HITACHI
Inspire the Next

Job Management Partner 1 Version 10

Job Management Partner 1/Integrated Management - Manager Administration Guide

3021-3-307-20(E)

Notices

■ Relevant program products

For details about the supported OS versions, and about the OS service packs and patches required by Job Management Partner 1/Integrated Management - Manager and Job Management Partner 1/Integrated Management - View, see the release notes for the relevant product.

Job Management Partner 1/Integrated Management - View (for Windows):

P-2W2C-6HAL Job Management Partner 1/Integrated Management - View 10-50

The above product includes the following:

P-CC242C-6HAL Job Management Partner 1/Integrated Management - View 10-50 (for Windows Server 2003 and Windows XP Professional)

P-CC2A2C-6HAL Job Management Partner 1/Integrated Management - View 10-50 (for Windows 8.1, Windows 8, Windows Server 2012, Windows 7, Windows Server 2008, and Windows Vista)

Job Management Partner 1/Integrated Management - Manager (for Windows):

P-2W2C-8EAL Job Management Partner 1/Integrated Management - Manager 10-50

The above product includes the following:

P-CC242C-8EAL Job Management Partner 1/Integrated Management - Manager 10-50 (for Windows Server 2003)

P-CC2A2C-8EAL Job Management Partner 1/Integrated Management - Manager 10-50 (for Windows Server 2012, Windows Server 2008)

Job Management Partner 1/Integrated Management - Manager (for Solaris):

P-9D2C-8EAL Job Management Partner 1/Integrated Management - Manager 10-50

Job Management Partner 1/Integrated Management - Manager (for AIX):

P-1M2C-8EAL Job Management Partner 1/Integrated Management - Manager 10-50

Job Management Partner 1/Integrated Management - Manager (for Linux 6.1 (x86) or later, Linux 6.1 (x64) or later, Linux 5.1 (x86) or later, and Linux 5.1 (AMD/Intel 64) or later):

P-812C-8EAL Job Management Partner 1/Integrated Management - Manager 10-50

■ Trademarks

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

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

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

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

Itanium is a trademark of Intel Corporation in the United States and other countries.

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

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

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

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

POSIX stands for Portable Operating System Interface for Computer Environment, which is a set of standard specifications published by the Institute of Electrical and Electronics Engineers, Inc.

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

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

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

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

VMware and VMware vSphere ESX are registered trademarks or trademarks of VMware, Inc. in the United States and/or other jurisdictions.

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

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

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

XPG4 stands for X/Open Portability Guide Issue 4, which is a set of specifications published by X/Open Company Limited.

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

The following program product contains some parts whose copyrights are reserved by Oracle Corporation, its subsidiaries, or affiliates: P-9D2C-8EAL.

The following program product contains some parts whose copyrights are reserved by UNIX System Laboratories, Inc.: P-9D2C-8EAL.

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

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

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

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

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

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

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

This product includes software developed by Andy Clark.

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

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

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

Other product and company names mentioned in this document may be the trademarks of their respective owners. Throughout this document Hitachi has attempted to distinguish trademarks from descriptive terms by writing the name with the capitalization used by the manufacturer, or by writing the name with initial capital letters. Hitachi cannot attest to the accuracy of this information. Use of a trademark in this document should not be regarded as affecting the validity of the trademark.

■ Microsoft product name abbreviations

This manual uses the following abbreviations for Microsoft product names.

Abbreviation		Full name or meaning
Hyper-V		Microsoft(R) Windows Server(R) 2008 Hyper-V(R)
		Microsoft(R) Windows Server(R) 2008 R2 Hyper-V(R)
		Microsoft(R) Windows Server(R) 2012 Hyper-V(R)
IE	Microsoft Internet Explorer	Microsoft(R) Internet Explorer(R)
	Windows Internet Explorer	Windows(R) Internet Explorer(R)
IIS	Internet Information Services	Microsoft(R) Internet Information Services 5.01 or later
SCVMM		Microsoft(R) System Center Virtual Machine Manager 2008
		Microsoft(R) System Center Virtual Machine Manager 2012
Windows 2000		Microsoft(R) Windows(R) 2000 Advanced Server Operating System
		Microsoft(R) Windows(R) 2000 Professional Operating System
		Microsoft(R) Windows(R) 2000 Server Operating System

Abbreviation		Full name or meaning
Windows 7		Microsoft(R) Windows(R) 7 Enterprise
		Microsoft(R) Windows(R) 7 Professional
		Microsoft(R) Windows(R) 7 Ultimate
Windows 8	Windows 8	Microsoft(R) Windows(R) 8 Enterprise
		Microsoft(R) Windows(R) 8 Pro
	Windows 8.1	Microsoft(R) Windows(R) 8.1 Enterprise
		Microsoft(R) Windows(R) 8.1 Pro
Windows Server 2003	Windows Server 2003	Microsoft(R) Windows Server(R) 2003, Enterprise Edition
		Microsoft(R) Windows Server(R) 2003, Standard Edition
	Windows Server 2003 (x64)	Microsoft(R) Windows Server(R) 2003, Enterprise x64 Edition
		Microsoft(R) Windows Server(R) 2003, Standard x64 Edition
	Windows Server 2003 R2	Microsoft(R) Windows Server(R) 2003 R2, Enterprise Edition
		Microsoft(R) Windows Server(R) 2003 R2, Standard Edition
	Windows Server 2003 R2 (x64)	Microsoft(R) Windows Server(R) 2003 R2, Enterprise x64 Edition
		Microsoft(R) Windows Server(R) 2003 R2, Standard x64 Edition
Windows Server 2008	Windows Server 2008	Microsoft(R) Windows Server(R) 2008 Enterprise
		Microsoft(R) Windows Server(R) 2008 Standard
	Windows Server 2008 (x64)	Microsoft(R) Windows Server(R) 2008 Enterprise x64
		Microsoft(R) Windows Server(R) 2008 Standard x64
	Windows Server 2008 R2 (x64)	Microsoft(R) Windows Server(R) 2008 R2 Datacenter x64
		Microsoft(R) Windows Server(R) 2008 R2 Enterprise x64
		Microsoft(R) Windows Server(R) 2008 R2 Standard x64
Windows Server 2012	Windows Server 2012	Microsoft(R) Windows Server(R) 2012 Datacenter
		Microsoft(R) Windows Server(R) 2012 Standard
	Windows Server 2012 R2	Microsoft(R) Windows Server(R) 2012 R2 Datacenter
		Microsoft(R) Windows Server(R) 2012 R2 Standard
Windows Vista		Microsoft(R) Windows Vista(R) Business
		Microsoft(R) Windows Vista(R) Enterprise
		Microsoft(R) Windows Vista(R) Ultimate

Abbreviation	Full name or meaning
Windows XP Professional	Microsoft(R) Windows(R) XP Professional Operating System

Windows is sometimes used generically, referring to Windows 8.1, Windows 8, Windows Server 2012, Windows 7, Windows Server 2008, Windows Vista, Windows Server 2003, Windows XP Professional, and Windows 2000.

■ 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

■ Copyright

Summary of amendments

The following table lists changes in this manual (3021-3-307-20(E)) and product changes related to this manual.

Changes	Location
JP1/IM files to back up were added as the email notification function was added. Notes on when a host name and IP address are changed were added. The causes and corrective actions were added for when an email does not reach the destination.	*1.1.1*, *2.2.1(1)*, *2.2.2(1)*, *10.5.1(57)*
The description that background colors can now be set on the **Severe Events** page was added.	*5.1.1*, *5.1.5*
The description that a view filter can now be used on the **Severe Events** page was added.	*5.1.5*, *5.7*
A step for selecting the range of events for which actions are to be suppressed was added to the procedure for using repeated event monitoring suppression (to suppress the actions associated with repeated events to which automated actions are assigned). Also, a procedure for setting notifications for when suppression continues was added.	*5.1.6(1)*, *5.1.6(2)*
Procedures for suppressing event forwarding when a large numbers of events occur were added.	*5.1.7*
Setting the event acquisition range at login is now available.	*5.1.11*
The description that the *Job Management Partner 1/Integrated Management - Manager Overview and System Design Guide* should be referred to for details about the specified display event period was added.	*5.1.12*
The description that a view filter is applied only on the **Monitor Events** page was deleted because a view filter can now be applied on the **Severe Events** page.	*5.1.13*
The following procedures for setting the severity of events in the GUI were added: • Setting the severity of events when the system is set up • Setting the severity of events during operation • Changing an additional severity changing definition to a severity changing definition	*5.3*

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

Preface

This manual explains administration, operations, and troubleshooting for Job Management Partner 1/Integrated Management - Manager and Job Management Partner 1/Integrated Management - View.

In this manual, Job Management Partner 1/Integrated Management is abbreviated to *JP1*, and Job Management Partner 1/Integrated Management - Manager and Job Management Partner 1/Integrated Management - View are generically referred to as *JP1/Integrated Management* or *JP1/IM*.

■ Intended readers

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

- System administrators who implement centralized monitoring of events that occur in the system
- System administrators who implement centralized monitoring of the system by associating the status of the infrastructure used to manage the system with the events that occur in the system.

■ 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.
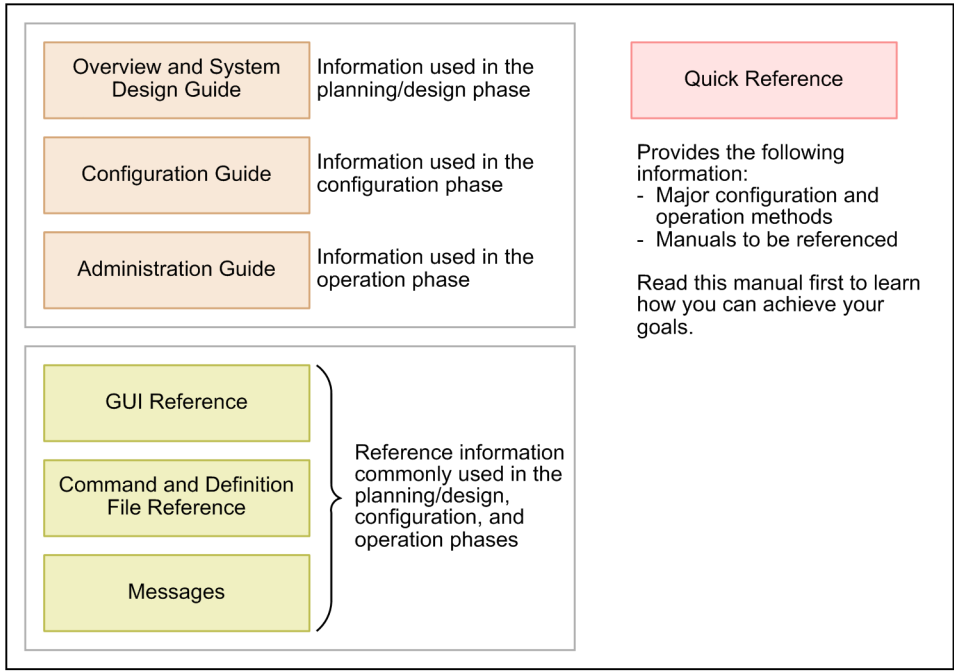
PART 4. Troubleshooting

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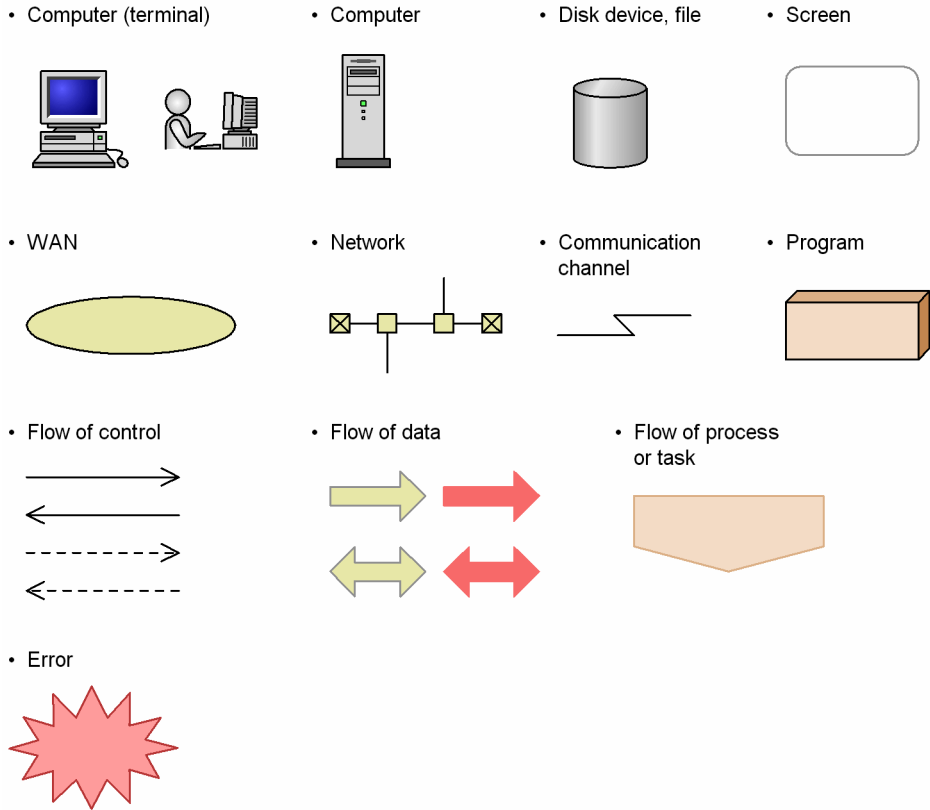
■ Manual suite

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.

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

■ 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

Font and symbol conventions are classified as:

- General font conventions
- Conventions in syntax explanations

These conventions are described below.

General font conventions

The following table lists the general font conventions:

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

Examples of coding and messages appear as follows (although there may be some exceptions, such as when coding is included in a diagram):

```
MakeDatabase

...

StoreDatabase temp DB32
```

In examples of coding, an ellipsis (`...`) indicates that one or more lines of coding are not shown for purposes of brevity.

Conventions in syntax explanations

Syntax definitions appear as follows:

Store**D**atabase [temp|perm] (*database-name ...*)

The following table lists the conventions used in syntax explanations:

Example font or symbol	Convention
StoreDatabase	Code-font characters must be entered exactly as shown.
database-name	This font style marks a placeholder that indicates where appropriate characters are to be entered in an actual command.
SD	Bold code-font characters indicate the abbreviation for a command.
<u>perm</u>	Underlined characters indicate the default value.
[ ]	Square brackets enclose an item or set of items whose specification is optional. If multiple items are enclosed, either omit them all or select one of them. Example: [A] means either nothing or A must be specified. [B|C] means nothing, or B, or C must be specified.
|	Only one of the options separated by a vertical bar can be specified at the same time. Example: A|B|C means A, or B, or C.
...	An ellipsis (...) indicates that the item or items enclosed in ( ) or [ ] immediately preceding the ellipsis may be specified as many times as necessary.
{ }	One of the items or sets of items enclosed in curly brackets must be selected. Inside the curly brackets, each item or set of items is separated by a vertical bar (|). Example: {A|B|C} means that A, or B, or C must be specified.
Δ	Indicates a space. Δ_0: Zero or more spaces (space can be omitted). Δ_1: One or more spaces (space cannot be omitted).
▲	Indicates a tab. Example: ▲ A means that a tab character precedes A.

Conventions 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	*View-path*	*system-drive*:\Program Files\Hitachi\JP1CoView
JP1/IM - Manager	*Manager-path*	*system-drive*:\Program Files\Hitachi\JP1IMM

Product name	Installation folder	Default installation folder[#]
	Console-path	*system-drive*:\Program Files\Hitachi\JP1Cons
	Scope-path	*system-drive*:\Program Files\Hitachi\JP1Scope
JP1/Base	*Base-path*	*system-drive*:\Program Files\Hitachi\JP1Base

#: Denotes the installation folder for each product when a default installation is performed.

For Windows 8.1, Windows 8, Windows Server 2012, Windows 7, Windows Server 2008, and Windows Vista, the location represented by *system-drive*:\Program Files is determined at installation by an OS environment variable and might differ depending on the environment.

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

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

■ Conventions: Version numbers

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

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

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

■ Online manuals

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

The HTML manual has the same contents as this manual.

To view the HTML manual:

- In JP1/IM - View, choose **Help** and then **Help Contents**.

Note:

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

Contents

Part 2: Operation

Part 4: Troubleshooting

10 Troubleshooting   206

Index   312

1

JP1/IM System Maintenance

This chapter explains JP1/IM system maintenance.

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

1.1 Managing the configuration information

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

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

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

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

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

- Host name
- IP address
- PP version (match the format of VVRRRZZ)
- 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.

1.1.1 Backup (in Windows)

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

If you change the JP1/IM configuration, make a backup. When you make a backup of JP1/IM, be sure to make a backup of JP1/Base at the same time. For details about how to back up the definition files that are configured by JP1/Base users, see the *Job Management Partner 1/Base User's Guide*.

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

- The definition files may be modified during execution in some cases. If a backup is made while a definition file is being modified, the backup file will be corrupted.
  Immediately following the backup operation, compare the collected backup file with the original file to make sure their contents match.

- When you make a backup, do not lock the target file. If you need to lock the file, first log out from all viewers that are connected, and then copy the target file to another file. After you have copied it, compare the copied file with the original file to make sure their contents match, and then back up the copied file.

Back up all of the files shown in the table below. If you back up only some of the files, relationships with the remaining files might become inconsistent, preventing the system from operating correctly.

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

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

Table 1–1: JP1/IM files to back up

Product name		File name	Description
Common to all products		Backup files created in *6.2.2(4) Copying the common definition information* in the *Job Management Partner 1/Integrated Management - Manager Configuration Guide*	Common definition information backup file[#1]
JP1/IM - Manager	JP1/IM - Central Console	*Console-path*\conf\jp1co_env.conf	IM environment definition file
		Console-path\conf\jp1co_param.conf	IM parameter definition file
		Console-path\conf\jp1co_param_V7.conf	IM parameter definition file
		Console-path\conf\jp1co_service.conf	Extended startup process definition file
		Console-path\conf\jp1co_system.conf	IM server system environment settings file
		Console-path\conf\action\actdef.conf	Automated action definition file
		Console-path\conf\console\actprofile\actprofile_*JP1-user-name*	Action profile
		Console-path\conf\console\actprofile\actprofile2_*JP1-user-name*	
		Console-path\conf\console\actprofile\actprofile_0950_*JP1-user-name*	
		Console-path\conf\console\attribute*.conf	Definition file for extended event attributes
		Console-path\conf\console\filter*.conf	Filter definition file
		Console-path\conf\console\filter\attr_list\common_exclude_filter_attr_list.conf	Common-exclusion-conditions display item definition file
		Console-path\conf\console\filter\auto_list\common_exclude_filter_auto_list.conf	Common-exclusion-conditions auto-input definition file
		Console-path\conf\console\mapping\mapping.conf	Event information mapping definition file

Product name	File name	Description
	Console-path\conf\console\monitor*.conf	Definition file for opening monitor windows
	Console-path\conf\console\object_type*	Definition file for object types
	Console-path\conf\console\profile\.system	System profile
	Console-path\conf\console\profile\defaultUser	JP1/IM - View user profile (default)
	Console-path\conf\console\profile\profile_*JP1-user-name*	JP1/IM - View user profile
	Console-path\conf\console\profile\systemColor.conf	System color definition file
	Console-path\www\console.html[#2]	Web-based operation definition file
	Console-path\default\console.conf[#2]	Communication environment definition file
	Console-path\conf\console\correlation\view_cor.conf	Settings file for the consolidated display of repeated events
	Console-path\conf\console\correlation\view_cor_*JP1-user-name*.conf	Settings file for the consolidated display of repeated events
	Console-path\conf\console\rmtcmd\cmdbtn.conf	Command button definition file
	Console-path\conf\health\jcohc.conf	Health check definition file
	Console-path\conf\hostmap\user_hostmap.conf	Event-source-host mapping definition file
	Console-path\conf\action\actnotice.conf	Automatic action notification definition file
	Console-path\conf\processupdate\processupdate.conf	Status event definition file
	Console-path\conf\guide\jco_guide.txt	Event guide information file
	Console-path\conf\system\event_storm*.conf	Repeated event condition definition file
	Console-path\conf\console\event_storm\attr_list\event_storm_attr_list.conf	Display item definition file for repeated event condition
	Console-path\conf\console\event_storm\auto_list\event_storm_auto_list.conf	Auto-input definition file for repeated event condition
	Console-path\conf\console\incident\incident.conf	Definition file for manually registering incidents
	user-selected-folder*user-selected-file-name*	Event guide message file

Product name		File name	Description
		All files under *Console-path*\conf\evgen\	Definition files for correlation event generation
		user-selected-folder*file-name*.conf	Correlation event generation definition file
		Console-path\conf\action\attr_list\attr_list.conf	File that defines which items are displayed for event conditions
		Console-path\conf\mail\jimmail.conf	Email environment definition file
	JP1/IM - Central Scope	*Scope-path*\conf\jcs_guide*.txt	Guide information file
		Scope-path\conf\jcs_hosts	Host information file
		Scope-path\conf\action_complete_on.conf	Settings file for completed-action linkage function
		Scope-path\conf\action_complete_off.conf	
		user-selected-folder*user-selected-file-name*	Definition file for automatic delete mode of status change event
		user-selected-folder*user-selected-file-name*	Definition file for monitoring object initialization mode
		Scope-path\conf\auto_dbbackup_on.conf	Backup recovery settings file for monitored object database
		Scope-path\conf\auto_dbbackup_off.conf	
		Scope-path\conf\evhist_warn_event_on.conf	Settings file for the maximum number of status change events
		Scope-path\conf\evhist_warn_event_off.conf	
		user-selected-folder*user-selected-file-name*	Guide message file
		user-selected-folder*user-selected-file-name*	Definition file for on memory mode of status change condition
	IM Configuration Management	*Manager-path*\conf\imcf\jp1cf_applyconfig.conf	Apply-IM-configuration-method definition file
		Manager-path\conf\imcf\jp1cf_treedefaultpolicy.csv	Default monitoring policy definition file
		All files under *Manager-path*\data\imcf	System management information
		All files under *shared-folder*\JP1IMM\data\imcf	
		Manager-path\conf\agtless\targets\wmi.ini	Definition files regarding WMI authentication information
		shared-folder\JP1IMM\conf\agtless\targets\wmi.ini	
		Manager-path\conf\agtless\targets\ssh.ini	Definition files regarding SSH authentication information
		shared-folder\JP1IMM\conf\agtless\targets\ssh.ini	
JP1/IM - View		*View-path*\conf\webdata\en*.html	Web page call definition file
		View-path\conf\tuning.conf	IM - View settings file

Product name	File name	Description
	View-path\default\view.conf.update	Communication environment definition file
	View-path\default\tree_view.conf.update	
	View-path\conf\sovtoolexec\en\!JP1_CS_APP0.conf	Start program definition file
	View-path\conf\sovtoolitem\en\!JP1_CS_FTOOL0.conf	Toolbar definition file
	View-path\conf\sovtoolitem\en\!JP1_CS_FTREE0.conf	Icon operation definition file
	View-path\conf\appexecute\en*.conf	Definition file for executing applications
	View-path\conf\function\en*.conf	Definition file for the tool launcher
	user-selected-folder*user-selected-file-name*	Configuration file for monitoring tree
	Files under *View-path*\image\icon\	Icon file
	Files under *View-path*\image\visual\	Visual icon file[#3]
	Files under *View-path*\image\map\	Background-image-file-name
	View-path\conf\jcfview\jcfview.conf	Operation definition file for IM Configuration Management - View
	View-path\conf\jrmview\jrmview.conf	Operation definition file for Rule Operation - View[#4]
	View-path\default\jrmview_reg.conf	Common definition settings file[#4]

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

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

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

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

1.1.2 Recovery (in Windows)

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

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

Prerequisite conditions:

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

- JP1/Base and JP1/IM - Manager are stopped.

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

1.1.3 Backup (in UNIX)

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

If you change the JP1/IM configuration, make a backup. When you make a backup of JP1/IM, be sure to make a backup of JP1/Base at the same time. For details about how to back up the definition files that are configured by JP1/Base users, see the *Job Management Partner 1/Base User's Guide*.

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

- The definition files may be modified during execution in some cases. If a backup is made while a definition file is being modified, the backup file will be corrupted.
  Immediately following the backup operation, compare the collected backup file with the original file to make sure their contents match.

- When you make a backup, do not lock the target file. If you need to lock the file, first log out from all viewers that are connected, and then copy the target file to another file. After you have copied it, compare the copied file with the original file to make sure their contents match, and then back up the copied file.

Back up all of the files shown in the table below. If you back up only some of the files, relationships with the remaining files might become inconsistent, preventing the system from operating correctly.

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

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

Table 1–2: JP1/IM files to back up

Product name		File name	Description
Common to all products		Backup files created in *6.3.2(4) Copying the common definition information* in the *Job Management Partner 1/Integrated Management - Manager Configuration Guide*	Common definition information backup file[#1]
JP1/IM - Manager	JP1/IM - Central Console	`/etc/opt/jp1cons/conf/jp1co_env.conf`	IM environment definition file
		`/etc/opt/jp1cons/conf/jp1co_param.conf`	IM parameter definition file
		`/etc/opt/jp1cons/conf/jp1co_param_V7.conf`	IM parameter definition file
		`/etc/opt/jp1cons/conf/jp1co_service.conf`	Extended startup process definition file
		`/etc/opt/jp1cons/conf/jp1co_system.conf`	IM server system environment settings file

Product name	File name	Description
	`/etc/opt/jp1cons/conf/action/actdef.conf`	Automated action definition file
	`/etc/opt/jp1cons/conf/console/actprofile/` `actprofile_JP1-user-name`	Action profile
	`/etc/opt/jp1cons/conf/console/actprofile/` `actprofile2_JP1-user-name`	
	`/etc/opt/jp1cons/conf/console/actprofile/` `actprofile_0950_JP1-user-name`	
	`/etc/opt/jp1cons/conf/console/attribute/*.conf`	Definition file for extended event attributes
	`/etc/opt/jp1cons/conf/console/filter/*.conf`	Filter definition file
	`/etc/opt/jp1cons/conf/console/filter/attr_list/` `common_exclude_filter_attr_list.conf`	Common-exclusion-conditions display item definition file
	`/etc/opt/jp1cons/conf/console/filter/auto_list/` `common_exclude_filter_auto_list.conf`	Common-exclusion-conditions auto-input definition file
	`/etc/opt/jp1cons/conf/console/mapping/mapping.conf`	Event information mapping definition file
	`/etc/opt/jp1cons/conf/console/monitor/*.conf`	Definition file for opening monitor windows
	`/etc/opt/jp1cons/conf/console/object_type/*`	Definition file for object types
	`/etc/opt/jp1cons/conf/console/profile/.system`	System profile
	`/etc/opt/jp1cons/conf/console/profile/defaultUser`	JP1/IM - View user profile (default)
	`/etc/opt/jp1cons/conf/console/profile/profile_JP1-user-` `name`	JP1/IM - View user profile
	`/etc/opt/jp1cons/conf/console/profile/systemColor.conf`	System color definition file
	`/opt/jp1cons/www/console.html`[#2]	Web-based operation definition file
	`/etc/opt/jp1cons/default/console.conf`[#2]	Communication environment definition file
	`/etc/opt/jp1cons/conf/console/correlation/` `view_cor.conf`	Settings file for the consolidated display of repeated events
	`/etc/opt/jp1cons/conf/console/correlation/` `view_cor_JP1-user-name.conf`	Settings file for the consolidated display of repeated events
	`/etc/opt/jp1cons/conf/console/rmtcmd/cmdbtn.conf`	Command button definition file
	`/etc/opt/jp1cons/conf/health/jcohc.conf`	Health check definition file

1. JP1/IM System Maintenance

Product name		File name	Description
		`/etc/opt/jp1cons/conf/hostmap/user_hostmap.conf`	Event-source-host mapping definition file
		`/etc/opt/jp1cons/conf/action/actnotice.conf`	Automatic action notification definition file
		`/etc/opt/jp1cons/conf/processupdate/processupdate.conf`	Status event definition file
		`/etc/opt/jp1cons/conf/guide/jco_guide.txt`	Event guide information file
		`/etc/opt/jp1cons/conf/console/incident/incident.conf`	Definition file for manually registering incidents
		`/etc/opt/jp1cons/conf/system/event_storm/*.conf`	Repeated event condition definition file
		`/etc/opt/jp1cons/conf/console/event_storm/attr_list/event_storm_attr_list.conf`	Display item definition file for repeated event condition
		`/etc/opt/jp1cons/conf/console/event_storm/auto_list/event_storm_auto_list.conf`	Auto-input definition file for repeated event condition
		user-selected-directory/*user-selected-file-name*	Event guide message file
		All files under `/etc/opt/jp1cons/conf/evgen/`	Definition files for correlation event generation
		user-selected-directory/*file-name*`.conf`	Correlation event generation definition file
		`/etc/opt/jp1cons/conf/chsev/jcochsev.conf`	Severity changing definition file
		`/etc/opt/jp1cons/conf/action/attr_list/attr_list.conf`	File that defines which items are displayed for event conditions
	JP1/IM - Central Scope	`/etc/opt/jp1scope/conf/jcs_guide*.txt`	Guide information file
		`/etc/opt/jp1scope/conf/jcs_hosts`	Host information file
		`/etc/opt/jp1scope/conf/action_complete_on.conf`	Settings file for completed-action linkage function
		`/etc/opt/jp1scope/conf/action_complete_off.conf`	
		user-selected-directory/*user-selected-file-name*	Definition file for automatic delete mode of status change event
		user-selected-directory/*user-selected-file-name*	Definition file for monitoring object initialization mode
		`/etc/opt/jp1scope/conf/auto_dbbackup_on.conf`	Backup recovery settings file for monitored object database
		`/etc/opt/jp1scope/conf/auto_dbbackup_off.conf`	
		`/etc/opt/jp1scope/conf/evhist_warn_event_on.conf`	Settings file for the maximum number of status change events
		`/etc/opt/jp1scope/conf/evhist_warn_event_off.conf`	

Product name		File name	Description
		user-selected-directory/*user-selected-file-name*	Guide message file
		user-selected-directory/*user-selected-file-name*	Definition file for on memory mode of status change condition
	IM Configuration Management	`/etc/opt/jp1imm/conf/imcf/jp1cf_applyconfig.conf`	Apply-IM-configuration -method definition file
		`/etc/opt/jp1imm/conf/imcf/jp1cf_treedefaultpolicy.csv`	Default monitoring policy definition file
		All files under `/var/opt/jp1imm/data/imcf/`	System management information
		All files under *shared-directory*/`jp1imm/data/imcf/`	
		`/etc/opt/jp1imm/conf/agtless/targets/ssh.ini`	Definition files regarding SSH authentication information
		shared-directory/`jp1imm/conf/agtless/targets/ssh.ini`	

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

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

1.1.4 Recovery (in UNIX)

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

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

Prerequisite conditions:

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

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

1.2 Managing the databases

The JP1/IM system uses the following databases:

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

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

1.2.1 Database reorganization

(1) Reorganization of the command execution log

There is no need to reorganize the command execution log.

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

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

(3) Reorganization of the event database

There is no need to reorganize the event database.

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

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

(5) Reorganization of the IM database

This subsection explains the procedure for reorganizing the IM database.

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 an undue amount of time.

To prevent such things from happening, reorganize the IM database at a time such as below.

Note that because free space in the integrated monitoring database does not become fragmented, reorganization of the IM database is not necessary if only the integrated monitoring database is used.

- 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 integrated trace log or 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. Using the `jimdbreclaim` command, release the free space in the database.

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

2. Using the `jimdbrorg` command, reorganize the database.
   For details about the `jimdbrorg` command, see *jimdbrorg* (*1. Commands*) in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.

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

(b) Reorganizing the IM database in a cluster environment

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

To reorganize the IM database in a cluster environment:

1. Stop the JP1/IM - Manager service and the cluster database service.
   If JP1/IM - MO is being used, also stop the JP1/IM - Message Optimizer service of JP1/IM - MO on the connection source.

2. Using the `jimdbrorg` command, reorganize the database.
   For details about the `jimdbrorg` command, see *jimdbrorg* (*1. Commands*) in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.

3. Start the JP1/IM - Manager service and the cluster database service that you stopped in Step 1.
   If JP1/IM - MO is being used, also start the JP1/IM - Message Optimizer service of JP1/IM - MO on the connection source.

1.2.2 Database backup and recovery

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

- Host name
- IP address
- PP version (match the format of VVRRRZZ)
- 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.

Also, 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.

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

(c) Files to back up

The files to back up are listed below.

In Windows:

Table 1–3: Files to back up (Windows)

Information type	Files to back up
Command execution log file	All files under *Base-path*\log\COMMAND\
	All files under *shared-folder*\jp1base\log\COMMAND\
Action information file	*Console-path*\log\action\actinf.log
	shared-folder\jp1cons\log\action\actinf.log
Action hosts file	*Console-path*\log\action\acttxt{1|2}.log
	shared-folder\jp1cons\log\action\acttxt{1|2}.log

In UNIX:

Table 1–4: Files to back up (UNIX)

Information type	Files to back up
Command execution log file	All files under /var/opt/jp1base/log/COMMAND/
	All files under *shared-directory*/jp1base/log/COMMAND/
Action information file	/var/opt/jp1cons/log/action/actinf.log
	shared-directory/jp1cons/log/action/actinf.log
Action hosts file	/var/opt/jp1cons/log/action/acttxt{1|2}.log
	shared-directory/jp1cons/log/action/acttxt{1|2}.log

For details about the command execution log file, see the *Job Management Partner 1/Base User's Guide*.

(2) Monitored object database backup and recovery procedures

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

(a) Backup procedure

To back up the monitored object database:

1. Stop JP1/IM - Manager.

2. Back up the target files.
   The table below shows the files to back up.

   Table 1–5: Files to back up

OS	Information type	Files to back up
Windows	Monitored object database	All files under *Scope-path*\database\jcsdb\
		All files under *shared-folder*\jp1scope\database\jcsdb\
UNIX	Monitored object database	All files under /var/opt/jp1scope/database/jcsdb/
		All files under *shared-directory*/jp1scope/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 1–6: Files to back up

OS	Information type	Files to back up
Windows	Host information database	All files under *Scope-path*\database\jcshosts\
		All files under *shared-folder*\jp1scope\database\jcshosts\

OS	Information type	Files to back up
UNIX	Host information database	All files under `/var/opt/jp1scope/database/jcshosts/`
		All files under *shared-directory*`/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 *Job Management Partner 1/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 note**
>
> When you are backing up and recovering the event database, you must also back up and recover the command execution log at the same time.
>
> If you back up and recover only the event database, an inconsistency will occur in the association of JP1 event execution results and automated actions inside the event database.
>
> The results of automated actions executed before the event database recovery may be displayed as the execution results of automated actions for JP1 events registered after the event database recovery.

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

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

(a) Backup procedure

1. Stop JP1/IM - Manager.

2. Back up the target files.
   The table below shows the files to back up.

Table 1–7: Files to back up

OS	Files to back up
Windows	*Console-path*\log\response\resevent.dat
	shared-folder\jp1cons\log\response\resevent.dat
UNIX	/var/opt/jp1cons/log/response/resevent.dat
	shared-directory/jp1cons/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 note**
>
> 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*.

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

2. Use the jimdbbackup command to make a backup of the target database.
   For details about the jimdbbackup command, see *jimdbbackup* (*1. Commands*) in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.

3. Back up the target files.
   For details about which files to back up, see *1.1.1 Backup (in Windows)* and *1.1.3 Backup (in UNIX)*.

4. Start the JP1/IM - Manager service.
   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 on a physical host:

1. Stop the JP1/IM - Manager service.

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

2. Using the `jimdbrecovery` command, recover the target database.

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

3. Place the backed up files in their respective directories.

   With IM configuration management enabled, place the backed up files in their respective directories.

4. Start the JP1/IM - Manager service.

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

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

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

To back up the IM database in a cluster environment:

1. Stop the JP1/IM - Manager service and the cluster database service.

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

2. Using the `jimdbbackup` command, make a backup of the target database.

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

3. Back up the target files.

   For details about which files to back up, see *1.1.1 Backup (in Windows)* and *1.1.3 Backup (in UNIX)*.

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

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

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

1. Stop the JP1/IM - Manager service and the cluster database service.

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

2. Using the `jimdbrecovery` command, recover the target database.

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

3. Place the backed up files in their respective directories.

   With IM configuration management enabled, place the backed up files in their respective directories.

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

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

1.2.3 Re-creating a database and changing its settings

(1) Re-creating the command execution log

To re-create the command execution log:

1. Stop JP1/IM - Manager.

2. Stop JP1/Base.

3. Delete the command execution log file, the action information file, and the action hosts file shown in the table below.
   In Windows:

   Table 1–8: Files to delete (Windows)

Information type	Files to delete
Command execution log file	All files under *Base-path*\log\COMMAND\
	All files under *shared-folder*\jp1base\log\COMMAND
Action information file	*Console-path*\log\action\actinf.log
	shared-folder\jp1cons\log\action\actinf.log
Action hosts file	*Console-path*\log\action\acttxt{1|2}.log
	shared-folder\jp1cons\log\action\acttxt{1|2}.log

   In UNIX:

   Table 1–9: Files to delete (UNIX)

Information type	Files to delete
Command execution log file	All files under /var/opt/jp1base/log/COMMAND/
	All files under *shared-directory*/jp1base/log/COMMAND/
Action information file	/var/opt/jp1cons/log/action/actinf.log
	shared-directory/jp1cons/log/action/actinf.log
Action hosts file	/var/opt/jp1cons/log/action/acttxt{1|2}.log
	shared-directory/jp1cons/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 the procedure, in the JP1/Base User's Guide, see the chapter that explains Event Service environment setup, and see Procedure for initializing Event Service in the Event Service troubleshooting section.

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 on how to re-create the command execution log, see .

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

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

1. Stop JP1/IM - Manager.

2. Execute the JP1/Base jevdbinit command without the -s option.
   If you execute the jevdbinit command without the -s option, the serial numbers in the pre-initialization event database are inherited.

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

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

For details on how to re-create the command execution log, see .

For details on the `jevdbinit` command, see the chapter about commands in the "Job Management Partner 1/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 the procedure, in the JP1/Base User's Guide, see the chapter that explains Event Service environment setup, and see Procedure for initializing Event Service in the Event Service troubleshooting section.

(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.

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 chapter that explains Event Service environment setup and setup of JP1 event forwarding in the *Job Management Partner 1/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 *Job Management Partner 1/Base User's Guide*.

