.	An invalid value was specified for the <code>authentication.mode</code> in the Promitor Scraper runtime configuration file (<code>runtime.yaml</code>).	Review the specified content for the <code>authentication.mode</code> in the Promitor Scraper runtime configuration file (<code>runtime.yaml</code>).
Validation failed: Azure authentication is not configured correctly - No identity was configured for service	When a secret has not been registered for connecting to Azure Monitor, and <code>metrics.resources</code> is not specified by any metric in the Promitor Scraper configuration file (<code>metrics-declaration.yaml</code>), a value is not specified for <code>authentication.mode</code> in	Review the specified content for the <code>authentication.mode</code> in the Promitor Scraper runtime configuration file (<code>runtime.yaml</code>).

Message	Cause	Countermeasures
<p>principle authentication</p> <p>Promitor is not configured correctly. Please fix validation issues and re-run.</p>	<p>the Promitor Scraper runtime configuration file (runtime.yaml).</p>	
	<p>When Serviceprincipal is specified for authentication.mode in the Promitor Scraper runtime configuration file (runtime.yaml), and metrics.resources is not specified by any metric in the Promitor Scraper configuration file (metrics-declaration.yaml), a value is not specified for authentication.identityId in the Promitor Scraper runtime configuration file (runtime.yaml).</p>	<p>Review the specified content for the authentication.identityId in the Promitor Scraper runtime configuration file (runtime.yaml).</p>
<p>Failed to scrape resource for metric '<i>metric-name</i>' AADSTS700016: Application with identifier '<i>specified-character-string</i>' was not found in the directory '<i>Azure-directory-name</i>'. This can happen if the application has not been installed by the administrator of the tenant or consented to by any user in the tenant. You may have sent your authentication request to the wrong tenant. Promitor Scraper Agent has encountered an unexpected error. Please open an issue at https://github.com/tomkerkhove/promitor/issues to let us know about it.</p> <p>Failed to bind to address http://[::]:<i>port</i>: address already in use.</p>	<p>When the authentication.mode is ServicePrincipal in the Promitor Scraper runtime configuration file (runtime.yaml), an invalid value was specified for the authentication.identityId.</p>	<p>Review the specified content for the authentication.identityId in the Promitor Scraper runtime configuration file (runtime.yaml).</p>
	<p>A port that is already in use was specified for the server.httpPort in the Promitor Scraper runtime configuration file (runtime.yaml).</p>	<p>Specify a port that is not in use for the server.httpPort in the Promitor Scraper runtime configuration file (runtime.yaml).</p>
<p>Promitor Scraper Agent has encountered an unexpected error. Please open an issue at https://github.com/tomkerkhove/promitor/issues to let us know about it.</p> <p>Failed to convert configuration value at 'server:HttpPort' to type 'System.Int32'.</p>	<p>An invalid value was specified for the server.httpPort in the Promitor Scraper runtime configuration file (runtime.yaml).</p>	<p>Review the specified content for the server.httpPort in the Promitor Scraper runtime configuration file (runtime.yaml).</p>
<p>Promitor Scraper Agent has encountered an unexpected error.</p>	<p>An invalid value was specified for the metricsConfiguration.absolutePath</p>	<p>Review the specified content for the metricsConfiguration.absolutePath</p>

Message	Cause	Countermeasures
<p>Please open an issue at https://github.com/tomkerkhove/promitor/issues to let us know about it.</p> <p>Could not find file '<i>path</i>'.</p>	<p>in the Promitor Scraper runtime configuration file (runtime.yaml).</p>	<p>in the Promitor Scraper runtime configuration file (runtime.yaml).</p>
<p>Promitor Scraper Agent has encountered an unexpected error. Please open an issue at https://github.com/tomkerkhove/promitor/issues to let us know about it.</p> <p>Could not find a part of the path '/config/metrics-declaration.yaml'.</p>	<p>A value was not specified for <code>metricsConfiguration.absolutePath</code> in the Promitor Scraper runtime configuration file (runtime.yaml).</p>	<p>Review the specified content for the <code>metricsConfiguration.absolutePath</code> in the Promitor Scraper runtime configuration file (runtime.yaml).</p>
<p>Promitor Scraper Agent has encountered an unexpected error. Please open an issue at https://github.com/tomkerkhove/promitor/issues to let us know about it.</p> <p>Failed to convert configuration value at 'resourceDiscovery:Port' to type 'System.Int32'.</p>	<p>An invalid value was specified for the <code>resourceDiscovery.port</code> in the Promitor Scraper runtime configuration file (runtime.yaml).</p>	<p>Review the specified content for the <code>resourceDiscovery.port</code> in the Promitor Scraper runtime configuration file (runtime.yaml).</p>
<p>AuthorizationFailed: The client '<i>client-ID</i>' with object id '<i>object-ID</i>' does not have authorization to perform action 'microsoft.insights/metricDefinitions/read' over scope '<i>resource-Uri</i>' or the scope is invalid. If access was recently granted, please refresh your credentials</p>	<p>When the <code>authentication.mode</code> is <code>ServicePrincipal</code> in the Promitor Scraper runtime configuration file (runtime.yaml), and <code>metrics.resources</code> is specified in the Promitor configuration file (metrics-declaration.yaml), an invalid value was specified for <code>azureMetadata.resourceGroupName</code> in the Promitor configuration file (metrics-declaration.yaml).</p>	<p>Review the content specified for <code>azureMetadata.resourceGroupName</code> in the Promitor configuration file (metrics-declaration.yaml).</p>
<p>Failed to scrape resource for metric '<i>metric-name</i>'</p> <p>System.Net.Http.HttpRequestException: Resource temporarily unavailable (<i>host-name:port-number</i>)</p>	<p>The Scraper is disconnected from the network.</p>	<p>Connect the network.</p>

Message	Cause	Countermeasures
Failed to discover resources for group resource-group-name. System.Threading.Tasks.TaskCanceledException: The request was canceled due to the configured HttpClient.Timeout of 100 seconds elapsing.	The Scraper attempt to retrieve information from the Resource Discovery who is disconnected from the network.	Connect the network.
Failed to scrape resource for metric ' <i>metric-name</i> ' System.Net.Http.HttpRequestException: Name or service not known (<i>host-name:port-number</i>)	The Scraper was started with the incorrect proxy.	Review the proxy settings.
Failed to discover resources for group kubernetes-service-group. System.Net.Http.HttpRequestException: Response status code does not indicate success: 500 (Internal Server Error).	The Scraper attempt to retrieve information from the Resource Discovery with an incorrect proxy configured.	Review the proxy settings.

(b) Resource Discovery logs

Message	Cause	Countermeasures
Unhandled exception in job Azure Subscription Discovery One or more errors occurred. ([subscriptions] cannot be Null. (Parameter 'subscriptions'))	Specified an identity with insufficient permissions for the Reader role.	Grant permissions that meet or exceed the requirements of the Reader role.
ClientSecretCredential authentication failed: AADSTS700016: Application with identifier ' <i>specified-character-string</i> ' was not found in the directory ' <i>Azure-directory-name</i> '. This can happen if the application has not been installed by the administrator of the tenant or consented to by any user in the tenant. You may have sent your	When the authentication.mode is ServicePrincipal in the Promitor Resource Discovery runtime configuration file (runtime.yaml), Resource Discovery was started with an incorrect value registered as the secret for connecting to Azure Resource Graph.	Review the secret for connecting to Azure Resource Graph.
	When the authentication.mode is ServicePrincipal in the Promitor Resource Discovery runtime configuration file (runtime.yaml), an invalid value was specified for the authentication.identityId.	Review the specified content for the authentication.identityId in the Promitor Resource Discovery runtime configuration file (runtime.yaml).

Message	Cause	Countermeasures
authentication request to the wrong tenant.		
Unhandled exception in job Azure Subscription Discovery One or more errors occurred. (ClientSecretCredential authentication failed: AADSTS900023: Specified tenant identifier ' <i>specified-character-string</i> ' is neither a valid DNS name, nor a valid external domain.	When the authentication.mode is ServicePrincipal in the Promitor Resource Discovery runtime configuration file (runtime.yaml), a value in an invalid format was specified for azureLandscape.tenantId in the Promitor Resource Discovery configuration file (resource-discovery-declaration.yaml).	Review the content specified for azureLandscape.tenantId in the Promitor Resource Discovery configuration file (resource-discovery-declaration.yaml).
Unhandled exception in job Azure Subscription Discovery One or more errors occurred. (ClientSecretCredential authentication failed: AADSTS90002: Tenant ' <i>specified-character-string</i> ' not found. Check to make sure you have the correct tenant ID and are signing into the correct cloud. Check with your subscription administrator, this may happen if there are no active subscriptions for the tenant.	When the authentication.mode is ServicePrincipal in the Promitor Resource Discovery runtime configuration file (runtime.yaml), a tenant ID that does not exist was specified for azureLandscape.tenantId in the Promitor Resource Discovery configuration file (resource-discovery-declaration.yaml).	Review the content specified for azureLandscape.tenantId in the Promitor Resource Discovery configuration file (resource-discovery-declaration.yaml).
Validation failed: - No tenant id was configured Promitor is not configured correctly. Please fix validation issues and re-run.	A value was not specified for azureLandscape.tenantId in the Promitor Resource Discovery configuration file (resource-discovery-declaration.yaml).	Review the content specified for azureLandscape.tenantId in the Promitor Resource Discovery configuration file (resource-discovery-declaration.yaml).
Operation returned an invalid status code 'BadRequest'	A value in an invalid format was specified for azureLandscape.subscriptions.subscriptionId in the Promitor Resource Discovery configuration file (resource-discovery-declaration.yaml).	Review the content specified for azureLandscape.subscriptions.subscriptionId in the Promitor Resource Discovery configuration file (resource-discovery-declaration.yaml).
[queriedSubscriptions] cannot be Null. (Parameter 'queriedSubscriptions')	A subscription ID that does not exist was specified for azureLandscape.subscriptions.subscriptionId in the Promitor Resource Discovery configuration file (resource-discovery-declaration.yaml).	Review the content specified for azureLandscape.subscriptions.subscriptionId in the Promitor Resource Discovery configuration file (resource-discovery-declaration.yaml).

Message	Cause	Countermeasures
<p>Validation failed:</p> <ul style="list-style-type: none"> - No subscription id(s) were configured to query <p>Promitor is not configured correctly. Please fix validation issues and re-run.</p>	<p>A value was not specified for <code>azureLandscape.subscriptions.subscriptionId</code> in the Promitor Resource Discovery configuration file (<code>resource-discovery-declaration.yaml</code>).</p>	<p>Review the content specified for <code>azureLandscape.subscriptions.subscriptionId</code> in the Promitor Resource Discovery configuration file (<code>resource-discovery-declaration.yaml</code>).</p>
<p>Promitor Discovery Agent has encountered an unexpected error. Please open an issue at https://github.com/tomkerkhove/promitor/issues to let us know about it.</p> <p>Value cannot be null. (Parameter 'text')</p>	<p>A value was not specified for <code>resourceDiscoveryGroups.name</code> in the Promitor Resource Discovery configuration file (<code>resource-discovery-declaration.yaml</code>).</p>	<p>Review the content specified for <code>resourceDiscoveryGroups.name</code> in the Promitor Resource Discovery configuration file (<code>resource-discovery-declaration.yaml</code>).</p>
<p>Promitor Discovery Agent has encountered an unexpected error. Please open an issue at https://github.com/tomkerkhove/promitor/issues to let us know about it.</p> <p>Failed to convert configuration value at 'authentication:Mode' to type 'Promitor.Integrations.Azure.Authentication.AuthenticationMode'.</p>	<p>An invalid value was specified for the <code>authentication.mode</code> in the Promitor Resource Discovery runtime configuration file (<code>runtime.yaml</code>).</p>	<p>Review the specified content for the <code>authentication.mode</code> in the Promitor Resource Discovery runtime configuration file (<code>runtime.yaml</code>).</p>
<p>Validation failed:</p> <p>Azure authentication is not configured correctly - No identity was configured for service principle authentication</p> <p>Promitor is not configured correctly. Please fix validation issues and re-run.</p>	<p>A secret has not been registered for connecting to Azure Resource Graph, and a value is not specified for <code>authentication.mode</code> in the Promitor Resource Discovery runtime configuration file (<code>runtime.yaml</code>).</p>	<p>Review the specified content for the <code>authentication.mode</code> in the Promitor Resource Discovery runtime configuration file (<code>runtime.yaml</code>).</p>
	<p>When the <code>authentication.mode</code> is <code>ServicePrincipal</code> in the Promitor Resource Discovery runtime configuration file (<code>runtime.yaml</code>), a value was not specified for the <code>authentication.identityId</code>.</p>	<p>Review the specified content for the <code>authentication.identityId</code> in the Promitor Resource Discovery runtime configuration file (<code>runtime.yaml</code>).</p>
<p>Promitor Discovery Agent has encountered an unexpected error. Please open an issue at https://github.com/tomkerkhove/promitor/issues to let us know about it.</p> <p>Failed to bind to address <code>http://[::]:port</code>: address already in use.</p>	<p>A port that is already in use was specified for the <code>server.httpPort</code> in the Promitor Resource Discovery runtime configuration file (<code>runtime.yaml</code>).</p>	<p>Review the specified content for the <code>server.httpPort</code> in the Promitor Resource Discovery runtime configuration file (<code>runtime.yaml</code>).</p>

Message	Cause	Countermeasures
ClientSecretCredential authentication failed: Retry failed after 2 tries. Retry settings can be adjusted in ClientOptions.Retry. (Resource temporarily unavailable (<i>host-name:port-number</i>)) (The operation was canceled.)	The Scraper and the Resource Discovery started while disconnected from the network.	Connect the network.
Unhandled exception in job Azure Subscription Discovery System.AggregateException: One or more errors occurred. (ClientSecretCredential authentication failed: Retry failed after 4 tries. Retry settings can be adjusted in ClientOptions.Retry. (Resource temporarily unavailable (<i>host-name:port-number</i>)) (Resource temporarily unavailable (<i>host-name:port-number</i>)) (Resource temporarily unavailable (<i>host-name:port-number</i>)) (Resource temporarily unavailable (<i>host-name:port-number</i>)))	The Resource Discovery started while disconnected from the network.	Connect the network.
Unhandled exception in job Azure Subscription Discovery System.AggregateException: One or more errors occurred. (Resource temporarily unavailable (<i>host-name:port-number</i>))	It was disconnected from the network while the Resource Discovery was running.	Connect the network.
ClientSecretCredential authentication failed: Retry failed after 4 tries. Retry settings can be adjusted in ClientOptions.Retry. (Name or service not known (<i>host-name:port-number</i>)) (Name or service not known (<i>host-name:port-number</i>)) (Name or service not known (<i>host-name:port-number</i>))	The Resource Discovery was started with the incorrect proxy.	Review the proxy settings.