4. Start the JP1/Base (and JP1/IM - Manager) that you stopped in Step 2.

5. Start the JP1/Base that you stopped in Step 1.

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

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

Figure 1–1: Example showing hosts and forwarding destination hosts on which event databases are to be re-created
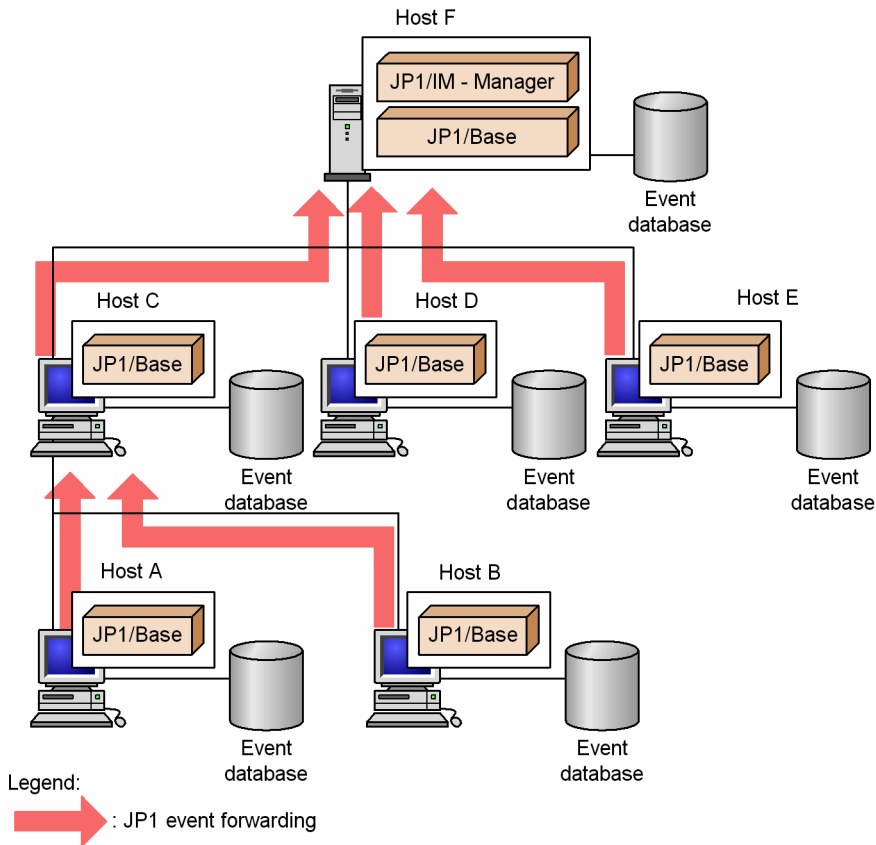
To re-create (delete) the event database of host A, it is necessary to delete the event databases of Hosts C and F, which are the forwarding destination hosts for JP1 events.

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

1. Stop JP1/IM - Manager.

2. Delete the file for accumulated response-waiting events.

Table 1–10: Files to delete

OS	Files to delete
Windows	*Console-path*\log\response\resevent.dat
	shared-folder\jp1cons\log\response\resevent.dat
UNIX	/var/opt/jp1cons/log/response/resevent.dat
	shared-directory/jp1cons/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.

(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 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`

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

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

2. Back up the database.

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

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

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

   Unset up only those databases that have been set up.

4. Edit the setup information file.

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

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

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

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

6. Recover the database.

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

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

7. Restart the JP1/IM - Manager service.

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

   `jcoimdef -db ON`

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

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

- Procedure when stopping system monitoring via Central Console

1. Stop the JP1/IM - Manager service.

2. Back up the database.

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

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

3. Unset up the integrated monitoring database and the IM Configuration Management database.
Unset up only those databases that have been set up.

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

5. Set up the integrated monitoring database and the IM Configuration Management database.
Set up only those databases that you unset up in Step 3.
During setup, you need to specify a database size that is larger than the size of the database you backed up, and the same database directory that was used during the backup.

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

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

7. Start the JP1/IM - Manager service.

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

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

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

1. Isolate the integrated monitoring database and the IM Configuration Management database.
Isolate the integrated monitoring database and the IM Configuration Management database so that Central Console only uses the JP1/Base event database.
Execute the following command, and then restart JP1/IM - Manager:
`jcoimdef -db OFF -h` *logical-host-name*

For details about the `jcoimdef` command, see *jcoimdef* (*1. Commands*) in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.
If JP1/IM - MO is being used, also stop the JP1/IM - Message Optimizer service of JP1/IM - MO on the connection source.

2. Stop the cluster database service.
Stop the cluster database service registered in the cluster software.

3. Back up the database.
Execute the `jimdbbackup` command with the `-m EXPAND` option specified.

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

4. Unset up the integrated monitoring database and the IM Configuration Management database.
Unset up only those databases that have been set up.

5. Edit the cluster setup information file.

Change the size specified in the database size (IMDBSIZE) of the cluster setup information file.

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

   Set up only those databases that were unset up in Step 4.

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

7. Recover the database.

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

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

8. Start the cluster database service.

   Start the cluster database service you stopped in Step 2.

9. Restart the JP1/IM - Manager service.

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

   jcoimdef -db ON -h *logical-host-name*

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

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

- Procedure when stopping system monitoring via Central Console

1. Stop the JP1/IM - Manager service and the cluster database service.

   Stop the JP1/IM - Manager service and the cluster database service registered in the cluster software.

2. Back up the database.

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

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

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

   Unset up only those databases that have been set up.

4. Edit the cluster setup information file.

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

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

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

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

6. Recover the database.

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

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

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

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

(6) Procedure for changing the IM database port

To change the IM database port:

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

2. Back up the database.
   Execute the `jimdbbackup` command with the `-m MAINT` option specified.
   For details about the `jimdbbackup` command, see *jimdbbackup* (*1. Commands*) in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.

3. Unset up both the integrated monitoring database and the IM Configuration Management database.
   Unset up only those databases that have been set up.

4. Edit the setup information file.
   Change the port number described in the setup information file.

5. Set up both the integrated monitoring database and the IM Configuration Management database.
   Set up only those databases that were unset up in Step 3.

6. Recover the database.
   Execute the `jimdbrecovery` command with the `-m MAINT` option specified.
   For details about the `jimdbrecovery` command, see *jimdbrecovery* (*1. Commands*) in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.

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

(7) Procedure for rebuilding the IM database

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

To rebuild the IM database:

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

2. Back up the database.
   Execute the `jimdbbackup` command with the `-m MAINT` option specified.
   For details about the `jimdbbackup` command, see *jimdbbackup* (*1. Commands*) in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.

3. Unset up both the integrated monitoring database and the IM Configuration Management database.
   Unset up only those databases that have been set up.

4. Change the name of the host on which JP1/IM - Manager has been installed.

5. This step is not necessary if the host name is not changed.

6. 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.

7. Recover the database.
   Execute the `jimdbrecovery` command with the `-m MAINT` option specified.
   For details about the `jimdbrecovery` command, see *jimdbrecovery* (*1. Commands*) in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.

8. Start JP1/IM - Manager.
   Start the JP1/IM - Manager of the host to be changed. When you are setting up a logical host, you need to edit the logical host name in the cluster setup information file.
   If JP1/IM - MO is being used, also start the JP1/IM - Message Optimizer service of JP1/IM - MO on the connection source.

1.3 Managing the disk capacity

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

1.3.1 Managing the IM database capacity

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

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

For details about increasing the log file size, see *1.3.2 Managing the log file size*.

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

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

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

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

   The following table shows the items that are displayed.

   Table 1–11: Displayed items

Displayed item	Description
Percentage of events that have not been saved	Shows the percentage of JP1 events within the integrated monitoring database that have not been output or saved (a ratio relative to the maximum capacity of 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* (*1. Commands*) in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.

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

To set up a deletion warning notification:

1. Enable the issuance of deletion warning notification events.

   Executing the `jcoimdef -dbntc ON` command enables the function that issues a deletion warning notification event when the percentage of JP1 events within the integrated monitoring database that have not been output and saved (a ratio relative to the maximum capacity of the integrated monitoring database) exceeds the deletion warning notification level. 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%. You can specify a value between 20 and 80 for the deletion warning notification level. The default is 80.

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

For details about when the IM configuration management database is used, see *1.2.1(5) Reorganization of the IM database*.

1.3.2 Managing the log file size

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

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

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

1.3.3 Managing dump files

If JP1/IM, JP1/Base, or a user program abnormally terminates because of a problem, a dump file such as a Dr. Watson log (in Windows) or a core dump (in UNIX) may 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.

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

1.4 Using historical reports

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

1.4.1 Outputting events to a CSV file

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

- Outputting a snapshot of event information to a CSV file

  A snapshot means extraction of information at a specific time. The snapshot of event information displayed in JP1/IM - View can output JP1 events that are filtered according to the operation. For example, a snapshot showing the host or product where a problem has occurred, or a snapshot showing the corrective action being taken can be used as a system problem report.

  For details about how to output the events list displayed in the Event Console window to a CSV file, see *5.9.1 Outputting an events list to a CSV file*.

- Outputting the content of the event database to a CSV file

  Using the `jevexport` 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 `jevexport` command to output the content of the agent's event database to a CSV file.

  For details about the `jevexport` command, see the chapter that explains commands in the *Job Management Partner 1/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* (*1. Commands*) in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.

1.4.2 Correlation event generation history

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

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

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

1.5 Migrating the configuration information and databases

1.5.1 Configuration information and databases to be migrated

This subsection explains the migration target when the configuration information and databases of JP1/IM are migrated.

Note that the configuration information and databases of JP1/IM need to be migrated when one of the following items of the migration-destination host is different:

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

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

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

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

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

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

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

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

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

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

To apply the imported IM configuration management information to the system, see *8.7.3 Applying the imported management information of IM Configuration Management to a system*.

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

(4) JP1/IM - View

Configuration information and databases must be re-created on the host at the migration destination.

(5) IM database

For details about migrating the IM database, see *1.2.3(7) Procedure for rebuilding the IM database*.

The directory for storing the IM database on the host at the migration destination must have the same configuration as the migration-source directory.

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 *Job Management Partner 1/Integrated Management - Manager Overview and System Design Guide*. For details about how to carry out setting tasks, see the *Job Management Partner 1/Integrated Management - Manager Configuration Guide* and the *Job Management Partner 1/Base User's Guide*.

2.2 Changing the settings of the host on which JP1/IM runs

This section explains the tasks you must perform to change the settings of the host on which JP1/IM is running.

- Effects of changing the host name, IP address, and system date/time of the host on which JP1/IM is running, and the tasks you must perform to make these changes
- The tasks you must perform to change the passwords of the manager and monitored remote hosts in a remote monitoring configuration
- The tasks you must perform to change the date/time of a monitored host

When, for example, it is necessary to make changes in the network configuration, use the explanations given in this section to perform the necessary tasks.

2.2.1 Effects of a host name change and the necessary tasks

This subsection explains the effects of a host name change and the tasks you must perform as a result of this change.

(1) Effects of a host name change

(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.

(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.

(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.

(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.

(f) Host name 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.

(2) Tasks that become necessary as a result of a host name change

(a) Tasks required in JP1/IM - Manager and JP1/IM - View

You must redistribute the system configuration. The procedure follows.

To redistribute the system configuration:

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 how to redistribute the system configuration, see *1.9 Setting the system hierarchy (when IM Configuration Management is used)*, *1.10 Setting the system hierarchy (when IM Configuration Management is not used)* (in Windows) or *2.9 Setting the system hierarchy (when IM Configuration Management is not used)* (in UNIX) in the *Job Management Partner 1/Integrated Management - Manager Configuration Guide*.

(b) Tasks required in JP1/Base

You must first terminate JP1/Base and then restart it.

(c) Tasks required in the IM database

See *1.2.3(7) Procedure for rebuilding the IM database*.

(3) When a cluster system is used

To change a logical host name in an environment in which a cluster system is running, delete the logical host name before the change. Then, set up the logical host name following the change so that it can operate in a cluster operation system.

In Windows:

For details about how to delete a logical host, see *6.2.6 Deleting the IM databases and logical host* in the *Job Management Partner 1/Integrated Management - Manager Configuration Guide*. For the setup method, see *6.2.2 Installing and setting up the logical host (new installation and setup)* or *6.2.3 Installing and setting up the logical host (upgrade installation and setup)* in the *Job Management Partner 1/Integrated Management - Manager Configuration Guide*.

In UNIX:

For details about how to delete a logical host, see *6.3.6 Deleting the IM databases and logical host* in the *Job Management Partner 1/Integrated Management - Manager Configuration Guide*. For the setup method, see *6.3.2 Installing and setting up the logical host (new installation and setup)* or *6.3.3 Installing and setting up the logical host (upgrade installation and setup)* in the *Job Management Partner 1/Integrated Management - Manager Configuration Guide*.

> ▌ **Important note**
>
> JP1 events that were issued under the old host name are processed as described below after the host name is changed.

- **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.

2.2.2 Effects of an IP address change and the necessary tasks

This subsection explains the effects of an IP address change and the tasks you must perform as a result of this change.

(1) Effects of an IP address change

(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.

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

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

If an IP address defined as the SMTP server and POP3 server in the mail environment definition file needs to be changed, you must change the IP address setting in the mail environment definition file.

(2) Tasks that become necessary as a result of an IP address change

(a) Tasks required in JP1/IM - Manager and JP1/IM - View

You must restart JP1/IM - Manager and JP1/IM - View. The procedure follows.

To restart JP1/IM - Manager and JP1/IM - View:

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.

(b) Tasks required in JP1/Base

You must first terminate JP1/Base, and then restart it.

(c) Tasks required in the IM database

You must first terminate the IM database, and then restart it.

2.2.3 Tasks that become necessary as a result of a system date/time change

This subsection explains the procedure for changing the system date/time while JP1/IM is running, and provides related notes.

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

(1) Returning the system time to a past date/time

When you change the system time, avoid changing it to a past date/time.

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

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

If you need to set the system date/time back to the original date/time after having intentionally set it forward to a future date/time for testing purposes, use the following procedure.

(a) Resetting the manager's system 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

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

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

1. Stop JP1/IM - Manager.

2. Stop JP1/Base.

3. Perform unsetup for the IM database.

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

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

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

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

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

   In Windows:

   Table 2–1: Files to delete (Windows)

File name	Storage location
Action information file	*Console-path*\log\action\actinf.log
	shared-folder\jp1cons\log\action\actinf.log
Action hosts file	*Console-path*\log\action\acttxt{1|2}.log
	shared-folder\jp1cons\log\action\acttxt{1|2}.log
Command execution log file	All files under *Base-path*\log\COMMAND\
	All files under *shared-folder*\jp1base\log\COMMAND\
Event database	IMEvent*.* files under *Base-path*\sys\event\servers\default\[#]
	IMEvent*.* files under *shared-folder*\jp1base\event\[#]

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

   In UNIX:

   Table 2–2: Files to delete (UNIX)

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

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

6. Set up the IM database.

7. Start JP1/Base.

8. Start JP1/IM - Manager.

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

1. From JP1/IM - View, log on to JP1/IM - Manager (JP1/IM - 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.

(b) Resetting the agent's system date/time back to the original date/time

When you reset the agent's system date/time back to the original date/time, you must reset both the event database of the JP1/Base on the applicable host and the JP1/Base time on the host at the event forwarding destination. For details such as the relevant procedure, see the explanation on necessary tasks when the system date/time is changed in the chapter about changing settings during operation of JP1/Base in the *Job Management Partner 1/Base User's Guide*.

(2) Setting forward a system clock that is slower than the current 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.

2.2.4 Necessary tasks when changing the passwords of the manager and monitored remote hosts in a remote monitoring configuration

If you change the passwords of a monitored remote host and the manager that manages the remote hosts, you must review 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.

> **Reference 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 *3.1.4 Changing host information* in the *Job Management Partner 1/Integrated Management - Manager Configuration Guide*.

For details about the Remote Monitoring Settings window and the System Common Settings window, see the following sections in the manual *Job Management Partner 1/Integrated Management - Manager GUI Reference*.

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

2.2.5 Necessary tasks when changing the date/time of a monitored host

The following describes the effects of changing the date/time of a monitored host, and the tasks that are required when you make these changes.

(1) Changing the date/time of a monitored host in an agent configuration

When changing the date/time of a monitored host in an agent configuration, perform the tasks required to change the system date/time described in the *Job Management Partner 1/Base User's Guide*.

(2) Returning the date/time of a monitored host in a remote monitoring configuration to a past date/time

If you reset the date/time of a monitored host in a remote monitoring configuration back to the original date/time after you have intentionally changed the date/time to a future date/time for testing or other purposes, you must delete the event log for the set future date/time on the host.

Use the following procedure to reset the date/time. Note that if the OS on a monitored host in remote monitoring configuration is UNIX, the following tasks are unnecessary.

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. Restart the stopped remote monitoring event log trap.

Note that if the difference between the date/time of the host on which JP1/IM is running and the date/time of a monitored host is greater than the monitoring interval, you cannot monitor the host by using a remote monitoring event log trap. When changing the date/time of a monitored host, also check the date/time of the host on which JP1/IM is running.

(3) Setting the date/time of a monitored host in a remote monitoring configuration forward

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.

2.3 Notes on changing the monitoring configuration from remote to agent

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

For an overview of managing a monitored remote host, see *6.6 Managing remotely monitored hosts* in the *Job Management Partner 1/Integrated Management - Manager Overview and System Design Guide*.

2.3.1 Notes on log file traps

When changing the monitoring configuration of log file traps, 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).

2.3.2 Notes on event log traps

When changing the monitoring configuration for event log traps, 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 on the JP1/Base event log trap action-definition file, see the chapter on definition files in the *Job Management Partner 1/Base User's Guide*.
- When the specified trap-interval is 181 or more, change the value to 180 or less.
- If trap-interval is not specified, the monitoring interval becomes shorter.
- If you want a JP1 event to be issued when event log acquisition fails during event log monitoring (as in remote monitoring), define jp1event-send as 1 (notify).

3

Starting and Stopping JP1/IM - Manager

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

3.1 Starting JP1/IM - Manager

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

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

For details about starting JP1/Base services, see the chapter about starting and stopping JP1/Base in the *Job Management Partner 1/Base User's Guide*.

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

The startup method varies depending on the OS that is being used. For details, see *3.1.1 In Windows* or *3.1.2 In UNIX*.

3.1.1 In Windows

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

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

To start up when the IM database is being used:

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

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

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

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

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

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

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

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

Before you can use startup control to start services, you must choose **Control Panel**, then **Administrative Tools**, and then **Services** in Windows. In the Services dialog box, you must set the startup method for the JP1/IM - Manager DB Server service and JP1/IM - Manager service to **Manual**. For details about startup control, see the chapter on setting up the service startup and stopping sequence (Windows only) in the *Job Management Partner 1/Base User's Guide*.

Starting the IM database

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

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

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

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

For details about startup control, see the chapter on setting up the service startup and stopping sequence (Windows only) in the *Job Management Partner 1/Base User's Guide*.

Starting JP1/IM - Manager

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

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

3.1.2 In UNIX

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

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

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

For details about how to set the automatic startup script, see *2.18.2 Setting automatic startup and automatic stop* in the *Job Management Partner 1/Integrated Management - Manager Configuration Guide*. For details about the automatic startup script, see *jco_start (UNIX only)* (*1. Commands*) in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.

To start JP1/IM - Manager without setting up the automatic startup script, execute the `/etc/opt/jp1cons/jco_start.model` script or a file into which this script has been copied.

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

For details about starting JP1/Base services, see the chapter about starting and stopping JP1/Base in the *Job Management Partner 1/Base User's Guide*.

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

For details about the start sequence, see *6.2.4 Registering into the cluster software (for Windows)* or *6.3.4 Registering into the cluster software (for UNIX)* in the *Job Management Partner 1/Integrated Management - Manager Configuration Guide*.

3.2 Stopping JP1/IM - Manager

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

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

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

3.2.1 In Windows

If JP1/Power Monitor has been installed, you can use the startup control of JP1/Base to stop a service. If you use startup control, JP1/IM - Manager, the IM database, and JP1/Base automatically stop in that order when you use JP1/Power Monitor to turn off the power. 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 *Job Management Partner 1/Base User's Guide*.

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

3.2.2 In UNIX

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

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

For details about how to set up the automatic termination script, see *2.18.2 Setting automatic startup and automatic stop* in the *Job Management Partner 1/Integrated Management - Manager Configuration Guide*. For details about the automatic termination script, see *jco_stop (UNIX only)* (*1. Commands*) in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File 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.

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.

3.3 Notes on starting and stopping

- If you restart Event Service of JP1/Base, you must also restart JP1/IM - Manager. In addition, you must restart the JP1/IM - View that was connected. If you do not restart it, you will have problems displaying events, for example.

- If a process does not stop even after you have stopped all services of JP1/IM - Manager for a logical host, you can execute the `jco_killall.cluster` command to forcibly stop the process. Use this command for stopping a process only when a process does not stop after you have used a normal method and stopped the JP1/IM - Manager services.

- If you collect a large number[1] of events during startup of JP1/IM - Manager, the startup time[2] will lengthen in proportion to the number of events that are collected. Consequently, the JP1/IM - Manager service (in Windows) or the `jco_start` command (in UNIX) may time out[3] and return an error value. In such a case, JP1/IM - Manager may appear not to be starting, but startup will be completed after a while.

  #1

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

  #2

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

  #3

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

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

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

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

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

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

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

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

4

JP1/IM - Manager Logon and Logoff

To use JP1/IM - View, you must log on to JP1/IM - Manager. This chapter explains how to log on to and log off from JP1/IM - Manager.

4.1 Logging on to JP1/IM - Manager

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

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

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

(1) Using JP1/IM - View

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

1. From the Windows **Start** menu, choose **Programs**, then **JP1_Integrated Management - View**, and then **Integrated View**.
   The Login window opens.

2. In the Login window, enter a user name, a password, and the name of the host to which you want to connect.
   You can use alphanumeric characters, 1 to 31 bytes, for the user name. The user name is not case sensitive.
   The password is case-sensitive.
   For the host to which to connect, specify the name of the host where the JP1/IM - Manager to which you are logging on is located. Specify a host name defined in the viewer or an IP address.
   For details about the Login window, see *1.2.1 Login window of Central Consol and Central Scope* in the manual *Job Management Partner 1/Integrated Management - Manager GUI Reference*.
   If you want to log in to Central Scope, advance settings for using the Central Scope functions are required.

3. Check the check boxes according to the functions you wish to use.
   You can check either one or both of them.
   If you check the **Central Console** check box, you will be connected to JP1/IM - Manager (JP1/IM - Central Console).
   If you check the **Central Scope** check box, you will be connected to JP1/IM - Manager (JP1/IM - Central Scope).

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

The user name you use for logon must be registered in advance. For details about user registration, see the chapter on setting up the user management function in the *Job Management Partner 1/Base User's Guide*.

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

Using the Web version of JP1/IM - View:

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

1. Open a Web browser and specify the following URL:
   `http://`*name-of-host-to-which-to-connect*`/JP1IM/console.html`

The Login window opens.

2. Enter your user name and password.

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

3. Click **OK**.

    The Event Console window opens.

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

(2) Using IM Configuration Management - View

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

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

    The Login window opens.

    If you want to start IM Configuration Management - View from the Windows **Start** menu, you must first execute the `jcovcfsetup` command and add **Configuration Management** to the Windows **Start** menu. For details about how to add **Configuration Management** to the Windows **Start** menu, see *1.20.3 Setting up and customizing IM Configuration Management - View* in the *Job Management Partner 1/Integrated Management - Manager Configuration Guide*.

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

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

    The password is case-sensitive.

    For the host to which to connect, specify the name of the host where the JP1/IM - Manager to which you are logging on 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 logon must be registered in advance. For details about user registration, see the chapter on setting up the user management function in the *Job Management Partner 1/Base User's Guide*.

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

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

(1) Using JP1/IM - View

This subsection explains how to use the `jcoview` command to log on 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 on

```
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 on to both JP1/IM - Central Console and JP1/IM - Central Scope of JP1/IM - Manager. If you specify only the -c argument, you will be logged on to JP1/IM - Central Console. If you specify only the -s argument, you will be logged on to JP1/IM - Central Scope. If you omit both the -c and -s arguments, you will be logged on to JP1/IM - 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 on via the GUI, see *4.1.1 Using the GUI to log on to JP1/IM - Manager*. For details about the `jcoview` command, see *jcoview (Windows only)* (*1. Commands*) in the manual *Job Management Partner 1/ Integrated Management - Manager Command and Definition File Reference*.

(2) Using IM Configuration Management - View

This subsection describes the method of using the `jcfview` command to log on 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 on

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

If you specify all arguments, you will be logged on 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 on via the GUI, see *4.1.1 Using the GUI to log on to JP1/IM - Manager*. For details about the `jcfview` command, see *jcfview (Windows only)* (*1. Commands*) in the manual *Job Management Partner 1/ Integrated Management - Manager Command and Definition File Reference*.

4.2 Logging off from JP1/IM - Manager

To log off from JP1/IM - Manager, use the following methods.

To log off from JP1/IM - Manager (JP1/IM - Central Console):

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

To log off from JP1/IM - Manager (JP1/IM - 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 off from JP1/IM - Manager (IM Configuration Management):

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

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

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

5

System Monitoring from Central Console

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

5.1 Monitoring the system based on JP1 events

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

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

Figure 5–1: Event Console window (Monitor Events page) display example
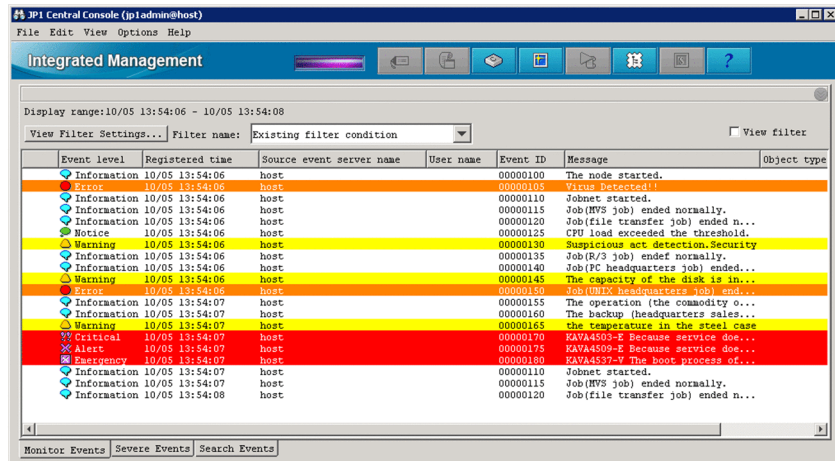
5.1.1 Viewing JP1 events

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 list. The JP1 event with the most recent arrival date/time is displayed at the very bottom.

(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 extended attributes instead of basic attributes or common 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* in the *Job Management Partner 1/Integrated Management - Manager Configuration Guide*.

For details about how to set up the severity changing function, see *4.11 Setting the severity changing function* in the *Job Management Partner 1/Integrated Management - Manager Configuration Guide*.

In the Preferences window, you can specify whether to save the column width for each display item when you log off, and whether to add background colors for specific events. For details about the Preferences window, see *2.22 Preferences window* in the manual *Job Management Partner 1/Integrated Management - Manager GUI Reference*.

(a) Attributes of JP1 events

The events list displays the attributes (basic attributes or common extended attributes) of each event. The default is that the severity level, registered time, registered host name, user name, event ID, message, object type, and action are displayed. You can change the items displayed in the events list from the Preferences window. For details about how to change displayed items, see *2.22 Preferences window* in the manual *Job Management Partner 1/Integrated Management - Manager GUI Reference*.

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

Table 5–1: Items displayed in the events list

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

Attribute	Explanation
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	Time at which the JP1 event arrived at the event database of the connected manager. 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.
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	JP1 event type. Either the correlation succeeded icon or the correlation failed icon is displayed. 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.
Action type	Action type. An icon indicating the action type (command) or (rule) is displayed.
Severity (before change)	Severity level before the change. This attribute can be set when the integrated monitoring database is used and the severity changing function is enabled.
Severity changing	When the severity level is changed, the icon is displayed. This attribute is displayed when the integrated monitoring database is used and the severity changing function is enabled.
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.

(b) Extended attributes of JP1 events

You can display the content of an 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 an extended attribute is displayed, it is preceded by the hash mark and a space (#).

To display an extended attribute, you need to map a display item to the extended attribute. For details about mapping extended attributes, see *5.1.3 Displaying extended attributes of JP1 events (mapping of event information)*.

(c) JP1 event response status

You can display a response status icon indicating the event's response status (Processed, Processing, or Held) in the far-left column of the events displayed in the events list. For details about how to display response status icons, see *5.1.4 Displaying the response status of JP1 events*.

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.

(2) Events displayed on the screen

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 and working with consolidated events, see *5.1.8 Displaying consolidated events when events with the same attributes occur consecutively*.

- Correlation events

  The icon ![icon] or ![icon] is displayed in **Type**.

  For details about displaying and handling correlation events, see *5.1.10 Displaying and handling correlation events*.

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* in the *Job Management Partner 1/Integrated Management - Manager Configuration Guide*.

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

Monitor Events page

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

Severe Events page

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

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

Even those JP1 events that are erased from the screen are registered in the event database. To view the JP1 events that have been erased from the screen, search for JP1 events. For details about how to search for JP1 events, see *5.5 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.

(3) Applying a filter

By applying a filter, you can restrict the JP1 events that are displayed in the Event Console window.

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

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

If a view filter is set, by selecting the filter you want to apply from the **Filter name** list box and selecting the **View Filter** check box, you can display only those JP1 events that satisfy the set filtering condition.

To display only severe events, switch to the **Severe Events** page. When a severe event is received, 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. For details about the **Severe Events** page, see *5.1.5 Displaying only severe events*.

You can set to save which view filter is applied, and whether the **View Filter** check box is selected, on the **Monitor Events** or **Severe Events** page (selected in the Event Console window). If you choose to save the applied status, it is saved when you log out from JP1/IM - View, and then restored at the next login. (Events will be displayed according to the status.)

5.1.2 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.

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

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

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

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

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

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

Table 5–2: Detailed JP1 event information

Display name	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).
Message	Message text that shows the content of the JP1 event.
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.
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.

Display name	Description
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.
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.
Associated serial numbers	Serial numbers of correlation source events, delimited by spaces and displayed in the following format: *serial-number* △ *serial-number* △ *serial-number* . . .
Correlation event generation condition name	Approved correlation event generation condition name.
Severity (before change)	When the integrated monitoring database is used and when a severity level is changed using the severity changing function, the urgency of the JP1 event before the change is displayed. The urgency level can take one of the following values (listed in descending order): `Emergency`, `Alert`, `Critical`, `Error`, `Warning`, `Notice`, `Information`, and `Debug`.
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.
Memo	When the integrated monitoring database is used and the function for setting memo entries is enabled, memo entries are displayed.
Monitoring suppression 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.

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

5.1.3 Displaying extended attributes of JP1 events (mapping of event information)

You can display the content of an extended attribute in the display item (basic attribute or common extended attribute) column of the events list.

An example follows.

Mapping definition settings:

The mapping definitions described below are set.

Event information mapping definition 1

> Mapping extended attribute `LOGHOST` to the registered host name.
>
> Mapping-target event ID: `12E0`

Event information mapping definition 2

> Mapping extended attribute `LOGTIME` to the arrival time.
>
> Mapping-target event ID: `12E0`

Events generated:

Events with the content listed below are generated.

Table 5–3: Event generation content

No.	Attribute	Content
1	Severity	`Error`
2	Registered time	`2001/10/30 17:47:31`
3	Arrival time	`2001/10/30 17:47:39`
4	Registered host name	`host_A`
5	User name	`jp1nps`
6	Event ID	`000012E0`
7	Message	`KAJC391-E ...`
8	LOGHOST	`loghost_1`
9	LOGTIME	`1003976997`[#]

#: In the time format, the value becomes `2001/10/25 11:29:57`.

Display in the Event Console window:

Normally, the events list in the Event Console window displays the contents of Nos. 1 to 7 in the above table, but because No. 8 is mapped to No. 4 and No. 9 is mapped to No. 3, the following is displayed:

Table 5–4: Event Console window display

Severity	Registered 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 an extended attribute, in the Event-Information Mapping Definitions window, map a display item to the extended attribute. To start the Event-Information Mapping Definitions window, you need `JP1_Console_Admin` permission. In addition, when the reference and operation permissions are set for a business group, operations in the Event-Information Mapping Definitions window might not be possible depending on the combination of JP1 resource group and JP1 permission level. For details, see *3.1.4(2) Assigning a JP1 resource group and permission level to a JP1 user* in the *Job Management Partner 1/Integrated Management - Manager Overview and System Design Guide*.

> **Reference note**
>
> Difference between event information mapping and source host mapping
>
> The event information mapping functionality maps the value of the 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 an 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 to map the extended attribute.
   You can select only the following items, which can be displayed in the events list on the **Monitor Events** page, **Severe Events** page, or **Search Events** page of the Event Console window:
   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 extended attribute you want to map.
   You can specify a maximum of 32 characters consisting of upper-case letters, numbers, and underscores. You need not specify E to indicate an extended attribute.
   Each display item can be mapped to a single extended attribute only.
   To map an extended attribute to Arrival time, Start time, or End time, specify an attribute name whose attribute value is a numeric value (from 0 to 2,147,483,647 seconds from January 1, 1970 UTC). If you specify a value other than a numeric value or an attribute having 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 00000000-7FFFFFFF.
   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 is clicked, the extended attribute is displayed along with this mapping definition.

You can specify the mapped extended attribute to filter JP1 events when using the view filter, severe event filter, and event receiver filter.

When an extended attribute is displayed, it is preceded by the hash mark and a space (#).

To specify a displayed extended attribute as the filtering condition, you need not enter "# ".

If you select the **Display** check box of the **Coloring** field in the Preferences window, 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 the extended event attributes to display extended attributes in the Event Details window. For details, see the following explanations:

Using the definition file for the extended event attributes to display extended attributes

   See *3.11 Displaying user-defined event attributes* in the *Job Management Partner 1/Integrated Management - Manager Overview and System Design Guide*.

About the definition file for the extended event attributes

   See *Definition file for extended event attributes* (*2. Definition Files*) in the manual *Job Management Partner 1/ Integrated Management - Manager Command and Definition File Reference*.

Note the following points when you are mapping 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 extended attribute to be mapped.

- 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 an 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 extended attribute are not input into the condition list.

5.1.4 Displaying the response status of JP1 events

You can indicate a response status for any event listed in the Event Console window by displaying a response status icon in the leftmost column of the window.

The table below shows the response status types and the corresponding response status icons.

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

Response status	Response status icon
Processed	⚑

Response status	Response status icon
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 the response status of a consolidated event is different from the response status of the repeated events.

When you use the repeated event monitoring suppression function, ! is displayed if the 1st to 100th repeated events (the 1st being the oldest) do not all have the same response status. It is not displayed if these events 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 ! symbol to appear.

When you use the consolidated display of repeated events function, ! is displayed if the response status differs among repeated events.

To set a response status for an event, select an event from the events list on the **Monitor Events** page, and then perform one of the operations listed below. If the searching host is the logged-in manager, you can also change the response status from the **Severe Events** page or **Search Events** page.

Regardless of the response status of the selected event, you can perform startup operations. Note that these operations require JP1_Console_Admin permission or JP1_Console_Operator permission.

- 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.

The information (Processed, Processing, Held, or Unprocessed) that indicates the response status of severe events, which was set on the **Monitor Events** page, is also reflected in the display of the same events on the **Severe Events** page. Note that the information indicating the response status of the events that were set on the **Monitor Events** page or **Severe Events** page is not reflected in the display of the same events on the **Search Events** page. Information indicating the response status of the events that were set up in another JP1/IM - View is not reflected in the display of the same events on the **Search Events** page, either.

The information (Processed, Processing, Held, or Unprocessed) that indicates the response status of an event is recorded in the integrated monitoring database of the logged-in manager or in the event database. Consequently, if you change the response status, the display on the **Monitor Events** page of other JP1/IM - Views that are logged on to the same manager is also changed (for a severe event, the display on the **Severe Events** page is also changed). For an event that has been forwarded from another host, the information in the integrated monitoring database or event database of the forwarding source host is not changed.

5.1.5 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 out of the JP1 events that are displayed on the **Monitor Events** page.

In the events list on the **Severe Events** page, a response status icon indicating a severe event's response status is displayed in the far-left column.

If the consolidated display of repeated events function is being used, response status icons for JP1 events are automatically displayed.

The following table shows the response status types and the corresponding response status icons.

Table 5–6: 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 the response status of a consolidated event is different from the response status of the repeated events.

  When you use the repeated event monitoring suppression function, ! is displayed if the 1st to 100th repeated events (the 1st being the oldest) do not all have the same response status. It is not displayed if these events 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 ! symbol to appear.

  When you use the consolidated display of repeated events function, ! is displayed if the response status differs among repeated events.

You can decide which icon to use for each situation based on the operation.

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.

When 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. In this case, the first severe event to be erased is a Processed severe event. If there are no Processed severe events, the oldest among the Unprocessed, Held, and Processing severe events is deleted. In this case, the oldest severe event is deleted regardless of its status. When you enable the integrated monitoring database, you can display all events stored in the integrated monitoring database. 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* in the *Job Management Partner 1/ Integrated Management - Manager Configuration Guide*.

When you use the repeated event monitoring suppression function, deleting a consolidated event from the events list deletes any of the oldest 100 repeated events that have not already been deleted. It does not delete the 101st and subsequent repeated events. Note that deleting a repeated event does not reduce the number of consolidated events.

If a view filter is set, you can further filter JP1 events to be 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 you select the **Display** check box of the **Coloring** field in the Preferences window, the background of a line in an event list is highlighted in the color for that event level.

5.1.6 Suppressing monitoring of large numbers of events by setting repeated event conditions

When you use the repeated event monitoring suppression function, you can consolidate JP1 events that meet specified conditions and display them on the Monitor Events page or Severe Events page of the Event Console window. You can set these conditions in the Repeated Event Condition Settings window.

For a general description of the repeated event monitoring suppression function, see *3.4 Suppressing display of repeated events* and *3.5 Suppressing monitoring of a large number of events* in the *Job Management Partner 1/Integrated Management - Manager Overview and System Design Guide*.

For details on how to enable the repeated event monitoring suppression function, see *4.3 Setting monitoring of repeated events to be prevented* in the *Job Management Partner 1/Integrated Management - Manager Configuration Guide*.

(1) Using repeated event monitoring suppression to suppress actions associated with repeated events to which automated actions are assigned

You can suppress the monitoring of repeated events by entering repeated event conditions in the Repeated Event Condition Settings window. By setting repeated event conditions when you first set up the JP1/IM system, you can suppress the repeated events that occur during system operation. You can also configure JP1/IM to suppress redundant actions when an automated action is assigned to a repeated event.

1. In the Event Console window, from the **Options** menu, choose **Repeated Event Condition Settings**.

   The List of Repeated Event Conditions window appears.

2. Click **Add**.

   The Repeated Event Condition Settings window appears.

3. On the Basic Settings page of the Repeated Event Condition Settings window, set the conditions for repeated events.

   The attribute names you can use as conditions are defined in the display item definition file for the repeated event condition (`event_storm_attr_list.conf`). For details on the display item definition file for the repeated event condition, see *Display item definition file for the repeated event condition (event_storm_attr_list.conf)* in *2. Definition Files* in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*. For details on repeated event conditions, see *2.17 Repeated Event Condition Settings window* in the manual *Job Management Partner 1/Integrated Management - Manager GUI Reference*.

4. Set the suppression options on the Basic Settings page of the Repeated Event Condition Settings window.

   The suppression options are **Suppress display of the repeated events list** and **Suppress actions of the repeated events**. To suppress actions associated with repeated events to which automated actions are assigned, select the **Suppress actions of the repeated events** check box, and then specify the range of events for which actions are to be suppressed. You can specify **All repeated events** or **Repeated events other than repeated start events** for the range.

   If **All repeated events** is selected:

   Actions are suppressed for all events to be suppressed that match the repeated event conditions being edited.

   If **Repeated events other than repeated start events** is selected:

   Actions are suppressed for all events to be suppressed that match the repeated event conditions being edited, except for repeated start events (which triggered suppression).

   For details about events for which actions are suppressed, see *3.5.8 Suppressing the execution of automated actions triggered by a large number of events* in the *Job Management Partner 1/Integrated Management - Manager Overview and System Design Guide*.

   When a new condition is added, only the **Suppress display of the repeated events list** check box is selected.

5. Click **OK**.

   The repeated event conditions appear in the List of Repeated Event Conditions window. You can view the repeated event conditions in this window.

6. In the List of Repeated Event Conditions window, click **Apply**.

7. A confirmation message appears. To apply the settings, click **Yes**.
   The repeated event conditions you added take effect.

(2) Determining whether suppression of repeated event monitoring continues and performing processing

You can determine whether suppression of repeated event monitoring continues for each specified interval (seconds), or every specified number of events. Then, if suppression continues, you can notify by issuing a JP1 event, or cancel suppression.

To specify the timing of checks to decide whether suppression continues, and the processing to be performed when suppression continues:

1. In the Event Console window, from the **Options** menu, choose **Repeated Event Condition Settings**.
   The List of Repeated Event Conditions window appears.

2. Display the Repeated Event Condition Settings window by either of the following methods:
   • Click the **Add** button in the List of Repeated Event Conditions window.
   • Select a repeated event condition displayed in the List of Repeated Event Conditions window, and then click the **Edit** button.

3. On the **Options** page of the Repeated Event Condition Settings window, select the **Enable** check box for **Checks for suppression to continue**.

4. Specify the timing of checks to decide whether suppression continues.
   Select either of the **Time** or **Number of events** radio button. For details about their difference, see *3.4.7 Issuing notifications when the suppression of repeated-event display continues* in the *Job Management Partner 1/Integrated Management - Manager Overview and System Design Guide*.

5. Select the actions to take when suppression continues.
   Select either the **Issue an event to notify that suppression will continue** or **Terminate suppression** radio button.
   When **Terminate suppression** is selected, if the **Issue an event to notify that suppression will be terminated** check box is selected, a JP1 event notifying that suppression will be terminated is issued.

6. Click the **OK** button.
   The repeated event condition is applied to the List of Repeated Event Conditions window.

7. In the List of Repeated Event Conditions window, click the **Apply** button.

8. A confirmation message appears. To apply the settings, click **Yes**.
   The repeated event condition is enabled.

(3) Suppressing repeated event monitoring based on a repeated 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 *additional repetition event conditions*.

1. In the event list in the Event Console window, select the JP1 event whose monitoring you want to suppress.

2. Display the Repeated Event Condition Settings window by choosing **Suppress by Repeated Event Conditions** from the **View** menu in the Event Console window. Alternatively, choose **Suppress by Repeated Event Condition** from the popup menu which appears on right clicking.

   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 on 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 *2. Definition Files* in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.

3. Edit the items in the Repeated Event Condition Settings window as needed.

4. Click **OK**.

   The additional repetition event conditions you set appear in the List of Repeated Event Conditions window. The 🖇 icon appears in the **Type** column for additional repetition event conditions added during system operation.

Supplementary note:

   JP1/IM - Manager begins consolidating repeated events when the number of JP1 events that match the conditions reaches a threshold. Monitoring of repeated events is not suppressed until this threshold is reached. If the number of JP1 events that match the repeated event conditions falls below the threshold and stays there for a certain period of time, JP1/IM - Manager stops consolidating the events. A maximum of 1,000,000 events can be consolidated into one event.

(4) Converting additional repetition event conditions to repeated event conditions

You can create repeated event conditions from the additional repetition event conditions you added during system operation.

1. Display the Repeated Event Condition Settings window by choosing **Repeated Event Condition Settings** from the **Options** menu in the Event Console window.

2. In the List of repeated event conditions area in the List of Repeated Event Conditions window, select an additional repetition event condition (a condition with the 🖇 icon in the **Type** column) that you want to convert to a repeated event condition.

3. Click **Type**.

4. A confirmation message appears. To change the condition to a repeated event condition, click **Yes**.

   The selected additional repetition event condition is converted to a 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 additional repetition event condition takes effect.

5.1.7 Suppressing event forwarding when a large numbers of events occur

This subsection explains how to suppress event forwarding from an agent to the manager, as an action to take when a large numbers of events occur.

For a general description of individual procedures, see *3.5.9 Suppressing the forwarding of a large number of events* in the *Job Management Partner 1/Integrated Management - Manager Overview and System Design Guide*.

For details about examination items of individual procedures, see *11.1.7 Considerations for suppressing the forwarding of a large number of events* in the *Job Management Partner 1/Integrated Management - Manager Overview and System Design Guide*.

(1) Suppressing, on the manager, event forwarding from an agent on which a large numbers of events occur

On the manager, you can suppress event forwarding from an agent, as an action to take when a large numbers of events occur on the agent.

In the procedure below, you can use the Event Console window to direct the manager host to execute a command. The following conditions are required to execute a command:

- A JP1 user who executes a 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 by using the JP1/Base configuration management.
- JP1 users and OS users are mapped on the manager host.
- OS users mapped with JP1 users have execute permission for the jevagtfw command on the manager host.
  For details about the jevagtfw command, see the chapter about commands in the *Job Management Partner 1/Base User's Guide*.

Before performing the procedure below, the **Command** button in the Event Details window must be enabled. For details about how to enable the **Command** button, see *1.16 Setting up a command execution environment* in the *Job Management Partner 1/Integrated Management - Manager Configuration Guide* for Windows, or see *2.15 Setting up a command execution environment* in the *Job Management Partner 1/Integrated Management - Manager Configuration Guide* for UNIX.

Also, mapping of the event source host must be enabled beforehand. For details about how to enable mapping of the event source host, see *4.12 Setting event source host mapping* in the *Job Management Partner 1/Integrated Management - Manager Configuration Guide*.

To use the manager to suppress, event forwarding from an agent on which a large numbers of events occur:

1. In the events list in the Event Console window, make sure that a lot of JP1 events are output from a specific agent.

2. Display the Event Details window for the relevant JP1 event.

3. Make sure that an event source host name is displayed for **Event attributes** in the Event Details window.

4. In the Event Details window, click the **Execute Command** button.

The Execute Command window appears.

5. In the Execute Command window, specify the `jevagtfw` command for **Command**. Specify the variable for the event source host as the argument.
Example of the command:

```
jevagtfw -s $EV"JP1_SOURCEHOST"
```

Also, make sure that the setting items in the Execute Command window are set as follows:

- **Command of managed host** is selected for **Command type**.
- **Inherit event information** is selected for **Event information to inherit**.
- The manager host name is set for **Target host**.

6. In the Execute Command window, click the **Execute** button.
The Preview Command Execution Content window appears.
Make sure that the contents of the command to be executed are correct.

7. In the Preview Command Execution Content window, click the **Execute** button to execute the `jevagtfw` command.
Event forwarding from the specified agent is suppressed.
You can check the execution result of the command in the **Log** area of the Execute Command window.

8. Identify why a large numbers of events are occurring, and then solve the problem.
While event forwarding is suppressed, investigate the event source agent, and then solve the problem.

> **Reference note**
>
> You can also execute a command previously registered to the **Command** button in the Execute Command window. You can click the **Command** button to suppress event forwarding by previously registering the `jevagtfw` command to the button. For details about how to register a command to the **Command** button, see *7.1.2 Executing a command by using the Command butto*n.

(2) Stopping, on the manager, a log file trap that issues a large numbers of events

The procedure below shows how to stop a specified 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.

Before performing the procedure below, IM Configuration Management must be used to manage the profile of the agent. For a general description of profile management by using IM Configuration Management, see *6.5 Profile management* in the *Job Management Partner 1/Integrated Management - Manager Overview and System Design Guide*. For details about how to set the profile by using IM Configuration Management, see *3.5 Setting the profiles* in the *Job Management Partner 1/Integrated Management - Manager Configuration Guide*.

Also, mapping of the event source host must also be enabled beforehand. For details about how to enable mapping of the event source host, see *4.12 Setting event source host mapping* in the *Job Management Partner 1/Integrated Management - Manager Configuration Guide*.

1. In the events list in the Event Console window, make sure that a lot of JP1 events issued by a log file trap are output.

2. Display the Event Details window for the relevant JP1 event.

3. 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** in the Event Details window, 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 select **Display Profiles** from the **View** menu.

   The Display/Edit Profiles window for the relevant host appears.

7. In the tree area, select **JP1/Base**, and then in 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 to be suppressed, and then in 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.

10. Identify why a lot of logs are occurring, and then solve the problem.

    While the log file trap is stopped, investigate the source application that output the logs, and then solve the problem.

(3) Automatically suppressing event forwarding from an agent by setting a threshold

To automatically suppress event forwarding by setting a threshold, in case a large numbers of events occur on an agent:

1. Edit the forwarding setting file on an agent on which event forwarding is to be automatically suppressed.

   Set the conditions for suppressing event forwarding (which is equivalent to the threshold of frequently occurring events) in the forwarding setting file of JP1/Base on the agent.

   Format of the condition for suppressing event forwarding:

   ```
   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 of the forwarding setting file (`forward`) in the *Job Management Partner 1/Base User's Guide*.

2. Enable the changes in the forwarding setting file.

   Reloading the forwarding setting file or restarting the event service enables 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 event source agent, and then solve the problem.

If the problem is solved and the event occurrence status matches the conditions for cancelling suppression of event forwarding, event forwarding resumes automatically.

5.1.8 Displaying consolidated events when events with the same attributes occur consecutively

When you consolidate the display of repeated events, JP1 events that have the same content and 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.

For a general description of the consolidated display of repeated events function, see *3.4.10 Suppressing repeated-event display by the consolidated display of repeated events* in the *Job Management Partner 1/Integrated Management - Manager Overview and System Design Guide*.

If you want to consolidate JP1 events that do not occur consecutively, or to specify event conditions or certain criteria under which consolidation should start, use repeated event monitoring suppression instead of the consolidated display of repeated events. For details on repeated event monitoring suppression, see *5.1.6 Suppressing monitoring of large numbers of events by setting repeated event conditions*.

1. From the menu in the Event Console window, choose **Options** and then **Preferences**.
   The Preferences window appears.

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.
   You can specify a time from 1 to 3,600 seconds. The default is 60 seconds.

4. Click **OK**.
   The settings take effect.
   Events that have been consolidated appear as a single event on the Monitor Events page and Severe Events page of the Event Console window. For details about how to check consolidated events, see *5.1.9 Checking repeated events and consolidated events and changing the response status*.

Supplementary note:
   The consolidated display of repeated events applies to events received after you configure the feature. Events received before this point are not subject to consolidated display. Event consolidation ends when more than a specified length of time has elapsed between the consolidation start event and the arrival of received events. A maximum of 100 events can be consolidated into a single event.

5.1.9 Checking repeated events and consolidated events and changing the response status

You can view detailed information about repeated events and consolidated events. You can also change the response status similarly to the case with monitoring repeated events. To change a response status, you need `JP1_Console_Admin` permission or `JP1_Console_Operator` permission.

(1) Viewing detailed information about a repeated event and changing the response status

1. Consolidate repeated events.

   For details on how to consolidate repeated events by suppressing monitoring of repeated events, see *5.1.6 Suppressing monitoring of large numbers of events by setting repeated event conditions*.

   For details about how to consolidate repeated events by configuring the consolidated display of repeated events function, see *5.1.8 Displaying consolidated events when events with the same attributes occur consecutively*.

2. On the Monitor Events page or Severe Events page of the Event Console window, select a consolidated event.

3. In the Event Console window, from the **View** menu, choose **Display Related Event List**[#].

   The Related Events (Summary) window appears.

4. In the **Related Events** area, right-click a repeated event and choose **Event Details** from the popup menu.

   The Event Details window appears. Review the content of the repeated event as needed.

   If you have enabled repeated event monitoring suppression, the 101st and subsequent repeated events do not appear in the Related Events (Summary) window. 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.

   To view the 101st and subsequent repeated events, search for events with the arrival times displayed in the **Events that cannot be displayed** area specified as a search condition. For details on how to search for events, see *5.5 Searching for JP1 events*.

5. To change the response status, right-click a repeated event in the **Related Events** area of the Related Events (Summary) window, and select the response status you want to assign in the popup menu.

   The response status of the repeated event changes.

   This does not change the response status of the consolidated event into which the repeated event is consolidated. Because the consolidated event now contains repeated events with different response statuses, ! is displayed as the response status for the consolidated event.

   For details on the types of response status and the corresponding icons, see *5.1.4 Displaying the response status of JP1 events*.

\#

   You cannot select this menu command when:

   • Multiple events are selected on the Monitor Events or Severe Events page

   • A non-consolidation event is selected

(2) Viewing detailed information about a consolidated event and changing the response status

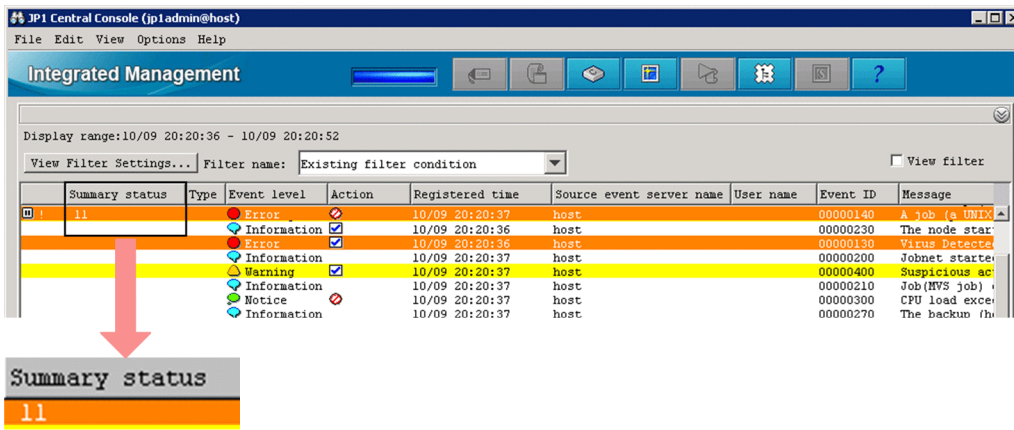1. Consolidate repeated events.

   For details on how to consolidate repeated events by suppressing monitoring of repeated events, see *5.1.6 Suppressing monitoring of large numbers of events by setting repeated event conditions*.

   For details about how to consolidate repeated events by enabling the consolidated display of repeated events function, see *5.1.8 Displaying consolidated events when events with the same attributes occur consecutively*.

2. View the consolidated event on the Monitor Events page or Severe Events page of the Event Console window.

   When events are consolidated, a consolidated event is displayed as shown below.

Figure 5–2: Example of displaying consolidated events

Summary Status

The **Summary Status** column shows the repetition count. The repetition count indicates the total number of consolidated events and repeated events. Nothing is displayed for non-consolidation events.

- For consolidation completion events

  The repetition count is displayed.

  If you have enabled repeated event monitoring suppression, the repetition count is within a range from 1 to 1,000,000.

  If you have enabled consolidated display of repeated events, the repetition count is within a range from 1 to 100.

- For events being consolidated

  A repetition count and the + symbol, indicating consolidation in progress, are displayed.

  A value from 1+ to 99+ is displayed. For example, when the repetition count is 1 (only a consolidation start event), 1+ is displayed. When the repetition count is 2 (a consolidation start event and 1 repeated event), 2+ is displayed. On the **Severe Events** page, if the consolidation start event has already been deleted and there are no repeated events, 0+ is displayed.

When you open the Related Events (Summary) window or delete consolidated events, the following is displayed:

- When the consolidation start event is deleted

  If you delete the consolidation start event on the **Severe Events** page of the Event Console window, that event is considered deleted, and **Del** is displayed to the right of the repetition count.

  Subsequently, when event consolidation is completed and events become deleted non-consolidation events, they are no longer displayed on the **Severe Events** page of the Event Console window.

- When repeated events are deleted

  When the consolidated display of repeated events function is used, if you delete repeated events from **Related Events** in the Related Events (Summary) window, the repetition count for consolidated events is reduced by the number of repeated events deleted.

When the repetition count for consolidation completion events reaches `1` because of deletion of repeated events, the remaining event becomes a non-consolidation event. Furthermore, if that non-consolidation event is already deleted, it is no longer displayed on the **Severe Events** page of the Event Console window.

When the repeated event monitoring suppression function is used, even if you delete repeated events, the repetition count for consolidated events is not reduced.

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 **Severe Events** page of the Event Console window.

If the response status of a consolidated event is different from the response status of repeated events, **!** is displayed in the response status display.

When you use the repeated event monitoring suppression function, ! is displayed if the 1st to 100th repeated events (the 1st being the oldest) do not all have the same status. It is not displayed if they 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 ! symbol to appear.

When you use the consolidated display of repeated events function, ! is displayed if the response status differs among repeated events.
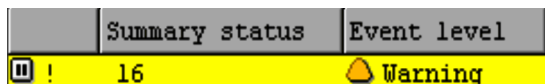
Action

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

Table 5–7: 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, ⊘ is displayed in the Event Console window.

When the action status of a consolidated event is different from the action status of a repeated event, ! 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.

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.

3. On the **Monitor Events** page or **Severe Events** page of the Event Console window, select a consolidated event.

4. In the Event Console window, from the **View** menu, choose Event Details[#].

The Event Details window appears. Review the content of the consolidated event as needed.

5. To change the response status, select a consolidated event on the **Monitor Events** page or **Severe Events** page of the Event Console window and perform one of the following operations:

- Display the **View** menu, and choose the response status you want to assign from the sub-menu.
- Right-click the consolidated event, and choose the response status you want to assign from the popup menu.

The response status of the consolidated event changes. The response statuses of all repeated events that have been received up to that point are also changed to the same response status. However, if the repeated event monitoring suppression function is used and 101 or more repeated events are consolidated, the response statuses of the 101th and subsequent repeated events are not changed.

The response status does not change for repeated events received after you change the response status. As a result, those repeated events have a different response status, and ! is displayed as the response status in the Event Console.

#

You cannot select this menu command when:

- Multiple events are selected on the Monitor Events or Severe Events page
- A non-consolidation event is selected

5.1.10 Displaying and handling correlation events

This subsection explains how to display and handle correlation events.

Displaying correlation events:

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

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

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

Note that **Type** is not a default display item. To display it, you must specify **Type** as a display item in the Preferences window. For details, see *2.22 Preferences window* in the manual *Job Management Partner 1/Integrated Management - Manager GUI Reference*.

Handling correlation events:

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 on 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.

To display correlation approval events and correlation failure events:

1. Select a correlation event on one of the following pages of the Event Console window:
   - **Monitor Events** page
   - **Severe Events** page
   - **Search Events** page

2. From the **View** menu, choose **Display Related Event List**. Alternatively, from the popup menu, choose **Display Related Event List**.

The Related Events (Correlation) or Related Events (Correlation fails) window opens and lists correlation events.

If you are using the repeated event monitoring suppression function or the consolidated display of repeated events function, correlation events may be consolidated and displayed as shown below.

Table 5–8: Example of consolidated display of correlation events

Display example	Explanation
Summary status / Type / Event level — 24 — Error	Correlation events have been consolidated.
Summary status / Type / Event level — 18+ — Error	Correlation events are being consolidated.
Summary status / Type / Event level — 15 Del — Alert	Correlation events that have been consolidated are deleted.
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.

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.

To display the correlation source event:

1. Select one correlation event that is consolidated from the **Monitor Events** page or **Severe Events** page of the Event Console window.

2. From the **View** menu, choose **Display Related Event List**. Alternatively, from the popup menu, choose **Display Related Event List**.

   The Related Events (Summary) window opens and lists correlation events.

3. Select one correlation event from **Related Events** in the Related Events (Summary) window.

4. From the popup menu, choose **Display Related Event List**.

   The Related Events (Correlation) or Related Events (Correlation fails) window opens and lists correlation source events.

For details about how to view events that are consolidated and displayed, see *5.1.8 Displaying consolidated events when events with the same attributes occur consecutively*.

To change the response status of a correlation event or correlation source event to Deleted, you must first open the Related Events (Correlation) or Related Events (Correlation fails) window from the **Severe Events** page. Make sure that either of the following windows is displayed:

- Severe Events
- Severe Events - Related Events (Summary)

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.

5.1.11 Displaying events by specifying the event acquisition range at login

If you set the number of days required for handling severe events as the event acquisition range at login, severe events other than ones already handled and the latest event are displayed when you log in to JP1/IM. You can specify the range by using the number of days or hours.

The way of specifying the event acquisition start location depends on whether the range is specified by the number of days or hours. The set number of days, the time on the host on which Central Console is running at login, and the base time are used for specification.

To specify the event acquisition range:

1. From the menu in the Event Console window, select **Options**, and then **System Environment Settings**.
   The System Environment Settings window appears.

2. On the **Display** tab, select the **Enable the Monitor Events page** or **Enable the Severe Events page** check box.
   Range of events to be collected is activated.

3. Specify **day(s)** and **Base time**, or **hours**.
   For **Base time**, you can specify the time that separates days in the range from 00:00 to 23:59. By default, the base time is 09:00.

> **Reference note**
>
> The display range of events depends on whether base time or current time is larger on the host on which Central Console is running at login. The following shows the display range of JP1 events for both cases:
>
> - When the current time on the host on which Central Console is running at login is larger than the base time of the current day:
>   The base time of the day calculated by (*current-day* - (*set-number-of-days* - 1)) is set for the event acquisition start location.
>
> - When the current time on the host on which Central Console is running at login is smaller than the base time of the current day:
>   The base time of the day calculated by (*current-day* - *set-number-of-days*) is set for the event acquisition start location.

At login, the latest event from the event acquisition start location is displayed. After that, an event is displayed when it occurs.

For example, when the acquisition range is set to 2 days and the base time is set to 09:30, if you log in at 09:15 on June 23, a list of JP1 events from 09:30 on June 21 to the latest event is displayed.

For **day(s)**, you can specify how many days of past JP1 events (from the current day) are displayed, in the range from 1 to 31. By default, **day(s)** is set to 1.

For **hours**, you can specify how many hours of events (occurring before the latest event) are acquired at login, in the range from 1 to 744. By default, **hours** is set to 1.

4. Click the **OK** button.
   The settings (event acquisition range at login) are applied, and the System Environment Settings window closes. At the next and subsequent logins, JP1 events occurring in the specified time period are displayed in the Event Console window.

In some cases, such as when the current time on the host on which Central Console is running at login is larger than the base time of the current day, the range specified as 1 day might not be 24 hours. When the monitoring work is taken over during a time period that includes the base time, if the predecessor's monitoring range is also taken over, add 1 day to the monitoring range or use the slider to display events.

For details about the event acquisition range at login, see *3.14 Range of events to be collected at login* in the *Job Management Partner 1/Integrated Management - Manager Overview and System Design Guide*.

5.1.12 Displaying events by specifying a time period

You can display a list of JP1 events by enabling the display of events for a specified time period. You can also use the Web version of the function for displaying events for a specified time period.

You can display events for a specified time period on the following pages:

- **Monitor Events** page
- **Severe Events** page

Event display for a specified period displays JP1 events that have passed all filters (event acquisition filter, user filter, severe events filter, and view filter) and whose repeated events have been consolidated.

This subsection explains how to enable the function for displaying events for a specified period of time, and how to specify the desired time period.

Whether a JP1 event falls within the specified time period is determined by comparing the time at which the JP1 event arrives 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 may be displayed. Therefore, we recommend that you synchronize the times of JP1/IM - Manager and JP1/IM - View before displaying events.

To display events for a specified time period:

1. From the menu in the Event Console window, choose **Options** and then **Preferences**.
   The Preferences window opens.

2. On the Event Attribute page, click 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.
   - When 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.
   - When 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, when the current time is 09:15, 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 are to be displayed. 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 events for the specified period, 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 on again, you can select both the **Specified display event period** check box and the **Specified display event period** menu, and you can display the events list of each page by applying event display for the specified period. If the function is disabled, you can hide both the **Specified display event period** check box and the **Specified display event period** menu, and you can display the events list of each page without applying event display for the specified period.

For details about the specified display event period, see *3.15 Specifying the event display period* in the *Job Management Partner 1/Integrated Management - Manager Overview and System Design Guide*.

5.1.13 Displaying events by specifying time

If a large number of JP1 events occur within a short time period and exceed the maximum number of events that can be displayed on the **Monitor Events** page, older events may 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* in the *Job Management Partner 1/Integrated Management - Manager Configuration Guide*.

You can specify the event display start-time on the following pages:

- **Monitor Events** page
- **Severe Events** page

The following describes the procedure for specifying an event display start-time to display JP1 events that are no longer visible.

To display events by specifying a start time:

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 on.

For details about the **event display start-time specification** area, see *Figure 2-4 Monitor Events page with the event display start-time specification area displayed* in *2.2 Monitor Events page* in the manual *Job Management Partner 1/Integrated Management - Manager GUI Reference*.

2. Move the slider to the time at which to start displaying events.

Based on the specified event display start-time, events that pass the user filter and view filter currently being applied are collected from the integrated monitoring database and displayed. The default for the maximum number of events that can be displayed (scroll buffer size) is 500. You can halt the collection of events beginning at the event display start-time by specifying a new event display start-time or by clicking the **Cancel** button.

You can specify a precise event display start-time using the **Event display start-time** text box. The default for the **Event display start-time** text box differs according to the time you log on to JP1/IM - Manager. If the logon time is later than the base time, the base time of the day you are logging on to JP1/IM - Manager is displayed by default.

Example: You log on 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 that you log on to JP1/IM - Manager is earlier than the base time, the base time of the day previous to logging on to JP1/IM - Manager is displayed by default.

Example: You log on 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 a new event is received, disable the automatic scrolling function.

5.1.14 Excluding JP1 events from monitoring by setting additional common exclusion-conditions

In the Common Exclusion-Condition Settings (Extended) window, you can select a JP1 event that you do not want to monitor in the Event Console window, and then right-click to display a popup menu. From the popup menu, choose **Exclude by Common Exclusion-Conditions** to register the JP1 event as a common exclusion-condition.

The registered common exclusion-condition is displayed as an additional common exclusion-condition in the System Environment Settings window.

(1) Setting additional common exclusion-conditions by using JP1 events that have occurred

1. If the common exclusion-condition is in basic mode, switch it to extended mode.

   For details about how to change the mode, see *4.2.4(3)(a) Switching between common exclusion-conditions basic mode and extended mode* in the *Job Management Partner 1/Integrated Management - Manager Configuration Guide*.

2. Select a JP1 event you want to exclude from the event list in the Event Console window.

3. Do either of the following to display the Common Exclusion-Condition Settings (Extended) window: In the Event Console window, choose **Display** and then **Exclude by Common Exclusion-Conditions**, or from the popup menu which appears on right clicking, choose **Exclude by Common Exclusion-Conditions**.

   The Common Exclusion-Condition Settings (Extended) window opens because the attribute of the JP1 event selected in step 2 has been automatically set as an event condition.

   The items that are automatically set can be changed by using the common-exclusion-conditions auto-input definition file (`common_exclude_filter_auto_list.conf`). For details about the common-exclusion-conditions auto-input definition file (`common_exclude_filter_auto_list.conf`), see *Common-exclusion-conditions auto-input definition file (common_exclude_filter_auto_list.conf)* in *2. Definition Files* in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.

   Nothing is displayed in **Common exclusion-conditions group ID** in the Common Exclusion-Condition Settings (Extended) window, and nothing can be set. The common exclusion-conditions group ID of an additional common exclusion-conditions group is assigned on registration.

4. Edit the necessary items in the Common Exclusion-Condition Settings (Extended) window.

5. Click the **OK** button.

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.

A message asking whether the type should be changed is displayed. If there is no problem, click the **OK** button.

4. 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 note**
>
> If you change an additional common exclusion-condition to a common exclusion-condition by mistake, click the **Close** button in the System Environment Settings window to cancel the change before clicking the **Apply** button.

5.1.15 Registering JP1 events as incidents in JP1/IM - Service Support (JP1/IM - Service Support linkage)

By linking JP1/IM - Manager with JP1/IM - Service Support, you can register JP1 events displayed in JP1/IM - View as incidents in JP1/IM - Service Support. For details on how to link JP1/IM - Manager with JP1/IM - Service Support, see *8.1.1 Enabling calling the JP1/IM - Service Support window* in the *Job Management Partner 1/Integrated Management - Manager Configuration Guide*.

You can register incidents in JP1/IM - Service Support by displaying the Select the process work board as the registration target window of JP1/IM - 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/IM - Service Support from each of these windows. The procedure for registering an incident in JP1/IM - Service Support

from the Select the process work board as the registration target window is described in the *Job Management Partner 1/Integrated Management - Service Support Operator's Guide*.

Note that registering JP1 events as incidents requires `JP1_Console_Admin` permission or `JP1_Console_Operator` permission.

(1) Displaying the Select the process work board as the registration target window from pages of the Event Console window

The following describes how to display the Select the process work board as the registration target window from the pages of the Event Console window. Note that although JP1 events registered in other event databases appear 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.

To display the Select the process work board as the registration target window:

1. From the list of events in the Event Console window, select a JP1 event that you want to register as an incident.

2. Right-click the event and choose **Register Incident**, or from the **View** menu, choose **Register Incident**.
   Your Web browser (Internet Explorer) opens and displays the Select the process work board as the registration target window of JP1/IM - Service Support.

(2) Displaying the Select the process work board as the registration target window from the Related Events window

To display the Select the process work board as the registration target window from the Related Events window:

1. From the JP1 events displayed in the Related Events window, select a JP1 event that you want to register as an incident.

2. Right-click the event and choose **Register Incident**.
   Your Web browser (Internet Explorer) opens and displays the Select the process work board as the registration target window of JP1/IM - Service Support.

(3) Displaying the Select the process work board as the registration target window from the Event Details window

To display the Select the process work board as the registration target window from the Event Details window:

1. In the Event Details window, click the **Register Incident** button.
   Your Web browser (Internet Explorer) opens and displays the Select the process work board as the registration target window of JP1/IM - Service Support.

5.1.16 Displaying operating procedures for JP1 events (JP1/IM - Navigation Platform linkage)

By linking JP1/IM - Manager with JP1/IM - Navigation Platform, you can access the descriptions of operating procedures provided by JP1/IM - Navigation Platform directly from a JP1 event in JP1/IM - View. This process uses single sign-on. For details on how to link JP1/IM - Manager with JP1/IM - Navigation Platform, see *8.2 Linking to JP1/IM - Navigation Platform* in the *Job Management Partner 1/Integrated Management - Manager Configuration Guide*.

To display the window of JP1/IM - Navigation Platform where work tasks are executed from the Event Details window using single sign-on:

1. In the Event Details window, click a link in the **Guide** area.

   Your Web browser (Internet Explorer) opens and displays the operating procedure that corresponds to the selected JP1 event in the window of JP1/IM - Navigation Platform where work tasks are executed.

5.1.17 Checking the rule startup request status and making a rule startup request (JP1/IM - Rule Operation linkage)

This subsection explains how to check whether a rule startup request was correctly reported to JP1/IM - Rule Operation when JP1/IM is linked to JP1/IM - Rule Operation. It also explains how to open the Rule Log Details window of JP1/IM - Rule Operation.

(1) Checking whether a rule startup request was reported to JP1/IM - Rule Operation

With a rule startup request, you can use the function for monitoring automated action status to monitor action status and delay. By setting up these items, you can detect the following types of problems at an early stage in their occurrence:

- Reporting of a rule startup request did not finish within the expected time frame, or took a long time to finish.

- Reporting of a rule startup request failed (with the `Fail`, `Error`, or `Error (Miss)` status).

When a problem is detected, you can generate a JP1 event (event ID = `2010` or `2011`) or execute a notification command.

For details about setup, see *4.5.3 Settings for monitoring the automated action execution status* in the *Job Management Partner 1/Integrated Management - Manager Configuration Guide*.

To check whether a rule startup request was reported:

1. In the Event Console window, monitor rule startup events.

   Rule startup events are those JP1 events that show 🇷 in **Action Type**.

2. Open the Action Log window or List of Action Results window, and check the execution results for rule startup requests.

   Check the execution status of the rule startup requests.

3. Cancel or re-execute rule startup requests as needed.

   If a rule startup request is stuck in `Running` status or is in `Error` status, it cannot be reported to JP1/IM - Rule Operation. Therefore, cancel or re-execute rule startup requests as needed.

When the function for monitoring automated action status is set for rule startup requests:

   When reporting using the delay monitoring function or status monitoring function is executed once, reporting is suppressed until the user cancels reporting suppression. When an error in a rule startup request is detected by the delay monitoring function or status monitoring function, after you have finished re-executing or have canceled the rule startup request, follow the procedure described below.

1. In the Event Console window, from the **Options** menu, display **Function-Status Notification Return**, and then **Action Delay Monitoring** and **Action Status Monitoring**, and then select a function name that is enabled.

   A suppressed function is displayed in gray letters. When you select a function name that is enabled, a dialog box asking whether to cancel reporting suppression opens.

2. Click **Yes** in the dialog box.

Reporting suppression is canceled, thus enabling monitoring again.

▌ Reference note

You can determine whether a rule startup request has matched the rule startup condition on the JP1/IM - Rule Operation side by checking the return code displayed in the following three windows:

- Action Log window

- List of Action Results window

- Action Log Details window

For details about the Action Log, List of Action Results, and Action Log Details windows, see *1. Window Transitions and Login Window* in the manual *Job Management Partner 1/Integrated Management - Manager GUI Reference*.

For details about operations such as checking automated action status and re-execution, also see *7.2.2 Checking the execution results of automated actions*.

(2) Displaying the Rule Log Details window of JP1/IM - Rule Operation

When a rule startup request is reported to JP1/IM - Rule Operation and satisfies the rule startup condition of JP1/IM - Rule Operation, you can display the Rule Log Details window of JP1/IM - Rule Operation from the following three windows:

- Action Log window

- List of Action Results window

- Action Log Details window

The procedure for each of these windows follows.

- Opening the Rule Log Details window of JP1/IM - Rule Operation from the Action Log window

To open the Rule Log Details window of JP1/IM - Rule Operation from the Action Log window:

1. Select a single rule startup event from the events list in the Event Console window.

2. Use one of the following methods to open the Action Log window:
   - From the menu bar, choose **View** and then **Action Log**.
   - From the popup menu, choose **Action Log**.
   - Click the **Action Log** button.

   The Action Log window opens.

3. Select a single rule startup request execution result.
   Rule startup events are those events that show 🅁 in **Type**. Additionally, make sure that **Return Code** in **Log** is 0.

4. Click the **Rule Log Details** button.
   The Rule Log Details window of JP1/IM - Rule Operation opens.

- Opening the Rule Log Details window of JP1/IM - Rule Operation from the List of Action Results window

To open the Rule Log Details window of JP1/IM - Rule Operation from the List of Action Results window:

1. In the Event Console window, choose **View** and then **List of Action Results**.
   The List of Action Results window opens. This window lists the results of both rule startup requests and automated actions.

2. Select a single rule startup request execution result.
   Rule startup events are those events that show in **Type**. Additionally, make sure that **Return Code** in **Log** is 0.

3. Click the **Rule Log Details** button.
   The Rule Log Details window of JP1/IM - Rule Operation opens.

- Opening the Rule Log Details window of JP1/IM - Rule Operation from the Action Log Details window

You can also open the Rule Log Details window of JP1/IM - Rule Operation from the Action Log Details window, which can be opened from the Action Log window and List of Action Results window that are explained above.

To open the Rule Log Details window of JP1/IM - Rule Operation from the Action Log Details window:

1. From **Log** in the Action Log window or the List of Action Results window, select a single rule startup request and click the **Details** button.
   The Action Log Details window opens.
   Make sure that **Return Code** (attribute name) in **Log** is 0.

2. Click the **Rule Log Details** button.
   The Rule Log Details window of JP1/IM - Rule Operation opens.

For details about the Action Log window, List of Action Results window, and Action Log Details window, see *1. Window Transitions and Login Window* in the manual *Job Management Partner 1/Integrated Management - Manager GUI Reference*.

For details about the Rule Log Details window, see the manual *Job Management Partner 1/Integrated Management - Rule Operation GUI Reference*.

5.2 Setting the response status of severe events

This section explains how to set the response status of severe events and how to delete severe events. Note that these operations require `JP1_Console_Admin` permission or `JP1_Console_Operator` permission.

Setting the response status of a severe event:

To set a response status for a severe event to match its actual response status, select a severe event from the events list on the **Severe Events** page, and then perform one of the following procedures. You can set a response status regardless of the response status of the selected severe event.

- On the **Severe Events** page, click the button for the response status you want to set.
- From the menu bar, choose **View**, and then from the submenu, select the response status you want to set.
- From the popup menu that opens when you right-click the mouse, select the response status you want to set.

Deleting a severe event:

To delete a severe event displayed on the **Severe Events** page, select the severe event you want to delete, and then perform one of the following procedures. You can delete the response status regardless of the response status of the selected severe event.

- From the menu bar, choose **View** and then **Delete**.
- From the popup menu that opens when you right-click the mouse, choose **Delete**.
- On the **Severe Events** page, click the **Delete** button.