Message	Cause	Countermeasures
(Name or service not known (<i>host-name:port-number</i>))		

(10) script_exporter logs

Message	Cause	Countermeasures
flag needs an argument: <i>command-line-option</i>	A value has not been specified in the command line option.	Review the command line option.
open <i>path</i> : no such file or directory	A path that does not exist has been specified for the command line option <code>--config.file</code> .	Review the command line option <code>--config.file</code> specified.
listen tcp: address <i>specified-character-string</i> : missing port in address	An invalid value was specified to the command line option <code>--web.listen-address</code> .	Review the command line option <code>--web.listen-address</code> specified.
<ul style="list-style-type: none"> For Windows listen tcp: lookup <i>host-name</i> : no such host <ul style="list-style-type: none"> For Linux listen tcp: lookup <i>host-name</i> on 10.0.0.1:53: read udp 10.1.0.1:46736->10.0.0.1:53: i/o timeout	An address that does not exist was specified to the command line option <code>--web.listen-address</code> .	Specify the correct host name.
<ul style="list-style-type: none"> For Windows listen tcp <i>:port</i> : bind: Only one usage of each socket address (protocol/network address/port) is normally permitted. <ul style="list-style-type: none"> For Linux listen tcp <i>:port</i> : bind: address already in use	A port already in use was specified to the command line option <code>--web.listen-address</code> .	Specify a port that is not in use.
invalid value " <i>specified-character-string</i> " for flag <code>-timeout-offset</code> : parse error	An invalid value was specified to the command line option <code>--timeout-offset</code> .	Review the command line option <code>--timeout-offset</code> specified.
invalid value " <i>specified-value</i> " for flag <code>-timeout-offset</code> : value out of range	A value out of float64 range was specified to the command line option <code>--timeout-offset</code> .	Review the command line option <code>--timeout-offset</code> specified.
<ul style="list-style-type: none"> For Windows open " <i>specified-path</i> ": The system cannot find the file specified. <ul style="list-style-type: none"> For Linux 	The incorrect path has been specified for the command line option <code>--config.file</code> .	Review the command line option <code>--config.file</code> specified.

Message	Cause	Countermeasures
open " <i>specified-path</i> ": no such file or directory		
mapping values are not allowed in this context	Invalid value type for the item found in the file specified for the command line option --config.file.	Check configuration file specifications for invalid line numbers that appear.
Script parameter is missing	The incorrect value has been specified for the name setting in scripts in the Script exporter configuration file (jpc_script_exporter.yml).	Review the content specified for the script.name in the Script exporter configuration file (jpc_script_exporter.yml).
Script not found	The incorrect value has been specified for the script setting in params in the Prometheus configuration file (jpc_prometheus_server.yml).	Review the content specified for the params.script in the Prometheus configuration file (jpc_prometheus_server.yml).
Script config " <i>script-name</i> " has neither 'script' nor 'command'	A value has not been specified the command setting in scripts in the Prometheus configuration file (jpc_script_exporter.yml).	Review the content specified for the scripts.command in the Prometheus configuration file (jpc_script_exporter.yml).
Script failed: exit status 1	Failed to run the script specified for the command setting in scripts in the Script exporter configuration file (jpc_script_exporter.yml).	Review the script specified.
Script ' <i>script-name</i> ' execution failed <ul style="list-style-type: none"> For Windows exec: <i>specified-character-string</i> : file does not exist <ul style="list-style-type: none"> For Linux fork/exec <i>specified-character-string</i> : exec format error	A file that cannot be executed has been specified for the command setting in scripts in the Script exporter configuration file (jpc_script_exporter.yml).	Review the content specified in the Script exporter configuration file (jpc_script_exporter.yml).
Script ' <i>script-name</i> ' execution failed <ul style="list-style-type: none"> For Windows exec: <i>specified-character-string</i> : Access is denied <ul style="list-style-type: none"> For Linux fork/exec <i>specified-character-string</i> : permission denied	A script without execute permissions has been specified for the command setting in scripts in the Script exporter configuration file (jpc_script_exporter.yml).	Change permissions to allow the script specified to be run.
Script ' <i>script-name</i> ' execution failed <ul style="list-style-type: none"> For Windows exec: " <i>specified-character-string</i> ": file does not exist <ul style="list-style-type: none"> For Linux fork/exec: " <i>specified-character-string</i> ": no such file or directory	A script that does not exist has been specified for the command setting in scripts in the Script exporter configuration file (jpc_script_exporter.yml).	Review the content specified for the scripts.command in the Script exporter configuration file (jpc_script_exporter.yml).

Message	Cause	Countermeasures
Script ' <i>script-name</i> ' execution failed <ul style="list-style-type: none"> For Windows exit status 1 <ul style="list-style-type: none"> For Linux signal: killed	Execution of the script timed out.	Review the content specified for the <code>scripts.timeout</code> Script exporter configuration file (<code>jpc_script_exporter.yml</code>).

(11) Logging Fluentd

Message	Cause	Action to be taken
<code>error="tail: 'path' parameter is required on tail input"</code>	In text-formatted log file monitoring definition file, path of the [Input Settings] section was not specified.	Correct text-formatted log file monitoring definition file.
<code>error="Unsupported timezone~"</code>	In text-formatted log file monitoring definition file, an invalid timezone was specified in the [Input Settings] section..	Correct text-formatted log file monitoring definition file.
<code>error="specifying timezone requires time format"</code>	In text-formatted log file monitoring definition file, timezone is specified without specifying the <code>time_format</code> of the [Input Settings] section..	Correct text-formatted log file monitoring definition file.
<code>error="valid options are string, unixtime, float, mixed but got ~"</code>	In text-formatted log file monitoring definition file, an invalid <code>time_type</code> was specified in the [Input Settings] section.	Correct text-formatted log file monitoring definition file.
<code>error="unknown encoding name~"</code>	In text-formatted log file monitoring definition file, an invalid <code>from_encoding</code> was specified in the [Input Settings] section.	Correct text-formatted log file monitoring definition file.
<code>error="No named captures in 'expression' parameter. The regexp must have at least one named capture"</code>	In text-formatted log file monitoring definition file, you specified a regular expression that does not include a named capture (<code>?<NAME> PATTERN</code>) in expression of the [Input Settings] section..	Correct text-formatted log file monitoring definition file.
<code>error="format should be Regexp, need //,~"</code>	In text-formatted log file monitoring definition file, the regular expression is specified without a delimiter (<code>/</code>) in the regular expression for parsing the log in the [Input Settings] section.	Correct text-formatted log file monitoring definition file.
<code>error="valid options are rfc3164, rfc5424, auto but got ~"</code>	In text-formatted log file monitoring definition file, an invalid <code>message_format</code> was specified in the [Input Settings] section.	Correct text-formatted log file monitoring definition file.
<code>error="'with_priority' parameter is required but ~ is specified"</code>	In text-formatted log file monitoring definition file, an invalid <code>with_priority</code> was specified in the [Input Settings] section.	Correct text-formatted log file monitoring definition file.
<code>"valid options are regexp, string but got~"</code>	In text-formatted log file monitoring definition file, an invalid <code>parser_type</code> was specified in the [Input Settings] section.	Correct text-formatted log file monitoring definition file.
<code>error="'support_colonless_ident' parameter</code>	In text-formatted log file monitoring definition file, an incorrect	Correct text-formatted log file monitoring definition file.

Message	Cause	Action to be taken
is required but ~ is specified"	support_colonless_ident was specified in the [Input Settings] section.	
got incomplete JSON array configuration at ~ (Fluent::ConfigParseError)	In text-formatted log file monitoring definition file, a regular expression is specified pattern the [Inclusion Settings] or [Exclusion Settings] section without a delimiter (/).	Correct text-formatted log file monitoring definition file.
error="Plugin 'tail' does not support multi workers configuration (Fluent::Plugin::TailInput)"	In text-formatted log file monitoring definition file, when workers parameter is specified to 2 or more, id of worker is specified more than once. Or, if you specify a workers parameter that is greater than or equal to 2, you did not specify the <worker> directive.	Correct text-formatted log file monitoring definition file.
error="Unknown parser plugin ~. Run 'gem search -rd fluent-plugin' to find plugins"	In text-formatted log file monitoring definition file, an invalid @type was specified for the <parse> directive in the [Input Settings] section.	Correct text-formatted log file monitoring definition file.
error="Invalid Bookmark XML is loaded.~"	In Windows event-log monitoring definition file, an invalid channels was specified in the [Input Settings] section.	Correct Windows event-log monitoring definition file.
error="Plugin 'windows_eventlog2' does not support multi workers configuration (Fluent::Plugin::WindowsEventLog2Input)"	In Windows event-log monitoring definition file, when workers parameter is specified to 2 or more, id of worker is specified more than once. Or, if you specify a workers parameter that is greater than or equal to 2, you did not specify the <worker> directive.	Correct Windows event-log monitoring definition file.
error="valid options are throw_exception,block, drop_oldest_chunk but got~"	In log monitoring common definition file, an invalid overflow_action was specified in the [Output Settings] section.	Correct log monitoring common definition file.
valid options are trace,debug,info,warn,error,fatal but got~ (Fluent::ConfigParseError)	In log monitoring common definition file, an invalid value was specified for log_level in the [System Settings] section.	Correct log monitoring common definition file.
invalid number of workers (must be > 0):0 (Fluent::ConfigError)	In log monitoring common definition file, an invalid workers parameter was specified in the [System Settings] section.	Correct log monitoring common definition file.
error="greater first_worker_id<1> than last_worker_id<0> specified by <worker> directive is not allowed. Available multi worker assign syntax is <smaller_worker_id>-<greater_worker_id>"	In log monitoring common definition file or log metrics definition file, the <worker N-M> directive specifies the number N>M.	Correct log monitoring common definition file and log metrics definition file.
error="worker id ~ specified by <worker> directive	You specified <worker> directive arguments in either log monitoring common definition file, text-formatted log file	Review log monitoring common definition file, text-formatted log file monitoring definition file, Windows

Message	Cause	Action to be taken
is not allowed. Available worker id is between ~"	monitoring definition file, Windows event-log monitoring definition file, or log metrics definition file that are beyond workers parameter. Or, you specify a nonzero id as an argument to the <worker N-M> or <worker> directive without specifying workers parameter.	event-log monitoring definition file, and log metrics definition file.
error="Missing worker id on <worker> directive"	You did not specify id of worker as an argument to the <worker> directive in either log monitoring common definition file, text-formatted log file monitoring definition file, Windows event-log monitoring definition file, or log metrics definition file.	Review log monitoring common definition file, text-formatted log file monitoring definition file, Windows event-log monitoring definition file, and log metrics definition file.
[error]: failed to read data from plugin storage file path=~	Storage file is corrupt.	Remove storage file. Then start it.
Not a directory @ dir_s_mkdir - ~ (Errno::ENOTDIR)	An invalid monitor name was set.	Review the monitor name.

(a) prometheus-client logs

Message	Cause	Countermeasures
metric name must match /[a-zA-Z_][a-zA-Z0-9_]*/ (ArgumentError)	The name field in <metric> in the log metrics definition file is empty.	Specify the name field in <metric> in the log metrics definition file.
docstring must be given (ArgumentError)	The desc field in <metric> in the log metrics definition file is empty.	Specify the desc field in <metric> in the log metrics definition file.
label <i>label-key</i> must not start with __ (Prometheus::Client::LabelSetValidator::ReservedLabelError)	In <labels> in the log metrics definition file, the <i>label-key</i> begins with a __ (two half-width underscore characters).	In <labels> in the log metrics definition file, specify a <i>label-key</i> that does not begin with a __ (two half-width underscore characters).
label name must match /(?-mix:\\A[a-zA-Z_][a-zA-Z0-9_]*\\Z)/ (Prometheus::Client::LabelSetValidator::InvalidLabelError)	In <labels> in the log metrics definition file, the label key does not match the regular expression /(?-mix:\\A[a-zA-Z_][a-zA-Z0-9_]*\\Z)/.	In <labels> in the log metrics definition file, specify a label key that matches the regular expression /(?-mix:\\A[a-zA-Z_][a-zA-Z0-9_]*\\Z)/.

(b) fluent-plugin-prometheus plug-in logs

Message	Cause	Countermeasures
config error file="physical-host-installation-directory/jplima/conf/jpc_fluentd_common.conf" error_class=Fluent::ConfigError error="Missing '@type'"	In <source> in the log metrics definition file, the @type prometheus setting does not exist.	In <source> in the log metrics definition file, specify @type prometheus.

Message	Cause	Countermeasures
parameter on <source> directive"		
config error file=" <i>physical-host-installation-directory</i> / jplima/conf/ jpc_fluentd_common.conf" error_class=Fluent::NotFoundPluginError error="Unknown input plugin ' <i>value-specified-for-@type</i> '. Run 'gem search -rd fluent-plugin' to find plugins"	In <source> in the log metrics definition file, @type is empty, or the <i>value-specified-for-@type</i> is not prometheus.	When using the log metrics feature, in <source> in the log metrics definition file, set @type to prometheus.
#0 unexpected error error_class=SocketError error="getaddrinfo: Name or service not known"	In <source> in the log metrics definition file, bind is an invalid value.	In <source> in the log metrics definition file, specify a value in the correct hostname for bind.
#0 unexpected error error_class=Errno::EADDRNOTAVAIL error="Cannot assign requested address - bind(2) for <i>user-specified-bind</i> : <i>user-specified-port</i> "	In <source> in the log metrics definition file, bind is an invalid format.	In <source> in the log metrics definition file, specify the value for bind in the correct IP address format.
config error file=" <i>physical-host-installation-directory</i> / jplima/conf/ jpc_fluentd_common.conf" error_class=Fluent::ConfigError error="Missing '@type' parameter on <match> directive"	In <match> in the log metrics definition file, the @type prometheus setting does not exist.	In <match> in the log metrics definition file, specify @type prometheus.
config error file=" <i>physical-host-installation-directory</i> / jplima/conf/ jpc_fluentd_common.conf" error_class=Fluent::NotFoundPluginError error="Unknown output plugin ' <i>value-specified-for-@type</i> '. Run 'gem search -rd fluent-plugin' to find plugins"	In <match> in the log metrics definition file, @type is empty, or the <i>value-specified-for-@type</i> is not prometheus.	When using the log metrics feature, in <match> in the log metrics definition file, set @type to prometheus.
section <section-name> is not used in <match> of prometheus plugin	In <match> in the log metrics definition file, the <i>section-name</i> specified is neither of the following: <ul style="list-style-type: none"> metric 	In <match> in the log metrics definition file, specify either of the following for the <i>section-name</i> : <ul style="list-style-type: none"> metric

Message	Cause	Countermeasures
	<ul style="list-style-type: none"> labels 	<ul style="list-style-type: none"> labels
<pre>unmatched end tag at fluentd_<any-name>_logmetrics.conf contents (Fluent::ConfigparseError)</pre>	In the log metrics definition file, either the start or end of the section has not been specified.	<p>Check whether the start and end of the following sections have been defined in the log metrics definition file:</p> <ul style="list-style-type: none"> <source> <parse> <match> <metric> <labels>
parameter ' <i>parameter-name</i> ' in section	In the <i>section</i> in the log metrics definition file, a parameter that cannot be used (<i>parameter-name</i>) has been specified.	In the <i>section</i> in the log metrics definition file, review the parameter (<i>parameter-name</i>) specified.
#0 unknown placeholder ' <i>placeholder</i> ' found	The <i>placeholder</i> set in the label section of the log metrics definition file is not a valid placeholder.	Review the contents of the <i>placeholder</i> set in the label section of the log metrics definition file.
<pre>config error file="physical-host- installation-directory/ jplima/conf/ jpc_fluentd_common.conf" error_class=Fluent::ConfigError error="labels section must have at most 1"</pre>	Multiple <labels> exist in parallel within a single section in the log metrics definition file.	Edit the log metrics definition file so that there is single <labels> entry within a section.
<pre>config error file="physical-host- installation-directory/ jplima/conf/ jpc_fluentd_common.conf" error_class=Fluent::ConfigError error="type option must be 'counter', 'gauge', 'summary' or 'histogram'"</pre>	<p>In the <i>type</i> field in <metric> in the log metrics definition file, characters strings other than those shown below have been specified, or the field has been left blank.</p> <ul style="list-style-type: none"> counter gauge <p>The <i>type</i> field in <metric> in the log metrics definition file does not exist.</p>	<p>Specify either of the following character strings in the <i>type</i> field in <metric> in the log metrics definition file:</p> <ul style="list-style-type: none"> counter gauge
<pre>#0 prometheus: failed to instrument a metric. error_class=ArgumentError error=#<ArgumentError: comparison of String with 0 failed> tag="user-specified-tag" name="user-specified-log- metric-name"</pre>	The counter-type log metric value defined in the log metrics definition file is neither a Ruby Integer nor a Float class value.	In <parse> in the log metrics definition file, verify whether expected log message values are extracted, or whether the expected item is specified in the key field in <metric>.
<pre>#0 prometheus: failed to instrument a metric. error_class=ArgumentError error=#<ArgumentError: value must be a number> tag="user-</pre>	The gauge-type log metric value defined in the log metrics definition file is neither a Ruby Integer nor a Float class value.	In <parse> in the log metrics definition file, verify whether expected log message values are extracted, or whether the expected item is specified in the key field in <metric>.