The deletion operation in this case deletes the severe event from the page only, and not from the event database or the integrated monitoring database.

The information (Processed, Processing, Held, Unprocessed) that indicates the response status of the severe event, which was set on the **Severe Events** page, is also reflected in the display of the same event on the **Monitor Events** page. However, the deletion information is not displayed.

The information (Processed, Processing, Held, Unprocessed, or Deleted) that indicates the response status of the severe event is recorded in the event database of the logged-in manager. Consequently, when the response status is changed, the display on the **Severe Events** page of other JP1/IM - Views logged on to the same manager is also changed (the display of information, except for deletion, is also changed on the **Monitor Events** page). In the case of a severe event that has been forwarded from another host, the information in the event database or integrated monitoring database of the forwarding source host is not changed.

You can also use the `jcochstat` command to set the response status of a severe event. For details about the `jcochstat` command, see *jcochstat* (*1. Commands*) in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.

5.3 Changing the severity level of 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* in the *Job Management Partner 1/Integrated Management - Manager Configuration Guide*.

For details about how to set up the severity changing function, see *4.11 Setting the severity changing function* in the *Job Management Partner 1/Integrated Management - Manager Configuration Guide*.

The following shows how to change the severity level of an event.

5.3.1 Setting the severity of events when the system is set up

To set a severity changing definition, set it in the GUI, or define it in the severity changing definition file and execute the `jco_spmd_reload` command to apply the setting.

> **❚ Important note**
>
> Do not set a severity changing 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 and memory might become different.

(1) Setting a definition in the Severity Change Definition Settings window

To set the severity changing definitions 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 and enable the severity changing function. 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* (*1. Commands*) in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.

2. In the Event Console window, select **Options**, and then **Severity Change Definitions**.
   The View Severity Change Definitions window appears.

3. Click the **Add**, **Edit**, **Copy**, or **Delete** button according to your needs.

   When the **Add** button is clicked:
   > The Severity Change Definition Settings window appears. You can set a new severity changing definition.

   When the **Edit** button is clicked:
   > The Severity Change Definition Settings window appears. You can edit the selected severity changing definition.

   When the **Copy** button is clicked:
   > The selected severity changing definition is copied and added to the View Severity Change Definitions window. `Copy` is added to the beginning of the copied severity changing definition.

When the **Delete** button is clicked:

The selected severity changing definitions are deleted.

In this case, Step 4 is skipped.

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 changing definition.

In the View Severity Change Definitions window, select the severity changing definition that was set in the Severity Change Definition Settings window, and then select the **Apply** check box to enable the severity changing definition. If you want to set multiple events, repeat Steps 3 to 5.

6. A confirmation message appears. To apply the settings, click **Yes**.

The severity changing definitions you set take effect.

(2) Setting a definition in the severity changing definition file

To set severity changing definitions 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 and enable the severity changing function. 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* (*1. Commands*) in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.

2. Define the severity level change for the event in the severity changing definition file.

Create a severity changing definition for each system. You can change the severity level within the following range: Emergency, Alert, Critical, Error, Warning, Notice, Information, and Debug.

For details about the severity changing definition file, see *Severity changing definition file (jcochsev.conf)* (*2. Definition Files*) in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.

Specification example for the severity changing definition file

```
DESC_VERSION=2
def severity-change-1
cmt comment
define enable
cnd
B.ID IN 100 200
E.SEVERITY IN Warning
B.SOURCESERVER IN hostA hostB hostC
end-cnd
sev Emergency
end-def
```

3. Restart the JP1/IM - Manager or execute the jco_spmd_reload command.

If you changed the severity changing function from Disabled status to Enabled in Step 1, you need to restart the JP1/IM - Manager.

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

The severity of the JP1 event after the change is applied is displayed under **Severity** in the events list. The severity of the JP1 event before the change is applied 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 the event database of Event Service is not changed.

A mapping definition is sometimes used for changing severity. When you use a mapping definition, you can display a different attribute under **Severity** in the events list.

5.3.2 Setting the severity of events during operations

During system operations, you can select an event you want to change, and add conditions of the severity changing 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 for which you want to change the severity, and from the popup menu that opens when you right-click the mouse, select **Add Severity Change Definition Settings**.
   The Add Severity Change Definition Settings window appears.

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 additional severity changing definition is applied to the View Severity Change Definitions window. An icon is displayed in the **Type** column of the severity changing definition that was added during operations.

5.3.3 Changing an additional severity changing definition to a severity changing definition

To change an additional severity changing definition added during system operations to a severity changing 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, select the additional severity changing definition (for which an icon is displayed in the **Type** column) you want to change to a severity changing definition.

3. Click the **Change Copy** button.

4. A confirmation message appears. To apply the settings, click **Yes**.
   The additional severity changing definition you selected is changed to a severity changing 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 changing definition you added takes effect.

5.4 Editing 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.

For details about how to set up the integrated monitoring database, see *1.4.2 Setting up the integrated monitoring database* in the *Job Management Partner 1/Integrated Management - Manager Configuration Guide*.

For details about how to enable the memo entry startup function, see *4.7 Setting memo entries* in the *Job Management Partner 1/Integrated Management - Manager Configuration Guide*.

The procedure for editing memo entries and committing the changes to the JP1 events in the integrated monitoring database follows. Note that these operations require `JP1_Console_Admin` permission or `JP1_Console_Operator` permission.

To edit a memo entry:

1. Open the Edit Event Details window.
   You can open the Edit Event Details window by clicking the **Edit** button in the Event Details window or by selecting a single event from the events list and selecting the **Edit Event Details** menu.

2. Describe a memo entry in the Edit Event Details window.

3. Click the **Apply** button in the Edit Event Details window.
   The memo entry is displayed in **Memo**, which is a display item in the events list, and in the Event Details window. The memo icon is also displayed for events that have memo entries.

5.5 Searching for JP1 events

You can use various conditions to search for JP1 events and display those JP1 events that satisfy the search condition.

This section explains how to search for JP1 events and how to display the search results.

For details about the search function, see *3.6 Searching for events* in the *Job Management Partner 1/Integrated Management - Manager Overview and System Design Guide*. For details about the window used to search for events, see *2.23 Event Search Conditions window* in the manual *Job Management Partner 1/Integrated Management - Manager GUI Reference*.

5.5.1 Search method

This subsection explains the method for searching 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* in the *Job Management Partner 1/Integrated Management - Manager Configuration Guide*.

(1) Search procedure

To search for JP1 events:

1. To use the attribute value of a JP1 event displayed in the events list as the search condition, select a JP1 event from the events list in the Event Console window.

2. In the Event Console window, choose **View** and then **Search Events**. Alternatively, on the **Search Events** page of the Event Console window, click the **Search Events** button.
   The Event Search Conditions window opens.

3. In the Event Search Conditions window, specify search conditions.
   In the Event Search Conditions window, specify the following items:

   - Specify the search object
     When you are using 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 connected host name is specified.
     When you are using the integrated monitoring database, if 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 using a viewer that is outside the firewall to search for events, since a single host IP address may appear differently when seen from outside or inside the firewall. When you use a viewer that is outside the firewall and you specify an IP address to search for events, specify an IP address that can be resolved inside the manager.

Specify an IP address also when you are connecting to an agent that is connected to multiple LANs via an NIC of a host other than the representative host.

- Specify a search direction

  Specify the direction in which to search the integrated monitoring database or the event database.

  Specify either **Past direction** or **Future direction** as the event search direction. The default is **Past direction**. For details, see *5.5.1(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 *OR*ed.

  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 an 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 *AND*ed.

  The items you can specify are the event source host name, registered host name, severity 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 (*Processed*, *Unprocessed*, *Processing*, or *Held*), action status (*Taken* or *Not taken*), memo, items for repeated events, and extended attributes.

  If the memo function is disabled, the memo item cannot be specified. Also, if the mapping of the event source host is invalid, the event source host name cannot be specified. If repeated event monitoring suppression is disabled, you cannot specify items related to repeated events.

  If the search object is the integrated monitoring database and if the severity changing function is being used, you can set the severity item to the severity after a change. You can also specify an original severity level and a new severity level.

  For the original severity level, you can specify a severity level prior to a change. For the new severity level, you can specify whether the severity level has been changed.

  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.

  You can also use a regular expression to specify a registered host name, object type, object name, root object type, root object name, occurrence, user name, message, product name, extended attribute, and event source host name. For details about using a regular expression to specify search conditions, see *5.5.1(3) Using regular expressions to specify search conditions*.

4. Click **OK**.

   When the **Search Events** page opens and the search begins, **Searching** is displayed in 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 have executed an event search with a wrong search condition, or when you have found the event you want 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 (the default is 20 events). 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 that are acquired with the **Search for Next Event** button above the events that are already displayed. Note that events are always displayed chronologically starting with the earlier ones (that is, of the events that are acquired, earlier events are displayed above later events).

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 toward 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 that are acquired with the **Search for Next Event** button below the events that are already displayed.

See the examples in *5.5.2 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 registered host name, object type, object name, root object type, root object name, occurrence, user name, message, product name, and an extended attribute.

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 an 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 explanation of regular expressions in the chapter on setup in the *Job Management Partner 1/Base User's Guide*.

5.5.2 Displaying the search results

Event search results are displayed on the **Search Events** page in the Event Console window.

In the Preferences window, you can specify the number of events that can be acquired in a single event search. For details about how to specify the event acquisition count in the Preferences window, see *2.22 Preferences window* in the manual *Job Management Partner 1/Integrated Management - Manager GUI Reference*.

In the events list on the **Search Events** page, a response status icon indicating a severe event's response status is displayed in the far left column.

The table below shows the response status types and the corresponding response status icons.

Table 5–9: Response status types and response status icons

Response status	Response status icon
Processed	⚑
Processing	▶
Held	⏸
Unprocessed	(No icon)

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 follow.

Assumptions:

- The number of events that can be acquired from a single event search is 20.
- Only the events shown below are stored in the event database.

Figure 5–3: 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:

Selecting the **Past direction** radio button in **Search direction** in the Event Search Conditions window displays the last 20 JP1 event entries registered in the event database in an event list.

Figure 5–4: Last 20 JP1 event entries

```
2000  07/01  00:41:00   Event 41
2000  07/01  00:42:00   Event 42
         (Omitted)
2000  07/01  00:59:00   Event 59
2000  07/01  01:00:00   Event 60
```

Clicking the **Search for Next Event** button adds the next set of 20 events and displays them above the events that are already displayed.

Figure 5–5: 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)                  ⎬ Added
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
```

Example 2:

Selecting the **Future direction** radio button in **Search direction** in the Event Search Conditions window displays the first 20 JP1 event entries registered in the event database in an event list.

Figure 5–6: First 20 JP1 event entries

```
2000  07/01  00:01:00  Event 01
2000  07/01  00:02:00  Event 02
        (Omitted)
2000  07/01  00:19:00  Event 19
2000  07/01  00:20:00  Event 20
```

Clicking the **Search for Next Event** button adds the next set of 20 events and displays them below the events that are already displayed.

Figure 5–7: Display after the Search for Next Event button is clicked

```
2000  07/01  00:01:00  Event 01
2000  07/01  00:02:00  Event 02
        (Omitted)
2000  07/01  00:19:00  Event 19
2000  07/01  00:20:00  Event 20
2000  07/01  00:21:00  Event 21  ⎞
2000  07/01  00:22:00  Event 22  ⎟
        (Omitted)                ⎬ Added
2000  07/01  00:39:00  Event 39  ⎟
2000  07/01  00:40:00  Event 40  ⎠
```

5.5.3 Setting a response status for an event search

On the **Search Events** page, you can set the response status to match the actual response status of the event while the search result event is being displayed. The following conditions must be satisfied before you can set a response status:

- The search result must be from a logged-in manager.

- You must have `JP1_Console_Admin` permission or `JP1_Console_Operator` permission.

Setting a response status on the Search Events page:

You can set one of the following four response statuses: Processed, Processing, Held, or Unprocessed.

To set a response status, select the event to be set on the **Search Events** page and perform one of the following operations:

- From the menu bar, choose **View**, and from the submenu, select the response status to be set.

- From the popup menu that opens when you right-click the mouse, select the response status you want to set.

The information (Processed, Processing, Held, or Unprocessed) that indicates the response status of the severe event, which was set up on the **Search Events** page, is also reflected in the display of the same event on the **Monitor Events** page and the **Severe Events** page.

The **Search Events** page displays the event content that was present when the search was executed. Therefore, the display will not change even if the event content is changed on other pages. To display the latest data, execute the search again.

When you want to specify the manager host as the search host, specify the host name or IPv4 address of the manager host.

5.6 Opening a monitor window for the application that issued JP1 events

You can open the monitor window of the program that is related to the received JP1 event to view the information or perform other operations. You cannot use this function in the Web version of JP1/IM - View.

To open a monitor window from the Event Console window:

1. From the events list in the Event Console window, select a JP1 event and choose **View** and then **Monitor**.

   Alternatively, click the [icon] icon on the toolbar, or choose **Monitor** from the popup menu.

   The monitor window (Web page or application program) of the corresponding program opens.

You can also open a monitor window by clicking the **Monitor** button in the Event Details window.

If there is no program that corresponds to the selected JP1 event or if the settings necessary for opening a monitor window have not been made, you cannot choose the menu or button. For details about how to open a monitor window, see *4.14 Setting monitor startup for linked products* in the *Job Management Partner 1/Integrated Management - Manager Configuration Guide*.

5.6.1 Supported programs

The following table lists programs that can open a monitor window.

Program name	Window type	Monitor start definition file name	Supported OS
JP1/NETM/Asset Information Manager	Web page	`hitachi_jp1_aim_mon.conf`	Windows other than Windows Vista and Windows 7
JP1/PFM	Web page	`hitachi_jp1_pfmmgr_mon.conf`	No restrictions
JP1/IM - Rule Operation	Application window	`hitachi_jp1_im_rm_mon.conf`	No restrictions
JP1/IM - Event Gateway for Network Node Manager i	Web page	`hitachi_jp1_im_egn_mon.conf`	No restrictions
JP1/Base (SNMP trap)	Web page	`hitachi_jp1_imevtgw_mon.conf`	No restrictions
JP1/AJS2 - Scenario Operation	Application window	`hitachi_jp1_ajs2so_mon.conf`	No restrictions
JP1/AJS3 (version 9 or later) or JP1/AJS2 (version 8 or earlier)	Application window	`hitachi_jp1_ajs2_mon.conf`	No restrictions
JP1/AJS2 mainframe	Application window	`hitachi_jp1_ajs2_mainframe_mon.conf`	No restrictions
Cosminexus Application Server	Application window	`hitachi_cosminexus_manager_mon.conf`	No restrictions

5.7 Enabling a view filter

To enable a view filter for the JP1 events being displayed on the **Monitor Events** and **Severe Events** pages of the Event Console window:

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 that is set by the filter are displayed on the **Monitor Events** and **Severe Events** pages of the Event Console window.

You must set up a view filter before you can enable it.

To set up a view filter:

   See *4.2.1 Settings for view filters* in the *Job Management Partner 1/Integrated Management - Manager Configuration Guide*.

5.8 Switching the event acquisition filter

From the multiple event acquisition filters that have been saved, you can select the filtering condition that JP1/IM uses when acquiring JP1 events from JP1/Base, and you can switch to this condition.

In an event acquisition filter, you can switch between enabling and disabling a common exclusion-condition, which is defined to temporarily exclude certain JP1 events from being acquired.

You switch the common exclusion-condition when it is necessary to exclude a host on which maintenance work is being performed from the monitoring object, so that the JP1 events generated on the host being maintained are temporarily filtered out and not acquired.

The following two methods are available for switching an event acquisition filter and a common exclusion-condition:

- Making the switch from the System Environment Settings window or Event Acquisition Conditions List window of JP1/IM - View
- Using the `jcochfilter` command to make the switch

Note, however, that if an event acquisition filter is running for a compatibility reason, you cannot switch it.

For details about the events that are generated when an event acquisition filter is switched, see *3.2.2 Event acquisition filter* in the *Job Management Partner 1/Integrated Management - Manager Overview and System Design Guide*.

5.8.1 Making a switch from the System Environment Settings window or Event Acquisition Conditions List window of JP1/IM - View

You can switch an event acquisition filter, and switch between enabling and disabling a common exclusion-condition, from the System Environment Settings window or Event Acquisition Conditions List window of JP1/IM - View.

To start the System Environment Settings window or Event Acquisition Conditions List window, you need `JP1_Console_Admin` permission. In addition, when the reference and operation permissions are set for a business group, operations in these windows might not be possible depending on the combination of JP1 resource group and JP1 permission level. For details, see *3.1.4(2) Assigning a JP1 resource group and permission level to a JP1 user* in the *Job Management Partner 1/Integrated Management - Manager Overview and System Design Guide*.

(1) Making the switch from the System Environment Settings window

(a) Switching an event acquisition filter

If the name of the event acquisition filter to be switched is clear, select that event acquisition filter from the System Environment Settings window, and then execute the switch.

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.

(b) Switching between enabling and disabling a common exclusion-condition

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.

(2) Making the switch from the Event Acquisition Conditions List window

(a) Switching the event acquisition filter

If you cannot identify the name of the event acquisition filter to be switched in the System Environment Settings window, you can check the setting details of event acquisition filters in the Event Acquisition Conditions List window, and then execute the switch.

To switch an event acquisition filter:

1. In the Event Console window, choose **Options** and then **System Environment Settings**.
   The System Environment Settings window opens.

2. In **Event acquisition conditions,** click the **Editing list** button.
   The Event Acquisition Conditions List window opens.

3. From **Filter list**, select an event acquisition filter.
   Select an event acquisition filter based on the filter ID or filter name. To check the content, select an event acquisition filter and click the **Edit** button. The Event Acquisition Settings window opens and you can check the content of the filter you selected.

4. Click **OK**.
   The display returns to the System Environment Settings window.

5. Click **Apply**.
   The setting is enabled.

In the Event Acquisition Conditions List window, you can add, edit, copy, and delete filtering conditions. For details, see *4.2.4 Settings for event acquisition filters* in the *Job Management Partner 1/Integrated Management - Manager Configuration Guide*.

(b) Switching between enabling and disabling a common exclusion-condition

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.

5.8.2 Making the switch using the jcochfilter command

You can use the `jcochfilter` command to switch an event acquisition filter, and to switch between enabling and disabling a common exclusion-condition.

To use the `jcochfilter` command to switch an event acquisition filter and to switch between enabling and disabling a common exclusion-condition, use the job scheduler function of JP1/AJS and execute the `jcochfilter` command at the specified time to create a jobnet that starts a maintenance job. You can also automate the process of changing the maintenance job and monitoring state.

(1) Switching 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* (*1. Commands*) in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.

To switch an event acquisition filter:

1. Enter the `jcochfilter` command and display an event acquisition conditions list.

   Examples follow of displaying an event acquisition conditions list on a physical host and a logical host.

   • Displaying an event acquisition conditions list on a physical host
     Enter the command as follows.
     ```
     jcochfilter
     ```
   • Displaying an event acquisition conditions list on logical host `hostA`
     Enter the command as follows.
     ```
     jcochfilter -h hostA
     ```

   A display example follows of an event acquisition conditions list on logical host `hostA`.

Figure 5–8: 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`

(2) Switching 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* (*1. Commands*) in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.

To switch between enabling and disabling a common exclusion-condition:

1. Enter the `jcochfilter` command and display an event acquisition conditions list.

   Examples of displaying an event acquisition conditions list on a physical host and a logical host are described below.

   • Displaying an event acquisition conditions list on a physical host

     Enter the command as follows.

     `jcochfilter`

- Displaying an event acquisition conditions list on logical host `hostA`

  Enter the command as follows.
  ```
  jcochfilter -h hostA
  ```

If JP1/IM - Manager on the specified host has not started, you cannot use the command to switch an event acquisition filter.

2. Select a common exclusion-conditions group based on the common exclusion-conditions group ID and the common exclusion-conditions group name.

3. Switch between enabling and disabling the common exclusion-conditions group.

   Use one of the following options to switch between enabling and disabling the common exclusion-conditions group.

   - `-e` option

     Specify the common exclusion-conditions group ID you want to enable.

     Unspecified common exclusion-conditions groups are disabled.

   - `-on` or `-off` option

     Specify the common exclusion-conditions group ID you want to enable.

     The enabling and disabling settings of unspecified common exclusion-conditions groups are not changed.

     These options can be used when the operating mode of the common exclusion-condition is extended mode.

   The following describes an example of switching between enabling and disabling common exclusion-conditions on the physical host and a logical host.

   - On the physical host, the common exclusion-conditions with common exclusion-conditions group ID 3 are enabled, and the common exclusion-conditions with common exclusion-conditions group IDs 1 and 2 are disabled (only the specified common exclusion-conditions groups are changed).

     This specification can be used when the operating mode of the common exclusion-condition is extended mode.
     ```
     jcochfilter -on 3 -off 1,2
     ```

   - On the physical host, the common exclusion-conditions with common exclusion-conditions group ID 3 are enabled, and the other common exclusion-conditions are disabled.
     ```
     jcochfilter -e 3
     ```

   - On logical host `hostA`, the common exclusion-conditions with common exclusion-conditions group ID 3 are enabled, and the other common exclusion-conditions are disabled.
     ```
     jcochfilter -e 3 -h hostA
     ```

5.9 Outputting the information displayed in JP1/IM - View to a CSV file

You can use one of the three methods described below to output the information displayed in JP1/IM - View to a CSV file.

- Save the JP1 events list information displayed in JP1/IM - View to a file.
- Use the `jcoevtreport` command to output the JP1 events registered in the integrated monitoring database to a CSV file.
- Copy selected parts of JP1 event information and action execution results to the clipboard.

This section explains each of these methods.

5.9.1 Outputting an events list to a CSV file

You can save the snapshot[#] of the events list that is displayed in JP1/IM - View to a CSV file. You cannot use this function in the Web version of JP1/IM - View.

#: A snapshot shows information extracted at a specific time.

You can output the following pages to a CSV file:

- **Monitor Events** page of the Event Console window
- **Severe Events** page of the Event Console window
- **Search Events** page of the Event Console window

To output information to a CSV file:

1. In the Event Console window, display the page you want to output to a CSV file.
   Use the tabs on the Event Console window to switch between the pages.
   The information being displayed in the events list on the displayed page is output to a CSV file. JP1 events and items not being displayed in the events list are not output.
   To narrow the JP1 events being displayed on the **Monitor Events** page, apply a view filter before proceeding to the next step.
   For the **Search Events** page, execute an event search to display the JP1 events to be output to a CSV file before proceeding to the next step.

2. In the Event Console window, choose **File** and then **Save Displayed Events**.
   The Save Displayed Events window opens.

3. Save the information in the desired folder under the desired file name.
   Save the information by specifying the desired folder name and file name.

5.9.2 Outputting the content of the integrated monitoring database to a CSV file

This subsection explains how to output the content of the integrated monitoring database to a CSV file. For details about the CSV output format and information that can be output in the CSV format, see *3.12.2 Saving event information in*

the integrated monitoring database (CSV report) in the *Job Management Partner 1/Integrated Management - Manager Overview and System Design Guide*.

To output information to a CSV file:

1. Specify the attributes of the JP1 events to be output to a CSV file in the `jcoevtreport` command.

   - Output range

     You can specify the output range by specifying the output-target start date option (`-s`) and the output-target end date option (`-e`) in the `jcoevtreport` command.

     Also, by specifying the filtering option (`-f`) in the `jcoevtreport` command, you can output to a CSV file only those JP1 events that match the condition specified by the system administrator.

     Additionally, by specifying the output-and-save output option (`-save`) in the `jcoevtreport` command, you can output and save the information of JP1 events registered in the integrated monitoring database. The system administrator can retain information on all JP1 events by regularly outputting and saving this information.

   - Output content

     By specifying the output item option (`-k`) in the `jcoevtreport` command, you can narrow the information specific to the JP1 events that are to be output to a CSV file.

     Furthermore, by specifying the maintenance information output option (`-sys`) in the `jcoevtreport` command, you can output to a CSV file the maintenance information on the JP1 events registered in the integrated monitoring database. Since the purpose of outputting the maintenance information is to collect data in the event of an error in the integrated monitoring database, you cannot specify or filter output items.

   - Output destination

     For ease of handling, the `jcoevtreport` command outputs JP1 event information to a separate CSV file each time it is executed. By specifying the `-o` option in the `jcoevtreport` command, you can change the name of an output destination file. Output destination file names use the following format: *output-file-name_serial-number*`.csv`.

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

2. Execute the `jcoevtreport` command to output the JP1 event information registered in the integrated monitoring database to CSV files.

5.9.3 Copying JP1 event information and action execution results to the clipboard

You can copy selected parts of JP1 event information and action execution results to the clipboard in the CSV format. You cannot use this function in the Web version of JP1/IM - View.

For details about information that can be copied to the clipboard in the CSV format and windows in which this function can be used, see *3.12.3 Copying JP1 event information and action execution results to the clipboard* in the *Job Management Partner 1/Integrated Management - Manager Overview and System Design Guide*.

To copy information to the clipboard in the CSV format:

1. Open the window containing the information you want to copy to the clipboard.

2. Select the information to copy.

3. Press the shortcut keys **Ctrl** + **C**.

The selected information is copied to the clipboard. In the Event Console window, you can also choose **Edit** and then **Copy** instead of pressing the shortcut keys **Ctrl** + **C**.

6

System Monitoring from Central Scope

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

6.1 Monitoring from the Monitoring Tree window

You can monitor the statuses of monitored objects from the Monitoring Tree window. You can also perform various types of operations, such as changing the statuses and monitoring statuses for the monitoring nodes (monitoring groups and monitored objects) displayed in the Monitoring Tree window.

When the monitoring range settings of the monitoring tree are enabled, the monitoring tree displays only the monitoring nodes that are set for the JP1 resource group of the logged-on 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 on 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 on to JP1/IM - Manager (JP1/IM - Central Scope).
- Click the **Central Scope** button in the Event Console window.
- From the menu bar in the Event Console window, choose **File** and then **Central Scope**.

A Monitoring Tree window display example follows.

Figure 6–1: Monitoring Tree window display example

Tree pane   Details pane   (can be switched to a map display)
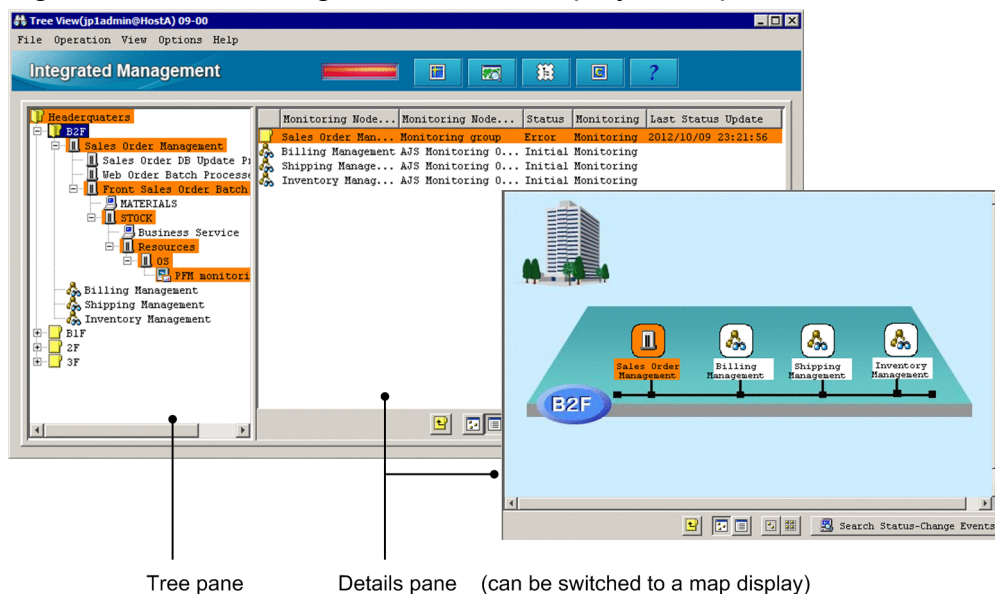
6.1.1 Changing the status of monitoring nodes

This subsection explains how to change the status of a monitoring node displayed in the Monitoring Tree window. The status that can be changed and the action that occurs at the time of the change differ depending on the monitoring node type (monitoring group or monitored object). For details, see *4.2.2 Statuses of monitoring nodes* in the *Job Management Partner 1/Integrated Management - Manager Overview and System Design Guide*.

Changing the status of a monitoring node requires at least `JP1_Console_Operator` permission. When the monitoring range settings of the monitoring tree are enabled, you can change the status of only those monitoring nodes that can be accessed with at least `JP1_Console_Operator` permission from among the monitoring nodes being displayed.

To change the status of a monitoring node:

1. Select a monitoring node displayed in the tree pane or details pane.

2. Use either of the following methods to change the status of the monitoring node:

   - From the menu bar, choose **Operation** and then **Change Status**, and then change the status to the desired one.

   - From the popup menu that opens when you right-click the mouse, choose **Change Status** and then change the status to the desired one.

   A confirmation dialog box opens.

3. In the configuration dialog box, click **Yes**.

6.1.2 Changing the monitoring status of monitoring nodes

This subsection explains how to change the monitoring status of a monitoring node. The action that occurs at the time of the change differs depending on the monitoring node type (monitoring group or monitored object). For details, see *4.2.2 Statuses of monitoring nodes* in the *Job Management Partner 1/Integrated Management - Manager Overview and System Design Guide*.

Changing the monitoring status of a monitoring node requires at least JP1_Console_Operator permission. When the monitoring range settings of the monitoring tree are enabled, you can change the status of only those monitoring nodes that can be accessed with at least JP1_Console_Operator permission from among the monitoring nodes being displayed.

To change the monitoring status of a monitoring node:

1. Select a monitoring node displayed in the tree pane or details pane.

2. Use one of the following methods to change the status of the monitoring node:

   - From the menu bar, choose **Operation** and then **Change Monitoring Status**, and then change the monitoring status to the desired one.

   - From the popup menu that opens when you right-click the mouse, choose **Change Monitoring Status**, and then change the monitoring status to the desired one.

   - From the popup menu that opens when you right-click the mouse, choose **Properties** and select either **Monitoring** or **Not Monitoring** from the **General** page, and then click **OK** or **Apply**.

   - Open the Properties window by double-clicking the selected monitoring node, select either **Monitoring** or **Not Monitoring** from the **General** page, and then click **OK** or **Apply** (limited to monitored objects only).

   > **❚ Important note**
   >
   > - If the monitoring status of a higher-order monitoring group is set to **Not Monitoring**, you cannot set a lower-order monitoring node alone to **Monitoring**.
   >
   > - When the monitoring status of a monitoring node is set to **Not Monitoring**, the status returns to the initial status.

6.1.3 Searching for monitoring nodes

This subsection explains how to search for monitoring nodes. When the monitoring range settings of the monitoring tree are enabled, you cannot execute a search using the virtual root node as the starting point. Furthermore, the virtual root node cannot be a search target.

To search for monitoring nodes:

1. Select a monitoring group displayed in the tree pane or details pane.
   You can restrict the monitoring nodes that can be searched to the selected monitoring group and the monitoring nodes that are in that monitoring group.

2. Use either of the following methods to open the Search window:
   - From the menu bar, choose **View** and then **Search**.
   - From the popup menu that opens when you right-click the mouse, choose **Search**.

3. Enter a condition into the Search window and click the **Search** button.
   Monitoring nodes that match the search condition are displayed in a list.

You can perform the following operations on the monitoring nodes that are displayed in the list:

- Change the status or monitoring status of a monitoring node.
  To change the status or monitoring status of a monitoring node, right-click to open the popup menu.
- With the target monitoring node selected, open the Monitoring Tree window.
  To do so in this case, double-click the mouse.

6.1.4 Searching for status-change events

This subsection explains how to search for status-change events.

1. Select a monitoring node whose status has changed.

2. Use one of the following methods to search for status-change events:
   - From the menu bar, choose **View** and then **Search Status-Change Events**.
   - From the popup menu that opens when you right-click the mouse, choose **Search Status-Change Events**.
   - Click the **Search Status-Change Events** button located in the lower portion of the details pane.

When you execute a status-change event search on a monitored object, up to 100 JP1 events matching the status change condition of that monitored object are displayed sequentially, starting with the earliest event, on the **Search Events** page of the Event Console window (the 101st and subsequent events are not displayed). Therefore, if the number of JP1 events displayed as search results has increased, we recommend that you manually change the status of the monitored object as needed.

If the number of JP1 events matching the status change condition of the monitored object exceeds 100, a warning JP1 event (event ID = 00003FB1) is generated. When this JP1 event is generated, check how JP1 events matching the status change condition are handled, and manually change the status of the monitored object.

When you execute a status-change event search on a monitoring group, up to 100 JP1 events matching the status change condition of the monitored objects in that monitored group are displayed sequentially on the **Search Events** page of the Event Console window, starting with the earliest event (the 101st and subsequent events are not displayed). Note that

if a status change condition has been defined for a monitoring group, only up to 100 status-change events requiring action are sequentially displayed, starting with the earliest event, even if there are events that changed the status of lower-order monitoring nodes.

> **▌ Important note**
>
> - When you manually change the status of a monitoring node, you clear the status-change event history. Consequently, you will not be able to search for (display) the status-change events that have occurred in the past. Therefore, before you manually change the status of a monitoring node, check how JP1 events matching the status-change condition are handled.
>
> - The JP1 events that can be searched using a status-change event search are restricted by a user filter (if the user is subject to restriction by a user filter).
>
> - We recommend that you open the Event Console window before searching for status-change events.
>
> - If the number of JP1 events matching the status-change condition of the monitored object exceeds 100, the completed-action linkage function becomes inactive. Therefore, if the number of JP1 events displayed as search results has increased, we recommend that you manually change the status of the monitored object as needed.

6.1.5 Displaying the attributes of monitoring nodes

To display the attributes of a monitoring node:

1. Select a monitoring node.

2. Use one of the following methods to open the Properties window:
   - From the menu bar, choose **View** and then **Properties**.
   - From the menu bar, choose **Options** and then **Basic Information**.
   - From the menu bar, choose **Options** and then **Status-Change Condition**.
   - From the menu bar, choose **Options** and then **Event-Issue Conditions**.
   - From the popup menu that opens when you right-click the mouse, choose **Properties**.
   - Double-click (limited to a monitored object).

A JP1 user having at least `JP1_Console_Operator` permission can change several of the attributes displayed in the Properties window. To change the attributes of a monitoring node, log on as a user with at least the operating permission of `JP1_Console_Operator`.

6.1.6 Displaying guide information

To display guide information:

1. Select a monitored object.

2. Use either of the following methods to open the Guide window.
   - From the menu bar, choose **View** and then **Guide**.
   - From the popup menu that opens when you right-click the mouse, choose **Guide**.

You must define in advance, in a guide information file, the conditions for displaying guide information according to various situations and the guide information content.

About the guide information function, definition file, and settings:

- About the details to set in the guide information and the guide function:

  See *4.8 Guide function* in the *Job Management Partner 1/Integrated Management - Manager Overview and System Design Guide*.

- About editing the guide information file:

  See *5.6 Editing guide information* in the *Job Management Partner 1/Integrated Management - Manager Configuration Guide*.

- About the format of the guide information file:

  See *Guide information file (jcs_guide.txt)* (*2. Definition Files*) in the manual *Job Management Partner 1/ Integrated Management - Manager Command and Definition File Reference*.

6.1.7 Opening the Visual Monitoring window

To open the Visual Monitoring window:

1. Use either of the following methods to display the Open Visual Monitoring Window window.

   - From the menu bar, choose **View** and then **Visual Monitoring**.

   - Click the [icon] icon in the toolbar.

2. Select a Visual Monitoring window name displayed in the Open Visual Monitoring Window window and click **OK**.

6.1.8 Displaying a login user list

To display a list of JP1 users that have logged on to JP1/IM - Manager (JP1/IM - Central Scope):

1. In the menu bar, choose **Options** and then **Login User List**.

6.1.9 Saving the information in the Monitoring Tree window on the local host

To save the information on the local host:

1. From the menu bar, choose **File** and then **Save Monitoring-Tree Status**.
   The file selection window opens.

2. Save the information in the desired folder under a desired name on the local host.
   The monitoring tree information is saved in a CSV file.

When the monitoring range settings of the monitoring tree are enabled, you cannot save the information in the Monitoring Tree window on the local host. To save the information, save it on the local host from the Monitoring Tree (Editing) window.

6.2 Monitoring from the Visual Monitoring window

You can monitor the statuses of monitored objects from the Visual Monitoring window.

When the monitoring range settings of the monitoring tree are enabled, the Visual Monitoring window displays only the monitoring nodes that are set for the JP1 resource group of the logged-on JP1 user. However, if the JP1 resource group is `JP1_Console` and if the user has logged on 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] icon in the toolbar of the Monitoring Tree window.

2. Select a Visual Monitoring window name displayed in the Open Visual Monitoring Window window and click **OK**.
   When the monitoring range settings of the monitoring tree are enabled, if a visual monitoring window does not contain any monitoring node that can be displayed, it is not displayed in the list in the Open Visual Monitoring Window window.

A Visual Monitoring window display example follows.

Figure 6–2: Visual Monitoring window display example
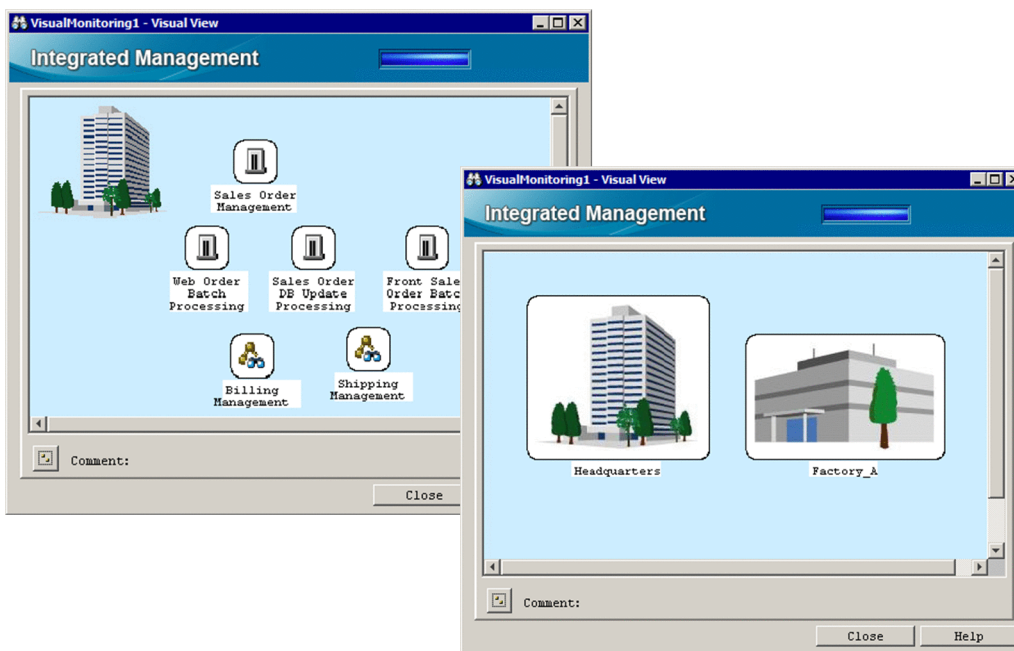
6.2.1 Opening the Monitoring Tree window from the Visual Monitoring window

To open the Monitoring Tree window from the Visual Monitoring window:

1. Select a monitoring node and double-click it.

The Monitoring Tree window opens with the monitoring node selected that you double-clicked in the Visual Monitoring window.

6.2.2 Changing the status of monitoring nodes

This subsection explains how to change the status of a monitoring node displayed in the Visual Monitoring window. The status that can be changed and the action that occurs at the time of the change differ depending on the monitoring node type (monitoring group or monitored object). For details, see *4.2.2 Statuses of monitoring nodes* in the *Job Management Partner 1/Integrated Management - Manager Overview and System Design Guide*.

Changing the status of a monitoring node requires at least JP1_Console_Operator permission. When the monitoring range settings of the monitoring tree are enabled, you can change the status of only those monitoring nodes that can be accessed with at least JP1_Console_Operator permission from among the monitoring nodes being displayed.

To change the status of a monitoring node:

1. Select a monitoring node.

2. From the popup menu that opens when you right-click the mouse, choose **Change Status** and change the status to the desired one.
   A confirmation dialog box opens.

3. In the configuration dialog box, click **Yes**.

6.2.3 Changing the monitoring status of monitoring nodes

This subsection explains how to change the monitoring status of a monitoring node. The action that occurs at the time of the change differs depending on the monitoring node type (monitoring group or monitored object). For details, see *4.2.2 Statuses of monitoring nodes* in the *Job Management Partner 1/Integrated Management - Manager Overview and System Design Guide*.

Changing the monitoring status of a monitoring node requires at least JP1_Console_Operator permission. When the monitoring range settings of the monitoring tree are enabled, you can change the status of only those monitoring nodes that can be accessed with at least JP1_Console_Operator permission from among the monitoring nodes being displayed.

To change the monitoring status of a monitoring node:

1. Select a monitoring node.

2. Use either of the following methods to change the status of the monitoring node:
   - From the popup menu that opens when you right-click the mouse, choose **Change Monitoring Status**, and then change the monitoring status to the desired one.
   - From the popup menu that opens when you right-click the mouse, choose **Properties** and select either **Monitoring** or **Not Monitoring** from the **General** page, and then click **OK** or **Apply**.

> **Important note**
>
> - If the monitoring status of a higher-order monitoring group is set to **Not Monitoring**, you cannot set a lower-order monitoring node alone to **Monitoring**. Check the monitoring status of the higher-order monitoring group in the Monitoring Tree window.
> - When the monitoring status of a monitoring node is set to **Not Monitoring**, the status returns to the initial status.

6.2.4 Searching for monitoring nodes

To search for monitoring nodes:

1. Select a monitoring group.
   You can restrict the monitoring nodes that can be searched to the selected monitoring group and the monitoring nodes that are in that monitoring group.

2. From the popup menu that opens when you right-click the mouse, choose **Search**.

3. Enter a condition into the Search window and click the **Search** button.
   Monitoring nodes that match the search condition are displayed in a list.

You can perform the following operations on the monitoring nodes that are displayed in the list:

- Change the status or monitoring status of a monitoring node.
  To change the status or monitoring status of a monitoring node, right-click to open the popup menu.

- With the target monitoring node selected, open the Monitoring Tree window.
  To do so in this case, double-click the mouse.

6.2.5 Searching for status-change events

To search for status-change events:

1. Select a monitoring node whose status has changed.

2. From the popup menu that opens when you right-click the mouse, choose **Search Status-Change Events**.

When you execute a status-change event search on a monitored object, up to 100 JP1 events matching the status-change condition of that monitored object are displayed sequentially, starting with the earliest event, on the **Search Events** page of the Event Console window (the 101st and subsequent events are not displayed). Therefore, if the number of JP1 events displayed as search results has increased, we recommend that you manually change the status of the monitored object as needed.

If the number of JP1 events matching the status-change condition of the monitored object exceeds 100, a warning JP1 event (event ID = 00003FB1) is generated. When this JP1 event is generated, check how JP1 events matching the status-change condition are handled, and manually change the status of the monitored object.

When you execute a status-change event search on a monitoring group, up to 100 JP1 events matching the status-change condition of the monitored objects in that monitored group are displayed sequentially on the **Search Events** page of the

Event Console window, starting with the earliest event (the 101st and subsequent events are not displayed). Note that if a status change condition has been defined for a monitoring group, only up to 100 status-change events requiring action are sequentially displayed, starting with the earliest event, even if there are events that changed the status of lower-order monitoring nodes.

> **▌ Important note**
>
> - When you manually change the status of a monitoring node, you clear the status-change event history. Consequently, you will not be able to search for (display) the status-change events that have occurred in the past. Therefore, before you manually change the status of a monitoring node, check how JP1 events matching the status-change condition are handled.
>
> - The JP1 events that can be searched using a status-change event search are restricted by a user filter (if the user is subject to restriction by a user filter).
>
> - We recommend that you open the Event Console window before searching for status-change events.
>
> - If the number of JP1 events matching the status change condition of the monitored object exceeds 100, the completed-action linkage function becomes inactive. Therefore, if the number of JP1 events displayed as search results has increased, we recommend that you manually change the status of the monitored object as needed.

6.2.6 Displaying the attributes of monitoring nodes

To display the attributes of a monitoring node:

1. Select a monitoring node.

2. From the popup menu that opens when you right-click the mouse, choose **Properties**.
   The Properties window opens.

A JP1 user having at least `JP1_Console_Operator` permission can change several of the attributes displayed in the Properties window. To change the attributes of a monitoring node, log on as a user with at least the operating permission of `JP1_Console_Operator`.

6.2.7 Displaying guide information

To display guide information:

1. Select a monitored object.

2. From the popup menu that opens when you right-click the mouse, choose **Guide**.

You must define in advance, in a guide information file, the conditions for displaying guide information according to various situations and the guide information content.

About the guide information function, definition file, and settings:

- About the details to set in the guide information and the guide function:
  See *4.8 Guide function* in the *Job Management Partner 1/Integrated Management - Manager Overview and System Design Guide*.

- About editing the guide information file:

  See *5.6 Editing guide information* in the *Job Management Partner 1/Integrated Management - Manager Configuration Guide*.

- About the format of the guide information file:

  See *Guide information file (jcs_guide.txt)* (*2. Definition Files*) in the manual *Job Management Partner 1/ Integrated Management - Manager Command and Definition File Reference*.

7

System Operation Using JP1/IM

This chapter explains the use of JP1/IM - View for system operations. For details about the windows explained in this chapter, see *2. Event Console Window* and *3. Monitoring Tree Window* in the manual *Job Management Partner 1/Integrated Management - Manager GUI Reference*.

7.1 Executing a command

You can execute commands on an agent host or a manager host. You can also execute the commands (client application) of a client host (viewer host). You can use this function when you are connected to JP1/IM - Manager (JP1/IM - Central Console) from JP1/IM - View.

If JP1/Base on the host stops while a command is being executed, `CMD.EXE` and the executing command (in Windows) or a shell and the executing command (in UNIX) might remain. In such cases, either manually stop the command or restart the host.

In addition, commands in the queue are discarded if JP1/Base on the host that stops while a command is being executed.

7.1.1 Executing a command by using Command Execution

The following operations require `JP1_Console_Admin` permission or `JP1_Console_Operator` permission.

- Executing a command on an agent host
- Executing a command on a manager host
- Executing a client application

To execute a command that inherits event information, select the JP1 event, and then execute the command.

The following describes the method of operation.

1. In the Event Console window, choose **Options** and then **Execute Command**, or from the toolbar, click the icon.
   The Execute Command window opens.

2. Select **Command type**.
   If you are executing a command on a managed host (agent host or manager host), select the **Command of managed host** radio button.
   If you are executing a client application, select the **Client application** radio button.

3. If necessary, select **Event Information to inherit**.
   If you want to inherit event information, select the **Inherit event information** check box.

4. For **Target host**, specify the host on which the command is to be executed.
   For the target host, specify the host name that is specified as the managed host in the system configuration definition.
   You can also select from the list box a host name that was specified in the past. A maximum of five host names specified in the past are saved in the list box.
   If you selected the **Inherit event information** check box in step 3, event information is inherited and automatically entered.
   You can also specify a host group name for the command target host. When you specify a host group name, the command will be executed on all hosts that comprise the host group. Host group names that can be specified are those that are defined by the login manager.
   For details about the procedure for defining host groups, see *1.16 Setting up a command execution environment* (in Windows) or *2.15 Setting up a command execution environment* (in UNIX) in the *Job Management Partner 1/ Integrated Management - Manager Configuration Guide*.

When you set a business group or monitoring group, you can specify a business group or a monitoring group for the target host name. The specification method follows.

Example: When business group `management system` is specified for the target host name

```
/Management system
```

For details about the specification method, see *3.1.4(3) How to specify business groups* in the *Job Management Partner 1/Integrated Management - Manager Overview and System Design Guide*.

5. In **Command**, specify the command to be executed. Also specify an **Environment variable file** as needed.

   Enter the command line to be executed in **Command**.

   You can also select from the list box a command that was specified in the past. To erase the history of commands specified in the past, click the **Clear History** button.

   For **Environment variable file**, specify the absolute path to the environment variable file located at the command target host.

   The following commands can be executed:

   When the command target host is running under UNIX

   • UNIX commands

   • Shell scripts

   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.)

   The following types of commands cannot be executed:

   • Commands that require interactive operations

   • Commands that open a window

   • Commands that come with an escape sequence or control code

   • Commands that do not end, such as a daemon

   • Commands that must interact with the desktop, such as Windows Messenger and DDE (in Windows)

   • Commands that shut down the OS, such as `shutdown` and `halt`

6. Click the **Execute** button.

   When the **Inherit event information** check box in **Event information to inherit** is not selected

   The command whose command type was selected in **Command type** is executed on the host specified in **Target host**. After the command is executed, **Time**, **Host**, and **Message** appear in **Log**. There is no need to perform the following steps.

   When the **Inherit event information** check box in **Event information to inherit** is selected

   The Preview Command Execution Content window opens. Go to the next step.

7. Check the information in the Preview Command Execution Content window.

   Check the information for **Target host**, **Command**, and **Environment variable file** after the variables are replaced.

   An item for which ⚠ is displayed has a setting error. Review the settings.

   For details about the Preview Command Execution Content window, see *2.39 Preview Command Execution Content window* in the manual *Job Management Partner 1/Integrated Management - Manager GUI Reference*.

8. Click the **Execute** button.

If there is no problem with the information in the Preview Command Execution Content window, the command is executed, and the Preview Command Execution Content window closes. After the command is executed, **Time**, **Host**, and **Message** appear in **Log** in the Execute Command window.

7.1.2 Executing a command by using the Command button

There are two ways to execute a command previously registered for a **Command** button, depending on the type of host on which the command is executed.

- Executing a command on an agent host or manager host
- Executing a command defined on the source host of the selected event

To execute a command, you need JP1_Console_Admin permission or JP1_Console_Operator permission. When you move the cursor to the **Command** button, the information set for the **Command** button is displayed in the Execute Command window. Before executing a command, make sure that you check the information for the command.

To execute a command that inherits event information, select the JP1 event, and then execute the command.

For details on how to set the **Command** button, refer to the following:

- For Windows

  1.16 Setting up a command execution environment in the *Job Management Partner 1/Integrated Management - Manager Configuration Guide*.

- For UNIX

  2.15 Setting up a command execution environment in the *Job Management Partner 1/Integrated Management - Manager Configuration Guide*.

(1) Executing a command on an agent host or manager host

The following describes how to immediately execute a command on an agent host or manager host.

(a) Immediately executing a command

To immediately execute a command after the **Command** button is clicked, create the following settings.

Event information is not inherited when the command is executed:

  Specify true for the qui parameter in the command button definition file. If you specify this parameter, when the **Command** button is clicked, a message asking whether the command is to be executed is not displayed, and the command is immediately executed on the agent host or manager host.

Event information is inherited when the command is executed:

  Specify false for the preview parameter in the command button definition file. If you specify this parameter, when the **Command** button is clicked, the Preview Command Execution Content window does not open, and the command is immediately executed.

The following describes the procedure for immediately executing a command:

1. In the Event Console window, select **Option** and then **Execute Command**. Alternatively, on the toolbar, click

    .

   The Execute Command window opens.

2. Click the **Command** button to which the command you want to execute has been assigned.

The command is executed.

(b) Executing a command after changing the information registered for the command

The following describes how to execute a command after changing the information registered for it.

When you execute a command that inherits event information, the Preview Command Execution Content window opens, and you can change the information for the command. The following operation is effective when you execute the command on a managed host that does not inherit events.

1. In the Event Console window, choose **Option** and then **Execute Command**. Alternatively, on the toolbar, click

    .

   The Execute Command window opens.

2. Right-click the **Command** button to which the command you want to execute has been assigned to display a popup menu.

3. On the popup menu, click **Custom Execution**.

   The setting information for the **Command** button is displayed in **Command type**, **Event information to inherit**, **Target host**, **Command**, and **Environment variable file** of the Execute Command window. You can now edit the setting information.

   Edit **Target host**, **Command**, and **Environment variable file** as needed.

4. Click the **Execute** button.

   The command is executed on the agent host or manager host.

(2) Executing a command defined on the source host of the selected event

The following applies to the source host of the event when the host is undergoing examination or when corrective action for an error is being performed for it. If you do not specify anything in **Target host**, but define a **Command** button, and then click the **Command** button, you can execute a command defined on the source host of the selected event. Note that even if the attribute of another JP1 event is mapped, the source host before the mapping is set in **Target host**.

The following describes the procedure for executing a command defined on the source host of the selected event.

1. In the Event Details window, choose the **Execute Command** button.

   The Event Details window opens.

2. Click the **Command** button to which the command you want to execute is assigned.

   Event information is not inherited when the command is executed:

   A message asking whether the command is to be executed is displayed. If there is no problem, you can click the **OK** button.

   The command defined on the source host of the selected event is executed. Note that when true is specified for the qui parameter in the command button definition file, the command is executed immediately without displaying any message. There is no need to perform the following steps.

   Event information is inherited when the command is executed:

   When false is specified for the preview parameter in the command button definition file, the command is executed immediately without displaying the Preview Command Execution Content window. There is no need to perform the following steps.

   When true is specified, the Preview Command Execution Content window opens. Go to the next step.

3. Check the information in the Preview Command Execution Content window.

   Check the information for **Target host**, **Command**, and **Environment variable file** after the variables are replaced.

   An item for which 🟡 is displayed has a setting error. Review the settings.

   For details about the Preview Command Execution Content window, see *2.39 Preview Command Execution Content window* in the manual *Job Management Partner 1/Integrated Management - Manager GUI Reference*.

4. Click the **Execute** button.

   If there is no problem in the information in the Preview Command Execution Content window, the command is executed, and the Preview Command Execution Content window closes. After the command is executed, **Time**, **Host**, and **Message** appear in **Log** in Execute Command window.

7.1.3 User that executes commands

Commands are executed by mapping the JP1 user who logged on to JP1/IM - Manager (JP1/IM - Central Console) 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 *Job Management Partner 1/Base User's Guide*.

7.1.4 Checking command execution status and deleting a command

After a command is executed from the Execute Command window of JP1/IM - View, if the message reporting execution termination (KAVB2013-I) is not displayed in **Log**, a problem may have occurred at the command execution host.

In this case, follow the procedure described below to check the command execution status, and if necessary, delete the command.

> ▌ **Important note**
>
> 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 *Job Management Partner 1/Base User's Guide*.

7.2 Executing automated actions and taking necessary steps

You can automatically execute an action (command) when a certain JP1 event is received. This function is called the *automated action function*. You can execute an action not only on the host on which the definition of automated actions is stored, but also on an agent host or manager host.

For details about how to define automated actions, see the following sections:

- For setting up automated actions (using the GUI)

  See *2.30 Action Parameter Definitions window* in the manual *Job Management Partner 1/Integrated Management - Manager GUI Reference*.

- For setting up automated actions (using a definition file)

  See *Automated action definition file (actdef.conf)* (*2. Definition Files*) in the manual *Job Management Partner 1/ Integrated Management - Manager Command and Definition File Reference*.

The following three types of status checks can be executed on automated actions:

- Checking the execution status of an automated action

  Checks whether a problem has occurred during execution of the automated action.

- Checking the execution result of the automated action and the operation needed (cancellation or re-execution of the automated action)

  Checks the execution result of the automated action that was executed. Additionally, checks detailed information or initiates manual re-execution of the automated action as needed.

- Checking the operating status of the automated action function

  Checks whether the automated action function is working. If not, automated actions cannot be executed.

The following subsections explain how to perform these checks and automated actions.

7.2.1 Checking the execution status of an automated action

When you enable the automated action execution monitoring (delay monitoring and status monitoring) function, you can quickly detect the occurrence of even the following problems.

- The automated action did not terminate within the expected time. Alternatively, it took a long time to terminate.

- Execution of the automated action failed (the status transitioned to `Fail`, `Error`, or `Error (Miss)`).

You must specify in advance, when you are defining the automated action, whether to enable the execution monitoring (delay monitoring and status monitoring) function. You must also set up a JP1 event to be generated or a notification command to be executed when a problem is detected.

For details about settings, see the following sections:

For setting up automated actions (using the GUI)

  See *2.30 Action Parameter Definitions window* in the manual *Job Management Partner 1/Integrated Management - Manager GUI Reference*.

  See *2.31.1 Action Parameter Detailed Definitions window* in the manual *Job Management Partner 1/Integrated Management - Manager GUI Reference*.

For setting up automated actions (using a definition file)

> See *Automated action definition file (actdef.conf)* (*2. Definition Files*) in the manual *Job Management Partner 1/ Integrated Management - Manager Command and Definition File Reference*.

For setting up JP1 event generation and notification commands

> See *Automatic action notification definition file (actnotice.conf)* (*2. Definition Files*) in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.

The checking procedure is described below. To enable the execution monitoring (delay monitoring and status monitoring) function again after an error has been detected, you need `JP1_Console_Admin` permission or `JP1_Console_Operator` permission. In addition, when the reference and operation permissions are set for a business group, operations in the Event-Information Mapping Definitions window might not be possible depending on the combination of JP1 resource group and JP1 permission level. For details, see *3.1.4(2) Assigning a JP1 resource group and permission level to a JP1 user* in the *Job Management Partner 1/Integrated Management - Manager Overview and System Design Guide*.

To check the execution status of an automated action:

1. In the Event Console window, check the execution status of the automated action. Alternatively, check whether a notification command has reported that an error occurred.

   If generation of a JP1 event was set, a JP1 event with event ID `2010` or `2011` is displayed in the events list. If execution of a notification command was set, the notification command reports the error.

   When you find out that an error has occurred based on the JP1 event or via notification by a notification command, proceed to the next step.

2. Using the Action Log window and the List of Action Results window, check the execution status of the automated action and then take the necessary steps.

   As needed, use the Action Log window and the List of Action Results window to check details or to cancel/re-execute the action. For details, see *7.2.2 Checking the execution results of automated actions*.

   Note that once notification by the delay monitoring function or status monitoring function is executed, further notification is suppressed until the user releases the notification suppression. Therefore, release the notification suppression as needed. To release a suppressed function, proceed to the next step.

3. From the menu in the Event Console window, choose **Options** and then **Function-Status Notification Return**, and then from **Action Delay Monitoring**, choose **Action Status Monitoring** and select the function name that is enabled.

   A suppressed function is displayed in gray letters (to indicate that it is disabled). When you select an enabled function name, a dialog box opens, asking you whether to release the notification suppression.

4. In the dialog box, click **Yes**.

   Clicking **Yes** releases the notification suppression, enabling the monitoring function again.

7.2.2 Checking the execution results of automated actions

You can check the execution results of automated actions in the Action Log window or List of Action Results window of JP1/IM - View. You can also check the execution results by using the `jcashowa` command.

In the Action Log window and List of Action Results window, you can also perform operations such as displaying action details and re-executing actions, in addition to checking execution results. The figure below shows the window transitions and operations related to automated actions.

Figure 7–1: Window transitions and operations related to automated actions
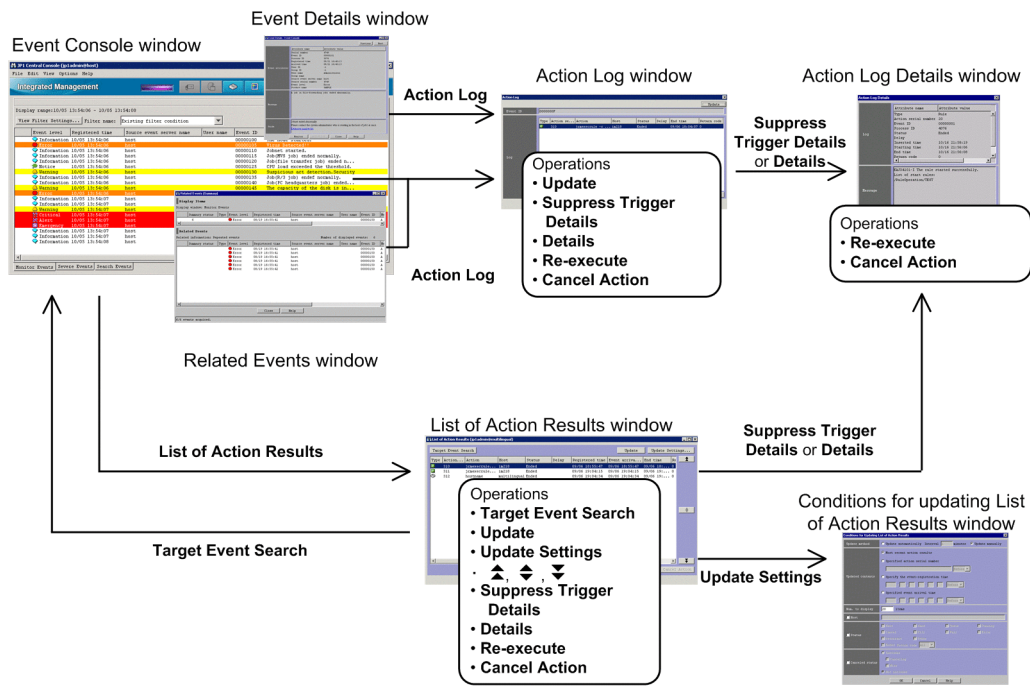
Operations are divided into those that display detailed information about action execution results and those for repeating an operation (re-execution or cancellation) on action execution results.

The procedures for checking the execution results and for repeating an operation (re-execution or cancellation) follow.

(1) Checking the execution results of automated actions

You can check the execution results of automated actions in the Action Log window or List of Action Results window, or by using the `jcashowa` command.

(a) Checking the execution results in the Action Log window

In the Action Log window, you can display the execution results of automated actions that were set for the events selected from the events list in the Event Console window.

To check the execution results in the Action Log window:

1. From the events list in the Event Console window, select an event for which the action icon is displayed in the **Action** column.

2. Using one of the following methods, open the Action Log window:
   - From the menu bar, choose **View** and then **Action Log**.
   - From the popup menu, choose **Action Log**.
   - Click the **Action Log** button.

   The Action Log window opens.

   The Action Log window displays the selected event IDs and the execution results of the automated actions that are specified for those event IDs.

3. To view the details of the execution result of each automated action, or to view the details about the automated action that became a trigger for suppressing an action, open the Action Log Details window.

To view the execution results of an automated action:

- From **Log**, select an automated action and click the **Details** button.

- Double-click an automated action displayed in **Log**.

To view the automated action that became a suppression trigger:

- From **Log**, select an automated action that is suppressed, and click the **Suppress Trigger Details** button.

The Action Log Details window opens.

This window displays the execution results and the message that was issued. For details about the execution results that are displayed, see *2.35 Action Log Details window* in the manual *Job Management Partner 1/Integrated Management - Manager GUI Reference*.

If the Related Events window is open, you can open the Action Log window by selecting an event that has the action icon attached and then choosing **Action Log** from the popup menu. If the Event Details window is open, you can open the Action Log window by clicking the **Action Log** button.

(b) Checking the execution results in the List of Action Results window

In the List of Action Results window, you can display the execution results of automated actions that were set by the logged-in manager. Set the condition for the automated actions to be displayed in the Conditions for Updating List of Action Results window.

To check the execution results in the List of Action Results window:

1. From the Event Console window, choose **View** and then **List of Action Results**.

   The List of Action Results window opens.

   From among the automated actions that were set by the logged-in manager, the List of Action Results window displays a list of those execution results for automated actions that satisfy the condition specified in the Conditions for Updating List of Action Results window.

2. To change the condition for displaying the execution results of automated actions, click the **Update Settings** button.

   The Conditions for Updating List of Action Results window opens.

   In this window, you can specify an updating method (automatic update or manual update) and an action result acquisition range, as well as a display item count and display condition to be used during updating. For details, see *2.37 Conditions for Updating List of Action Results window* in the manual *Job Management Partner 1/Integrated Management - Manager GUI Reference*.

3. To update the display content of the execution results of automated actions according to an updated condition, click the **Update** button.

   The display content is updated according to the content that is specified in the Conditions for Updating List of Action Results window.

4. To display the execution results of automated actions that occurred before the automated actions currently listed, click the [▲] icon. To display the execution results of automated actions that occurred after the automated actions currently listed, click the [▼] icon. To re-display execution results according to the updating condition that is specified in the Conditions for Updating List of Action Results window, click the [↕] icon.

5. To view the details of the execution result of each automated action, or to view the details about the automated action that became a trigger for suppressing an action, use one of the following methods to open the Action Log Details window:

   To view the details of the execution result of each automated action:

   - From Log, select an automated action and then click the **Details** button.

- Double-click an automated action displayed in **Log**.

To view the automated action that became a suppression trigger:

- From **Log**, select an automated action that is suppressed, and then click the **Suppress Trigger Details** button.

The Action Log Details window opens.

This window displays the execution result and the message that has been issued. For details about the execution results to be displayed, see *2.35 Action Log Details window* in the manual *Job Management Partner 1/Integrated Management - Manager GUI Reference*.

6. To display the JP1 event that triggered execution of the automated action, from **Log**, select an automated action, and then click the **Target Event Search** button.

An event search is executed and the **Search Events** page of the Event Console window displays the JP1 event that triggered execution of the automated action.

(c) Using the jcashowa command to check execution results

You can use the `jcashowa` command to display the execution results of automated actions. 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* (*1. Commands*) in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.

(2) Canceling automated actions

When an automated action is in one of the following statuses, you can cancel that automated action:

- `Wait`, `Queue`, or `Running`
- `Send (Miss)`, `Wait (Miss)`, `Queue (Miss)`, or `Running (Miss)`

You can cancel an automated action in the Action Log window, List of Action Results window, Action Log Details window, or by using the `jcacancel` command. To use one of these windows to cancel an automated action, you need `JP1_Console_Admin` permission or `JP1_Console_Operator` permission. In addition, when the reference and operation permissions are set for a business group, operations in the Event-Information Mapping Definitions window might not be possible depending on the combination of JP1 resource group and JP1 permission level. For details, see *3.1.4(2) Assigning a JP1 resource group and permission level to a JP1 user* in the *Job Management Partner 1/Integrated Management - Manager Overview and System Design Guide*.

(a) Canceling an automated action from the Action Log window or List of Action Results window

To cancel an automated action from the Action Log window or List of Action Results window:

1. Open the Action Log window or List of Action Results window.
   For details about how to open windows, see *7.2.2(1) Checking the execution results of automated actions*.

2. Select the automated action you want to cancel.

3. Click the **Cancel Action** button.

   The cancellation confirmation dialog box opens.

4. Click **OK**.

   The request to cancel the selected automated action is accepted.

5. To check the status following the cancellation, click the **Update** button.

(b) Canceling an automated action from the Action Log Details window

To cancel an automated action from the Action Log Details window:

1. Open the Action Log Details window.

   For details about how to open windows, see *7.2.2(1) Checking the execution results of automated actions*.

2. Click the **Cancel Action** button.

   The cancellation confirmation dialog box opens.

3. Click **OK**.

   The request to cancel the selected automated action is accepted.

4. To check the status following the cancellation, click the **Close** button and return to the Action Log window or List of Action Results window, and then click the **Update** button.

(c) Using the jcacancel command to cancel automated actions

You can use the `jcacancel` command to cancel automated actions. Use this command when you want to cancel automated actions in batches by host or system. Before executing the `jcacancel` command to cancel automated actions, confirm which automated actions will be canceled. For details about the confirmation method, see *7.2.2(1) Checking the execution results of automated actions*.

A command execution example follows. To cancel all automated actions that are queued or running on `host01` in a single batch, enter the following from the manager:

```
jcacancel -s host01
```

For details about the `jcacancel` command syntax and the execution result display method, see *jcacancel* (*1. Commands*) in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.

(3) Re-executing an automated action

When an automated action is in one of the following statuses listed, you can re-execute that automated action:

- `Deterrent`, `Ended`, `Error`, `Cancel`, or `Kill`
- `Ended (Miss)` or `Error (Miss)`

You can re-execute an automated action from the Action Log window, List of Action Results window, or Action Log Details window. To use one of these windows to re-execute an automated action, you need `JP1_Console_Admin` permission or `JP1_Console_Operator` permission.

In addition, when the reference and operation permissions are set for a business group, operations in the Event-Information Mapping Definitions window might not be possible depending on the combination of JP1 resource group

and JP1 permission level. For details, see *3.1.4(2) Assigning a JP1 resource group and permission level to a JP1 user* in the *Job Management Partner 1/Integrated Management - Manager Overview and System Design Guide*.

(a) Re-executing an automated action from the Action Log window or List of Action Results window

To re-execute an automated action from the Action Log window or List of Action Results window:

1. Open the Action Log window or List of Action Results window.
   For details about how to open windows, see *7.2.2(1) Checking the execution results of automated actions*.

2. Select the automated action you want to re-execute.

3. Click the **Re-execute** button.
   The re-execution request confirmation dialog box opens.

4. Click **OK**.
   The request to re-execute the selected automated action has been accepted.

5. To check the status following the re-execution, click the **Update** button to update the List of Action Results window.

(b) Re-executing an automated action from the Action Log Details window

To re-execute an automated action from the Action Log Details window:

1. Open the Action Log Details window.
   For details about how to open windows, see *7.2.2(1) Checking the execution results of automated actions*.

2. Click the **Re-execute** button.
   The re-execution request confirmation dialog box opens.

3. Click **OK**.
   The request to re-execute the selected automated action has been accepted.

4. To check the status following the re-execution, click the **Close** button to return to the Action Log window or the List of Action Results window, and then click the **Update** button.

7.2.3 Checking the operating status of the automated action function

If the automated action function is not running, no automated action is executed even if an event that triggers automated action is registered in the JP1/Base of the manager. You can use the `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 `jcachange` 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* (*1. Commands*) in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.

For the `jcachange` command and the display format

See *jcachange* (*1. Commands*) in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.

For details about how to start and stop JP1/IM - Manager:

See *3. Starting and Stopping JP1/IM - Manager*.

7.3 Opening other application windows from the Tool Launcher

The Tool Launcher window displays a list of programs linked to JP1/IM, and you can start a program from this window. You can start the following two types of programs:

Application programs in the viewer

> These are application programs that are installed on the same host as JP1/IM - View. When you select a program from the Tool Launcher, an executable file is started.

Web page

> When an application on the system provides a Web page, you can display that Web page. When you select a program from the Tool Launcher, a Web browser starts and displays the Web page.

To use these functions, you must set the URL of the Web page in advance. For details about the setting, see *Web page call definition file (hitachi_jp1_product-name.html)* (*2. Definition Files*) in the manual *Job Management Partner 1/ Integrated Management - Manager Command and Definition File Reference*.

Furthermore, before using the Tool Launcher to link to another product, check the operating environment (supported OS and browsers, for example) of that product.

An example of the Tool Launcher window follows.

Figure 7–2: Tool Launcher window example
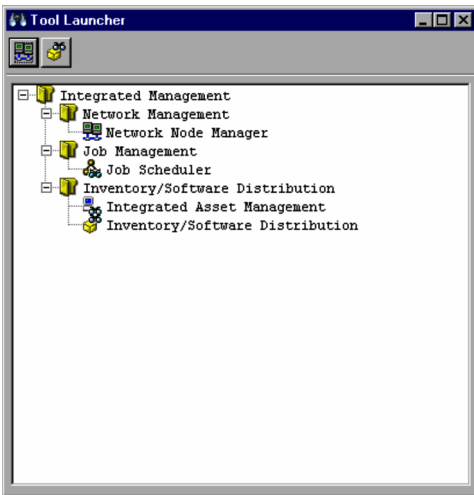
The above figure shows the Tool Launcher window when no application program linked to JP1/IM has been installed in the viewer. When an application program is installed in the viewer, that installed application program is added to the tree in the display.

For details about the programs to be linked, see *7.3.2 Functions that can be operated from the Tool Launcher window*.

7.3.1 Operations in the Tool Launcher window

The Tool Launcher window displays the functions of the programs linked to JP1/IM in a tree format. A folder expresses a function category. By double-clicking the end of the tree, you can open a Web page or application program window.

To display a Web page or open an application program window:

1. In the Event Console window, from the **Monitoring Tree** page, choose **Options** and then **Start Integrated Function Menu**. Alternatively, from the toolbar, click the icon.

   The Tool Launcher window opens.

   If `MENU_AUTO_START=ON` is specified in the `tuning.conf` file of JP1/IM - View, the Tool Launcher window automatically opens when you log in. For details on the `tuning.conf` file of JP1/IM - View, see *IM-View settings file (tuning.conf)* in *2. Definition Files* in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.

2. Expand the tree in the Tool Launcher and double-click the item you want to display.

   The window for the selected function opens.

   Note:

   When an application program is invoked from the Tool Launcher, the application program cannot start if the OS user that started JP1/IM - View does not have the necessary permissions to execute the application program being invoked.

   You must also start JP1/IM - View using the permissions that can execute the application program being invoked.

The functions listed in the table below can also be invoked from toolbar icons.

Table 7–1: Functions that can be invoked from toolbar icons

Function name	Icon
Network node manager	
Windows Remote Controller	
Inventory/Software Distribution	#

#: Windows 8.1, Windows 8, Windows Server 2012, Windows 7, Windows Server 2008, and Windows Vista version of JP1/IM - View cannot link to the Web page of JP1/Software Distribution Manager, and therefore the **Inventory/Software Distribution** icon is not displayed.

7.3.2 Functions that can be operated from the Tool Launcher window

The table below shows the functions that are displayed in the Tool Launcher window.

If the window type is an application window and the applicable program is not installed in the viewer, the function name is not displayed in the viewer.

For details about the supported version of linkage products, see the documentation of the applicable linkage product.

Table 7–2: Functions displayed in the Tool Launcher window

Menu item			Description of the function that starts			
Folder name	Subfolder name	Function name	Window type	Program name	Version for linking with JP1/IM - Manager	Supported OS
`Network Management`	--	`Network Node Manager`	Web page	JP1/Cm2/NNM	Version 8 or earlier	No restrictions

Menu item			Description of the function that starts			
Folder name	Subfolder name	Function name	Window type	Program name	Version for linking with JP1/IM - Manager	Supported OS
				HP NNM	Version 7.5 or earlier	
	--	`Internet Gateway`	Application window	JP1/Cm2/Internet Gateway Server	No restrictions	No restrictions
`Job Management`	--	`Job Scheduler`	Application window	JP1/AJS - View	No restrictions	No restrictions
	--	`Scenario Operation`	Application window	JP1/AJS2 - Scenario Operation View	No restrictions	No restrictions
	--	`Print Service`	Application window	JP1/NPS	No restrictions	No restrictions
	`File Transmission`	`Transmission Regist. & Exe.`	Application window	JP1/FTP	No restrictions	Windows Server 2008, Windows Server 2008 R2, Windows Server 2003, Windows Server 2003 R2
		`Log Information`	Application window			
		`Auto-Start Program Registration`	Application window			
`Inventory/ Software Distribution`	--	`Integrated Asset Management`	Web page	JP1/Asset Information Manager	No restrictions	Windows other than Windows Vista and Windows 7
	--	`Inventory/ Software Distribution #`	Web page	JP1/Software Distribution Manager	Version 7 or earlier	OSs other than Windows Vista
	--	`Facilities Asset Management`	Application window	JP1/NetInsight II - Facility Manager	No restrictions	No restrictions
	--	`Windows Remote Controller`	Application window	JP1/NETM/ Remote Control Manager	No restrictions	No restrictions
	--	`Distribution /Asset Management`	Application window	JP1/Software Distribution Manager	No restrictions	No restrictions
`Storage Management`	`Storage Area Management`	`Storage System Operation Management`	Application window	Hitachi Tuning Manager software	Version 3 or later	Windows, Solaris (SPARC), Linux
		`Storage Hardware Management`	Application window	Hitachi Device Manager software	Version 3 or later	
		`Storage Resource Management`	Application window	Hitachi Provisioning Manager	Versions from 03-50 to 06-40	

7. System Operation Using JP1/IM

Menu item			Description of the function that starts			
Folder name	Subfolder name	Function name	Window type	Program name	Version for linking with JP1/IM - Manager	Supported OS
		`Storage Replication Management`	Application window	Hitachi Replication Manager software	Version 03-50 or later (For versions earlier than version 5, Replication Monitor)	
		`Tiered Storage Resource Management`	Application window	Hitachi Tiered Storage Manager software	Version 4 or later	
		`Global I/O Path Operation Management`	Application window	Hitachi Global Link Manager software	Versions from 05-00 to 06-60	Windows 7 (SP none) Windows Server 2008, Windows Server 2008 (x64) (SP none or SP2) Windows Server 2008 R2 (x64) (SP none or SP1) Windows Vista (SP none, SP1, or SP2) Windows Server 2003 R2 (SP2) Windows XP Professional (SP2 or SP3)
`Server Management`	--	`Management Console`	Application window	JP1/Server Conductor	No restrictions	No restrictions
	--	`Web Console`	Web page			
`Hardware Management`	-	`SANRISE2000 Remote Console`	Application window	SANRISE	No restrictions	No restrictions
	-	`SANRISE H512/H48 Remote Control XP`	Application window			
`Automated Notification`	--	`Notification Rule Setting`	Application window	TELstaff	Version 9	• Microsoft(R) Windows Server(R) 2003, Standard Edition • Microsoft(R) Windows Server(R) 2003, Enterprise Edition • Microsoft(R) Windows Server(R) 2003 R2, Standard Edition • Microsoft(R) Windows Server(R) 2003 R2, Enterprise Edition • Microsoft(R) Windows Server(R)

Menu item			Description of the function that starts			
Folder name	Subfolder name	Function name	Window type	Program name	Version for linking with JP1/IM - Manager	Supported OS
						2003, Standard x64 Edition • Microsoft(R) Windows Server(R) 2003, Enterprise x64 Edition • Microsoft(R) Windows Server(R) 2003 R2, Standard x64 Edition • Microsoft(R) Windows Server(R) 2003 R2, Enterprise x64 Edition • Microsoft(R) Windows Server(R) 2008 Standard 32-bit • Microsoft(R) Windows Server(R) 2008 Enterprise 32-bit • Microsoft(R) Windows Server(R) 2008 Standard • Microsoft(R) Windows Server(R) 2008 Enterprise • Microsoft(R) Windows Server(R) 2008 R2 Standard • Microsoft(R) Windows Server(R) 2008 R2 Enterprise *Note:* • The terminal service in Windows Server 2003, Windows Server 2003 R2, Windows Server 2003 (x64), Windows Server 2003 R2 (x64), Windows Server 2008 32-bit, Windows Server 2008, and Windows Server 2008 R2 is not supported. • The cluster functionality in Windows Server 2003, Windows Server 2003 R2, Windows Server 2003 (x64), Windows Server 2003 R2 (x64), Windows Server 2008

7. System Operation Using JP1/IM

Menu item			Description of the function that starts			
Folder name	Subfolder name	Function name	Window type	Program name	Version for linking with JP1/IM - Manager	Supported OS
						32-bit, Windows Server 2008, and Windows Server 2008 R2 is not supported. • The Server Core installation environment in Windows Server 2008 32-bit, Windows Server 2008, and Windows Server 2008 R2 is not supported.
`Mainframe Linkage`	--	`VOS3 Console Operation`	Applicatio n window	VOS3 AOMPLUS(AO MPLUSCIF)	No restrictions	No restrictions
`Cosminexus Operation Management`	--	`Cosminexus Operation Management Portal`	Applicatio n window	Cosminexus Application Server	No restrictions	No restrictions

Legend:

--: None

#: The Windows Vista version of JP1/IM - View cannot link to the Web page of JP1/Software Distribution Manager, and therefore the **Inventory/ Software Distribution** icon is not displayed.

8

Managing the System Hierarchy using IM Configuration Management

This chapter explains how to use IM Configuration Management to manage the system hierarchy (IM configuration). For details about the windows described in this chapter, see *4. IM Configuration Management Window* in the manual *Job Management Partner 1/Integrated Management - Manager GUI Reference*.

8.1 Managing hosts

If you change the JP1/IM system configuration or the host information, such as the name or IP address of a managed host, you must review the information related to the hosts managed in the IM Configuration Management database.

Perform the following tasks from the IM Configuration Management - View to manage host information.

Registering hosts

To register a new host in the IM Configuration Management database, use the Register Host window, which you can open from the IM Configuration Management window.

For details about the method, see *3.1.1 Registering hosts* in the *Job Management Partner 1/Integrated Management - Manager Configuration Guide*.

Deleting a host

You can delete a host registered in the IM Configuration Management database on the **Host List** page of the IM Configuration Management window.

For details about the method, see *3.1.3 Deleting hosts* in the *Job Management Partner 1/Integrated Management - Manager Configuration Guide*.

Collecting information from hosts

You can collect host information from the **Host List** page or **IM Configuration** page of the IM Configuration Management window.

For details about when host information is collected or the collection method, see *3.1.5 Collecting information from hosts* in the *Job Management Partner 1/Integrated Management - Manager Configuration Guide*.

Changing the host information

To change the host information registered in the IM Configuration Management database, use the Edit Host Properties window, which you can open from the IM Configuration Management window.

For details about the method, see *3.1.4 Changing host information* in the *Job Management Partner 1/Integrated Management - Manager Configuration Guide*.

If you edit the host name registered in the system hierarchy (IM configuration), you must re-apply the system hierarchy. For details about the procedure for applying the system hierarchy, see *3.2.4(3) Applying a system hierarchy to a system managed by IM Configuration Management* in the *Job Management Partner 1/Integrated Management - Manager Configuration Guide*.

Displaying a host list

To display a list of the hosts registered in the IM Configuration Management database, use the **Host List** page of the IM Configuration Management window.

For details about the method, see *3.1.2 Displaying host information* in the *Job Management Partner 1/Integrated Management - Manager Configuration Guide*.

8.2 Managing the system hierarchy

If you change the system hierarchy (IM configuration), you must review the system configuration definition information registered in the IM Configuration Management database.

Perform the following tasks from the IM Configuration Management - View to manage the system hierarchy.

Collecting system hierarchy information

To collect the system configuration definition information, use the **Host List** page or **IM Configuration** page of the IM Configuration Management window. You can collect system configuration definition information from all hosts that constitute a system.

For details about the method, see *3.2.1 Collecting the system hierarchy* in the *Job Management Partner 1/Integrated Management - Manager Configuration Guide*.

Displaying the system hierarchy

To display the system hierarchy, use the **IM Configuration** page of the IM Configuration Management window.

For details about the method, see *3.2.2 Displaying the system hierarchy* in the *Job Management Partner 1/Integrated Management - Manager Configuration Guide*.

Verifying the system hierarchy

You can verify whether the collected configuration definition information matches the configuration definition information maintained by IM Configuration Management. To verify the configuration definition information, use the **Host List** page or **IM Configuration** page of the IM Configuration Management window.

For details about the method, see *3.2.3 Verifying the system hierarchy* in the *Job Management Partner 1/Integrated Management - Manager Configuration Guide*.

Editing the system hierarchy

You can edit the configuration definition information to add, move, and delete hosts. To edit the configuration definition information, use the Edit Agent Configuration window or the Edit Remote Monitoring Configuration window, which you can open from the IM Configuration Management window.

For details about the method, see *3.2.4 Editing the system hierarchy* in the *Job Management Partner 1/Integrated Management - Manager Configuration Guide*.

Applying the system hierarchy

You can apply the configuration definition information edited in the Edit Agent Configuration window or the Edit Remote Monitoring Configuration window to all the hosts constituting a system. To apply the configuration definition information, use the Edit Agent Configuration window or the Edit Remote Monitoring Configuration window.

For details about the method, see *3.2.4(3) Applying a system hierarchy to a system managed by IM Configuration Management* in the *Job Management Partner 1/Integrated Management - Manager Configuration Guide*.

Synchronizing system hierarchies

When the system hierarchy is defined separately by the integrated manager and the site managers, you must synchronize the system hierarchies used by the integrated manager and the site managers. To synchronize the system hierarchies, use the **IM Configuration** page of the IM Configuration Management window.

For details about the method, see *3.2.5 Synchronizing the system hierarchy* in the *Job Management Partner 1/ Integrated Management - Manager Configuration Guide*.

8.3 Managing the configuration of a virtual system

This section explains how to manage a system hierarchy that contains a virtual host (virtual system configuration) by operating IM Configuration Management - View or by executing a command.

The management of a virtual configuration requires virtualization software and virtual environment management software. For details about the software you can use, see *6.3 Virtualization configuration management* in the *Job Management Partner 1/Integrated Management - Manager Overview and System Design Guide*.

8.3.1 Registering a virtual system host

You can register a new virtual host in the system hierarchy by opening 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 *Job Management Partner 1/Integrated Management - Manager Configuration Guide*.

8.3.2 Displaying host information in a virtual system

This subsection explains how to display information about a host that is registered as a virtual host in the system hierarchy. To display host information, invoke the **Host List** page of the IM Configuration Management window.

1. In the IM Configuration Management window, click the **Host List** tab.
   The **Host List** page opens.

2. From the tree pane, select a virtual host.

3. Use either of the following methods to collect host information:
   - From the menu bar, choose **Operation** and then **Collect Host Information**.
   - From the popup menu that opens when you right-click the mouse, choose **Collect Host Information**.

   If you want to collect host information, JP1/Base must be running on the virtual host.
   Note that, because JP1/Base cannot be installed on VMware ESX and Virtage, executing **Collect Host Information** causes an error.

4. Click the **Basic Information** button, **Product Information** button, or **Service Information** button.
   Depending on the button you clicked, the node information display area displays different host information. You cannot click the **Lower Host Information** button.

8.3.3 Applying the management information to the Central Scope monitoring tree

To use Central Scope to monitor a virtual host registered in the system hierarchy, you need to export the management information of IM Configuration Management and import it into the monitoring tree information of Central Scope. The procedure follows.

1. Execute the `jcfexport` command.

Export the configuration information of IM Configuration Management.

2. Execute the `jcsdbexport` command.

   Export the monitoring tree information of Central Scope.

3. Using the output files of both the `jcfexport` and `jcsdbexport` commands as arguments, execute the `jcfmkcsdata` command.

   Merge the configuration information of IM Configuration Management with the monitoring tree information.

4. Execute the `jcsdbimport` command.

   Import the merged management information of IM Configuration Management and the monitoring tree information.

Using Central Scope - View, make sure that the merged virtual host is displayed.

8.4 Managing business groups

When monitoring targets are set as business groups, you must create, edit, and delete the business groups at the same time you review the configuration of business groups.

Creating a new business group

> For details about the procedure for creating a new business group, see *3.4.1(1)(a) Creating a business group* in the *Job Management Partner 1/Integrated Management - Manager Configuration Guide*.

Editing the registration information of a business group

> For details about the procedure for editing the registration information of a business group, see *3.4.1(1)(b) Editing the properties of a business group* in the *Job Management Partner 1/Integrated Management - Manager Configuration Guide*.

Deleting unnecessary business groups

> For details about the procedure for deleting unnecessary business groups, see *3.4.1(1)(c) Deleting a business group* in the *Job Management Partner 1/Integrated Management - Manager Configuration Guide*.

After creating, editing, or deleting business groups, you need to apply the hierarchy of the business groups and the monitoring groups to the monitoring tree. For details about the procedure for applying the management hierarchy, see *3.4.4(2) Applying business group information and monitoring group information to the Central Scope monitoring tree* in the *Job Management Partner 1/Integrated Management - Manager Configuration Guide*.

8.5 Managing profiles

If you change the content of a profile during system update or maintenance or apply the content of a profile to the profile of another host, you must review the profile registered in the IM Configuration Management database.

Perform the following tasks from the IM Configuration Management - View to manage profiles.

There are two types of profiles: one for valid configuration information and the other for the content of the configuration file.

Obtaining profiles

    You can obtain the following profiles:

- Valid JP1/Base configuration information on an agent host
- The JP1/Base configuration file on an agent host (log-file trap startup definition file)
- Valid configuration information for a monitored remote host

    For details about the method, see *3.5.1(2) Collecting profiles* in the *Job Management Partner 1/Integrated Management - Manager Configuration Guide*.

Obtaining a list of profiles

    You can obtain a list of profiles managed by JP1/Base on an agent host. This information is displayed in the tree pane of the Display/Edit Profiles window.

    For details about the method, see *3.5.1(1) Collecting profile lists* in the *Job Management Partner 1/Integrated Management - Manager Configuration Guide*.

Displaying profiles

    You can display the profiles for JP/Base on an agent host and a monitored remote host in the Display/Edit Profiles window.

    For details about the method, see *3.5.1(3) Displaying profiles* in the *Job Management Partner 1/Integrated Management - Manager Configuration Guide*.

Editing settings files

    You can edit settings files in the Display/Edit Profiles window. The following types of profiles can be edited by using a settings file:

- **Event Forwarding**
- **Log File Trapping**
- **Event Log Trapping**
- **Local Action**
- **Log File Trapping** under **Remote Monitoring**
- **Event Log Trapping** under **Remote Monitoring**

    For details about the method, see *3.5.1(5) Editing configuration files* in the *Job Management Partner 1/Integrated Management - Manager Configuration Guide*.

Applying edited settings file information

    You can apply edited settings file information.

    For details about the method, see *3.5.1(6) Applying edited information in configuration files* in the *Job Management Partner 1/Integrated Management - Manager Configuration Guide*.

8.6 Managing service operation status

This chapter explains how to use IM Configuration Management - View to manage the status of service operations on each host.

8.6.1 Collecting service operation information

In an agent configuration, you can collect information about the operation of services that are running on each host from the system hierarchy.

Note that in a remote monitoring configuration, you cannot collect service operation information.

To collect service operation information, use the **Host List** page or **IM Configuration** page of the IM Configuration Management window. The procedure differs according to the page you select.

(1) Collecting service operation information from the Host List page

To collect service operation information from the **Host List** page of the IM Configuration Management window:

1. In the IM Configuration Management window, click the **Host List** tab.
   The **Host List** page opens.

2. From the tree pane, select a host.
   You cannot collect service operation information by selecting **Host List**. Furthermore, the range of hosts from which operation information can be collected varies depending on the manager on which IM Configuration Management is running. For details about the range of hosts that can be selected, see *6.7.2 Collecting service activity information* in the *Job Management Partner 1/Integrated Management - Manager Overview and System Design Guide*.

3. Click the **Service Information** button.
   The collected service operation information is displayed in the node information display area.

4. From the menu bar, choose **Display** and then **Refresh**.
   The latest service option information is collected from the host, and the display in the node information display area is refreshed.

(2) Collecting service operation information from the IM Configuration page

To collect service operation information from the **IM Configuration** page of the IM Configuration Management window:

1. In the IM Configuration Management window, click the **IM Configuration** tab.
   The **IM Configuration** page opens.

2. From the tree pane, select a host.
   The range of hosts from which operation information can be collected varies depending on the manager on which IM Configuration Management is running. For details about the range of hosts that can be selected, see *6.7.2 Collecting service activity information* in the *Job Management Partner 1/Integrated Management - Manager Overview and System Design Guide*.

3. Use either of the following methods to collect host information.

- From the menu bar, choose **Operation** and then **Collect Host Information**.
- From the popup menu that opens when you right-click the mouse, click **Collect Host Information**.

4. Click the **Service Information** button.
   The collected service operation information is displayed in the node information display area.

5. From the menu bar, choose **Display** and then **Refresh**.
   The latest service option information is collected from the host, and the display in the node information display area is refreshed.

8.6.2 Service operation information display

For details about how to display the operation information of services that are running on each host from the system hierarchy (IM configuration), see *8.6.1 Collecting service operation information*.

The information on services in the IM Configuration Management window displays the following types of operation information:

Table 8–1: Operation information that is displayed for each service

Product name	Service name	Operating status
JP1/Base	JP1/Base	The operating status of the service is displayed as one of the following:
	Event Service	• `Running`
	Log file trap	• `Stopped`
JP1/IM - Manager	JP1/IM - Manager	• `Partially running` • `Collection failed`

Detailed Information in the IM Configuration Management window displays the execution results of the commands that collect information from individual services as follows.

Table 8–2: Commands that collect information about individual services

Service name	Collection command
JP1/Base	`jbs_spmd_status`
Event Service	`jevstat`
Log file trap	`jevlogstat ALL`
JP1/IM - Manager	`jco_spmd_status`
Log file trap (remote)	`jcfallogstat`[#]
Event log trap (remote)	`jcfaleltstat`[#]

#: Information corresponding to the collection command is output.

8.7 Exporting and importing management information of IM Configuration Management

This section explains how to execute commands to export and import the management information of IM Configuration Management.

8.7.1 Exporting management information of IM Configuration Management

By outputting (exporting) the management information of IM Configuration Management and then inputting (importing) it, you can copy management information from one host to another. Furthermore, 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 on the `jcfexport` command, see *jcfexport* in *1. Commands* in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.

(1) Host information

Information related to the host managed by IM Configuration Management is exported to the host input information file and the collected host information file.

For details about the host input information file, see *Host input information file (host_input_data.csv)* in *2. Definition Files* in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.

For details about the collected host information file, see *Collected host information file (host_collect_data.csv)* in *2. Definition Files* in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.

(2) System hierarchy information

The system hierarchy information is exported to a file. You can edit the exported file and import it.

The information that is output differs according to the system monitoring method:

- Agent monitoring
- Remote monitoring

(a) Configuration information for agent monitoring

The name of the file that is exported is `system_tree_information.txt`.

When remote monitoring is used, the configuration information for agent monitoring cannot be edited.

The following table describes the configuration information for agent monitoring that is output to the file.

Table 8–3: JP1/IM's system hierarchy information that is exported

Output item	Description of output value
[*managing-host*]	• 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.

Output item	Description of output value
	• 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 (*).
managed-host	• 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, and cannot be edited.

(3) Profile information

The profile information that is running on the host is exported. The files that are exported differ according to the system monitoring method:

- Agent monitoring
- Remote monitoring

(a) Profile information for agent monitoring

The profile information of the JP1/Base that is running on the host is exported. The file is exported to the first-level directory (*host-name*) and the second-level directory (JP1Base) under the definition_files directory. The log file trap action definition file is exported to the third-level directory (cf_log_file_trap). The following table describes the profile information that is exported.

Table 8–4: Name of the files for exporting profile information for agent monitoring

Profile information	Export file name
Event forwarding settings file	forward
Log-file trap action definition file	Any name
Log-file trap startup definition file	jevlog_start.conf
Event log-trap action definition file	ntevent.conf
Local action execution definition file	jbslcact.conf

(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 8–5: 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	jevlog_start.conf

Profile information	Export file name
Remote-monitoring event log trap action-definition file	`ntevent.conf`

(4) Remote authentication information

When remote monitoring is used, remote authentication information is exported. This information cannot be edited.

(5) Business group information

When business groups are used, information about the business groups is exported to a file named `monitoring_system_data.csv`. The following table describes the business group information output to `monitoring_system_data.csv`.

Table 8–6: 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 `LANG` environment variable on the manager. For details, see *Table 2-67 Character encoding of files* in *Host input information file (host_input_data.csv)* in *2. Definition Files* in the manual *Job Management Partner 1/ Integrated Management - Manager Command and Definition File Reference*.
Second line (header information)	Business group name	`Monitoring_system_name`
	Assigned JP1 resource group name	`JP1_resource_group_name`
	Comment	`Comment`
	Host name	`Host_name_list`
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	`Comment`
	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 (`""`))

#: Business group information is sorted in ascending order of business group name before being output.

The following shows an example of outputting business group information:

```
JP1/IM-CF;095000;UTF-8,,,

Monitoring_system_name,JP1_resource_group_name,Comment,Host_name_list

System1,,This is the empty system,

System2,Resource_A,This is System2,"host21,host22,host23,host24"

System3,Resource_A,This is System3,"host31,host32"
```

(6) Monitoring group information

When business groups are used, the monitoring group information of IM Configuration Management is exported to a file named `monitoring_group_data.csv`. The following table describes the monitoring group information that is output to `monitoring_group_data.csv`.

Table 8–7: Exported monitoring group information

Line	Output item	Output value
First line (header information)	Product name	`JP1/IM-CF`
	File format version	File format version For example, if the version of JP1/IM - Manager is 10-50, `101000` is output.
	Character code	Character code This depends on the setting of the `LANG` environment variable of the manager. For details, see *Table 2-67 Character encoding of files* in *Host input information file (host_input_data.csv)* in *2. Definition Files* in the manual *Job Management Partner 1/ Integrated Management - Manager Command and Definition File Reference*.
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 (`""`))

#: Monitoring group information is sorted in ascending order of monitoring group path and before being output.

The following shows an example of outputting monitoring group information:

```
JP1/IM-CF;101000;UTF-8,,

Monitoring_group_path,Comment,Host_name_list

/System1/Group1,This is the empty group,

/System1/Group2,This is Group2,host2

/System2/Group1,This is Group1,"host11,host12,host13,host14"
```

8.7.2 Importing management information of IM Configuration Management

If necessary, you can edit the management information of IM Configuration Management that has been output (exported) from a host, and you can input (import) the edited information onto a different host. You use the `jcfimport` 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 `jcfimport` command. For details on the `jcfimport` command, see *jcfimport* in *1. Commands* in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.

(1) Host information

In the case of manually-entered information, the content of the export file (`host_input_data.csv`) is imported.

The table below shows the items that are imported from the export file (`host_input_data.csv`) for manually-entered information, and the input range for each item.

Table 8–8: 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	`physical`, `logical`, `virtual`, or `unknown` may be input.	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
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`	Optional	Blank

Item	Input range	Required/Optional	Default
	`- Virtage`		
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[#3]	A character string of up to 255 bytes can be input. Permitted characters are alphanumeric characters other than control codes.	Optional	Blank
Domain name[#4]	A character string of up to 255 bytes can be input. Permitted characters are alphanumeric characters other than control codes.	Optional	Blank

Communication type[#5]	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`:
	　`http` or `https` 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[#6]	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[#7]	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. One of `disable`, `ssh`, and `wmi` can be input.	Optional	`disable`
Authentication information category[#8]	This item can be used for remote monitoring. Either `common` or `host` or else a blank can be input.	Optional	Blank

Legend:

　--: There is no default value.

#: A two-byte character is converted to three bytes.

#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: This item must be input when the virtual manager type is `vCenter`, `SCVMM`, or `HCSM`.

#4: This item must be input when the virtual manager type is `SCVMM`.

#5: This item must be input when the virtual manager type is `vCenter`, `HCSM`, or `KVM`.

#6: This item must be input when the virtual manager type is `HCSM` or `KVM`.

#7: This item must be input when the virtual manager type is `KVM`.

#8: 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 `http` or `https` 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	--	None	--	--
	`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`	None	--	--

Host type	Virtual manager type	Configuration information corresponding to virtual manager type	Required/Optional	Remarks
	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.
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.

Host type	Virtual manager type	Configuration information corresponding to virtual manager type	Required/Optional	Remarks
	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	--	None	--	--
Unknown	--	None	--	--

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.

If any of the conditions listed below applies to the content of the export file for the system hierarchy information, 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.

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 system hierarchy information 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 system hierarchy information 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 system hierarchy information, if the export file for the system hierarchy information is not found in the specified directory, an error message is displayed and the import operation is halted.

(b) Configuration information for remote monitoring

When remote monitoring is used, the content of the export file for the configuration information for remote monitoring is imported. The configuration information for remote monitoring cannot be edited.

(3) Profile information

The content of the export files for the profile information is imported. The file that is imported differs according to the system monitoring method:

- Agent monitoring
- Remote monitoring

Table 8–9: Export file for agent monitoring profile information to be imported

Profile information	Export file name
Event Forwarding Settings File	`forward`
Log-file trap action definition file	Any name
Log-file trap startup definition file	`jevlog_start.conf`
Event Log-Trap Action Definition File	`ntevent.conf`
Local Action Execution Definition File	`jbslcact.conf`

When agent monitoring profile information is imported, the destination is determined using the directory name under `definition_files` directory. The directory name on the hierarchy one step below the `definition_files` directory is read as a host name, and the directory name on the hierarchy two steps below the `definition_files` directory is read as a product name. The file stored in each directory is registered on the applicable host as settings information. Consequently, if you change the host name in the export file (`host_input_data.csv`) for host

information (manually-entered information), you must also change the directory name. If you do not change it, the profile information cannot be imported.

The profile information file is loaded as a character code described in `encode` of the export file (`data_information.txt`) for the export data information. For this character code, the environment variable `LANG` of the OS of the server that executed the export operation is set. When you import profile information, make sure that the character code described in the export file (`data_information.txt`) matches the character code of the profile information file.

If characters that do not have code compatibility or model-dependent characters are used in the host information, these characters may become garbled when they are imported.

If more than 10,000 hosts are defined, an error occurs and no file is imported.

If the export file for the profile (configuration file) contains an unsupported product or unsupported profile, these are ignored and processing continues.

(a) Remote monitoring profile information

When remote monitoring is used, the content of the export file for the remote monitoring profile information is imported. The remote monitoring profile information cannot be edited.

The following table describes the export files for remote monitoring profile information to be imported.

Table 8–10: 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 remote authentication information cannot be edited.

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).

The following table describes items that are imported and the input range of each item.

Table 8–11: Imported items (business group information)

Item	Input range	Required/Optional	Default
Business group name	A character string of up to 2,046 bytes can be input. Permitted characters are characters other than control codes. This item is case-sensitive.	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 character string of up to 80 bytes can be input. Permitted characters are characters other than control codes.	Optional	Blank
Host name	You can specify multiple hosts by delimiting them with commas. A character string of up to 255 bytes can be input for each host. Permitted characters are alphanumeric characters, periods (`.`) and hyphens (`-`). Control codes are not permitted.	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.

The following table describes items that are imported and the input range of each item.

Table 8–12: Imported items (monitoring group information)

Item	Input range	Required/Optional	Default
Monitoring group path	A character string of up to 2,046 bytes can be input. Permitted characters are characters other than control codes. This item is case-sensitive.	Required	--
Comment	A character string of up to 80 bytes can be input. Permitted characters are characters other than control codes.	Optional	Blank
Host name	You can specify multiple hosts by delimiting them with commas. A character string of up to 255 bytes can be input for each host. Permitted characters are alphanumeric characters, periods (`.`) and hyphens (`-`). Control codes are not permitted.	Optional	Blank

Legend:

--: There is no default value.

8.7.3 Applying the imported management information of IM Configuration Management to a system

After you have imported the management information of IM Configuration Management by executing the `jcfimport` command, perform the procedures described below to apply the imported management information.

(1) Collecting host information

To collect host information:

1. In the IM Configuration Management window, click the **Host List** or **IM Configuration** tab.
   The **Host List** page or **IM Configuration** page opens.

2. From the tree pane, select a host.
   If the selected host has lower-order hosts, you can also select a host from the **Lower Host Information** list that is displayed when you click the **Lower Host Information** button. In this case, you can select multiple hosts at the same time.

3. Use either of the following methods to collect host information:
   - From the menu bar, choose **Operation** and then **Collect Host Information**.
   - From the popup menu that opens when you right-click the mouse, choose **Collect Host Information**.

   When a message confirming collection of information from the selected host is issued, click **Yes**. Information is collected from the selected host.

(2) Applying the system hierarchy information

To apply the system hierarchy information:

(a) In an agent configuration

When the system hierarchy information is not applied, the tree in the **IM Configuration** tab in the IM Configuration Management window is displayed in gray.

Perform the following procedure to apply the system hierarchy information.

1. From the menu bar in the IM Configuration Management window, choose **Edit** and then **Edit Agent Configuration**.
   The Edit Agent Configuration window opens.

2. In the Edit IM Configuration window, check the **Acquire update right** check box.
   You can now edit the JP1/IM system configuration.

3. Select the highest node in the tree (integrated manager) and use either of the following methods to change the integrated manager:
   - From the menu bar, choose **Operation** and then **Exchange Hosts**.
   - From the popup menu that opens when you right-click the mouse, choose **Exchange Hosts**.

   This step is not necessary if the exporting host is the same as the importing host.

4. From the menu bar in the Edit Agent Configuration window, choose **Operation** and then **Apply Agent Configuration**.
   The system hierarchy information is applied to the actual system.

5. Clear the **Acquire update right** check box.

If you are acquiring the current system hierarchy, this operation is not necessary. From the menu bar in the IM Configuration Management window, choose **Edit** and then **Collect IM Configuration** to acquire the current system hierarchy.

(b) In a remote configuration

Perform the following procedure to apply the system hierarchy information.

1. From the menu bar in the IM Configuration Management window, choose **Edit** and then **Edit Remote Monitoring Configuration**.
   The Edit Remote Monitoring Configuration window opens.

2. In the Edit IM Configuration window, check the **Acquire update right** check box.
   You can now edit the JP1/IM system configuration.

3. Select the highest node in the tree (integrated manager) and use either of the following methods to change the integrated manager:

   - From the menu bar, choose **Operation** and then **Exchange Hosts**.
   - From the popup menu that opens when you right-click the mouse, choose **Exchange Hosts**.

   This step is not necessary if the exporting host is the same as the importing host.

4. From the menu bar in the Edit Remote Monitoring Configuration window, choose **Operation** and then **Apply Remote Monitoring Configuration**.
   The system hierarchy information is applied to the actual system.

5. Clear the **Acquire update right** check box.

If you are acquiring the current system hierarchy, this operation is not necessary. From the menu bar in the IM Configuration Management window, choose **Edit** and then **Collect IM Configuration** to acquire the current system hierarchy.

(3) Applying the profile information

Merely importing the management information of IM Configuration Management does not apply the configuration file to the system. Use either of the following methods to apply the configuration file:

- Batch-apply the configuration file
- Apply the configuration file to hosts individually

For details about how to apply the configuration file, see *3.5.1(6) Applying edited information in configuration file*s in the *Job Management Partner 1/Integrated Management - Manager Configuration Guide*.

If you are acquiring a system's current profile information, there is no need to apply the profile information. You can simply batch-collect profiles. For details about how to collect profile lists, see *3.5.1(1) Collecting profile lists* in the *Job Management Partner 1/Integrated Management - Manager Configuration Guide*.

9

Linking with BJEX or JP1/AS

JP1/IM can monitor the response-request messages issued by BJEX or JP1/AS as JP1 events, allowing operators to respond to these messages from JP1/IM - View. This chapter describes the functionality of JP1/IM that allows this to take place, and explains the process of linking JP1/IM with BJEX or JP1/AS. It also describes the command options you can use when linking with BJEX or JP1/AS.

9.1 Overview of BJEX and JP1/AS linkage

BJEX is a product that realizes mainframe-like job management in an open system. JP1/AS is a system used to create and execute shell scripts that serve as batch jobs. A job management system that links with JP1/AJS to control batch jobs (jobs that execute batch processing) is called a *batch job execution system*. By deploying JP1/IM in a batch job execution system, you can monitor the execution status and results of batch jobs in JP1/IM - View based on the JP1 events issued by BJEX or JP1/AS.

The messages output by BJEX and JP1/AS include response-request messages that require the operator to respond to them while a batch job is executing. BJEX and JP1/AS issue response-request messages as JP1 events. JP1/IM allows you to monitor these JP1 events and respond to the messages as needed. The JP1 events that correspond to response-request messages are called *response-waiting events*. The functionality of JP1/IM that manages and responds to response-waiting events is called the *response-waiting event management function*. JP1/IM uses this function when linking with BJEX or JP1/AS. It is disabled by default. Enable the response-waiting event management function when linking with BJEX or JP1/AS.

9.1.1 System configuration when linking JP1/IM with a batch job execution system

This section describes the configuration of a system in which JP1/IM links with a batch job execution system.

Figure 9–1: Configuration example of batch job execution system with JP1/IM
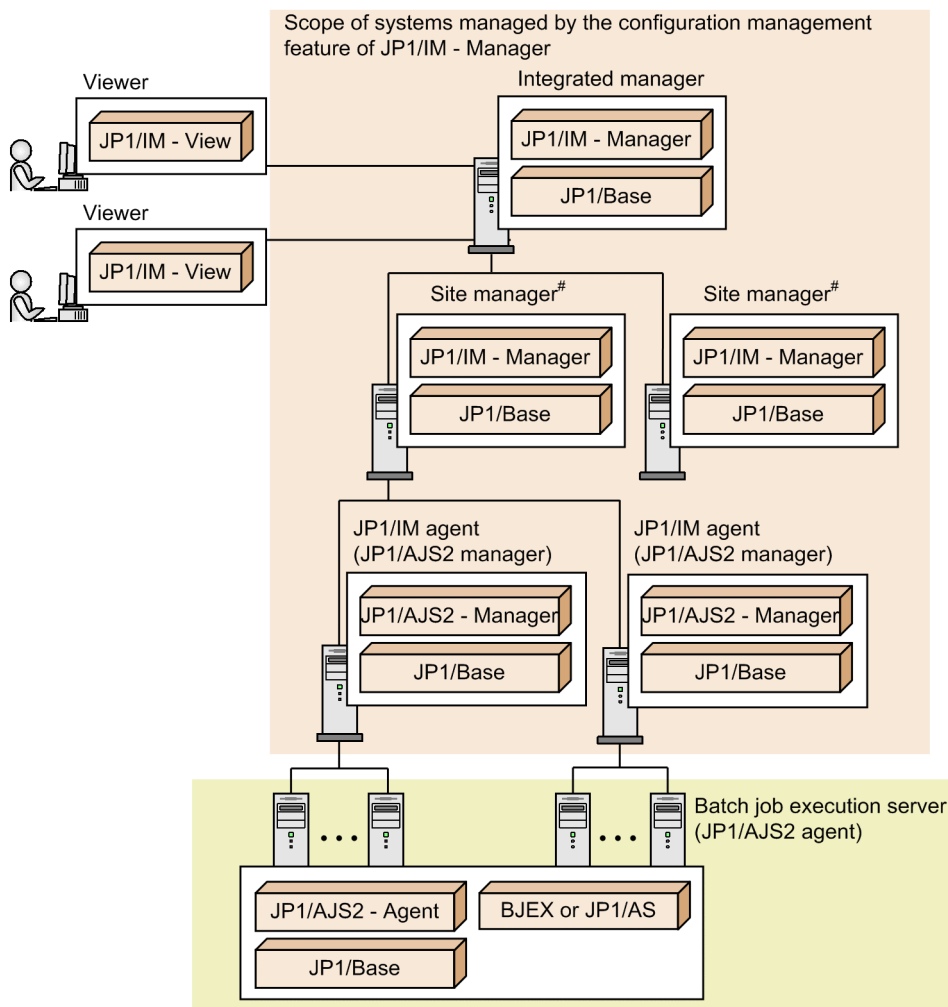
#: Can be a site manager or relay manager.

In the example in the figure, JP1/IM is configured as a hierarchical system that incorporates site managers. The JP1/IM system in the figure monitors a batch job execution system.

The role and prerequisite products of each server are described below. For a list of supported operating systems, see the documentation for the product concerned. For details on version requirements, see the JP1/IM - Manager release notes.

Viewer

　　Connects to JP1/IM - Manager from JP1/IM - View to monitor and work with events. The prerequisite products for a viewer are:

　　• JP1/IM - View[#]

　　　#: In the Web-based JP1/IM - View, you can monitor response-waiting events in the same manner as ordinary JP1 events. However, only a limited range of functions are available. For details, see *9.4 Working with response-waiting events*.

Integrated manager

　　A server that manages systems from an integrated perspective. The prerequisite products for an integrated manager are:

　　• JP1/IM - Manager

　　• JP1/Base

Site manager or relay manager

> A server subordinate to an integrated manager. You can use site managers and relay managers when you want to manage large-scale systems in a hierarchy. The prerequisite products for a site manager or relay manager are:
>
> - JP1/IM - Manager
> - JP1/Base

JP1/IM agent (JP1/AJS manager)

> A server monitored by JP1/IM. In the example in the figure, JP1/IM agents also function as JP1/AJS managers. The prerequisite products for a JP1/IM agent are:
>
> - JP1/AJS - Manager
> - JP1/Base

Batch job execution server (JP1/AJS agent)

> A server that executes processing, such as batch jobs, in response to requests from JP1/AJS - Manager. A batch job execution server can link with JP1/IM even if it is not part of the system whose configuration is being managed by JP1/IM. JP1/IM - Manager links with BJEX or JP1/AS on the batch job execution server in a 1:n ratio (where n is an integer of 1 or higher). For details on how to configure linkage with BJEX or JP1/AS, see *9.3 Configuring JP1/IM to link with BJEX and JP1/AS*.
>
> The prerequisite products for a batch job execution server are:
>
> - JP1/AJS - Agent
> - JP1/Base
> - BJEX or JP1/AS

9.2 JP1/IM functionality for BJEX and JP1/AS linkage

This section describes the JP1/IM functionality that is used when linking with BJEX or JP1/AS.

9.2.1 Handling response-waiting events in JP1/IM

The following response-waiting events are issued when a batch job enters a status where it is waiting for a response from an operator:

- In BJEX
  Event ID: `00005C21`

- In JP1/AS
  Event ID: `00007121`

To monitor response-waiting events in JP1/IM, you need to configure BJEX or JP1/AS to issue the response-waiting event directly to the JP1/IM - Manager host (the integrated manager). You also need to enable the response-waiting event management function in JP1/IM - Manager.

(1) Paths through which response-waiting events are issued

BJEX and JP1/AS issue JP1 events (including response-waiting events) directly to the integrated manager, not by the usual forwarding paths provided by JP1/Base. To have BJEX issue all JP1 events directly to the integrated manager, specify the JP1/IM - Manager host name in 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 JP1 events arrive from BJEX or JP1/AS and other products 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, JP1 events issued by BJEX, JP1/AS, and the other products on the BJEX or JP1/AS host 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 JP1 event.

The following figure shows the paths through which JP1 events are forwarded from BJEX and JP1/AS hosts:

Figure 9–2: Forwarding paths of JP1 events issued by BJEX and JP1/AS hosts
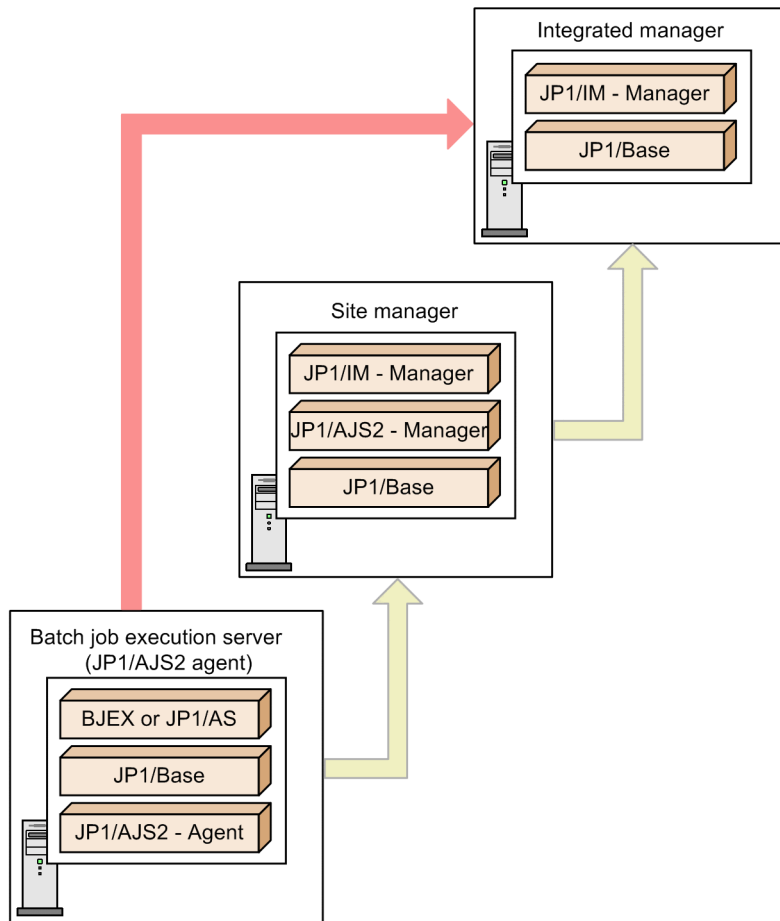
Legend:

→ : Path through which BJEX and JP1/AS issues JP1 events

→ : Path through which JP1/AJS2 and JP1/Base issue JP1 events
(using the forwarding path of JP1/Base)

> **Important note**
>
> 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 on how to enable this setting, see *9.3 Configuring JP1/IM to link with BJEX and JP1/AS*.

Note that you can still monitor waiting-response events as ordinary JP1 events if you do not enable the response-waiting
event management function and the setting that allows users to respond to and work with these events.

> **Important note**
>
> Response-waiting events are handled as such if they are received by JP1/IM - Manager after the response-waiting event management function is enabled. Response-waiting events received before the function is enabled are handled as ordinary JP1 events.

9.2.2 Monitoring response-waiting events

Because JP1/IM handles response-waiting events in the same manner as ordinary JP1 events, you can use automated action notification and other JP1/IM features with these events.

The following describes how each of the following features works with waiting-response events. Features that are not described here work the same way as with ordinary JP1 events.

- Monitoring in the Event Console window
- JP1 event filtering
- Monitoring repeated events
- Searching for events
- Outputting information from JP1/IM - View in CSV format

(1) Monitoring in the Event Console window

Waiting-response events appear in the lists of events on the Monitor Events page, Severe Events page, and Search Events page, like ordinary JP1 events. The Response-Waiting Events page only shows response-waiting events. This page is displayed only when the response-waiting event management function and the setting that allows users to respond to and work with response-waiting events is enabled. Note that the Response-Waiting Events page does not appear in the Web-based JP1/IM - View.

From the list of events in the Event Console window, you can perform the following operations and configuration with respect to response-waiting events in the same manner as ordinary JP1 events:

- Display detailed information about a response-waiting event
- Open the monitors of linked products
- Display execution results of automated actions
- Change display items for JP1 events
- Set the background color for JP1 events
- Set the response status for response-waiting events
- Specify the event display period

For details on these features, see *3.1 Centralized monitoring using JP1 events* in the *Job Management Partner 1/ Integrated Management - Manager Overview and System Design Guide*.

(a) Monitoring on the Response-Waiting Events page

The Response-Waiting Events page displays a list of response-waiting events for which a response is not yet provided. This page is shown below.

Figure 9–3: Response-Waiting Events page
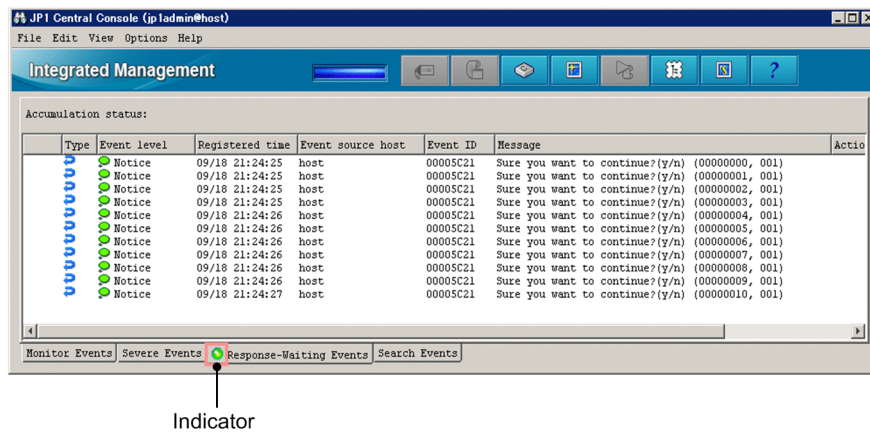
Indicator

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 on what causes response-waiting events to be released from the hold-and-accumulate state, see *9.2.3 Accumulation of response-waiting events*.

The indicator on the tab becomes unlit after all response-waiting events have disappeared from the Response-Waiting Events page.

To allow the operator to distinguish response-waiting events, the ⮌ icon appears in the **Type** column for these events on each page of the Event Console window.

Note that the Response-Waiting Events page does not display the background colors that have been assigned to JP1 events.

(2) Filtering response-waiting events

You can use the following filters to filter response-waiting events:

- Event receiver filter
- Severe events filter
- View filter

When you enable the response-waiting event management function, items that allow the operator to select whether to display response-waiting events appear in the condition definition windows for the event receiver filter and severe events filter. To filter response-waiting events using the view filter, the response-waiting event management function and the setting that allows users to respond to and work with response-waiting events must be enabled.

For details about the windows in which filter conditions are defined, see *2.42.8 Filter condition definition windows* in the manual *Job Management Partner 1/Integrated Management - Manager GUI Reference*.

Note that event acquisition filters do not allow you to specify conditions that specifically identify response-waiting events. Configure event acquisition filters so that they filter events at the product level for products that issue response-waiting events.

(3) Consolidated display of response-waiting events

If a network problem or some other issue causes the same batch job to issue the same response-waiting event several times in succession, the events are displayed as a single *consolidated event*. Events are only consolidated on the Monitor Events page and Severe Events page.

If identical response-waiting events are issued as a result of an error of some kind, the operator does not need to respond to each and every event. If you respond to one of these waiting-response events, you do not need to respond to the others. However, response-waiting events that no longer require a response remain on the Response-Waiting Events page until they are released from the hold-and-accumulate state. For details on how to release these events, see *9.2.3 Accumulation of response-waiting events*.

(4) Searching for response-waiting events

When searching for JP1 events, you can specify a response-waiting event as a search condition. Conditions that apply to response-waiting events only appear in the Event Search Conditions window if you enable the response-waiting event management function and the setting that allows users to respond to and work with response-waiting events.

For details about the Event Search Conditions window, see *2.42.7 Event Search Conditions window* in the manual *Job Management Partner 1/Integrated Management - Manager GUI Reference*.

You can only respond to response-waiting events from the search results if you search the logged-in JP1/IM manager host for response-waiting events. If you do not specify the logged-in manager host, you cannot respond to the response-waiting events that appear in the search results.

(5) Outputting information from JP1/IM - View in CSV format

You can output information about response-waiting events displayed in the list of events in CSV format. You can output CSV information in two ways:

- Save the information in the list of events to a file

  You can save a snapshot of the event information displayed in JP1/IM - View to a CSV file. A snapshot means information extracted at a specific time.

- Copy JP1 event information, action execution results, or other information to the clipboard

  If the feature that allows you to copy information to the clipboard is enabled, you can copy selected parts of response-waiting event information, action execution results, and other information to the clipboard in CSV format. This feature is enabled by default.

The following table shows the events lists whose response-waiting events can be saved to a CSV file or copied to the clipboard in CSV format.

Table 9–1: Events lists that can be output to a CSV file or copied to the clipboard

Operation	Monitor Events page	Severe Events page	Related Events window	Response-Waiting Events page	Search Events page
CSV output	Y	Y	N	Y	Y

Operation	Monitor Events page	Severe Events page	Related Events window	Response-Waiting Events page	Search Events page
Copy to clipboard	Y	Y	Y	Y	Y

Legend:

Y: Can be saved or copied.

N: Cannot be saved or copied.

When you save information about response-waiting events to a CSV file or copy it to the clipboard, the icon in the **Type** column is replaced with the text `Response-waiting event` in the CSV data. If icons indicating a repeated event and a response-waiting event are output for an event, the icons are replaced with the text `Repeated event,` `Response-waiting event` in the CSV data. When you output the information on the Response-Waiting Events page in CSV format, **Response-Waiting Events** appears as the name of the source window in the header information.

For details on 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)* in the *Job Management Partner 1/Integrated Management - Manager Configuration Guide*.

9.2.3 Accumulation of response-waiting events

When you enable the response-waiting event management function, response-waiting events that arrive in the event database on the manager host are recorded in a *file for accumulated response-waiting events* in addition to the event database. A maximum of 2,000 response-waiting events are stored in this file. This process is called *accumulation of response-waiting events*.

The Response-Waiting Events page displays information about the response-waiting events in the file for accumulated response-waiting events.

(1) When response-waiting events are released from the hold-and-accumulate state

Response-waiting events are deleted from the file for accumulated response-waiting events and released from the hold-and-accumulate state when:

- An operator successfully responds to a response-waiting event

- The response-waiting event is canceled in BJEX or JP1/AS

- An operator manually releases the event from the hold-and-accumulate state

- There are more than 2,000 response-waiting events

  In this case, accumulated response-waiting events are released in order from the oldest.

- You disable the response-waiting event management function and restart JP1/IM - Manager

A response-waiting event that is released from the hold-and-accumulate state disappears from the Response-Waiting Events page when you next refresh the list of events in JP1/IM - View. Note that such events, while no longer appearing in the Response-Waiting Events page, still appear in search results in the Search Events page as long as they remain in the event database.

(2) Notification when the number of response-waiting events exceeds 2,000

JP1/IM - Manager monitors the number of response-waiting events in the hold-and-accumulate state, and notifies the operator when the number exceeds 2,000 by issuing a JP1 event (event ID: `00003F41`). The message KAVB0551-E also appears on the Response-Waiting Events page.

Figure 9–4: Response-Waiting Events page when the number of response-waiting events exceeds 2,000
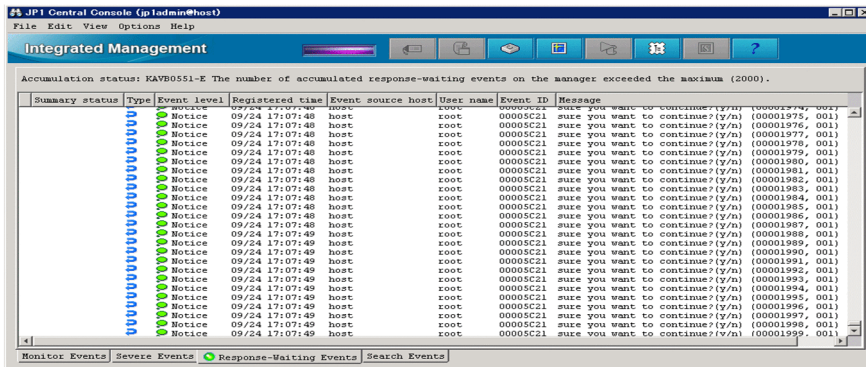
The JP1 event reporting that the number of response-waiting events in the hold-and-accumulate state has exceeded the maximum is issued only once. The message KAVB0551-E remains on the Response-Waiting Events page. When the number of events in the hold-and-accumulate state exceeds the limit, take action as described in the message to resume monitoring events in the hold-and-accumulate state in the usual way. Then the message KAVB0551-E disappears from the Response-Waiting Events page. The JP1 event is issued again when the number of events next exceeds 2,000.

For details on how to resume monitoring of events in the hold-and-accumulate state, see *9.4.4 Resuming monitoring of events in the hold-and-accumulate state*.

Responding to response-waiting events that have been released from the hold-and-accumulate state

You can respond to a response-waiting event that was removed from the Response Waiting Events page after exceeding the maximum number of events by searching for the event from the Search Events page. You can identify an event that was released from the hold-and-accumulate state by viewing the KAVB1801-E message in the integrated trace log on the manager host.

If the response-waiting event was also deleted from the event database, you can respond to the event by executing the response command (`bjexchmsg` or `adshchmsg`) on the host that issued the event.

9.2.4 Responding to response-waiting events

You can respond to response-waiting events from JP1/IM - View. For example, a message might ask the operator if he or she wants to continue batch processing, to which the operator can respond `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 9–5: Enter Response window
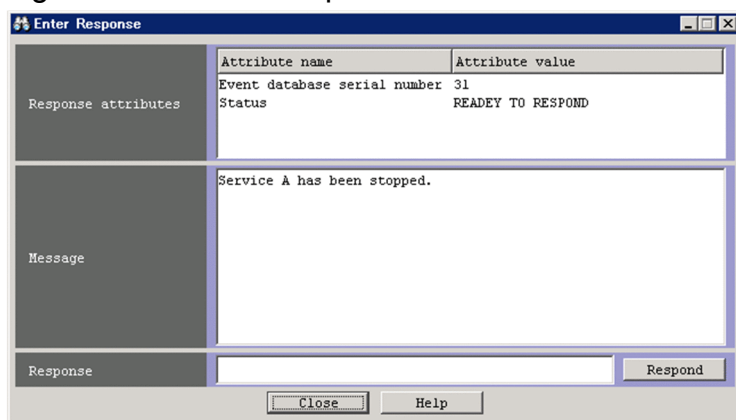
The following table lists the statuses that appear as the value of the **Status** attribute in the **Response attributes** area:

Table 9–2: Statuses of source processes for response-waiting events

Source process status	Description	Can response be entered
READY TO RESPOND	The job that issued the event is waiting for a response.	Y
NO LONGER MANAGED BY BJEX or NO LONGER MANAGED BY JP1/AS	One of the following applies: • 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 on how to set the timeout time, see *9.3.4(1) Setting the timeout time for connections*.

(2) Conditions for responding to response-waiting events

You can respond to response-waiting events under the following conditions:

- The operating permission of the responding JP1 user is JP1_Console_Operator or higher.
- You have not yet responded to the event.
  You can only respond once to a response-waiting event, even if you acquire the event again by changing the event acquisition start location of the event acquisition filter.
- The response-waiting event was received after you enabled the response-waiting event management function.
  You cannot respond to response-waiting events received while the response-waiting event management function is disabled.
- When searching for events, the logged-in manager host is specified as the search target.

Note that you cannot respond to response-waiting events from the Web-based JP1/IM - View.

(3) Using the response command of BJEX or JP1/AS

If a communication error between the source process and JP1/IM - Manager prevents you from responding to an event from JP1/IM - View, you can use the response command (bjexchmsg or adshchmsg) provided by the source process on the source host. You can also use this approach to respond to events that were released from the hold-and-accumulate state and removed from the event database.

9.2.5 Canceling response-waiting events

In some circumstances, such as after canceling a BJEX or JP1/AS job from JP1/AJS or deleting a job in BJEX or JP1/AS, a response-waiting event might remain in the system despite no longer requiring a response. In this scenario, BJEX issues a cancelation event (event ID: 00005C22, 00005C23, or 00005C24) to JP1/IM - Manager as soon as the job is canceled. JP1/AS also sends a cancelation event (event ID: 00007122, 00007123, or 00007124) to JP1/IM - Manager. When JP1/IM - Manager receives this cancelation 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*.

You can also cancel response-waiting events manually from JP1/IM - View. To cancel a response-waiting event that is no longer required, release the event from the hold-and-accumulate state in JP1/IM - View.

9.3 Configuring JP1/IM to link with BJEX and JP1/AS

This section describes how to configure JP1/IM - Manager to link with BJEX or JP1/AS. The descriptions in this section assume that JP1/IM - Manager is already set up.

We recommend the following configuration for JP1/Base and JP1/IM - Manager:

- JP1/Base and JP1/IM - Manager are in a cluster configuration on the manager host.
- The health check function is enabled for JP1/Base and JP1/IM - Manager.

9.3.1 Configuring JP1/IM - Manager

The following describes how to configure JP1/IM - Manager.

(1) Enabling the response-waiting event management function

Enable the response-waiting event management function in JP1/IM - Manager. After enabling the response-waiting event management function, you can:

- Accumulate response-waiting events
- Cancel response-waiting events
- Enable the settings that allow users to respond to and work with response-waiting events
  The relevant settings appear in the Preferences window.
- Filter response-waiting events
  Items that allow you to select whether to filter response-waiting events appear in the Detailed Settings for Event Receiver Filter window and the Severe Event Definitions window.

To enable the response-waiting event management function:

1. Execute the `jcoimdef` command.
   Execute `jcoimdef -resevent ON`.

2. Restart JP1/IM - Manager.
   Note: The feature is not enabled if you use the `jco_spmd_reload` command.

For details on the `-resevent` option of the `jcoimdef` command, see *9.5.1 jcoimdef*.

(2) Configuring the event acquisition filter

Configure the event acquisition start location so that processing continues from where it last stopped.

To set the start location of the event acquisition filter:

1. Execute the `jcoimdef` command.
   Execute `jcoimdef -b -1`.

2. Restart JP1/IM - Manager or execute the `jco_spmd_reload` command.

For details on the `jcoimdef` command, see *jcoimdef* in *1. Commands* in the *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.

For details on the `jco_spmd_reload` command, see *jco_spmd_reload* in *1. Commands* in the *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.

9.3.2 Configuring JP1/IM - View

The following describes how to configure JP1/IM - View.

(1) Enabling the setting that allow users to respond to and work with response-waiting events

In the Preferences window of JP1/IM - View, you can enable the setting that allows individual users to respond to and work with response-waiting events. After you enable this setting, users can:

- Monitor response-waiting events
  The Response-Waiting Events page appears in the Event Console window.

- Respond to response-waiting events
  Users can respond to these events in the Enter Response window.

- Search for response-waiting events
  Items that relate to response-waiting events can now be specified as search conditions in the Search Events window.

- Filter response-waiting events
  Items that allow the operator to select whether to display response-waiting events appear in the Settings for View Filter window.

To allow users to respond to and work with response-waiting events:

1. Display the Preferences window.
   In the Event Console window, from the **Options** menu, choose **User Preferences**.

2. In the **Response-waiting event** area, select the **Enable** check box.

3. Click **OK**.

For details about the Preferences window, see *2.42.6 Preferences window* in the manual *Job Management Partner 1/ Integrated Management - Manager GUI Reference*.

(2) Configuring the event receiver filter

You can use an event receiver filter to limit which JP1 events each user can monitor. If you do not wish for a particular user to view response-waiting events, configure the event receiver filter to hide those events. By default, response-waiting events are displayed.

For details on how to create and modify an event receiver filter, see *4.2.2 Settings for event receiver filters* in the *Job Management Partner 1/Integrated Management - Manager Configuration Guide*.

For details about the Detailed Settings for Event Receiver Filter window, see *2.42.8 Filter condition definition windows* in the manual *Job Management Partner 1/Integrated Management - Manager GUI Reference*.

9.3.3 Configuring JP1/Base

In JP1/Base on the authentication server, assign the appropriate operating permissions to JP1 users who will work with response-waiting events.

The following operations require `JP1_Console_Operator` permission or higher:

- Responding to waiting-response events
- Manually releasing response-waiting events from the hold-and-accumulate state

The following operations require `JP1_Console_Admin` permission or higher:

- Resuming monitoring of response-waiting events in the hold-and-accumulate state

For details on how to assign permissions, see the chapter describing user management setup in the *Job Management Partner 1/Base User's Guide*.

9.3.4 Communication settings between BJEX or JP1/AS and JP1/IM - Manager

This section describes the settings that govern communication between BJEX or JP1/AS and JP1/IM - Manager.

(1) Setting the timeout time for connections

You can change the length of time after which a timeout occurs for connections established for purposes such as checking the status of the source process or entering a response. Under most circumstances, you do not need to change this setting. If you frequently encounter error messages (KAVB0554-E or KAVB0555-E) due to network congestion or heavy loads on the source server, set a longer timeout time. You can set the timeout time in JP1/IM - Manager.

To change the timeout time for connections:

1. Define the following parameter in a file you create on the manager.

   [*logical-host-name*\JP1CONSOLEMANAGER]

   "`RESEV_TIMEOUT_MAX`"=dword:*hexadecimal-value*

   Replace *logical-host-name* with `JP1_DEFAULT` if the host is a physical host, and the logical host name if the host is a logical host.

   Specify the timeout time as a hexadecimal value within a range from 60 to 3,600 seconds. The default is `dword: 0000003c` (60 seconds).

2. Execute the `jbssetcnf` command.

   Execute the `jbssetcnf` command with the definition file you created specified in a command argument. When you execute the `jbssetcnf` command, the setting in the definition file is applied to the common definition information. For details on the `jbssetcnf` command, see the *Job Management Partner 1/Base User's Guide*.

3. Execute the `jco_spmd_reload` command or restart JP1/IM - Manager.

   The new definition takes effect.

   For details on the `jco_spmd_reload` command, see *jco_spmd_reload* in *1. Commands* in the *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.

(2) Configuring packet filtering in firewall environments

In an environment that uses a firewall, configure packet filtering so that BJEX or JP1/AS can communicate with JP1/IM - Manager through the firewall. The following table shows the port numbers used for communication between BJEX or JP1/AS and JP1/IM - Manager, and the direction in which packets pass through the firewall:

Table 9–3: Port numbers used for communication between BJEX or JP1/AS and JP1/IM - Manager

Service	Port	Traffic direction
jp1bsplugin	20306/tcp	JP1/IM - Manager -> BJEX or JP1/AS
jp1imevt	20098/tcp	BJEX or JP1/AS -> JP1/IM - Manager

Legend:
-> : Direction of established connection

For details on 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 *Job Management Partner 1/Base User's Guide*
- Port numbers used by JP1/IM: *C. Port Numbers* in the *Job Management Partner 1/Integrated Management - Manager Overview and System Design Guide*

9.3.5 Configuring BJEX or JP1/AS

This section describes how to configure BJEX or JP1/AS when linking with JP1/IM - Manager.

(1) Specifying the link-target JP1/IM - Manager

BJEX and JP1/AS can link with one JP1/IM - Manager host, which you must specify in the appropriate configuration file. To specify the link-target JP1/IM - Manager host for BJEX, specify the JP1/IM - Manager host name in the BJEX configuration file (`bjex.conf`). To specify the link-target host for JP1/AS, specify the host name in the JP1/AS environment file.

(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.

9.4 Working with response-waiting events

This section describes the operations you can perform on response-waiting events.

> **▌ Important note**
>
> Restrictions affecting the Web-based JP1/IM - View
>
> From the Web-based JP1/IM - View, you cannot respond to response-waiting events, release an event from the hold-and-accumulate state, or resume monitoring of events in the hold-and-accumulate state. The Response-Waiting Events page does not appear in the Event Console window in the Web-based JP1/IM - View. However, you can change the response status of response-waiting events and register incidents manually.

9.4.1 Flow of tasks for responding to response-waiting events