Message	Cause	Countermeasures
<code>specified-tag" name="user-specified-log-metric-name "</code>		
<pre>#0 prometheus: failed to instrument a metric. error_class=Prometheus::Client::LabelSetValidator::InvalidLabelSetError error=#<Prometheus::Client::LabelSetValidator::InvalidLabelSetError: labels must have the same signature (keys given: [:label-key] vs. keys expected: [:label-key]> tag="user-specified-tag" name="user-specified-log-metric-name"</pre>	In the log metrics definition file, a log metric (<i>user-specified-log-metric-name</i>) with the same name, type, and desc is defined, and these log metrics have different <labels> definitions.	In the log metrics definition file, review the content of all log metric (<i>user-specified-log-metric-name</i>) <labels> definitions.
<pre>config error file="physical-host-installation-directory/ jplima/conf/ jpc_fluentd_common.conf" error_class=Fluent::ConfigError error="metric requires 'name' option"</pre>	The name setting in <metric> in the log metrics definition file does not exist.	Specify the name setting in <metric> in the log metrics definition file.
<pre>config error file="physical-host-installation-directory/ jplima/conf/ jpc_fluentd_common.conf" error_class=Fluent::ConfigError error="metric requires 'desc' option"</pre>	The desc setting in <metric> in the log metrics definition file does not exist.	Specify the desc setting in <metric> in the log metrics definition file.
<pre>config error file="physical-host-installation-directory/ jplima/conf/ jpc_fluentd_common.conf" error_class=Fluent::ConfigError error="gauge metric requires 'key' option"</pre>	Although gauge is specified as the type setting in <metric> in the log metrics definition file, the key setting does not exist.	Specify the key setting in <metric> in the log metrics definition file.
<pre>user-specified-log-metric-name has already been registered as log-metric-type type (Fluent::Plugin::Prometheus::AlreadyRegisteredError)</pre>	In the log metrics definition file, a log metric (<i>user-specified-log-metric-name</i>) with the same name and desc is defined, with different type values specified.	In the log metrics definition file, review the content of all log metric (<i>user-specified-log-metric-name</i>) type definitions.

Message	Cause	Countermeasures
<i>user-specified-log-metric-name</i> has already been registered with different docstring	In the log metrics definition file, a log metric (<i>user-specified-log-metric-name</i>) with the same name and type is defined, with different desc values specified.	In the log metrics definition file, review the content of all log metric (<i>user-specified-log-metric-name</i>) desc definitions.

(12) web_exporter log

Message	Cause	Countermeasures
"KNBC20148-E An operation on files or directories failed. (paths=["JPI/IM-Agent-Installation-destination\jplima\logs\web_exporter\trace\storage-folder-name-of-the-trace-file"], maintenance information = os.Stat,CreateFile JPI/IM-Agent-Installation-destination\jplima\logs\web_exporter\trace\storage-folder-name-of-the-trace-file: The filename, directory name, or volume label syntax is incorrect.)"	The number of characters in the folder name where the trace file is stored exceeds the maximum number of characters in the folder name of 255 characters.	Check the following setting items so that the number of characters in the storage folder name of the trace file is 255 characters or less. <ul style="list-style-type: none"> Name Parameter Settings for Playwright configuration file

See the tables below for Playwright log.

(a) playwright test log

Message	Cause	Countermeasures
Error: No tests found	There is no web scenario file.	Create a web scenario and place it in the correct directory.
	Web scenario file extension is incorrect.	Correct the extension of the Web scenario file.
	Test is not defined in Web scenario file.	Create a Web scenario file and place it in the correct directory.
Error: EPERM: operation not permitted, open 'C:\Users\Administrator\Documents\playwright\tests\im-login-logout.spec.ts' Error: No tests found	You do not have access to the web scenario file.	Check the privileges of the executing user.
SyntaxError: C:\Users\Administrator\Documents\playwright\tests\im-login-logout.spec.ts: Unexpected token (12:0) (omitted) Error: No tests found	The syntax of the web scenario file is incorrect.	Create the web scenario file again.
ReferenceError: xpect is not defined		
Error: locator.click: Test timeout of 30000ms exceeded. Call log: - waiting for getByRole('button', { name: 'xxxx' })	The character code of the web scenario file is incorrect (not UTF-8).	Correct the character code of the web scenario file.
Error: page.goto: net::ERR_CONNECTION_REFUSED at (URL)	The monitored Web service is stopped.	Start the Web service to be monitored and try again.

Message	Cause	Countermeasures
<pre>Error: page.goto: net::ERR_CONNECTION_TIMED_OUT at <URL> Call log: - navigating to "<URL>", waiting until "load" 6 7 test('test', async ({ page }) => { > 8 await page.goto('<URL>'); ^ 9 }); at C:\Program Files\Hitachi\jplima\lib\playwright\tests\ webscenal.spec.ts:8:14, file = C:\Program Files\Hitachi\jplima\lib\playwright\tests\ webscenal.spec.ts, column = 14, line = 8</pre>	The monitored host is stopped.	Start the monitored host and try again.
<p>To determine the success or failure of the login with Playwright test, it is necessary to check (assert) whether the element that is normally displayed on the screen after login is displayed. Therefore, if the login fails, the failure of the screen assertion check after the login operation is output as an error. If the assertion is not performed, the login success or failure is not determined, and even if the login fails, it may be determined that Web scenario was executed successfully.</p> <p>If you specify a definition that asserts that main locator is to be displayed after the login in and the assertion fails, you receive the following error:</p> <pre>Error: Timed out 5000ms waiting for expect(locator).toBeVisible() Locator: getByRole('main') Expected: visible Received: hidden Call log: - expect.toBeVisible with timeout 5000ms - waiting for getByRole('main') 7 await page.locator('input[name="password"]').fil l('pass'); 8 await page.getByRole('button', { name: 'login' }).click(); > 9 await expect(page.getByRole('main')).toBeVisibl e(); ^ 10 await page.getByRole('button', { name: 'logout' }).click(); 11 await expect(page.locator('#login- wave-bg')).toBeVisible(); 12 }); at C:\Users\Administrator\Documents\playwrigh t\tests\im-login-logout.spec.ts:9:40</pre>	Logon operations on the login window (entering a user name and password, clicking the log In button) fail.	Check the cause of the login failure.
	HTTP authentication (Basic authentication) fails.	Check the cause of authentication failure.
<pre>Error: page.goto: net::ERR_BAD_SSL_CLIENT_AUTH_CERT at https://ip-10-0-70-12/formauth/ Call log:</pre>	The certificate is incomplete (TLS client authentication fails).	Check whether the client certificate or registry key settings are correct.

Message	Cause	Countermeasures
- navigating to "https://ip-10-0-70-12/formauth/", waiting until "load"		
<pre>Error: page.goto: net::ERR_CERT_COMMON_NAME_INVALID at <URL1> Call log: - navigating to \"<URL1>\", waiting until \"load\" 6 7 test('test', async ({ page }) => { > 8 await page.goto('<URL1>'); ^ 9 await page.goto('<URL2>'); 10 await expect(page.getByRole('button', { name: 'login' })).toBeVisible(); 11 }); at C:\Program Files\Hitachi\jplima\lib\playwright\tests\ webscenal.spec.ts:8:14, file = C:\Program Files\Hitachi\jplima\lib\playwright\tests\ webscenal.spec.ts, column = 14, line = 8)"</pre>	The certificate is incomplete (TLS server authentication fails).	Check whether the settings of the server certificate are correct.
<pre>Error: browser.newContext: Browser needs to be launched with the global proxy. If all contexts override the proxy, global proxy will be never used and can be any string, for example \"launch({ proxy: { server: 'http://per- context' } })\", file = , column = 0, line = 0</pre>	In Playwright configuration file, use.proxy parameter is specified but use.launchOptions.proxy.server is not specified.	Add a proxy.server entry in launchOptions.
<pre>Error: page.goto: net::ERR_PROXY_CONNECTION_FAILED at https://ip-10-0-70-12/formauth/ Call log: - navigating to \"<URL>\", waiting until \"load\" 6 7 test('test', async ({ page }) => { > 8 await page.goto('<URL>'); ^ 9 }); at C:\Program Files\Hitachi\jplima\lib\playwright\tests\ webscenal.spec.ts:8:14, file = C:\Program Files\Hitachi\jplima\lib\playwright\tests\ webscenal.spec.ts, column = 14, line = 8</pre>	The proxy service specified in the use.proxy parameter in the Playwright configuration file is down.	Start the proxy service.
<pre>Error: page.goto: net::ERR_TIMED_OUT at https://ip-10-0-70-12/formauth/ Call log: - navigating to \"<URL>\", waiting until \"load\" 6 7 test('test', async ({ page }) => { > 8 await page.goto('<URL>'); ^</pre>	In Playwright configuration file, use.proxy parameter is specified but use.launchOptions.proxy.server is not specified.	Start the proxy host.

Message	Cause	Countermeasures
<pre> 9 }); at C:\Program Files\Hitachi\jplima\lib\playwright\tests\ webscenal.spec.ts:8:14, file = C:\Program Files\Hitachi\jplima\lib\playwright\tests\ webscenal.spec.ts, column = 14, line = 8 </pre>		
<pre> Error: page.goto: net::ERR_HTTP_RESPONSE_CODE_FAILURE at <URL> Call log: - navigating to "<URL>", waiting until "load" 6 7 test('test', async ({ page }) => { > 8 await page.goto('<URL>'); ^ 9 }); at C:\Program Files\Hitachi\jplima\lib\playwright\tests\ webscenal.spec.ts:8:14, file = C:\Program Files\Hitachi\jplima\lib\playwright\tests\ webscenal.spec.ts, column = 14, line = 8 </pre>	<p>Basic authentication of the proxies specified in the use.proxy parameter in the Playwright configuration file fails.</p>	<p>Check whether the username and password specified in use.proxy parameter are correct.</p>

(b) playwright codegen log

Message	Cause	Countermeasures
<pre> Error: t.parse: Executable doesn't exist at C:\Users\Administrator\AppData\Local\ms- playwright\chromium-1105\chrome- win\chrome.exe +-----+ -----+ Looks like Playwright Test or Playwright was just installed or updated. Please run the following command to download new browsers: npx playwright install <3 Playwright Team +-----+ -----+ </pre>	<p>The browser used by Codegen is not installed.</p>	<p>Install the prerequisite browser for Web scenario monitoring function</p>

(c) playwright show-trace log

Message	Cause	Countermeasures
<pre> Could not load trace from ./tests. Make sure a valid Playwright Trace is accessible over this url. Drop Playwright Trace to load or Select file(s) </pre>	<p>The specified trace file cannot be opened, or the path of the trace file is incorrect.</p>	<p>Click Select file(s) to start Explorer and select a trace file.</p>

(13) vmware_exporter log

Message	Cause	Countermeasures
'Error creating vcenter API session ({}).format(e)	<ul style="list-style-type: none">• Incorrect access-information creation (IP address/username/password is incorrect)• Incomplete certificate	Review the command line options.
"Error, you must have a default section in config file (for now) " Additional Notes Together with the above log, two Traceback logs related to exit and message are output as a log of the existing OSS, but this is resolved by addressing to this message.	"default" is not defined in the config file.	Define "default" in the config file and run again.

12.5.2 What happens and how to recover from major input errors

(1) Prometheus server scrape specified an incorrect host or port

Phenomenon

Scrape fails and the UP metric is collected as 0.

The latest information is not displayed in the TRE information of the integrated operation viewer for data acquired via the Prometheus server with incorrect scrape destination settings.

Recovery methods

Correct the scrape definition and reload or restart the Prometheus server.

(2) You specified an incorrect host or port as the remote write destination of the Prometheus server

Phenomenon

The latest information is not displayed in the TRE information of the integrated operation viewer for data acquired via the Prometheus server with incorrect remote light destination settings.

Recovery methods

Correct the remote write definition and reload or restart the Prometheus server.

(3) You specified an incorrect host or port as the Prometheus server alert notification destination.

Phenomenon

Regarding alerts generated from Prometheus server with incorrect alert notification destination settings, the latest information is not displayed in the JP1 event list of the integrated operation viewer.

Recovery methods

Correct the notification destination definition and reload or restart the Prometheus server.

(4) You specified an incorrect host or port as the Alertmanager notification destination

Phenomenon

Regarding alerts sent from Alertmanager with incorrect notification destination settings, the latest information is not displayed in the JP1 event list of the integrated operation viewer.

Recovery methods

Correct the notification destination definition and reload or restart Alertmanager.

(5) Blackbox exporter has specified an incorrect host or port to monitor

Phenomenon

Acquisition of monitoring destination information fails, and `probe_success` metric is collected as 0.

Recovery methods

Correct the monitored host and port definitions and reload or restart the Prometheus server.

(6) Prometheus server definition file format is incorrect

Phenomenon

When the Prometheus server reload API is executed, the STAY code 500 is returned and the following message is displayed:

```
failed to reload config: couldn't load configuration (--config.file="file-path"): parsing YAML file file-path: yaml: unmarshal errors: line line-number: field test not found in type config.plain
```

Recovery methods

Check the `file-path` and `line-number` in the message, correct the definitions, and reload or restart the Prometheus server.

(7) Incorrect format of discovery configuration file

Phenomenon

Despite successful execution of the `jddcreatetree` and `jddupdatetree` commands, the IM management node with the information described in the discovery configuration file is not displayed in the integrated operation viewer.

Recovery methods

Check whether the format of the discovery configuration file is correct, such as specifying colons and making sure that the number of half-width spaces is correct. After correcting the error, run the `jddcreatetree` and `jddupdatetree` commands (specify configuration change mode (`-c` option)) again).

(8) Log monitoring common definition file format is invalid

Description

For `path` parameter in the `<buffer>` directive in log monitoring common definition file (`jpc_fluentd_common.conf`), if a pathname greater than 256 bytes is specified, or a path with `:`, `,`, `;`, `*`, `?`, `"`, `<`, `>`, `|`, tabs, or spaces is specified, it will continue to be logged repeatedly with the following error in fluentd:

```
unexpected error error_class = Errno::ENOENT error="No such file or directory @ dir_s_mkdir - directory-name "
```

Corrective action

Verify that log monitoring common definition file (jpc_fluentd_common.conf) <buffer> directive contains the correct path parameter format and settings.

(9) Text-formatted log file monitoring definition file format is invalid

Description

If the `pos_file` parameter in the [Input Settings] section of text-formatted log file monitoring definition file (fluentd_@@trapname@@_tail.conf) is specified to be blank or string exceeds the upper limit of OS filename, it will continue to be logged with the following repetition in fluentd:

```
unexpected error error_class = Errno::ENOENT error="No such file or directory @ rb_sysopen - directory-name "
```

Corrective action

For the `pos_file` parameter in the [Input Settings] section of text-formatted log file monitoring definition file (fluentd_@@trapname@@_tail.conf), make sure that the format and settings are correct.

(10) Script exporter executed a script that does not exist

Result

The `script_success` metric is collected as 0. In addition, the `script_exit_code` metric is collected as -1.

Recovery method

Correct the definition, and then reload or restart Script exporter.

(11) An invalid host and port were specified for Promitor Scaper Resource Discovery

Result

No metric acquired from Resource Discovery.

Recovery method

Correct the definition, and then reload or restart the Promitor Scaper.

12.5.3 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 JPI/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 *JPI/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 9.4.4(3)(c) *Environment for command execution* in the *JP1/Integrated Management 3 - 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\jp1base\log\COMMAND`)
`Jischk -13 Base-path\log\COMMAND\ACTISAMLOGV8`
- In UNIX

Execute the following command:

```
cd /var/opt/jp1base/log/COMMAND
```

(For a logical host: cd *shared-directory*/jp1base/log/COMMAND)

```
/opt/jp1base/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*\jp1base\log\COMMAND)

```
Jischk -l3 Base-path\log\COMMAND\CMDISAMLOGV8
```

- In UNIX

Execute the following command:

```
cd /var/opt/jp1base/log/COMMAND
```

(For a logical host: cd *shared-directory*/jp1base/log/COMMAND)

```
/opt/jp1base/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 *JP1/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 *JP1/Base User's Guide*.

```
cd Base-path\log\COMMAND
```

(For a logical host: cd *shared-folder*\jp1base\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/jp1base/log/COMMAND
```

(For a logical host: `cd shared-directory/jp1base/log/COMMAND`)

```
/opt/jp1base/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/jp1base/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\jp1base\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 12–29: 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 12–30: 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/jp1base/log/COMMAND/actisamlogv8.DAT • /var/opt/jp1base/log/COMMAND/actisamlogv8.K01

File name	Location
	<ul style="list-style-type: none"> • /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 12–31: 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 12–32: 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 • <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 12–33: 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 12–34: 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
Command execution log file	All files under /var/opt/jplbase/log/COMMAND/
	All files under <i>shared-directory</i> /jplbase/log/COMMAND/

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 [8.1.4 Checking command execution status and deleting a command](#) in this manual, and see [9.4.4\(6\) Commands for troubleshooting in the JP1/Integrated Management 3 - 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 [9.4.8 JP1/Base health check function](#) in the [JP1/Integrated Management 3 - 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 [14.7.6 Command execution environment](#) in the [JP1/Integrated Management 3 - 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 `jcshostsimport -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_spmd_status` command to make sure the `jcsmain` process is not active.
2. Execute the `Jismlocktr` 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 `Jismlocktr` 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 `jcccmddef` 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 12–35: 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 12–36: 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 `jcccmddef` 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: *1.19.7(1) Executing the Central Scope upgrade command* in the *JP1/Integrated Management 3 - Manager Configuration Guide*
UNIX: *2.18.11(2) Executing the Central Scope upgrade command* in the *JP1/Integrated Management 3 - Manager Configuration Guide*
- For a logical host
Windows: *7.6 Upgrade installation and setup of logical hosts (for Windows)* in the *JP1/Integrated Management 3 - Manager Configuration Guide*
UNIX: *8.6 Upgrade installation and setup of logical hosts (for UNIX)* in the *JP1/Integrated Management 3 - 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_spmd_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_spmd_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_spmd_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_spmd_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/jplscope/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 `jplhosts` information or the `jplhosts2` 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 3 - 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 JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*. For details about the `hosts` setting of the OS, see *14.4.1 Host names and IP addresses in the JP1/Integrated Management 3 - 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 *12.5.3(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 *5.2.3 Status change conditions in the JP1/Integrated Management 3 - 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 *JP1/Integrated Management 3 - Manager Command, Definition File and API 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.4 Operating permissions required for IM Configuration Management* in the *JP1/Integrated Management 3 - 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 *1.18.2 NetBIOS settings (NetBIOS over TCP/IP) (for Windows)* in the *JP1/Integrated Management 3 - 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 *2.17.1 Configuring SSH (for UNIX)* in the *JP1/Integrated Management 3 - 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 *12.5.3(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>12.3.1(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.
Windows application and system event logs	<ol style="list-style-type: none"> 1. Select the target event log from Event Viewer.

Data to be collected	Method
	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 3 - 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 *JP1/Integrated Management 3 - 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 *12.5.3(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 *12.5.3(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 5-31 Items additionally displayed on the Configuration File page (when an item under Log File Trapping selected)* in *5.9.2 Configuration File page* in the *JP1/Integrated Management 3 - 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 3 - Manager Configuration Guide*:

- *1.18.1 Configuring WMI (for Windows)*
- *1.18.2 NetBIOS settings (NetBIOS over TCP/IP) (for Windows)*
- *1.18.3 Configuring SSH (for Windows)*

When the JP1/IM - Manager host is a UNIX host:

2.17.1 Configuring SSH (for UNIX) in the *JP1/Integrated Management 3 - 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_spm�_status (for a logical host: jbs_spm�_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 [12.5.3\(51\) 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 *14.3.10(2)(b) Changing JP1 event attributes (Setting for JP1/IM - Manager)* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

- For 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 `jbssetcnf` 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 *12.5.3(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.

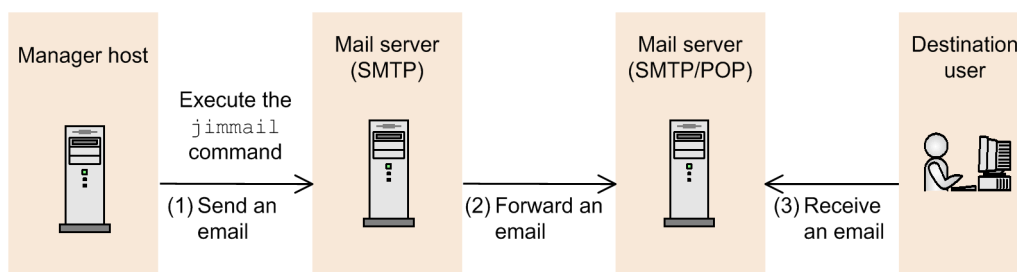
JP1/IM - Manager interprets JP1/SES-format events by using the character encoding that JP1/IM - Manager uses to operate. Therefore, if the character encoding of a JP1/SES-format event is different from the JP1/IM - Manager encoding, the displayed JP1/SES-format event might be unreadable or contain some 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 *JP1/Integrated Management 3 - 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\JMn
set PDUXPLDIR=%PDDIR%\UXPLDIR
```

2. Execute the following command to display the IM database log:

```
IM-database-service-installation-directory\JMn\bin\pdcat
```

- In Linux

1. Execute the following command to set up environment variables:

```
export PDDIR=IM-database-service-installation-directory/JMn
export LD_LIBRARY_PATH=$PDDIR/lib/:$LD_LIBRARY_PATH
```

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 `jimdbupdate` 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 `jcodbsetup` 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 `jbsetcnf` 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 JP1/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 `jp1convn.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 `jp1convn.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 `jp1convMn.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 `jp1convMn.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 JP1/IM - View environment settings; this value is fixed.

"JP1COVIEW_LOGSIZE"=`dword:hexadecimal-value`

Specifies the maximum size of the `jp1csov[_old].log` file for the process-specific trace log.

Specify a hexadecimal value in bytes 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 `jp1csovM[_old].log` file for the process-specific trace log.

Specify a hexadecimal value in bytes 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\jp1\jp1_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 *JP1/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.

(64) Actions to take when JP1/IM - View does not start

When JP1/IM - View starts, a contiguous memory space is allocated as the Java heap space. This allocation requires a contiguous space. Depending on the condition of the memory used in your environment, the attempt to allocate the Java heap space might fail and JP1/IM - View might not start.

If the Login window does not appear when you attempt to start JP1/IM - View, take the action shown below.

Corrective action:

1. Make a backup copy of the following file and save it to your working folder: *JP1/IM - View-installation-folder\conf\jcoview.conf*.
2. In a text editor, open the following file: *JP1/IM - View-installationfolder\conf\jcoview.conf*. Next, change the value of the `-Xmx` option so that the resulting value is the current value minus 100.

Example change:

Before change

```
[JavaVM]
Options=-Xms32m -Xmx768m -Dsun.java2d.noddraw=true
```

After change

```
[JavaVM]
Options=-Xms32m -Xmx668m -Dsun.java2d.noddraw=true
```

3. Start JP1/IM - View.
4. If JP1/IM - View starts, proceed to step 5.
If JP1/IM - View cannot be started, go back to step 2. to further decrease the value of the `-Xmx` option by 100, and then proceed to step 3..

- Repeat steps 2. and 3. until JP1/IM - View starts successfully.
5. Terminate JP1/IM - View.
 6. In a text editor, open the following file: *JP1/IM - View-installationfolder\conf\jcoview.conf*. Next, change the value of the `-Xmx` option so that the resulting value is the current value plus 12.
 7. Start JP1/IM - View.
 8. If JP1/IM - View starts, go back to steps 5. and 6. to further increase the value of the `-Xmx` option by 12, and then proceed to step 7..
- Repeat steps 5., 6., and 7. until it is confirmed that JP1/IM - View cannot be started.
- If JP1/IM - View cannot be started, change the current value of the `-Xmx` option back to the value that was used the last time JP1/IM - View was started.
- The resulting value of the `-Xmx` option is the maximum size of the Java heap space that can be allocated by JP1/IM - View in your environment.

(65) Action to taken when IM configuration management successfully collects host information but fails to collect profiles

The message KNAN22403-E: Acquisition of the profile list failed. (Detail Information: A communication error occurred.) *is displayed.*

Cause 1

A firewall is blocking communications that are necessary for profile collection.

Corrective action 1

Make sure that the settings allow communications to and from the `jp1bscom` service.

For details, see the explanations in the *JP1/Base User's Guide* about the Port numbers for JP1/Base, and about the Direction in which data passes through the firewall.

Cause 2

If JP1/IM is operated in one of the following ways, communication from the agent host to the manager host (duplicate communication) fails.

- When the IP bind method is used for separated networks (when `physical_ipany.conf` or `logical_ipany.conf` is applied)
- When the address is converted (NAT) between the manager and agent hosts

Corrective action 2

If name resolution is not set up to be performed via duplicate communication protocol using IM configuration management:

Specify settings so that name resolution is performed via duplicate communication protocol using IM configuration management.

For details, see the explanation in the *JP1/Base User's Guide* on Setting a duplicate communication protocol using IM configuration management.

If name resolution is set up to be performed via duplicate communication protocol using IM configuration management:

Specify settings so that the agent host is able to resolve the name of the manager host. In addition, specify settings so that the IP address of the manager host for which the agent host performed name resolution matches the IP address to which the JP1/Base instance of the manager host is bound.

For details, see the explanation in the *JP1/Base User's Guide* on Setting a duplicate communication protocol using IM configuration management.

(66) Actions to take when the configuration of linked JP1/AJS is not displayed in the integrated operation viewer

If the configuration of JP1/AJS that has been linked with JP1/IM - Manager (Intelligent Integrated Management Base) is not displayed in the integrated operation viewer, take the action shown below.

Cause

A nonexistent file is specified for the `cmdpath` attribute in the adapter command settings file.

Corrective action

Review the setting of the `cmdpath` attribute in the adapter command settings file.

For details about the `cmdpath` attribute, see *Chapter 4. User-created Plug-ins* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

(67) How to respond if the KNAN11199-E message is output after executing the `jimdbupdate` command, or if the IM database cannot start after executing the `jimdbupdate` command

The message "KNAN11199-E Failed to update the IM database service." is output after executing the `jimdbupdate` command, or the IM database cannot start after executing the `jimdbupdate` command.

Cause

Open the following file in text editor, and then check the text on line 14.

For Windows

- On physical host
`value-of-setup-information-file-IMDBENVDIR\JM0\CONF\pdsys`
- On logical host
`value-of-IMDBENVDIR-for-cluster-setup-information-file\JMn#\CONF\pdsys`

#: *n* is the LOGICALHOSTNUMBER value of cluster setup information file

For UNIX

- On physical host
`value-of-setup-information-file-IMDBENVDIR/JM0/conf/pdsys`
- On logical host
`value-of-IMDBENVDIR-for-cluster-setup-information-file/JMn#/conf/pdsys`

#: *n* is the LOGICALHOSTNUMBER value of cluster setup information file

If the text on line 14 is "`set pd_max_users = 96`", this could be due to the following causes.

- After the `jimdbupdate` command output the following messages and then ended, either the `jimdbupdate` command was re-executed or the IM database started.
`KNAN11034-E An attempt to stop the IM database service has failed.`
`KNAN11199-E Failed to update the IM database service.`
- A procedure that differs from the IM database update procedure listed in the *JP1/Integrated Management 3 - Manager Configuration Guide* was performed.

Corrective action

For Windows

If the problem occurred on a physical host, perform the following steps. You do not need to re-execute the `jimdbupdate` command after the steps have been completed.

1. Execute the `jimdbstop` command (with the `-f` option specified), and then stop the IM database.

```
jimdbstop -f
```

Check that one of the following messages has been output.

```
KNAN11186-I Processing to stop the IM database service ended normally.
```

```
KNAN11183-I The IM database service is stopped.
```

```
KNAN11046-E The service JP1/IM3-Manager DB Server is not running.
```

2. Open the following file using text editor.

```
value-of-setup-information-file-IMDBENVDIR\JM0\CONF\pdsys
```

3. Inside the file opened in step 2, change the value of line 14 (`set pd_max_users`) to the following value and save the file.

(Before change)

```
set pd_max_users = 96
```

(After change)

```
set pd_max_users = 32
```

4. Start JP1/IM3-Manager DB Server service.

5. Execute the `jimdbstatus` command, and then check that the IM database service is operational.

```
jimdbstatus
```

The KNAN11182-I message is output.

```
KNAN11182-I The IM database service is running.
```

If the IM database service is not operational, execute the `jimdbstatus` command every 10 seconds, and then wait until the service is operational.

6. Stop JP1/IM3-Manager DB Server service.

7. Reopen the file opened in step 2 using text editor.

8. Inside the file opened in step 7, change the value of line 14 (`set pd_max_users`) to the following value and save the file.

(Before change)

```
set pd_max_users = 32
```

(After change)

```
set pd_max_users = 96
```

9. Start JP1/IM3-Manager DB Server service.

10. Start JP1/IM3-Manager service.

If the problem occurred on a logical host in a cluster system, perform the following steps. You do not need to re-execute the `jimdbupdate` command after the steps have been completed.

1. By operating the cluster software, place the following services offline and make sure that the following services were stopped on both active host and standby host. If the services are running, stop the services.

- JP1/IM3 - Manager Service on the logical host (service name that is displayed: `JP1/IM3-Manager_logical-hostname`)

- JP1/IM3 - Manager DB Cluster Service on the logical host (service name that is displayed: JP1/IM3-Manager DB ClusterService_ *logical-host-name*)
 - The IM database service on the logical host (service name that is displayed: JP1/IM3-Manager DB Server_ *logical-host-name*)
2. On the active host, start the following service from the service window of the OS:
The IM database service on the logical host (service name that is displayed: JP1/IM3-Manager DB Server_ *logical-host-name*)
 3. On the active host, execute the `jimdbstop` command to stop the IM databases.
`jimdbstop -f -h logical-host-name`
Check that one of the following messages has been output.
KNAN11186-I Processing to stop the IM database service ended normally.
KNAN11183-I The IM database service is stopped.
 4. On active host, open the following file using text editor.
`value-of-IMDBENVDIR-for-cluster-setup-information-file\JMn#\CONF\pdsys`
#: *n* is the LOGICALHOSTNUMBER value of cluster setup information file
 5. Inside the file opened in step 4, change the value of line 14 (`set pd_max_users`) to the following value and save the file.
(Before change)
`set pd_max_users = 96`
(After change)
`set pd_max_users = 32`
 6. On the active host, start the following service from the service window of the OS:
JP1/IM3 - Manager DB Cluster Service on the logical host (service name that is displayed: JP1/IM3-Manager DB Cluster Service_ *logical-host-name*)
 7. On the active host, execute the `jimdbstatus` command, and then check that the IM database service is operational.
`jimdbstatus -h logical-host-name`
The KNAN11182-I message is output.
KNAN11182-I The IM database service is running.
If the IM database service is not operational, execute the `jimdbstatus` command every 10 seconds, and then wait until the service is operational.
 8. On the active host, execute the `jimdbstop` command to stop the IM databases.
`jimdbstop -h logical-host-name`
Check that KNAN11186-I message has been output.
KNAN11186-I Processing to stop the IM database service ended normally.
 9. On the active host, stop the following service from the service window of the OS by order:
 - JP1/IM3 - Manager DB Cluster Service on the logical host (service name that is displayed: JP1/IM3-Manager DB Cluster Service_ *logical-host-name*)
 - The IM database service on the logical host (service name that is displayed: JP1/IM3-Manager DB Server_ *logical-host-name*)
 10. On active host, reopen the file opened in step 4 using text editor.
 11. Inside the file opened in step 10, change the value of line 14 (`set pd_max_users`) to the following value and save the file.

(Before change)

```
set pd_max_users = 32
```

(After change)

```
set pd_max_users = 96
```

12. In addition to transferring the shared disk and the logical IP address assigned to the active host to the standby host, make sure that the shared disk and the logical IP address can be used on the logical host.

13. On the standby host, start the following service from the service window of the OS:

The IM database service on the logical host (service name that is displayed: JP1/IM3-Manager DB Server_ *logical-host-name*)

14. On the standby host, execute the `jimdbstop` command to stop the IM databases.

```
jimdbstop -f -h logical-host-name
```

Check that one of the following messages has been output.

```
KNAN11186-I Processing to stop the IM database service ended normally.
```

```
KNAN11183-I The IM database service is stopped.
```

15. On the standby host, start the following service from the service window of the OS:

JP1/IM3 - Manager DB Cluster Service on the logical host (service name that is displayed: JP1/IM3-Manager DB Cluster Service_ *logical-host-name*)

If the service started successfully, perform step 24 after stopping the following services from the service window of the OS:

- JP1/IM3 - Manager DB Cluster Service on the logical host (service name that is displayed: JP1/IM3-Manager DB Cluster Service_ *logical-host-name*)

- The IM database service on the logical host (service name that is displayed: JP1/IM3-Manager DB Server_ *logical-host-name*)

If the service failed to start, perform the procedure beginning with step 16.

16. On standby host, open the following file using text editor.

```
value-of-IMDBENVDIR-for-cluster-setup-information-file\JMn#\CONF\pdsys
```

#: *n* is the LOGICALHOSTNUMBER value of cluster setup information file

17. Inside the file opened in step 16, change the value of line 14 (`set pd_max_users`) to the following value and save the file.

(Before change)

```
set pd_max_users = 96
```

(After change)

```
set pd_max_users = 32
```

18. On the standby host, start the following service from the service window of the OS:

JP1/IM3 - Manager DB Cluster Service on the logical host (service name that is displayed: JP1/IM3-Manager DB Cluster Service_ *logical-host-name*)

19. On the standby host, execute the `jimdbstatus` command, and then check that the IM database service is operational.

```
jimdbstatus -h logical-host-name
```

The KNAN11182-I message is output.

```
KNAN11182-I The IM database service is running.
```

If the IM database service is not operational, execute the `jimdbstatus` command every 10 seconds, and then wait until the service is operational.

20. On the standby host, execute the `jimdbstop` command to stop the IM databases.


```
jimdbstop -h logical-host-name
```

 Check that KNAN11186-I message has been output.


```
KNAN11186-I Processing to stop the IM database service ended normally.
```
21. On the standby host, stop the following service from the service window of the OS by order:
 - JP1/IM3 - Manager DB Cluster Service on the logical host (service name that is displayed: JP1/IM3-Manager DB Cluster Service_*logical-host-name*)
 - The IM database service on the logical host (service name that is displayed: JP1/IM3-Manager DB Server_*logical-host-name*)
22. On standby host, reopen the file opened in step 16 using text editor.
23. Inside the file opened in step 22, change the value of line 14 (`set pd_max_users`) to the following value and save the file.

(Before change)

```
set pd_max_users = 32
```

(After change)

```
set pd_max_users = 96
```
24. In addition to transferring the shared disk and the logical IP address assigned to the standby host to the active host, make sure that the shared disk and the logical IP address can be used on the logical host.
25. By operating the cluster software on the active host, place the following services online and start them by order:
 - The IM database service on the logical host (service name that is displayed: JP1/IM3-Manager DB Server_*logical-host-name*)
 - JP1/IM3 - Manager DB Cluster Service on the logical host (service name that is displayed: JP1/IM3-Manager DB Cluster Service_*logical-host-name*)
 - JP1/IM3 - Manager Service on the logical host (service name that is displayed: JP1/IM3-Manager_*logical-host-name*)

For Linux

If the problem occurred on a physical host, perform the following steps. You do not need to re-execute the `jimdbupdate` command after the steps have been completed.

1. Execute the `jimdbstop` command (with the `-f` option specified), and then stop the IM database.


```
jimdbstop -f
```

 Check that KNAN11186-I or KNAN11183-I message has been output.


```
KNAN11186-I Processing to stop the IM database service ended normally.  
KNAN11183-I The IM database service is stopped.
```
2. Open the following file using text editor.


```
value-of-setup-information-file-IMDBENVDIR/JM0/conf/pdsys
```
3. Inside the file opened in step 2, change the value of line 14 (`set pd_max_users`) to the following value and save the file.

(Before change)

```
set pd_max_users = 96
```

(After change)

```
set pd_max_users = 32
```
4. Execute `jimdbstart` command in `/opt/jp1imm/bin/imdb` to start the IM database.

```
jimdbstart
```

- Execute the `jimdbstatus` command, and then check that the IM database service is operational.

```
jimdbstatus
```

The KNAN11182-I message is output.

```
KNAN11182-I The IM database service is running.
```

If the IM database service is not operational, execute the `jimdbstatus` command every 10 seconds, and then wait until the service is operational.

- Execute the `jimdbstop` command (without option) to stop the IM databases.

```
jimdbstop
```

Check that KNAN11186-I message has been output.

```
KNAN11186-I Processing to stop the IM database service ended normally.
```

- Reopen the file opened in step 2 using text editor.

- Inside the file opened in step 7, change the value of line 14 (`set pd_max_users`) to the following value and save the file.

(Before change)

```
set pd_max_users = 32
```

(After change)

```
set pd_max_users = 96
```

- Start JP1/IM - Manager.

If the problem occurred on a logical host in a cluster system, perform the following steps. You do not need to re-execute the `jimdbupdate` command after the steps have been completed.

- Check that the active logical hosts' JP1/IM - Manager have stopped. If JP1/IM2 - Manager has started, make sure to stop it.
- On the active host, execute the `jimdbstop` command to stop the IM databases.

```
jimdbstop -f -h logical-host-name
```

Check that KNAN11186-I or KNAN11183-I message has been output.

```
KNAN11186-I Processing to stop the IM database service ended normally.
```

```
KNAN11183-I The IM database service is stopped.
```

- On active host, open the following file using text editor.

```
value-of-IMDBENVDIR-for-cluster-setup-information-file/JMn#/conf/pdsys
```

#: *n* is the LOGICALHOSTNUMBER value of cluster setup information file.

- Inside the file opened in step 3, change the value of line 14 (`set pd_max_users`) to the following value and save the file.

(Before change)

```
set pd_max_users = 96
```

(After change)

```
set pd_max_users = 32
```

- On active host, execute `jimdbstart` command in `/opt/jp1imm/bin/imdb` to start the IM database.

```
jimdbstart -h logical-host-name
```

- On the active host, execute the `jimdbstatus` command, and then check that the IM database service is operational.

```
jimdbstatus -h logical-host-name
```

The KNAN11182-I message is output.

KNAN11182-I The IM database service is running.

If the IM database service is not operational, execute the `jimdbstatus` command every 10 seconds, and then wait until the service is operational.

7. On the active host, execute the `jimdbstop` command to stop the IM databases.

```
jimdbstop -f -h logical-host-name
```

Check that KNAN11186-I message has been output.

KNAN11186-I Processing to stop the IM database service ended normally.

8. On active host, reopen the file opened in step 3 using text editor.

9. Inside the file opened in step 8, change the value of line 14 (`set pd_max_users`) to the following value and save the file.

(Before change)

```
set pd_max_users = 32
```

(After change)

```
set pd_max_users = 96
```

10. In addition to transferring the shared disk and the logical IP address assigned to the active host to the standby host, make sure that the shared disk and the logical IP address can be used on the logical host.

11. On the standby host, execute the `jimdbstop` command to stop the IM databases.

```
jimdbstop -f -h logical-host-name
```

Check that KNAN11186-I or KNAN11183-I message has been output.

KNAN11186-I Processing to stop the IM database service ended normally.

KNAN11183-I The IM database service is stopped.

12. On standby host, execute `jimdbstart` command in `/opt/jplimm/bin/imdb` to start the IM database.

```
jimdbstart -h logical-host-name
```

- If the following message is output, perform step 11 again. After stopping the IM database, perform step 20.

KNAN11180-I Processing to start the IM database service ended normally.

- If the following message is output, perform the procedure beginning with step 13.

KNAN11035-E An attempt to start the IM database service has failed.

13. On standby host, open the following file using text editor.

```
value-of-IMDBENVDIR-for-cluster-setup-information-file/JMn#/conf/pdsys
```

#: *n* is the LOGICALHOSTNUMBER value of cluster setup information file.

14. Inside the file opened in step 13, change the value of line 14 (`set pd_max_users`) to the following value and save the file.

(Before change)

```
set pd_max_users = 96
```

(After change)

```
set pd_max_users = 32
```

15. On standby host, execute `jimdbstart` command in `/opt/jplimm/bin/imdb` to start the IM database.

```
jimdbstart -h logical-host-name
```

16. On the standby host, execute the `jimdbstatus` command, and then check that the IM database service is operational.

```
jimdbstatus -h logical-host-name
```


The KNAN11182-I message is output.

KNAN11182-I The IM database service is running.

If the IM database service is not operational, execute the `jimdbstatus` command every 10 seconds, and then wait until the service is operational.

17. On the standby host, execute the `jimdbstop` command to stop the IM databases.

```
jimdbstop -f -h logical-host-name
```

Check that KNAN11186-I message has been output.

KNAN11186-I Processing to stop the IM database service ended normally.

18. On standby host, reopen the file opened in step 12 using text editor.

19. Inside the file opened in step 18, change the value of line 14 (`set pd_max_users`) to the following value and save the file.

(Before change)

```
set pd_max_users = 32
```

(After change)

```
set pd_max_users = 96
```

20. In addition to transferring the shared disk and the logical IP address assigned to the standby host to the active host, make sure that the shared disk and the logical IP address can be used on the logical host.

21. By operating the cluster software on the active host, start JP1/IM - Manager on the logical host.

(68) How to respond if the `__configurationGet` method is not executed in your user-created plug-in

If the `__configurationGet` method is not executed in your user-created plug-in, check if the adapter command settings file is saved in the ASCII character code.

For details about the adapter command settings file, see *7.3.2 Adapter command settings file* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

(69) What to do if updating IM database with `jimdbupdate` command fails and a KNAN11215-E message is displayed

The message "KNAN11215-E Failed to update the IM database service. Try again from the version update step." is displayed.

Cause

The following factors can occur:

- When updating IM database, an error occurred due to insufficient memory, file locking, etc., and IM database update has failed and is in an invalid status.

Corrective Action

Take appropriate action according to the cause.

- If an error message was output prior to KNAN11215-E message, take appropriate action for the message. After taking corrective action, restore JP1/Base and JP1/IM - Manager to the status prior to the version upgrade, and start again from the version upgrade, referring to the following steps. To restore the status prior to the version upgrade, use the backup of JP1/Base and JP1/IM - Manager obtained prior to the version upgrade installation. The following shows an example of the procedure for upgrading from version 12 to version 13.

Steps		Description
1	Uninstalling JP1/IM - Manager (version13)	Manually uninstall IM database. #1
2		Uninstall JP1/IM - Manager.
3	Uninstalling JP1/Base (version13)	If the settings have been changed after upgrading JP1/Base to version 13, make a backup.
4		Uninstall JP1/Base. #1
5	Installing and Restoring JP1/Base (Version 12)	Install JP1/Base of the version prior to the upgrade. #1#2
6		Restore JP1/Base configuration and event database. #2
7	Installing and Restoring JP1/IM - Manager (Version 12)	Install JP1/IM - Manager of the version prior to the upgrade.
8		Use the backup file acquired prior to the version upgrade to recover JP1/IM - Manager settings.
9		Set up IM database.
10		Recover IM database using the backup file taken prior to the version upgrade.
11	JP1/Base version upgrades (from version 12 to version 13) and restores	Perform a JP1/Base upgrade. #2
12		If you made a backup in step 3, use it to recover.
13	Upgrading JP1/IM - Manager (Version 12 to Version 13)	Perform a JP1/IM - Manager upgrade.
14		Run <code>jimdbupdate</code> command to refresh IM database.

#1

Includes OS restart.

#2

If you have JP1/AJS or other products that are used with JP1/Base installed, you will need to do the same for those products.

In addition, uninstallation is performed first from higher-level products. Installation and version upgrading are performed first from JP1/Base.

(70) Integrated operation viewer tree does not display monitored IM management nodes, Trend view does not show performance data, or some portion is missing

Item number	Key factors	Corrective action
1	Prometheus server is hesitation and does not scrape.	Start the Prometheus server.
2	The scrape is failing because the exporter is hesitation.	Launch Exporter.
3	Communication failure has occurred between Prometheus server and JP1/IM - Manager (Intelligent Integrated Management Infrastructure) host, so performance data cannot be sent.	Resolve the communication failure.
4	Reverted the system time of the monitored host.	Wait until the system time on the monitored host returns to the time before the change.
5	After changing the scrape interval of the Prometheus server from 1 m of Differential Gear, the value of the PromQL statement in the metric definition file has not been changed.	If you change scrape interval of Prometheus server from its default value (1m), you must review the value "time to back" (specified in square brackets []) specified in range Vector

Item number	Key factors	Corrective action
		type in PromQL expression of metric definition-file. Specify at least twice scrape interval.
6	The length of the character string set in IM management node label name (jp1_pc_nodelabel value) exceeds the upper limit. URL encoding limit is 234 bytes (26 characters for all multibyte characters).	Set the jp1_pc_nodelabel so that the value does not exceed the upper limit by the setting procedure (same for Linux) described in 1.21.2(3)(g) <i>Configure the settings when the label name (jp1_pc_nodelabel value) of the IM management node exceeds the upper limit (for Windows) (optional)</i> in the manual <i>JP1/Integrated Management 3 - Manager Configuration Guide</i> .

(71) No JP1 Events Notified to integrated operation viewer

Item number	Key factors	Corrective action
1	Prometheus server is hesitation and does not scrape.	Start the Prometheus server.
2	The scrape is failing because the exporter is hesitation.	Launch Exporter.
3	Notifications are not made because Alertmanager is hesitation.	Launch Alertmanager.
4	JP1 event cannot be notified because of a communication failure between Alertmanager and JP1/IM (Intelligent Integrated Management Platform) host.	Resolve the communication failure.

(72) JP1/IM - Agent is notified of an outage (if you are monitoring JP1/IM - Agent processing).

Item number	Key factors	Corrective action
1	The JP1/IM - Agent process being monitored has hesitation.	Launch the JP1/IM - Agent process.

(73) IM management node for Yet another cloudwatch exporter Is Not Created

Item number	Key factors	Corrective action
1	CloudWatch is not displaying metrics.	Perform operations such as launching an instance (in the case of EC2) so that you can check the metrics in CloudWatch.
2	You haven't set jp1_pc_nodelabel tags on the resource.	Set jp1_pc_nodelabel tags for each resource in AWS.
3	Yet another cloudwatch exporter is misconfigured.	<ul style="list-style-type: none"> Check if the Connection settings to CloudWatch are correct. Check that the values specified for setting items such as type, metrics, etc. are correct.
4	Prometheus, scraping Yet another cloudwatch exporter, has set the scrape interval to a value greater than 10 minutes.	Set the scrape interval to no more than 10 minutes.
5	There is a difference of more than 10 minutes between the system time of the JP1/IM - Manager host and the Yet another cloudwatch exporter host.	Correct the system time skew.

(74) If you start the service of the integrated agent in a Windows environment, the status goes to the running status but changes to the stopped status immediately.

Item number	Key factors	Corrective action
1	<p>The integrated agent process consists of a Windows serviced process and a service process.</p> <p>This behavior occurs when the integrated agent service is started with only the Windows serviced process stopped and the service process not stopped.</p>	<p>In Task Manager, make sure that the process for each of the following services is running: If only one process is running, run End Task Manager to stop the process and start the service.</p> <ul style="list-style-type: none"> • JP1/IM3-Agent imagent.exe, jpc_imagent_service.exe • JP1/IM3-Agent proxy imagentproxy.exe, jpc_imagentproxy_service.exe • JP1/IM3-Agent action imagentaction.exe, jpc_imagentaction_service.exe • JP1/IM3-Agent Alert forwarder alertmanager.exe, jpc_alertmanager_service.exe • JP1/IM3-Agent metric forwarder prometheus.exe, jpc_prometheus_server_service.exe • JP1/IM3-Agent Synthetic metric collector blackbox_exporter.exe, jpc_blackbox_exporter_service.exe • JP1/IM3-Agent Windows metric collector windows_exporter.exe, jpc_windows_exporter_service.exe • JP1/IM3-Agent AWS metric collector ya_cloudwatch_exporter.exe jpc_ya_cloudwatch_exporter_service.exe • JP1/IM3-Agent Azure metric collector promitor_scraper.exe jpc_promitor_scraper_service.exe • JP1/IM3-Agent Azure resource discovery promitor_resource_discovery.exe, jpc_promitor_resource_discovery_service.exe • JP1/IM3-Agent Script metric collector script_exporter.exe, jpc_script_exporter_service.exe • JP1/IM3-Agent Log trapper ruby.exe (1+number of workers), jpc_fluentd_service.exe

(75) In Windows, when a service of the integrated agent is started or stopped, Error 1067 is notified to the standard error output of net commands and dialogs on the service screen, and the service fails to start or stop.

Item number	Key factors	Corrective action
1	<p>The integrated agent process consists of a Windows serviced process and a service process.</p> <p>This behavior occurs when only the Windows serviceization process is stopped and the service process is not stopped, and the integrated agent service is started or stopped.</p>	<p>This is same with (74).</p>

(76) Service does not start

Item number	Key factors	Corrective action
1	The definition file is incorrect.	<p>Check the following definition file formats, settings, character codes, newline codes, etc. for errors. For details about the format of each file, see the appropriate definition file in the <i>JP1/Integrated Management 3 - Manager Command, Definition File and API Reference</i>.</p> <ul style="list-style-type: none"> • Alertmanager <ul style="list-style-type: none"> - Alertmanager configuration file - Service definition file (For Windows) - Unit definition file (For Linux) • Prometheus server <ul style="list-style-type: none"> - Prometheus configuration file[#] - Alert configuration file[#] - Node exporter discovery configuration file[#] - Windows exporter discovery configuration file[#] - Blackbox exporter (HTTP/HTTPS monitoring) discovery configuration file[#] - Blackbox exporter (ICMP Monitoring) discovery configuration file[#] - Yet another cloudwatch exporter discovery configuration file[#] - User-specific discovery configuration file[#] - Service definition file (For Windows) - Unit definition file (For Linux) • Node exporter <ul style="list-style-type: none"> - Unit definition file • Windows exporter <ul style="list-style-type: none"> - Windows exporter configuration file - Service definition file • Blackbox exporter <ul style="list-style-type: none"> - Blackbox exporter configuration file - Service definition file (For Windows) - Unit definition file (For Linux) • Yet another cloudwatch exporter <ul style="list-style-type: none"> - Yet another cloudwatch exporter configuration file - Unit definition file <p>#</p> <p>The Prometheus server definition file can be validated with the <code>promtool check config</code> command.</p>
2	There is a duplicate of the port used by the other process and the port used by the JP1/IM - Agent process.	<p>The ports used by JP1/IM - Agent can be checked in the unit definition file or by the following command-line options listed in the service definition file:</p> <ul style="list-style-type: none"> • For Prometheus server, Alertmager, Node exporter, Blackbox exporter <pre>--web.listen-address=IP-address:port-number</pre> • For Windows exporter <pre>--telemetry.addr=IP-address:port-number</pre> • Yet another cloudwatch exporter <pre>-listen-address=IP-address:port-number</pre>

Item number	Key factors	Corrective action
		<p>Stop the JP1/IM - Agent process, and then run the following command to verify that the port specified in the command line option above is not in use:</p> <ul style="list-style-type: none"> • For Windows environment netstat -ane • For Linux environment ss -ant <p>If it is in use, change the port settings so that they do not overlap. For details on how to change the port number setting, see the appropriate explanation in <i>1.21.2 Settings of JP1/IM - Agent</i> (for Windows) and <i>2.19.2 Settings of JP1/IM - Agent</i> (for UNIX) in the <i>JP1/Integrated Management 3 - Manager Configuration Guide</i>.</p>

(77) JP1/IM - Agent process is running but does not work properly

Item number	Key factors	Corrective action
1	There is a duplicate of the port used by the other process and the port used by the JP1/IM - Agent process.	<p>The ports used by JP1/IM - Agent can be checked in the unit definition file or by the following command-line options listed in the service definition file:</p> <ul style="list-style-type: none"> • For Prometheus server, Alertmanager, Node exporter, Blackbox exporter --web.listen-address=<i>IP-address:port-number</i> • For Windows exporter --telemetry.addr=<i>IP-address:port-number</i> • Yet another cloudwatch exporter -listen-address=<i>IP-address:port-number</i> <p>Stop the JP1/IM - Agent process, and then run the following command to verify that the port specified in the command line option above is not in use:</p> <ul style="list-style-type: none"> • For Windows environment netstat -ane • For Linux environment ss -ant <p>If it is in use, change the port settings so that they do not overlap. For details on how to change the port number setting, see the appropriate explanation in <i>1.21.2 Settings of JP1/IM - Agent</i> (for Windows) and <i>2.19.2 Settings of JP1/IM - Agent</i> (for UNIX) in the <i>JP1/Integrated Management 3 - Manager Configuration Guide</i>.</p>

(78) If you execute a REST API provided by JP1/IM - Agent while JP1/IM - Agent process is running, there is no response, or an error is returned.

Item number	Key factors	Corrective action
1	There is a duplicate of the port used by the other process and the port used by the JP1/IM - Agent process.	<p>The ports used by JP1/IM - Agent can be checked in the unit definition file or by the following command-line options listed in the service definition file:</p> <ul style="list-style-type: none"> • For Prometheus server, Alertmanager, Node exporter, Blackbox exporter --web.listen-address=<i>IP-address:port-number</i>

Item number	Key factors	Corrective action
		<ul style="list-style-type: none"> • For Windows exporter --telemetry.addr= IP-address :port-number • Yet another cloudwatch exporter -listen-address=IP-address :port-number <p>Stop the JP1/IM - Agent process, and then run the following command to verify that the port specified in the command line option above is not in use:</p> <ul style="list-style-type: none"> • For Windows environment netstat -ane • For Linux environment ss -ant <p>If it is in use, change the port settings so that they do not overlap. For details on how to change the port number setting, see the appropriate explanation in <i>1.21.2 Settings of JP1/IM - Agent</i> (for Windows) and <i>2.19.2 Settings of JP1/IM - Agent</i> (for UNIX) in the <i>JP1/Integrated Management 3 - Manager Configuration Guide</i>.</p>

(79) Blackbox_exporter does not monitor correctly

Item number	Key factors	Corrective action
1	<p>Possible causes include:</p> <ul style="list-style-type: none"> • You have specified a host name that does not exist in the discovery configuration file (file_sd_config_blackbox_module-name.yml). • The monitored host specified discovery configuration file (file_sd_config_blackbox_module-name.yml) is stopped. • The monitored service specified in the discovery configuration file (file_sd_config_blackbox_http.yml) is stopped. • You have specified the wrong URL in the discovery configuration file (file_sd_config_blackbox_http.yml). • You have specified an incorrect value for the compressor in the Blackbox exporter configuration file (blackbox_exporter.yml). • The credentials specified in the Blackbox exporter configuration file (blackbox_exporter.yml) are incorrect. • The Blackbox exporter configuration file (blackbox_exporter.yml) source_ip_address incorrectly. • The certificate specified in the Blackbox exporter configuration file (blackbox_exporter.yml) does not exist. • The certificate specified in the Blackbox exporter configuration file (blackbox_exporter.yml) is incorrect. 	<p>Make sure that:</p> <ul style="list-style-type: none"> • The monitored object is operating normally • file_sd_config_blackbox_module-name.yml is correct. • blackbox_exporter.yml description is correct. <p>If there are no problems with the above, you should Output and investigate the detailed log of the blackbox_exporter to determine the cause. Perform the following steps:</p> <ol style="list-style-type: none"> 1. Change the blackbox_exporterSlag level setting from "info" (Differential Gear) to "debug". 2. Rewrite --log.level described in the unit definition file or service definition file from "info" to "debug". 3. Restart the service. 4. Restarting the service will enable the log level setting change. 5. After monitoring with blackbox_exporter and reproducing the phenomenon, collect blackbox_exporterSlag and contact the system administrator. <p>If you change the log level to "debug", a large number of logs will be Output, so it is necessary to return the log level to "info" after collecting the log.</p>

(80) User-defined Exporter does not monitor correctly

Item number	Key factors	Corrective action
1	<p>This could be due to:</p> <ul style="list-style-type: none"> • Cause caused by user-defined Exporter 	<p>Check the following points.</p> <ul style="list-style-type: none"> • Check if user-defined Exporter is operating normally. Use a curl or browser to scrape user-defined Exporter to verify that it can be retrieved successfully. If it is not, it is

Item number	Key factors	Corrective action
	<ul style="list-style-type: none"> No settings of scrape job for user-defined Exporter are added to Prometheus configuration file (jpc_prometheus_server.yml), or the settings are incorrect. You have not created a user-specific discovery configuration file (file_sd_config_<any-name>.yml) or the configuration is incorrect. 	<p>probably due to user-defined Exporter, check the source of user-defined Exporter.</p> <ul style="list-style-type: none"> If you are not having trouble working with user-defined Exporter, you may not be able to scrape from Prometheus server, so check whether a scrape job is defined in Prometheus configuration file (jpc_prometheus_server.yml) and user-specific discovery configuration file (file_sd_config_<any-name>.yml) is created.

(81) Log trapper monitored logs or event logs are not published as a JP1 event

Item number	Key factors	Corrective action
1	<p>This could be due to:</p> <ul style="list-style-type: none"> Fluentd monitor definition file is incorrect. 	<p>Check the following files for errors in format, settings, character codes, and line feed codes.</p> <ul style="list-style-type: none"> Log monitoring common definition file (jpc_fluentd_common.conf) Log monitoring target definition file (jpc_fluentd_common_list.conf) Text-formatted log file monitoring definition file (fluentd_@@trapname@@_tail.conf.template) Windows event-log monitoring definition file (fluentd_@@trapname@@_wevt.conf.template)

(82) Unable to acquire the Script exporter metric

Item number	Primary cause	Countermeasures
1	The executed script terminated abnormally.	Correct the script executed by Script exporter, and then restart Script exporter.
2	Attempted to execute a file without execute permissions.	Change the file permissions for the file being executed.

(83) Unable to acquire the Promitor metric

Item number	Primary cause	Countermeasures
1	Resource Discovery has stopped.	Start Resource Discovery.
2	Incorrect Resource Discovery setup.	Check whether type and other settings are correct.
3	Incorrect Scraper setup.	<ul style="list-style-type: none"> Check whether the connection settings for Resource Discovery are correct. Check whether resourceType, metricName, and other settings are correct.

(84) The tree of JP1/Base or JP1/IM - Manager of event-forwarding relay source is not displayed

Item number	Primary cause	Countermeasures
1	This could be due to: <ul style="list-style-type: none">When event-forwarding relay source JP1/IM - Agent starts, it may fail to send the configuration information. (JP1/IM - Agent starts even if the configuration information fails to be sent.)	Check whether any errors in the jima_message.log of the event forwarding relay source for the JP1/IM - Agent. If an error has been output, take appropriate action according to the error message. Then, restart JP1/IM - Agent and refresh the tree.

(85) The tree of JP1/Base or JP1/IM - Manager of event-forwarding relay source is not configured

Item number	Primary cause	Countermeasures
1	This could be due to: <ul style="list-style-type: none">Event-forwarding relay function in JP1/IM - Agent sends the relay source configuration to JP1/IM - Manager only if the relay source configuration changes. If JP1/IM - Manager is restored, the configuration data of the relay source that JP1/IM - Manager maintains may be out of date and not updated.	In event-forwarding relay source JP1/IM - Agent installation folder (shared folder for logical hosts), remove the files under tmp/jbs fwd folder and restart JP1/IM - Agent. After that, perform tree update.

12.5.4 Actions to take when the JP1/IM - Agent cannot connect to the JP1/IM - Manager

(1) TLS is enabled for the JP1/IM - Manager, however TLS is disabled for the JP1/IM - Agent

KNBC20057-W is issued. As details, "received an error response status" is output.

Enable TLS for the JP1/IM - Agent.

(2) TLS is disabled for the JP1/IM - Manager, however TLS is enabled for the JP1/IM - Agent

KNBC20057-W is issued. As details, "http: server gave HTTP response to HTTPS client" is output.

Disable TLS for the JP1/IM - Agent.

(3) Certificate is invalid

KNBC20057-W is issued. As details, "x509: certificate signed by unknown authority" is output.

Set correct certificate for the JP1/IM - Agent.

(4) Certificate has expired

KNBC20057-W is issued. As details, "x509: certificate has expired or is not yet valid" is output.

Set correct certificate for the JP1/IM - Agent.

(5) The initial secret has not been registered, or the initial secret is invalid

KNBC20057-W is issued. As details, "An authentication error occurred. (URL path = /ima/api/v1/-/healthy)" is output.

Set correct certificate for the JP1/IM - Agent.

Index

A

actions to take when

additional common exclusion-conditions cannot be set [499](#)

attempt to start profile of remote monitoring log file trap fails in IM Configuration Management [518](#)

automated action is delayed [492](#)

characters are unreadable JP1/SES-format events are received [523](#)

command execution log file is damaged [486](#)

command execution or batch file executed in automated action does not terminate normally [499](#)

connection to JP1/Base fails [480](#)

correlation events cannot be displayed in JP1/IM - View [497](#)

definition menu is not displayed in Event Console window [480](#)

earlier version of JP1/IM - Manager or JP1/IM - View is being used [494](#)

email does not reach destination in email notification function of JP1/IM - Manager [523](#)

error message indicating invalid port number is issued after IM database has been set up [509](#)

event information cannot be inherited [484](#)

event search cannot be executed [506](#)

filter does not work correctly because source host name is different from monitored host name [522](#)

IM Configuration Management failed to apply system hierarchy [511](#)

IM Configuration Management failed to collect operation definition file for log file trap [512](#)

IM database cannot be started or database-related commands cannot be executed [511](#)

IM database cannot be terminated [508](#)

IM database setup fails [509](#)

JP1/IM - Manager cannot be uninstalled [509](#)

JP1/IM - View cannot display any log file traps that are active [512](#)

JP1/IM - View window cannot be displayed after you have logged in [498](#)

JP1 events are displayed late in Event Console window [504](#)

KAVB5150-W is displayed in detailed information for action result [493](#)

many JP1 events occurred for which correlation events were generated [496](#)

memo entries cannot be set up [507](#)

menu items such as Register Host and Edit Agent Configuration are disabled in IM Configuration Management - View [513](#)

monitored object database cannot be unlocked [493](#)

monitored object database is damaged [492](#)

no JP1 event is displayed in Event Console window [503](#)

no response-waiting events are displayed in JP1/IM - View [502](#)

Processing dialog box continues to open in IM Configuration Management - View [517](#)

profile settings file does not match valid configuration information [513](#)

remote monitored log file name is incorrect [519](#)

response-waiting events are displayed as ordinary events [503](#)

same JP1 event is received redundantly in remote monitoring log file trap of IM Configuration Management [518](#)

setup information file is output as invalid during IM database setup [510](#)

source host name is different from host name registered in IM Configuration Management [522](#)

status cannot be changed [505](#)

trapped JP1 event message shows unreadable characters [480](#)

tree area on IM Configuration page in IM Configuration Management - View is displayed in gray [517](#)

unknown is displayed as automated action execution status [491](#)

valid configuration information of remote monitoring log file trap or remote monitoring event log trap cannot be viewed in IM Configuration Management [514](#)

virtualization system configuration cannot be collected in IM Configuration Management [514](#)

you cannot connect to IM database [508](#)

you cannot connect to remotely monitored host [519](#)

you cannot execute command [481](#)

you cannot execute commands from Command button [485](#)

you cannot log in from JP1/IM - View [477](#)

you cannot start client applications [485](#)

Actions to take when an automated action is not executed [536](#)

actions to take when filter does not work correctly because source host name is different from monitored host name [522](#)

Actions to take when JP1/IM - View does not start 536

additional common exclusion-condition

changing additional common exclusion-condition to common exclusion-condition 199

Setting an additional common exclusion-condition to exclude a JP1 event from the monitoring target or action execution 198

additional common exclusion-conditions

setting additional common exclusion-conditions by using JP1 events that have occurred 198

trouble shooting (additional common exclusion-conditions cannot be set) 499

additional common exclusion-condition to common exclusion-condition

changing 199

applying edited settings file information 283

automated actions

canceling 269

checking execution results of 266

checking execution status of 265

checking operating status of 271

executing 265

re-executing 270

setting up 265

automatic startup and stop, examples of 135

B

backing up 54

command execution log 55

configuration information (UNIX) 32

configuration information (Windows) 23

database 54

event database 57

file for accumulated response-waiting events 58

host information database 57

IM database 58

monitored object database 56

Backup and recovery procedure of Intelligent Integrated Management Database 61

batch file, abnormally terminated 499

batch job execution system 319

system configuration when linking with batch job execution systems 319

BJEX linkage commands

jcoimdef 341

jim_log.bat (Windows only) 341

jim_log.sh (UNIX only) 342

business groups

managing 282

C

canceling automated actions 269

Central Console

JP1 event grouping 211

Central Console, monitoring system from 174

Central Scope

monitoring from Monitoring Tree window 244

monitoring from Visual Monitoring window 249

monitoring system from 243

changing

additional common exclusion-condition to common exclusion-condition 199

changing JP1 event display messages 215

database settings 63

JP1/IM settings 93

monitoring status of monitoring nodes 245, 250

status of monitoring nodes 244, 250

changing monitoring configuration

notes on changing monitoring configuration from remote to agent 119

changing response status

changing 188

Changing the message displayed for a JP1 event 215

checking

command execution status 263

execution results of automated actions 266

execution status of automated actions 265

operating status of automated actions 271

Checking detailed information about a correlation event and changing the response status 190

cluster system, operations in 130, 133

collecting (UNIX)

RAS information 430

collecting (Windows)

RAS information 424

command, executing

by using Command button 261

by using command line 259

defined on source host of selected event 262

command execution log

backing up 55

procedures for backing up and recovering 55

recovering 55

re-creating 63

reorganizing 52

- command execution status, checking 263
- commands
 - actions to take when you cannot execute 481
 - deleting 263
 - user who executes 263
- commands, executing 259
- common exclusion-condition
 - using command to switch 197
- configuration information
 - managing 23
 - migrating 84
- consolidated
 - consolidated display when events with same attributes occur consecutively 236
- consolidated display
 - consolidated display when events with same attributes occur consecutively 236
- consolidated event
 - setting response status for repeated events 189
- consolidated events in events list, displaying 180
- conventions
 - diagrams 10
 - fonts and symbols 11
 - mathematical expressions 12
 - version numbers 12
- correlation event generation history 82
- correlation events in events list, displaying 182
- correlation source event
 - displaying 191
 - from Related Events (Correlation) or Related Events (Correlation fails) window, deleting 192
 - from Related Events (Correlation) or Related Events (Correlation fails) window, setting response status for 191
- CSV file
 - outputting events to 82

D

- data, collecting 421
- database management 52
 - backing up command execution log 55
 - backing up event database 57
 - backing up file for accumulated response-waiting events 58
 - backing up host information database 57
 - backing up IM database 58
 - backing up monitored object database 56
 - changing IM database port 72

- expanding IM database size 68
- recovering command execution log 55
- recovering event database 57
- recovering file for accumulated response-waiting events 58
- recovering host information database 57
- recovering IM database 58
- recovering monitored object database 56
- reorganizing event database 52
- reorganizing file for accumulated response-waiting events 52
- reorganizing IM database 52
- databases
 - backing up 54
 - changing settings of 63
 - managing 52
 - migrating 84
 - recovering 54
 - re-creating 63
 - reorganizing 52
- data collection tool
 - executing (UNIX) 429
 - executing (Windows) 422
- deleting commands 263
- detailed information about repeated events
 - checking, and changing the response status for 189
- diagram conventions 10
- disk capacity, managing 75
- displaying
 - attributes of monitoring nodes 247, 252
 - consolidated events 236
 - guide information 247, 252
 - login user list 248
- displaying, detailed JP1 event information 184
- Displaying extended attributes of JP1 events (mapping of event information) 208
- displaying performance reports for JP1 events when linking with JP1/PFM 240
- displaying search results (JP1 event) 205
- dump files, managing 81

E

- email notification function
 - actions to take when email does not reach destination 523
- error information
 - collecting (UNIX) 430
 - collecting (Windows) 424

- event
 - event by specifying event display start-time, displaying 200
 - consolidated display when events with same attributes occur consecutively 236
 - forwarding from agent, preparing to suppress 221
 - severity level of, changing 212
- event acquisition filter
 - applying filter 183
 - switching 194
 - using jcochfilter command to switch 196
- Event Console window
 - actions to take when definition menu is not displayed in 480
 - actions to take when no JP1 event is displayed in 503
 - events displayed in events list in 179
- event database
 - backing up 57
 - procedures for backing up and recovering 57
 - recovering 57
 - re-creating 64
 - reorganizing 52
- event display
 - displaying event by specifying event display start-time 200
- event forwarding
 - handling occurrence of large number of events by suppressing event forwarding from agent 224
 - on agent, setting threshold for automatically suppressing 229
- event information
 - actions to take when event information cannot be inherited 484
- events
 - occurrence of, handling large number of 219
 - occurrence of by suppressing event forwarding from agent, handling large number of 224
 - outputting (to CSV file) 82
 - stopping, on manager, log file trap that issues large numbers of 235
- event search direction 205
- event service
 - actions to take when connection to JP1/Base fails 480
- Exclusion history and definition history of common exclusion conditions 83
- executing
 - automated actions 265
 - commands (on agent or manager host) 261

- extended recovery
 - failed, actions to take for 532

F

- file for accumulated response-waiting events 327
 - backing up 58
 - procedures for backing up and recovering 58
 - recovering 58
 - re-creating 67
 - reorganizing 52
- filter 193
 - applying 183
- font conventions 11

G

- grouping
 - JP1 event 211
- guide information, displaying 247, 252

H

- handling
 - general procedures and preparation for handling occurrence of large number of events 219
 - handling occurrence of large number of events 219
- historical reports, using 82
- host information
 - collecting 278
- host information database
 - backing up 57
 - procedures for backing up and recovering 57
 - recovering 57
 - re-creating 64
 - reorganizing 52
- host management
 - changing information 278
 - collecting information 278
 - deleting (IM Configuration Management window) 278
 - displaying lists 278
 - registering 278
- host name
 - actions to take when source host name is different from host name registered in IM Configuration Management 522
 - changing 97
 - cluster system, logical 105
 - mail server 105
- host name, changing 97

- hosts
 - managing 278
- 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 534
- How to restart the system if you change the IP address of the manager or JP1/Base 110

I

- IM Configuration Management
 - actions to take when attempt to start profile of remote monitoring log file trap fails in IM Configuration Management 518
 - actions to take when same JP1 event is received redundantly in remote monitoring log file trap of IM Configuration Management 518
 - actions to take when virtualization system configuration cannot be collected in IM Configuration Management 514
 - applying imported management information of 300
 - applying management information to Central Scope monitoring tree 280
 - exporting and importing management information of IM Configuration Management 286
 - exporting management information of 286
 - importing management information of 290
 - managing business groups 282
 - managing hosts 278
 - managing profiles 283
 - managing service operation status 284
 - managing system hierarchy using 277
- 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 513
 - actions to take when Processing dialog box continues to open in IM Configuration Management - View 517
- IM Configuration page
 - actions to take when tree area on IM Configuration page in IM Configuration Management - View is displayed in gray 517
- IM database
 - actions to take when IM database cannot be started or database-related commands cannot be executed 511
 - backing up 58
 - changing port of 72
 - expanding size of 68

- recovering 58
- reorganizing 52
- IM database capacity
 - managing 75
- IM database setup
 - actions to take when error message indicating invalid port number is issued after IM database has been set up 509
 - actions to take when IM database setup fails 509
 - actions to take when setup information file is output as invalid during IM database setup 510
- incident
 - displaying JP1/Service Support from Event Details window 239
 - displaying JP1/Service Support from pages of Event Console window 238
 - displaying JP1/Service Support from Related Events window 238
- individual log 347
- Intelligent Integrated Management Base
 - Checking performance data and handling the problem (link with JP1/PFM) 167
 - Handling errors by viewing suggestions 167
 - JP1 events 150
 - Logging in to the system with single sign-on through linkage with external products using OIDC authentication 168
 - Notes on operating 171
 - Port number is changed 120
 - Sharing information using a direct access URL 169
 - System Monitoring 146
 - Understanding how extensive a problem that occurred during operation of a job is and handling it (link with JP1/AJS) 166
 - Understanding in advance which root jobnets are affected before the definition or content of a job is changed (link with JP1/AJS) 167
 - Using signs to avoid failures (link with JP1/AJS) 166
 - Viewing links with other products 166
 - Viewing the system status 147
- IP address
 - changing 107
 - of mail server 110
- IP address, changing 107
- items, displayed in events list 175

J

- JP1/AS linkage commands
 - jcoimdef 341

- jim_log.bat (Windows only) 341
- jim_log.sh (UNIX only) 342
- JP1/IM
 - changing configuration of 92
 - changing severity level of JP1 events 212
 - collecting data 421
 - correcting problems 442
 - data that needs to be collected when problem occurs 391
 - editing JP1 memo entries 186
 - linking with BJEX 318
 - logging in 142
 - logging in to JP1/IM - Manager 142
 - logging out 145
 - logging out of JP1/IM - Manager 145
 - log information types 345
 - managing configuration information 23
 - managing databases 52
 - managing disk capacity 75
 - monitoring from Monitoring Tree window 244
 - monitoring from Visual Monitoring window 249
 - monitoring system from Central Scope 243
 - opening monitor window of application that issued JP1 events 239
 - opening other application windows from Tool Launcher 273
 - outputting dump file for (UNIX) 429
 - outputting thread dump for (Windows) 421
 - searching for JP1 events 203
 - settings information, changing 93
 - starting 127
 - stopping 132
 - switching event acquisition filter to be applied 194
 - system maintenance 22
 - system operation using 258
 - troubleshooting 343
 - troubleshooting procedure 344
 - using historical reports 82
- JP1/IM files for backup 24, 32
- JP1/IM filter
 - applying 193
- JP1/IM - Manager
 - in which communication encryption function is enabled, actions to take when error is displayed on 525
 - log files (Central Console) (UNIX) 369
 - log files (Central Console) (Windows) 349
 - log files (Central Scope) (UNIX) 376
 - log files (Central Scope) (Windows) 357
 - log files and folders (IM Configuration Management) (UNIX) 378
 - log files and folders (IM Configuration Management) (Windows) 359
 - logging in to 142
 - logging out of 145
 - login and logout 141
 - notes on starting 139
 - notes on stopping 139
 - starting 126–128
 - stopping 126, 132
 - Using a Web browser to log in to 142
 - using command to log in to 144
 - using GUI to log in to 142
- JP1/IM system
 - applying system hierarchy 279
 - collecting system hierarchy information 279
 - displaying system hierarchy 279
 - editing system hierarchy 279
 - synchronizing system hierarchies 279
 - verifying system hierarchy 279
- JP1/IM - View
 - actions to take when no response-waiting events are displayed in 502
 - actions to take when response-waiting events are displayed as ordinary events 503
 - actions to take when you cannot log in from 477
 - executing commands by using Command button 261
 - executing commands by using Command Execution 259
 - log files and folders 368
 - opening monitor window of application that issued JP1 events 239
 - opening other application windows from Tool Launcher 273
 - switching common exclusion-condition from Event Acquisition Conditions List window 195
 - switching common exclusion-condition from System Environment Settings window 195
 - switching event acquisition filter from Event Acquisition Conditions List window 195
 - switching event acquisition filter from System Environment Settings window 194
 - system operation 258
 - when communication encryption function is enabled, actions to take when error is displayed in 528
- JP1/Navigation Platform

displaying operating procedures for JP1 events
(linking with JP1/Navigation Platform) 239

JP1/PFM

displaying performance reports for JP1 events when
linking with JP1/PFM 240
operating 240

JP1/Service Support

from Event Details window, displaying 239
from pages of Event Console window, displaying 238
from Related Events window, displaying 238
operating 238
registering JP1 events as incidents in JP1/IM -
Service Support (linking with JP1/IM - Service
Support) 238

JP1 event

as incidents in JP1/IM - Service Support (linking with
JP1/IM - Service Support), registering 238
by linking with other products, handling 238
changing severity level of JP1 events 212
displaying 175
displaying detailed information 184
displaying only severe events 193
displaying operating procedures for (linking with JP1/
Navigation Platform) 239
displaying program-specific extended attributes of
(displaying program-specific extended attributes)
208
displaying program-specific extended attributes of
(mapping event information) 208
displaying search results 205
display messages, changing 215
grouping 211
opening monitor window of application that issued
239
program-specific extended attributes of (displaying
program-specific extended attributes) 178
program-specific extended attributes of (event
information mapping) 179
response status 179
searching for 203
search method 203
search procedure 203
setting JP1 event response statuses 187
to be displayed by specifying time period, narrowing
201
viewing 175

JP1 event information

by operation, customizing 208

JP1 event response status

setting 187

settings for 187

JP1 events

actions to take if JP1 events are not received even
when remote monitoring event log trap is running in
IM Configuration Management 516

actions to take if JP1 events are not received even
when remote monitoring log file trap is running in IM
Configuration Management 515

items that can be displayed 176

using historical information of 82

JP1 events response status

from events list, setting 188

JP1 memo entry

editing 186

K

KAVB0002-E	483
KAVB0104-E	478
KAVB0109-E	478
KAVB0256-E	500
KAVB0415-E	481
KAVB0416-E	481
KAVB0417-E	481
KAVB0418-E	482
KAVB0419-E	482
KAVB0422-E	482
KAVB0423-E	482
KAVB1034-E	485
KAVB1036-W	484
KAVB1037-E	483, 485
KAVB1040-W	484
KAVB1041-W	484
KAVB1042-W	484
KAVB1043-W	484
KAVB1044-W	484
KAVB1046-E	484
KAVB1153-E	500
KAVB1154-W	500
KAVB1155-E	499
KAVB1157-E	500
KAVB1158-W	501
KAVB1159-W	501
KAVB1160-W	501
KAVB1161-W	501
KAVB1162-W	501
KAVB1163-E	499

KAVB1200-E 478
 KAVB1956-E 525
 KAVB1957-E 525
 KAVB1958-E 529
 KAVB1959-E 529
 KAVB1969-W 530
 KAVB1971-W 530
 KAVB1972-W 526
 KAVB2027-E 482
 KAVB2031-E 483
 KAVB2239-E 492
 KAVB6601-E 529
 KAVB6602-E 529
 KAVB6603-W 530
 KAVB7247-E 492
 KAVB7248-E 492
 KAVB7602-E 526
 KAVB7810-E 526
 KAVB7812-E 527
 KAVB7818-E 527
 KAVB8452-E 483
 KAVB8817-E 525
 KAVB8818-E 525
 KNAN11215-E 545
 KNAN20100-E 478
 KNAN20101-E 478
 KNAN20102-E 479
 KNAN20103-E 479
 KNAN20104-E 479
 KNAN20121-E 529
 KNAN20122-E 529
 KNAN20123-W 530
 KNAN20124-W 530
 KNAN20141-E 529
 KNAN20142-E 530
 KNAN20143-W 530
 KNAN20144-W 531
 KNAN21400-W 521
 KNAN21402-E 521
 KNAN21403-E 521
 KNAN21404-E 531
 KNAN22017-E 519
 KNAN22403-E 537
 KNAN24155-E 527
 KNAN26039-E 518
 KNAN29095-E 527
 KNAN29097-W 528

KNAN29098-E 527

L

linkage

BJEX configuration 335
 BJEX linkage configuration 332
 BJEX or JP1/AS configuration 335
 BJEX or JP1/AS linkage configuration 332
 communication settings between BJEX and JP1/IM - Manager 334
 JP1/AS configuration 335
 JP1/AS linkage configuration 332
 JP1/IM functionality for BJEX linkage 322
 JP1/IM functionality for BJEX or JP1/AS linkage 322
 JP1/IM functionality for JP1/AS linkage 322
 linking with BJEX 341
 linking with BJEX or JP1/AS 341
 linking with JP1/AS 341
 overview of BJEX linkage 319
 overview of BJEX or JP1/AS linkage 319
 overview of JP1/AS linkage 319

linked products

BJEX 318
 linking with JP1/AS 318

linking

handling JP1 events by linking with other products 238
 with BJEX or JP1/AS 318
 with JP1/AS 318

linking with JP1/Navigation Platform

operating 239

log

common message 345
 files and directory list 348
 integrated trace 345
 operation 347
 types of information 345

log file size, managing 78

log file trap

stopping, on manager, log file trap that issues large numbers of events 235

login 142

Using a Web browser 142
 using GUI 142

login user list, displaying 248

logout 145

M

- maintenance 22
- management information, exporting and importing 286
- manager or agent, resetting the date/time of
 - returning the time 111
- manager or agent, tasks required when date of is changed 111
- managing
 - business groups 282
 - configuration information 23
 - configuration of virtual system 280
 - databases 52
 - disk capacity 75
 - hosts 278
 - IM database capacity 75
 - profiles 283
 - service operation status 284
- mathematical expression conventions 12
- message
 - changing JP1 event display messages 215
- migrating configuration information and databases 84
- monitored host in a remote monitoring configuration, tasks required when date of is changed 117
- monitored object database
 - backing up 56
 - procedures for backing up and recovering 56
 - recovering 56
 - re-creating 64
 - reorganizing 52
- monitoring
 - from Monitoring Tree window 244
 - from Visual Monitoring window 249
- monitoring nodes
 - changing monitoring status of 245, 250
 - changing status of 244, 250
 - displaying attributes of 247, 252
 - searching for 246, 251
- monitoring tree
 - changing monitoring status of monitoring nodes in 245
 - changing status of monitoring nodes in 244
 - displaying attributes of monitoring nodes in 247
 - displaying guide information in 247
 - searching for monitoring nodes in 246
 - searching for status-change events in 246
- Monitoring Tree window
 - monitoring from 244

- opening, from Visual Monitoring window 249
- saving information in 248
- monitor window 239
- monitor window of application, opening 239

N

- non-cluster system
 - logical host, operating (startup) 130
 - logical host, operating (termination) 134
- notes on
 - starting JP1/IM - Manager 139
 - stopping JP1/IM - Manager 139

O

- opening
 - Monitoring Tree window from Visual Monitoring window 249
 - other application windows from Tool Launcher 273
 - Visual Monitoring window 248
- opening monitor window
 - opening monitor window of application that issued JP1 events 239
- operating
 - changing severity level of JP1 events 212
 - deleting severe events 188
 - displaying detailed JP1 event information 184
 - displaying JP1 event search results 205
 - displaying only severe events 193
 - displaying operating procedures for JP1 events (linking with JP1/Navigation Platform) 239
 - displaying performance reports for JP1 events when linking with JP1/PFM 240
 - editing memo entry 186
 - executing commands by using Command button 261
 - executing commands by using Command Execution 259
 - opening monitor window 239
 - registering JP1 events as incidents in JP1/IM - Service Support (linking with JP1/IM - Service Support) 238
 - searching for JP1 events 203
 - setting response status for JP1 events from events list 188
 - switching event acquisition filter 194
- operation content
 - checking (UNIX) 430
 - checking (Windows) 423
- operations

- displaying login user list 248
- login 142
- logout 145
- opening Visual Monitoring window 248
- saving information in Monitoring Tree window on local host 248
- searching for monitoring nodes 251
- searching for monitoring nodes from monitoring tree 246
- starting JP1/IM - Manager 127
- stopping JP1/IM - Manager 132
- Tool Launcher window 273
- Using a Web browser to log in 142
- using command to log in 144
- using GUI to log in 142

P

- passwords of a monitored host in a remote monitoring configuration, tasks required when changed 118
- preparing
 - general procedures and preparation for handling occurrence of large number of events 219
 - preparing to suppress event forwarding from agent 221
- Procedure for re-distributing the system configuration when the host name of a manager or JP1/Base is changed 104
- procedures
 - changing IM database port 72
 - expanding IM database size 68
 - troubleshooting 344
- process status, checking 421, 429
- profiles, managing 283
 - displaying profiles 283
 - editing settings files 283
 - obtaining list of profiles 283
 - obtaining profiles 283
- program-specific extended attributes of JP1 events
 - displaying (displaying program-specific extended attributes) 208
 - displaying (mapping event information) 208

R

- RAS information
 - collecting (UNIX) 430
 - collecting (Windows) 424
- recovering 54
 - command execution log 55

- configuration information (UNIX) 38
- configuration information (Windows) 31
- database 54
 - event database 57
 - file for accumulated response-waiting events 58
 - host information database 57
 - IM database 58
 - monitored object database 56
- re-creating
 - command execution log 63
 - databases 63
 - event database 64
 - file for accumulated response-waiting events 67
 - host information database 64
 - monitored object database 64
- re-executing automated actions 270
- regular expression
 - to specify search conditions, using (event search) 205
- Related Events window
 - operating JP1 events from 189
- remote monitoring log file trap
 - notes applying before starting remote monitoring log file trap by using IM Configuration Management 518
- reorganizing 52
 - command execution log 52
 - event database 52
 - file for accumulated response-waiting events 52
 - host information database 52
 - IM database 52
 - monitored object database 52
- repeated events
 - consolidated event 189
- repeated events that are consolidated into consolidated event
 - checking detailed information about 189
 - setting response status for 189
- response-waiting event management function 319, 323
- response-waiting events 319
 - accumulating 327
 - canceling 330
 - handling in JP1/IM 322
 - issuing paths 322
 - manually removing from accumulation 339
 - monitoring 324
 - monitoring in Central Console 336
 - monitoring in Central Scope 338

- responding to [328, 339](#)
- resuming monitoring in hold-and-accumulate state [340](#)

S

- saving information in Monitoring Tree window on local host [248](#)
- searching
 - monitoring nodes [246, 251](#)
 - status-change events [251](#)
 - status-change events from monitoring tree [246](#)
- searching for
 - JP1 event [203](#)
- searching for JP1 events
 - operating [203](#)
 - search procedure [203](#)
- search method (JP1 event) [203](#)
- service operation information
 - displaying [285](#)
 - managing [284](#)
- setting
 - setting additional common exclusion-conditions by using JP1 events that have occurred [198](#)
 - setting threshold for automatically suppressing event forwarding on agent [229](#)
- setting additional common exclusion-conditions by using JP1 events that have occurred [198](#)
- Setting an additional common exclusion-condition to exclude a JP1 event from the monitoring target or action execution [198](#)
- settings information, changing [93](#)
- severe event
 - displaying [193](#)
- severe event filter
 - applying filter [183](#)
- Severe Events page
 - deleting severe events from [188](#)
- specifying
 - specifying repeated event conditions [230](#)
- starting
 - JP1/IM - Manager [127](#)
 - notes on [139](#)
- status-change events, searching [246, 251](#)
- stopping
 - JP1/IM - Manager [132](#)
 - notes on [139](#)
 - stopping, on manager, log file trap that issues large numbers of events [235](#)

- suppressing
 - handling occurrence of large number of events by suppressing event forwarding from agent [224](#)
 - preparing to suppress event forwarding from agent [221](#)
- symbol conventions [11](#)
- system date, changing of [111](#)
- system hierarchies
 - managing [277, 279](#)
- system monitoring from Central Console [174](#)
- System Monitoring from the Intelligent Integrated Management Base [146](#)
- system time, resetting of
 - advancing the time [114](#)

T

- Taking actions for the generation of a large number of events [219](#)
- Tasks necessary what you need to do immediately after you change the host name of the manager or JP1/Base [102](#)
- Tasks necessary when configuration of event-forwarding relay source for integrated agent host is changed [123](#)
- Tasks to be performed when the IP address of a manager or JP1/Base is changed [109](#)
- threshold
 - setting threshold for automatically suppressing event forwarding on agent [229](#)
- Tool Launcher
 - functions that can be operated from [274](#)
 - opening other application windows from [273](#)
 - operations in [273](#)
- troubleshooting [343, 442](#)
 - corrective actions [442](#)
 - data collection method [421](#)
 - data that needs to be collected [391](#)
 - log information types [345](#)
 - procedure [344](#)

U

- Unable to acquire the Promitor metric [552](#)
- Unable to acquire the Script exporter metric [552](#)
- unreadable characters
 - actions to take when trapped JP1 event message shows unreadable characters [480](#)
- user-defined extended attribute to JP1 events that match condition, adding [211](#)
- user dump

- collecting (Windows only) [424](#)
- user who executes commands [263](#)
- Using a Web browser to log in to JP1/IM - Manager (Intelligent Integrated Management Base) [142](#)

V

- version number conventions [12](#)
- view filter
 - applying filter [183](#)
- viewing, JP1 events [175](#)
- Viewing JP1 events (Events window) [150](#)
- virtual host, registering [280](#)
- virtual system
 - displaying host information in [280](#)
 - managing configuration of [280](#)
- Visual Monitoring window
 - changing monitoring status of monitoring nodes in [250](#)
 - changing status of monitoring nodes in [250](#)
 - displaying attributes of monitoring nodes from [252](#)
 - displaying guide information from [252](#)
 - monitoring from [249](#)
 - opening [248](#)
 - opening Monitoring Tree window from [249](#)
 - searching for monitoring nodes in [251](#)
 - searching for status-change events in [251](#)

W

- What to do if you change the host name of a manager or JP1/Base [103](#)
- 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 [533](#)
- Work when you change IP address of the manager or JP1/Base [109](#)

 **Hitachi, Ltd.**

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