This section describes the flow of tasks for monitoring and responding to response-waiting events in Central Console and Central Scope.

(1) Monitoring response-waiting events in Central Console

The following figure shows an overview of how to monitor and respond to response-waiting events in Central Console:

Figure 9–6: Monitoring and responding to response-waiting events in Central Console

1. A response-waiting event appears on the Response-Waiting Events page.

Icon indicating a response-waiting event
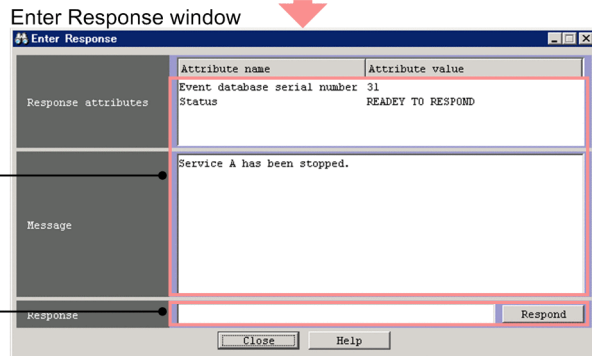
Response-Waiting Events page

2. Display the Enter Response window.

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.

Response-Waiting Events page
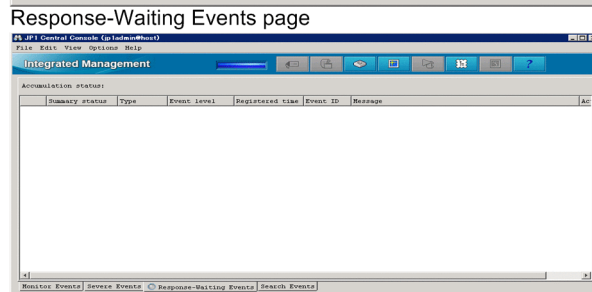
6. When you search for the response-waiting event in the Search Events page, the event appears in *Processed* status in the search results.

Icon indicating *Processed* status
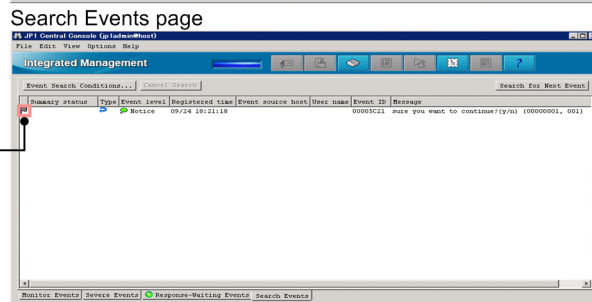
Search Events page

Legend:

: Operation performed by user

The numbers in the figures correspond to the steps below:

1. When JP1/IM - Manager receives a response-waiting event, the event appears on the Response-Waiting Events page of the Event Console window.

2. Display the Enter Response window for the response-waiting event.

3. Check the status of the source process and the message contents.

   Make sure that the status of the source process is READY TO RESPOND.

4. Enter a response in the **Response** area and then click **Respond**.

5. If the response is successful, the response-waiting event disappears from the Response-Waiting Events page.

6. When you search for a response-waiting event from the Search Events window, the event appears in the search results with the status *Processed*.

(2) Monitoring response-waiting events in Central Scope

The following figure shows an overview of how to monitor and respond to response-waiting events in Central Scope:

Figure 9–7: Monitoring and responding to response-waiting events in Central Scope

1. A response-waiting event matches a status change condition of a monitored object, causing the status of the object to change.

2. Display the response-waiting event by searching for the status-change event.

3. Display the Enter Response window.

4. Check the status of the source process of the response-waiting event, and the message contents.

5. Enter a response and then click **Respond**.

6. When you search for the response-waiting event in the Search Events page, the event appears in Processed status in the search results.

Processed icon

7. The response-waiting event transitioning to Processed status causes the status of the monitored object to automatically return to Normal.

Legend:

: Operation performed by user

The numbers in the figures correspond to the steps below:

1. When JP1/IM - Manager receives a response-waiting event that matches the status change condition for a monitored object, the status of the monitored object changes.

2. Search for the status change event from the monitored object and display response-waiting events in the Search Events page.

3. Display the Enter Response window for the response-waiting event.

4. Check the status of the source process and the message contents.
   Make sure that the status of the source process is `READY TO RESPOND`.

5. Enter a response in the **Response** area and then click **Respond**.

6. If the response is successful, the response-waiting event appears in the search results with the status *Processed* when you search from the Search Events window again.

7. With the response to the response-waiting event now complete, the status of the monitored object in the Monitoring Tree window returns to normal.

9.4.2 Responding to response-waiting events

The conditions under which you can respond to a response-waiting event are described in *9.2.4(2) Conditions for responding to response-waiting events*. You must have JP1_Console_Operator permission or higher to perform this operation.

To respond to a response-waiting event:

1. Use one of the following methods to display the Enter Response window:
   - On the Response-Waiting Events page or Search Events page, select a response-waiting event, and from the **View** menu, choose **Enter Response**.
   - On the Response-Waiting Events page, Search Events page, or Related Events window, right-click a response-waiting event and choose **Enter Response** from the popup menu.
   - In the Event Details window, click **Enter Response**.

2. Enter a response in the **Response** area of the Enter Response window.
   Check the message contents and enter an appropriate response.
   - You can enter a maximum of 512 bytes.
   - You can enter characters in the 0x20 to 0x7E range of the ASCII character set.

3. Click **Respond**.
   A confirmation dialog box appears. Click **Yes** to submit the response to the response-waiting event. Click **No** to return to the Enter Response window without submitting the response.
   If the response is successful, the response-waiting event disappears from the Response-Waiting Events page, and the response status of the event changes to *Processed*.

9.4.3 Manually releasing response-waiting events from the hold-and-accumulate state

If an event no longer requires a response, or the event was not released from the hold-and-accumulate state despite a successful response, you can manually release the event from the hold-and-accumulate state. Note that this operation requires JP1_Console_Operator permission or higher.

To release a response-waiting event from the hold-and-accumulate state:

1. Display the Response-Waiting Events page of the Event Console window.

2. Check the status of the source process of the response-waiting event you want to release.
   Display the Enter Response window by selecting the response-waiting event you want to release. Make sure that the status of the source process is NO LONGER MANAGED BY BJEX or ALREADY RESPONDED.

3. Change the response status of the response-waiting event to *Processed*.

   If the event can be released, change the status of the event to *Processed* by choosing **Processed** from the **View** menu.

4. Select the response-waiting event that you want to release from the hold-and-accumulate state, and from the **View** menu, choose **Remove Accumulated Events**. Alternatively, right-click the event and choose **Remove Accumulated Events** from the popup menu.

   You can select multiple response-waiting events. When you click **Remove Accumulated Events**, the selected events are removed from the hold-and-accumulate state.

   The response-waiting events disappear from the Response-Waiting Events page when you refresh the list of events.

You cannot accumulate an event again after releasing it. If you inadvertently release a response-waiting event, you can respond to the event by searching for it from the Search Events page.

9.4.4 Resuming monitoring of events in the hold-and-accumulate state

When normal monitoring of events in hold-and-accumulate state is resumed after the number of accumulated response-waiting events has exceeded 2,000, you can be notified by a JP1 event when the number of accumulated events once again exceeds 2,000. This operation requires `JP1_Console_Admin` permission.

Before you resume monitoring accumulated events, identify and respond to the overflowed response-waiting events by reviewing the integrated trace log on the manager. For details on how to respond to response-waiting events that have been released from the hold-and-accumulate state, see *9.2.3(2) Notification when the number of response-waiting events exceeds 2,000*.

To resume monitoring of events in the hold-and-accumulate state:

1. In the Event Console window, from the **Options** menu, choose **Function-Status Notification Return** and then **Monitor Accumulation Status**.

   The system resumes monitoring the events in the hold-and-accumulate state. The message KAVB0551-E disappears from the **Accumulation status** area of the Response-Waiting Events page when you next refresh the Event Console window.

9.5 Command usage when linking with BJEX or JP1/AS

This section describes the command options you need to use when linking with BJEX or JP1/AS. For information about other options and details of the commands themselves, see *1. Commands* in the *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*. Note that the *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference* does not describe the options for linking with BJEX.

9.5.1 jcoimdef

The `jcoimdef` command is used to set up the system environment for JP1/IM - Manager, and to reference settings. When you execute this command, the settings are output to standard output.

You can specify the following option when linking with BJEX or JP1/AS:

`-resevent ON|OFF`

Specify the `-resevent ON` option to enable the response-waiting event management function. To disable the function, specify `-resevent OFF`.

If you execute the `jcoimdef` command with the `-resevent` option to enable or disable the response-waiting event management function while JP1/IM - Manager is running, you will need to restart JP1/IM - Manager. You will also need to restart any instances of JP1/IM - View that are connected to JP1/IM - Manager.

For details on the `jcoimdef` command, see *jcoimdef* in *1. Commands* in the *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.

9.5.2 jim_log.bat (Windows only)

`jim_log.bat` is a tool for collecting data when an error occurs in JP1/IM - Manager or JP1/IM - View. The data collected by this tool includes maintenance information for JP1/IM - Manager, JP1/IM - View, and JP1/Base, system information from the OS, and integrated trace logs.

You can specify the following option when linking with BJEX or JP1/AS:

`-a`

Specify this option to prevent the tool from collecting the file for accumulated response-waiting events.

The file for accumulated response-waiting events collected by `jim_log.bat` is stored in the following folders as primary data:

Internal folder for primary data on physical hosts

data-folder`\jp1_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 on the `jim_log.bat` tool, see *jim_log.bat (Windows only)* in *1. Commands* in the *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.

9.5.3 jim_log.sh (UNIX only)

`jim_log.sh` is a tool for collecting data when an error occurs in JP1/IM - Manager. The data collected by this tool includes maintenance information for JP1/IM - Manager and JP1/Base, system information from the OS, and integrated trace logs.

You can specify the following option when linking with BJEX or JP1/AS:

`-a`

Specify this option to prevent the tool from collecting the file for accumulated response-waiting events.

The file for accumulated response-waiting events collected by `jim_log.sh` is stored in the following directories as primary data:

Internal directory for primary data on physical hosts

`./var/opt/jp1cons/log/response`

Internal directory for primary data on logical hosts

`./`*shared-disk*`/jp1cons/log/response`

For details on the `jim_log.sh` tool, see *jim_log.sh (UNIX only)* in *1. Commands* in the *Job Management Partner 1/ Integrated Management - Manager Command and Definition File Reference*.

10

Troubleshooting

This chapter explains how to handle problems if they occur in JP1/IM. It also explains items that tend to cause problems.

10.1 Troubleshooting procedure

The figure below shows the procedure to follow when a problem occurs in JP1/IM.

Figure 10–1: Troubleshooting procedure
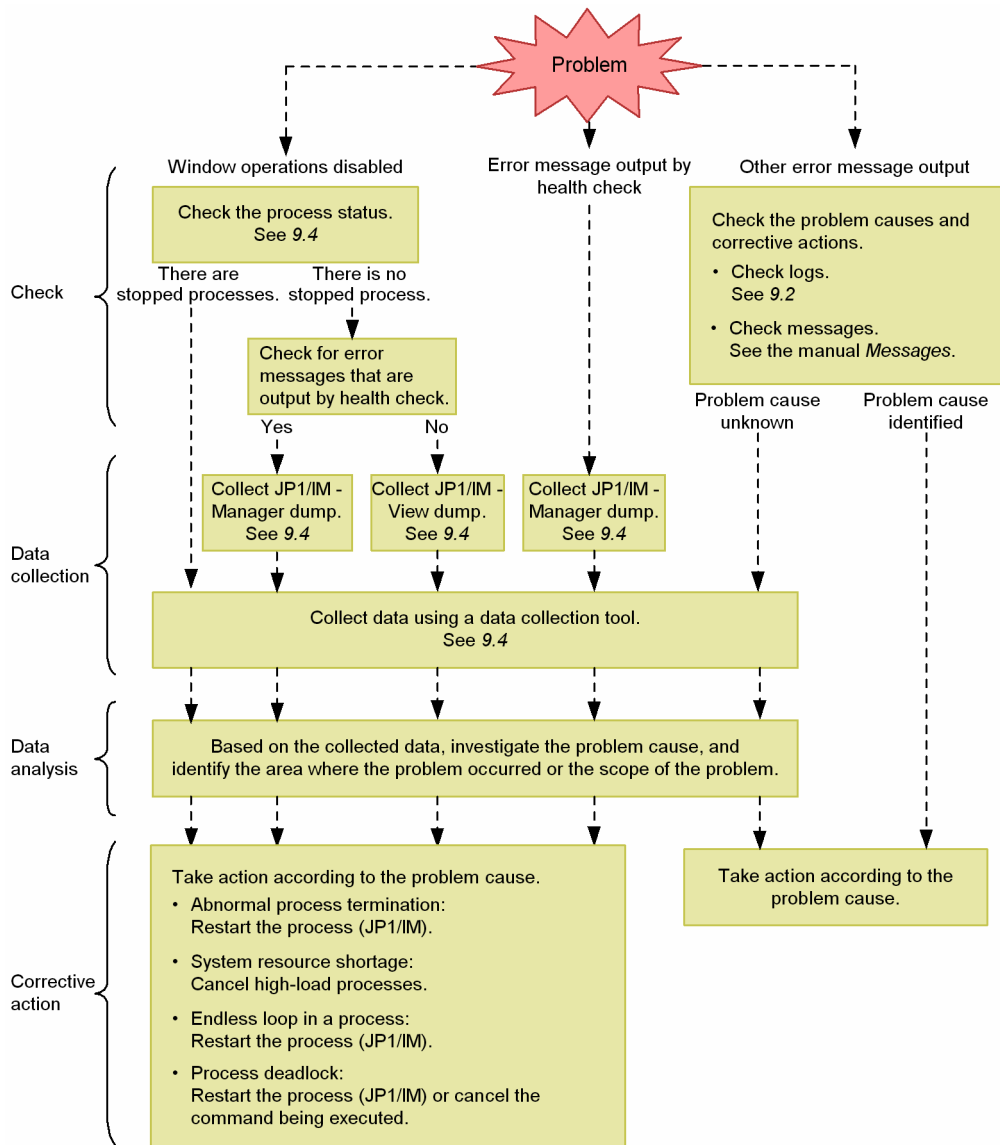
10.2 Log information types

The following two types of logs are output by JP1/IM:

- Common message log
- Integrated trace log

This section explains these two types of log information.

10.2.1 Common message log

The common message log contains log information for the system administrator and reports system problems. The common message log reports a minimal amount of necessary problem information.

The common message log is output to the syslog file in UNIX, and to the Windows Event Log in Windows.

In UNIX, the common message log is output to the following files:

- `/var/adm/messages` (in Solaris)
- Files under `/var/adm/syslog/` (in AIX)
- `/var/log/messages` (in Linux)

> **▌Important note**
>
> In UNIX, when a message is being output to the syslog file, the message may be incomplete.

10.2.2 Integrated trace log

The integrated trace log contains log information that is obtained by using the Hitachi Network Objectplaza Trace Library (`HNTRLib2`) to integrate the trace information that is output by individual programs into a single output file. The integrated trace log outputs more detailed messages than the common message log.

The default output destination of the integrated trace log is as follows:

In Windows:
   system-drive`\Program Files\Hitachi\HNTRLib2\spool\hntr2{1|2|3|4}.log`

In UNIX:
   `/var/opt/hitachi/HNTRLib2/spool/hntr2{1|2|3|4}.log`

You can view the integrated trace log file from a text editor of your choice. The figure below shows an output example of the integrated trace log.

Figure 10–2: Integrated trace log file output example
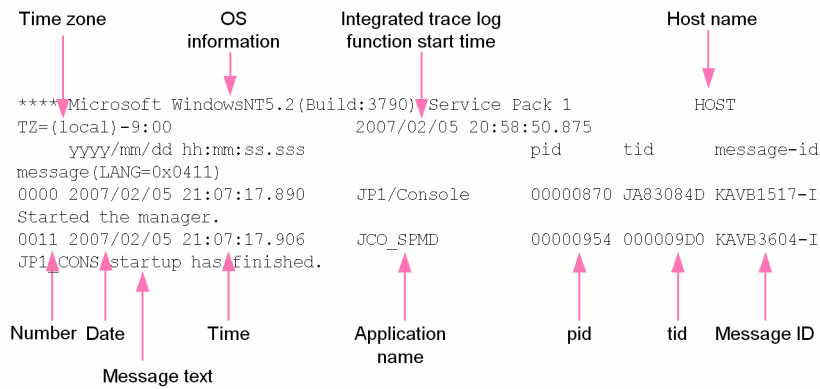
The header information that is output to the integrated trace log file and the output items are explained below.

Table 10–1: Integrated trace log file header information

Header information	Explanation
OS information	Information on the OS under which the Hitachi Network Objectplaza Trace Library (HNTRLib2) started.
Host name	The name of the host on which the Hitachi Network Objectplaza Trace Library (HNTRLib2) started.
Time zone	In Windows: 　OS's time zone In UNIX: 　Environment variable TZ of the integrated trace process. 　If the environment variable TZ is not set up, Unknown is output.
Integrated trace log function start time	Time at which the Hitachi Network Objectplaza Trace Library (HNTRLib2) started.

Table 10–2: Integrated trace log file output items

Output items	Explanation
Number (4 digits)	Trace code serial number A number is assigned to each process that outputs a log.
Date (10 bytes)	Trace collection date: $yyyy/mm/dd$ (year/month/day)
Time (12 bytes)	Trace collection time (local time): $hh:mm:ss.sss$ (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: • JP1/IM-Manager Service 　JP1/IM-Manager • Event Base Service 　evflow • Automatic Action Service 　jcamain • Event Generation Service 　evgen • Central Scope Service 　jcsmain • IM Configuration Management Service 　jcfmain

Output items	Explanation

	• Process management
	`JCO_SPMD`
	• `jcochstat` command
	`jcochngstat`
	• Other commands
	command-name
	
	The following AP names are output by JP1/IM - View:
	• Central Console - View
	`JP1/IM-View`
	• Central Scope - View
	`JP1/IM-View`
	• IM Configuration Management - View
	`JP1/IM-View`
	• Edit Tree window
	`JP1/IM-Edit`

pid	Process ID assigned by the OS
tid	Thread ID for identifying a thread
Message ID	Message ID explained in the message output format. Message ID used by this product.
Message text	Message text that is output to the integrated trace log. Message text that is output from this product.

The log time that is output to the integrated trace log is formatted according to the time zone of the process that output the log.

Consequently, if a user who has changed the environment variable *TZ* starts a service or executes a command, a time that is different from the time zone that is set in the OS may be output.

10.2.3 Log files and directory list

This subsection explains the types of log information that are output by JP1/IM, default file names, and directory names.

Note that the files explained here are output for product maintenance purposes. Therefore, there is no need for the user to view or modify these files. If a problem such as a system error occurs, the user may be asked to temporarily retain these files on site for the purpose of collecting data.

(1) In Windows

The tables below show the default log files and folders that are output by the Windows version of JP1/IM.

The *Log type* column lists the log types that are output by JP1/IM.

The *Default file name and folder name* column describes log file names as absolute paths when JP1/IM - Manager, JP1/IM - View, or JP1/Base is installed in the default mode. *Default file name and folder name* in a cluster operation system describes the log file names of shared folders as absolute paths.

The *Maximum disk usage* column shows the maximum disk space used by each log file. When there are multiple log files, the combined total is given.

The *File-switching timing* column shows how JP1/IM times output destination log file switching. When the file reaches the size shown in this column or when the event shown in this column occurs, the output destination is switched. If there

are multiple log files and if the maximum disk usage is reached, files are overwritten, beginning with the ones that have the oldest update dates.

Table 10–3: JP1/IM - Manager (JP1/IM - Central Console) log files and folders (Windows)

Log type	Default file name and folder name	Maximum disk usage	File-switching timing
Process management log	*Console-path*\log\JCO_SPMD{1|2|3}.log	384 KB	128 KB
	Console-path\log\JCO_SPMD_COMMAND{1|2|3}.log	384 KB	128 KB
	shared-folder\jp1cons\log\JCO_SPMD{1|2|3}.log	384 KB	128 KB
	shared-folder\jp1cons\log\JCO_SPMD_COMMAND{1|2|3}.log	384 KB	128 KB
Stack trace log	*Console-path*\log\javalog0{1|2|3|4}.log	1 MB	At startup or 256 KB
	shared-folder\jp1cons\log\javalog0{1|2|3|4}.log	1 MB	At startup or 256 KB
Logical host settings program log	*Console-path*\log\jp1hasetup.{log|log.old}	2,000 KB	1,000 KB
Setup log	*Console-path*\log\command\comdef[_old].log	512 KB	256 KB
Event console log	*Console-path*\log\console\EVCONS{1|2|3}.log	30,720 KB	10,240 KB
	Console-path\log\console\jp1cons{1|2|3|4}.log	20,480 KB	5,120 KB[1]
	Console-path\log\console\evtcon_exe{1|2|3}.log	256 KB **x 3**	256 KB
	Console-path\log\console\JCOAPI{1|2|3}.log	96KB	32KB
	Console-path\log\console\jp1consM{1|2...|20}.log	100 MB	5 MB[1]
	Console-path\log\console\jp1filterDef{1|2|3|4|5}.log	100 MB	20 MB
	Console-path\log\console\jp1bizGroupDef{1|2}.log	10 MB	5 MB
	Console-path\log\console\jp1cmdButtonDef{1|2|3|4|5}.log	25 MB	5 MB
	shared-folder\jp1cons\log\console\EVCONS{1|2|3}.log	30,720 KB	10,240 KB
	shared-folder\jp1cons\log\console\jp1cons{1|2|3|4}.log	20,480 KB	5,120 KB[1]
	shared-folder\jp1cons\log\console\evtcon_exe{1|2|3}.log	256 KB **x 3**	256 KB
	shared-folder\jp1cons\log\console\JCOAPI{1|2|3}.log	96 KB	32 KB

Log type	Default file name and folder name	Maximum disk usage	File-switching timing
	shared-folder\jp1cons\log\console\jp1consM{1|2...|20}.log	100 MB	5 MB[#1]
	shared-folder\jp1cons\log\console\jp1filterDef{1|2|3|4|5}.log	100 MB	20 MB
	shared-folder\jp1cons\log\console\jp1bizGroupDef{1|2}.log	10 MB	5 MB
	shared-folder\jp1cons\log\console\jp1cmdButtonDef{1|2|3|4|5}.log	25 MB	5 MB
Automated action trace log	*Console-path*\log\action\JCAMAIN{1|2|3|4|5}.log	25,600 KB[#2]	5,120 KB
	shared-folder\jp1cons\log\action\JCAMAIN{1|2|3|4|5}.log	25,600 KB[#2]	5,120 KB
Product information log	*Console-path*\log\hliclib\hliclibtrc{1|2|3|4|5}.log	5 MB	1 MB
	Console-path\log\hliclib\hlicliberr{1|2|3|4|5}.log	5 MB	1 MB
	Console-path\log\hliclib\hliclibmgrtrc{1|2|3|4|5}.log	5 MB	1 MB
	Console-path\log\hliclib\hliclibmgrerr{1|2|3|4|5}.log	5 MB	1 MB
	shared-folder\jp1cons\log\hliclib\hliclibtrc{1|2|3|4|5}.log	5 MB	1 MB
	shared-folder\jp1cons\log\hliclib\hlicliberr{1|2|3|4|5}.log	5 MB	1 MB
	shared-folder\jp1cons\log\hliclib\hliclibmgrtrc{1|2|3|4|5}.log	5 MB	1 MB
	shared-folder\jp1cons\log\hliclib\hliclibmgrerr{1|2|3|4|5}.log	5 MB	1 MB
Action information file	*Console-path*\log\action\actinf.log	626 KB[#3]	No switching
	shared-folder\jp1cons\log\action\actinf.log	626 KB[#3]	No switching
Action host name file	*Console-path*\log\action\acttxt{1|2}.log	48.9 MB[#4]	When the action information file wraps around
	shared-folder\jp1cons\log\action\acttxt{1|2}.log	48.9 MB[#4]	When the action information file wraps around
Action re-execution file	*Console-path*\log\action\actreaction	300 MB	When system switching occurs
	shared-folder\jp1cons\log\action\actreaction	300 MB	When system switching occurs
jcochafmode, jcochstat, and	*Console-path*\log\command\CMD{1|2|3}.log	3,072 KB	1,024 KB
	Console-path\log\command\jp1cons_cmd{1|2}.log	12,288 KB	6,144 KB

Log type	Default file name and folder name	Maximum disk usage	File-switching timing
`jcoevtreport` command trace logs[#5]	*Console-path*\log\command\jp1consM_cmd{1|2}.log	12,288 KB	6,144 KB
Plug-in log	*Console-path*\log\command\jcoplugin{1|2|3}.log	3 MB	1 MB
Reporting status storage file	*Console-path*\log\notice\notice_stat.dat	72B	No switching
	shared-folder\jp1cons\log\notice\notice_stat.dat	72B	No switching
Action definition backup file	*Console-path*\log\action\actdefbk.conf	2,048 KB	No switching
	shared-folder\jp1cons\log\action\actdefbk.conf	2,048 KB	No switching
Event base trace log	*Console-path*\log\evflow\EVFLOW{1|2|3|4|5|6|7|8|9|10}.log	100 MB	10 MB
	Console-path\log\evflow\jp1evflowM{1|2...|20}.log	100 MB	5 MB
	Console-path\log\evflow\jp1actDef{1|2|3|4|5}.log	25 MB	5 MB
	Console-path\log\evflow\jp1chsevDef{1|2|3|4|5}.log	25 MB	5 MB
	Console-path\log\evflow\jp1hostmapDef{1|2|3|4|5}.log	25 MB	5 MB
	Console-path\log\evflow\evflow_exe{1|2|3}.log	256 KB **x 3**	256 KB
	shared-folder\jp1cons\log\evflow\EVFLOW{1|2|3|4|5|6|7|8|9|10}.log	100 MB	10 MB
	shared-folder\jp1cons\log\evflow\jp1evflowM{1|2...|20}.log	100 MB	5 MB
	shared-folder\jp1cons\log\evflow\jp1actDef{1|2|3|4|5}.log	25 MB	5 MB
	shared-folder\jp1cons\log\evflow\jp1chsevDef{1|2|3|4|5}.log	25 MB	5 MB
	shared-folder\jp1cons\log\evflow\jp1hostmapDef{1|2|3|4|5}.log	25 MB	5 MB
	shared-folder\jp1cons\log\evflow\evflow_exe{1|2|3}.log	256 KB **x 3**	256 KB
Matching information file	*Console-path*\log\evflow\evflowinf.log	12B	No switching
	shared-folder\jp1cons\log\evflow\evflowinf.log	12B	No switching
Event base error log	*Console-path*\log\evflow\jp1evflow{1|2|3|4}.log	20,480 KB	5,120 KB
	shared-folder\jp1cons\log\evflow\jp1evflow{1|2|3|4}.log	20,480 KB	5,120 KB
Event base stack trace	*Console-path*\log\evflow\javalog0{1|2|3|4}.log	1 MB	At startup or 256 KB

10. Troubleshooting

Log type	Default file name and folder name	Maximum disk usage	File-switching timing
	shared-folder\jp1cons\log\evflow\javalog0{1|2|3|4}.log	1 MB	At startup or 256 KB
Automated action error log	*Console-path*\log\action\jp1act{1|2|3}.log	15,360 KB	5,120 KB
	shared-folder\jp1cons\log\action\jp1act{1|2|3}.log	15,360 KB	5,120 KB
Correlation event generation history file	*Console-path*\operation\evgen\egs_discrim{1|2|3}.log[#6]	30 MB[#6]	10 MB[#6]
	shared-folder\jp1cons\operation\evgen\egs_discrim{1|2|3}.log[#6]	30 MB[#6]	10 MB[#6]
Correlation event generation trace log	*Console-path*\log\evgen\EVGEN{1|2|3}.log	15 MB	5 MB
	Console-path\log\evgen\evgen_exe{1|2|3}.log	256 KB **x** 3	256 KB
	shared-folder\jp1cons\log\evgen\EVGEN{1|2|3}.log	15 MB	5 MB
	shared-folder\jp1cons\log\evgen\evgen_exe{1|2|3}.log	256 KB **x** 3	256 KB
Correlation event generation individual log	*Console-path*\log\evgen\jp1egs{1|2}.log	20 MB	10 MB
	Console-path\log\evgen\jp1egsM{1|2}.log	20 MB	10 MB
	shared-folder\jp1cons\log\evgen\jp1egs{1|2}.log	20 MB	10 MB
	shared-folder\jp1cons\log\evgen\jp1egsM{1|2}.log	20 MB	10 MB
Correlation event generation individual log (for commands)	*Console-path*\log\evgen\jp1egs_cmd{1|2|3|4}.log	20 MB	5 MB
	Console-path\log\evgen\jp1egsM_cmd{1|2|3|4}.log	20 MB	5 MB
Correlation event generation stack trace log	*Console-path*\log\evgen\javalog0{1|2|3|4}.log	1 MB	At startup or 256 KB
	shared-folder\jp1cons\log\evgen\javalog0{1|2|3|4}.log	1 MB	At startup or 256 KB
Correlation event generation process inheriting definition file	*Console-path*\log\evgen\egs_discrim_info{1|2|3|4}.dat	312 MB[#7]	At termination
	shared-folder\jp1cons\log\evgen\egs_discrim_info{1|2|3|4}.dat	312 MB[#7]	At termination
Correlation event generation definition application log	*Console-path*\log\evgen\jp1egsDefine{1|2}.log	10 MB	5 MB
	shared-folder\jp1cons\log\evgen\jp1egsDefine{1|2}.log	10 MB	5 MB
File for accumulated response-waiting events[#8]	*Console-path*\log\response\resevent.dat	40 MB	No switching
	shared-folder\jp1cons\log\response\resevent.dat	40 MB	No switching

Log type	Default file name and folder name	Maximum disk usage	File-switching timing
Backup file for accumulated response-waiting events	*Console-path*\log\response\resevent.dat.dump	40 MB	No switching
	shared-folder\jp1cons\log\response\resevent.dat.dump	40 MB	No switching
Command execution history folder	*Base-path*\log\COMMAND\	See the *Job Management Partner 1/Base User's Guide*.	
	shared-folder\jp1base\log\COMMAND\		
Remote command log	*Base-path*\log\JCOCMD\jcocmd_result{1|2|3}.log		
	Base-path\log\JCOCMD\jcocmdapi{1|2|3}.log		
	Base-path\log\JCOCMD\jcocmdapi_trace{1|2|3}.log		
	Base-path\log\JCOCMD\jcocmdcom{1|2|3}.log		
	Base-path\log\JCOCMD\jcocmdcom_trace{1|2|3}.log		
	Base-path\log\JCOCMD\jcocmdexe{1|2|3}.log		
	Base-path\log\JCOCMD\jcocmdexe_trace{1|2|3}.log		
	Base-path\log\JCOCMD\jcocmdrouter{1|2|3}.log		
	Base-path\log\JCOCMD\jcocmdrouter_trace{1|2|3}.log		
	Base-path\log\JCOCMD\JCOCMDCMD{1|2|3}.log		
	shared-folder\jp1base\log\JCOCMD\jcocmd_result{1|2|3}.log		
	shared-folder\jp1base\log\JCOCMD\jcocmdapi{1|2|3}.log		
	shared-folder\jp1base\log\JCOCMD\jcocmdapi_trace{1|2|3}.log		
	shared-folder\jp1base\log\JCOCMD\jcocmdcom{1|2|3}.log		
	shared-folder\jp1base\log\JCOCMD\jcocmdcom_trace{1|2|3}.log		
	shared-folder\jp1base\log\JCOCMD\jcocmdexe{1|2|3}.log		
	shared-folder\jp1base\log\JCOCMD\jcocmdexe_trace{1|2|3}.log		
	shared-folder\jp1base\log\JCOCMD\jcocmdrouter{1|2|3}.log		

Log type	Default file name and folder name	Maximum disk usage	File-switching timing
	shared-folder\jp1base\log\JCOCMD\jcocmdrouter_trace{1|2|3}.log		
	shared-folder\jp1base\log\JCOCMD\JCOCMDCMD{1|2|3}.log		
Configuration management log	*Base-path*\log\route\JBSRT{1|2|3}.log		
	shared-folder\jp1base\log\route\JBSRT{1|2|3}.log		
Trace log file	*Base-path*\sys\tmp\event\logtrap\jelallog\jelallog{1|2|3|4|5}.log		
	Base-path\sys\tmp\event\logtrap\jelalelt\jelalelt{1|2|3|4|5}.log		
Integrated monitoring database application log	*Console-path*\log\evflow\EVFLOW_DBAPI{1|2...|16}.log	200 MB	12.5 MB
	Console-path\log\console\EVCONS_DBAPI{1|2|3|4|5}.log	50 MB	10 MB
	Console-path\log\command\CMD_DBAPI{1|2|3|4|5}.log	50 MB	10 MB
	shared-folder\jp1cons\log\evflow\EVFLOW_DBAPI{1|2...|16}.log	200 MB	12.5 MB
	shared-folder\jp1cons\log\console\EVCONS_DBAPI{1|2|3|4|5}.log	50 MB	10 MB
API log for the IM Configuration Management database	*Console-path*\log\evflow\EVFLOW_CFDBAPI{1|2|3}.log	30 MB	10 MB
	Console-path\log\console\EVCONS_CFDBAPI{1|2|3}.log	30 MB	10 MB
	Console-path\log\command\CMD_CFDBAPI{1|2|3}.log	30 MB	10 MB
	shared-folder\jp1cons\log\evflow\EVFLOW_CFDBAPI{1|2|3}.log	30 MB	10 MB
	shared-folder\jp1cons\log\console\EVCONS_CFDBAPI{1|2|3}.log	30 MB	10 MB
jcodbsetup command log	*Console-path*\log\imdb\jcodbsetup{1|2}.log	512 KB	256 KB
jcodbunsetup command log	*Console-path*\log\imdb\jcodbunsetup{1|2}.log	512 KB	256 KB

Note: The logs above are process-by-process trace logs. The process-by-process trace log is the log information that is output by each function of JP1/IM. It is output to a different log file depending on the function that is being used. Since the process-by-process trace log contains product information, its content is not made public.

#1: The file size may be dozens of kilobytes larger than this value.

#2: You can set this value to be from 64 kilobytes to 100 megabytes, as described in *Automated action environment definition file (action.conf.update)* (*2. Definition Files*) in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.

#3: You can set this value to be from 1 to 4,096 kilobytes, as described in *Automated action environment definition file (action.conf.update)* (*2. Definition Files*) in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.

#4: This is the value when the size of the action information file is the default value (626 kilobytes). You can use the following estimation formula to estimate the maximum disk usage by this file. Each time an action is performed, the size increases by 5 kilobytes.

((*action information file size* / 64 bytes) - 1) **x** 5 kilobytes

#5: The files are output to the jcochstat and jcochafmode 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* (*2. Definition Files*) in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.

#7: This file is used to output the memory information for inheriting data during correlation event generation, and therefore its size varies depending on the correlation event generation condition and the correlation-source event. For details about estimating the size of this file, see the JP1/IM - Manager release notes.

#8: This file is created when you start JP1/IM - Manager after enabling the response-waiting event management function.

Table 10–4: JP1/IM - Manager (JP1/IM - 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
	shared-folder\JP1Scope\log\jcsmain_trace_ping{1|2|3}.log	6 MB	2 MB
Logical host settings program log	*Scope-path*\log\jp1hasetup.{log|log.old}	2,000 KB	1,000 KB
Database operation API trace log	*Scope-path*\log\jcsmain_trace_db{1|2|3}.log	6 MB	2 MB
	shared-folder\JP1Scope\log\jcsmain_trace_db{1|2|3}.log	6 MB	2 MB
jcshostsexport command log	*Scope-path*\log\jcshostsexport{1|2|3}.log	6 MB	2 MB
	shared-folder\JP1Scope\log\jcshostsexport{1|2|3}.log	6 MB	2 MB
jcshostsimport command log	*Scope-path*\log\jcshostsimport{1|2|3}.log	6 MB	2 MB
	shared-folder\JP1Scope\log\jcshostsimport{1|2|3}.log	6 MB	2 MB
jcsdbsetup command log	*Scope-path*\log\jcsdbsetup{1|2|3}.log	6 MB	2 MB
	shared-folder\JP1Scope\log\jcsdbsetup{1|2|3}.log	6 MB	2 MB
jcschstat command log	*Scope-path*\log\jcschstat{1|2|3}.log	6 MB	2 MB
	shared-folder\JP1Scope\log\jcschstat{1|2|3}.log	6 MB	2 MB
jcsdbexport command log	*Scope-path*\log\jcsdbexport{1|2|3}.log	6 MB	2 MB

Log type	Default file name and folder name	Maximum disk usage	File-switching timing
	shared-folder\JP1Scope\log\jcsdbexport{1|2|3}.log	6 MB	2 MB
jcsdbimport command log	*Scope-path*\log\jcsdimport{1|2|3}.log	6 MB	2 MB
	shared-folder\JP1Scope\log\jcsdbimport{1|2|3}.log	6 MB	2 MB
jcsdbconvert command log	*Scope-path*\log\jcsdbconvert{1|2|3}.log	6 MB	2 MB
	shared-folder\JP1Scope\log\jcsdbconvert{1|2|3}.log	6 MB	2 MB
jp1csverup command log	*Scope-path*\log\jp1csverup_front{1|2|3}.log	6 MB	2 MB
jp1cshaverup command log	*shared-folder*\JP1Scope\log\jp1cshaverup_front{1|2|3}.log	6 MB	2 MB

Table 10–5: 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	*Manager-path*\log\imcf\jcfallogtrap{1|2|3|4|5|6|7|8|9|10}.log	20 MB	2 MB
	Manager-path\log\imcf\jcfallogtrap_VM_trace{1|2|3}.log	3 MB	1 MB
	Manager-path\log\imcf\jcfallogtrap_trace_auth{1|2|3|4|5|6|7|8|9|10}.log	20 MB	2 MB
	Manager-path\log\imcf\jcfmain{1|2|3|4|5|6|7|8|9|10}.log	20 MB	2 MB
	Manager-path\log\imcf\jcfmain_trace{1|2|3|4|5|6|7|8|9|10}.log	20 MB	2 MB
	Manager-path\log\imcf\jcfmain_VM_trace{1|2|3}.log	3 MB	1 MB
	shared-folder\JP1IMM\log\imcf\jcfallogtrap{1|2|3|4|5|6|7|8|9|10}.log	20 MB	2 MB
	shared-folder\JP1IMM\log\imcf\jcfallogtrap_VM_trace{1|2|3}.log	3 MB	1 MB
	shared-folder\JP1IMM\log\imcf\jcfallogtrap_trace_auth{1|2|3|4|5|6|7|8|9|10}.log	20 MB	2 MB
	shared-folder\JP1IMM\log\imcf\jcfmain{1|2|3|4|5|6|7|8|9|10}.log	20 MB	2 MB
	shared-folder\JP1IMM\log\imcf\jcfmain_trace{1|2|3|4|5|6|7|8|9|10}.log	20 MB	2 MB
	shared-folder\JP1IMM\log\imcf\jcfmain_VM_trace{1|2|3}.log	3 MB	1 MB

Log type	Default file name and folder name	Maximum disk usage	File-switching timing
Communication trace log	*Manager-path*\log\imcf \jcfmain_trace_com{1|2|3|4|5|6|7|8|9|10}.log	20 MB	2 MB
	Manager-path\log\imcf\jcfmain_ping{1|2|3|4|5|6|7|8|9|10}.log	20 MB	2 MB
	shared-folder\JP1IMM\log\imcf \jcfmain_trace_com{1|2|3|4|5|6|7|8|9|10}.log	20 MB	2 MB
	shared-folder\JP1IMM\log\imcf \jcfmain_ping{1|2|3|4|5|6|7|8|9|10}.log	20 MB	2 MB
Authentication trace log	*Manager-path*\log\imcf \jcfmain_trace_auth{1|2|3|4|5|6|7|8|9|10}.log	20 MB	2 MB
	shared-folder\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	*Manager-path*\log\imcf\jp1hasetup.{log|log.old}	2,000 KB	1,000 KB
Database operation API trace log	*Manager-path*\log\imcf \jcfmain_trace_db{1|2|3|4|5|6|7|8|9|10}.log	20 MB	2 MB
	shared-folder\JP1IMM\log\imcf \jcfmain_trace_db{1|2|3|4|5|6|7|8|9|10}.log	20 MB	2 MB
Command common log	*Manager-path*\log\imcf\jcfcommand{1|2|3}.log	3 MB	1 MB
	shared-folder\JP1IMM\log\imcf \jcfcommand{1|2|3}.log	3 MB	1 MB
jcfallogstart command log	*Manager-path*\log\imcf\jcfallogstart{1|2|3}.log	9 MB	3 MB
	Manager-path\log\imcf \jcfallogstart_VM_trace{1|2|3}.log	3 MB	1 MB
	shared-folder\JP1IMM\log\imcf \jcfallogstart{1|2|3}.log	9 MB	3 MB
	shared-folder\JP1IMM\log\imcf \jcfallogstart_VM_trace{1|2|3}.log	3 MB	1 MB
jcfallogstat command log	*Manager-path*\log\imcf\jcfallogstat{1|2|3}.log	9 MB	3 MB
	Manager-path\log\imcf \jcfallogstat_VM_trace{1|2|3}.log	3 MB	1 MB
	shared-folder\JP1IMM\log\imcf \jcfallogstat{1|2|3}.log	9 MB	3 MB
	shared-folder\JP1IMM\log\imcf \jcfallogstat_VM_trace{1|2|3}.log	3 MB	1 MB

Log type	Default file name and folder name	Maximum disk usage	File-switching timing
jcfallogstop command log	*Manager-path*\log\imcf\jcfallogstop{1|2|3}.log	9 MB	3 MB
	Manager-path\log\imcf\jcfallogstop_VM_trace{1|2|3}.log	3 MB	1 MB
	shared-folder\JP1IMM\log\imcf\jcfallogstop{1|2|3}.log	9 MB	3 MB
	shared-folder\JP1IMM\log\imcf\jcfallogstop_VM_trace{1|2|3}.log	3 MB	1 MB
jcfallogreload command log	*Manager-path*\log\imcf\jcfallogreload{1|2|3}.log	9 MB	3 MB
	Manager-path\log\imcf\jcfallogreload_VM_trace{1|2|3}.log	3 MB	1 MB
	shared-folder\JP1IMM\log\imcf\jcfallogreload{1|2|3}.log	9 MB	3 MB
	shared-folder\JP1IMM\log\imcf\jcfallogreload_VM_trace{1|2|3}.log	3 MB	1 MB
jcfallogdef command log	*Manager-path*\log\imcf\jcfallogdef{1|2|3}.log	9 MB	3 MB
	Manager-path\log\imcf\jcfallogdef_VM_trace{1|2|3}.log	3 MB	1 MB
	shared-folder\JP1IMM\log\imcf\jcfallogdef{1|2|3}.log	9 MB	3 MB
	shared-folder\JP1IMM\log\imcf\jcfallogdef_VM_trace{1|2|3}.log	3 MB	1 MB
jcfaleltstart command log	*Manager-path*\log\imcf\jcfaleltstart{1|2|3}.log	6 MB	2 MB
	Manager-path\log\imcf\jcfaleltstart_VM_trace{1|2|3}.log	3 MB	1 MB
	shared-folder\JP1IMM\log\imcf\jcfaleltstart{1|2|3}.log	6 MB	2 MB
	shared-folder\JP1IMM\log\imcf\jcfaleltstart_VM_trace{1|2|3}.log	3 MB	1 MB
jcfaleltstat command log	*Manager-path*\log\imcf\jcfaleltstat{1|2|3}.log	6 MB	2 MB
	Manager-path\log\imcf\jcfaleltstat_VM_trace{1|2|3}.log	3 MB	1 MB
	shared-folder\JP1IMM\log\imcf\jcfaleltstat{1|2|3}.log	6 MB	2 MB
	shared-folder\JP1IMM\log\imcf\jcfaleltstat_VM_trace{1|2|3}.log	3 MB	1 MB
jcfaleltstop command log	*Manager-path*\log\imcf\jcfaleltstop{1|2|3}.log	6 MB	2 MB
	Manager-path\log\imcf\jcfaleltstop_VM_trace{1|2|3}.log	3 MB	1 MB

Log type	Default file name and folder name	Maximum disk usage	File-switching timing
	shared-folder\JP1IMM\log\imcf\jcfaleltstop{1|2|3}.log	6 MB	2 MB
	shared-folder\JP1IMM\log\imcf\jcfaleltstop_VM_trace{1|2|3}.log	3 MB	1 MB
jcfaleltreload command log	*Manager-path*\log\imcf\jcfaleltreload{1|2|3}.log	6 MB	2 MB
	Manager-path\log\imcf\jcfaleltreload_VM_trace{1|2|3}.log	3 MB	1 MB
	shared-folder\JP1IMM\log\imcf\jcfaleltreload{1|2|3}.log	6 MB	2 MB
	shared-folder\JP1IMM\log\imcf\jcfaleltreload_VM_trace{1|2|3}.log	3 MB	1 MB
jcfaleltdef command log	*Manager-path*\log\imcf\jcfaleltdef{1|2|3}.log	6 MB	2 MB
	Manager-path\log\imcf\jcfaleltdef_VM_trace{1|2|3}.log	3 MB	1 MB
	shared-folder\JP1IMM\log\imcf\jcfaleltdef{1|2|3}.log	6 MB	2 MB
	shared-folder\JP1IMM\log\imcf\jcfaleltdef_VM_trace{1|2|3}.log	3 MB	1 MB
jcfcolvmesx command log	*Manager-path*\log\imcf\jcfcolvmesx_trace{1|2|3}.log	3 MB	1 MB
jcfcolvmscvmm command log	*Manager-path*\log\imcf\jcfcolvmscvmm_trace{1|2|3}.log	3 MB	1 MB
jcfcolvmvirtage command log	*Manager-path*\log\imcf\jcfcolvmvirtage_trace{1|2|3}.log	3 MB	1 MB
jcfcolvmvc command log	*Manager-path*\log\imcf\jcfcolvmvc_trace{1|2|3}.log	3 MB	1 MB
jcfcolvmkvm command log	*Manager-path*\log\imcf\jcfcolvmkvm_trace{1|2|3}.log	3 MB	1 MB
jcfcolvmhcsm command log	*Manager-path*\log\imcf\jcfcolvmhcsm_trace{1|2|3}.log	3 MB	1 MB
jcfexport command log	*Manager-path*\log\imcf\jcfexport_VM_trace{1|2|3}.log	3 MB	1 MB
	shared-folder\JP1IMM\log\imcf\jcfexport_VM_trace{1|2|3}.log	3 MB	1 MB
jcfimport command log	*Manager-path*\log\imcf\jcfimport_VM_trace{1|2|3}.log	3 MB	1 MB
	shared-folder\JP1IMM\log\imcf\jcfimport_VM_trace{1|2|3}.log	3 MB	1 MB
jcfmkhostsdata command log	*Manager-path*\log\imcf\jcfmkhostsdata_trace{1|2|3}.log	3 MB	1 MB
Stack trace log	*Manager-path*\log\imcf\javalog{1|2|3|4}.log	1 MB	At startup or 256 KB

Note: The logs above are process-by-process trace logs. The process-by-process trace log is the log information that is output by each function of JP1/IM. It is output to a different log file depending on the function that is being used. Since the process-by-process trace log contains product information, its content is not made public.

Table 10–6: 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]	*View-path*\log\VIEW{1|2|3}.log	30,720 KB	10,240 KB
	View-path\log\jp1conv{1|2|3|4}.log	20,480 KB	5,120 KB[2]
	View-path\log\jp1convM{1|2...|20}.log	102,400 KB	5,120 KB[2]
	View-path\log\jp1csov[_old].log	6,144 KB	3,072 KB[2]
	View-path\log\jp1csovM[_old].log	6,144 KB	3,072 KB[2]
	View-path\log\imrm\jp1rmJP1-IM-RM View{1|2|3}.log[3]	3,072 KB	1,024 KB
	View-path\log\imrm\jp1rmJP1-IM-RM View_dbg{1|2|3}.log[3]	3,072 KB	1,024 KB
	View-path\log\jrmview\view{1|2|3}.log[3]	3,072 KB	1,024 KB
Stack trace log[1]	*View-path*\log\javalog0{1|2}.log	512 KB	At startup or 256 KB
Integrated trace log	*system-drive*:\Program Files\Hitachi \HNTRLib2\spool\hntr2{1|2|3|4}.log	1,024 KB	256 KB
Product information log[1]	*View-path*\log\hliclib\hliclibtrc{1|2|3|4|5}.log	5 MB	1 MB
	View-path\log\hliclib\hlicliberr{1|2|3|4|5}.log	5 MB	1 MB
	View-path\log\hliclib\hliclibmgrtrc{1|2|3|4|5}.log	5 MB	1 MB
	View-path\log\hliclib\hliclibmgrerr{1|2|3|4|5}.log	5 MB	1 MB

Note: When you use Windows 8.1, Windows 8, Windows Server 2012, Windows 7, Windows Server 2008, or Windows Vista, replace *View-path* \log\ with *system-drive*:\ProgramData\Hitachi\jp1\jp1_default\JP1CoView\log\.

#1: This log is a process-by-process trace log. The process-by-process trace log is the log information that is output by each function of JP1/IM. It is output to a different log file depending on the function that is being used. Since the process-by-process trace log contains product information, its content is not made public.

#2: The file size may be dozens of kilobytes larger than this value.

#3: This log is output only when JP1/IM - Rule Operation is linked.

Table 10–7: 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[#]	*View-path*\log\jcfview\VIEW{1|2|3}.log	30 MB	10 MB
Stack trace log[#]	*View-path*\log\jcfjavalog{1|2}.log	512 KB	At startup or 256 KB
Integrated trace log	system-drive:\Program Files\Hitachi \HNTRLib2\spool\hntr2{1|2|3|4}.log	1,024 KB	256 KB

Note: When you use Windows 8.1, Windows 8, Windows Server 2012, Windows 7, Windows Server 2008, or Windows Vista, replace *View-path* `\log\` with *system-drive*`:\ProgramData\Hitachi\jp1\jp1_default\JP1CoView\log\`.

#: This log is a process-by-process trace log. The process-by-process trace log is the log information that is output by each function of JP1/IM. It is output to a different log file depending on the function that is being used. Since the process-by-process trace log contains product information, its content is not made public.

(2) In UNIX

The tables below show the default log files and folders that are output by the UNIX version of JP1/IM.

The *Log type* column lists the log types that are output by JP1/IM.

The *Default file name and folder name* column describes log file names as absolute paths when JP1/IM - Manager or JP1/Base is installed in the default mode. *Default file name and folder name* in a cluster operation system describes the log file names of shared folders as absolute paths.

The *Maximum disk usage* column shows the maximum disk space used by each log file. When there are multiple log files, the combined total is given.

The *File-switching timing* column shows how JP1/IM times output destination log file switching. When the file reaches the size shown in this column or when the event shown in this column occurs, the output destination is switched. If there are multiple log files and if the maximum disk usage is reached, files are overwritten, beginning with the ones that have the oldest update dates.

Table 10–8: JP1/IM - Manager (JP1/IM - Central Console) log files and folders (UNIX)

Log type	Default file name and folder name	Maximum disk usage	File-switching timing
Process management log[1]	`/var/opt/jp1cons/log/JCO_SPMD{1|2|3}.log`	384 KB	128 KB
	`/var/opt/jp1cons/log/JCO_SPMD_COMMAND{1|2|3}.log`	384 KB	128 KB
	shared-directory`/jp1cons/log/JCO_SPMD{1|2|3}.log`	384 KB	128 KB
	shared-directory`/jp1cons/log/JCO_SPMD_COMMAND{1|2|3}.log`	384 KB	128 KB
Stack trace log[1]	`/var/opt/jp1cons/log/javalog0{1|2|3|4}.log`	1 MB	At startup or 256 KB
	shared-directory`/jp1cons/log/javalog0{1|2|3|4}.log`	1 MB	At startup or 256 KB
JP1/IM startup log[1]	`/var/opt/jp1cons/log/jco_start.log[.old]`	1 KB	At startup
	shared-directory`/jp1cons/log/jco_start_`*logical-host-name*`.log[.old]`	1 KB	At startup
JP1/IM kill log[1,2]	*shared-directory*`/jp1cons/log/jco_killall.cluster{none|1|2|3|4}`	2 KB	When the `jco_killall.cluster` command is executed
Setup log	`/var/opt/jp1cons/log/JCO_SETUP/jco_setup.log`	100 KB	During installation
	`/var/opt/jp1cons/log/JCO_SETUP/jco_inst.log`[1]	100 KB	During installation

Log type	Default file name and folder name	Maximum disk usage	File-switching timing
	/var/opt/jp1cons/log/jco_setup/*logical-host-name*/jco_setup.log[1]	100 KB	During installation
	/var/opt/jp1cons/log/jco_setup/*logical-host-name*/reg.txt[1]	100 KB	During installation
	/var/opt/jp1cons/log/jco_setup/*logical-host-name*/reg_def.txt[1]	100 KB	During installation
	/var/opt/jp1cons/log/command/comdef[_old].log[1]	512 KB	256 KB
Event console log[1]	/var/opt/jp1cons/log/console/EVCONS{1|2|3}.log	30,720 KB	10,240 KB
	/var/opt/jp1cons/log/console/jp1cons{1|2|3|4}.log	20,480 KB	5,120 KB[3]
	/var/opt/jp1cons/log/console/JCOAPI{1|2|3}.log	96 KB	32 KB
	/var/opt/jp1cons/log/console/jp1consM{1|2...|20}.log	100 MB	5 MB[3]
	/var/opt/jp1cons/log/console/jp1filterDef{1|2|3|4|5}.log	100 MB	20 MB
	/var/opt/jp1cons/log/console/jp1bizGroupDef{1|2}.log	10 MB	5 MB
	/var/opt/jp1cons/log/console/evtcon_exe{1|2|3}.log	256 KB **x 3**	256 KB
	/var/opt/jp1cons/log/console/jp1cmdButtonDef{1|2|3|4|5}.log	25 MB	5 MB
	shared-directory/jp1cons/log/console/EVCONS{1|2|3}.log	30,720 KB	10,240 KB
	shared-directory/jp1cons/log/console/jp1cons{1|2|3|4}.log	20,480 KB	5,120 KB[3]
	shared-directory/jp1cons/log/console/JCOAPI{1|2|3}.log	96 KB	32 KB
	shared-directory/jp1cons/log/console/jp1consM{1|2...|20}.log	100 MB	5 MB[3]
	shared-directory/jp1cons/log/console/jp1filterDef{1|2|3|4|5}.log	100 MB	20 MB
	shared-directory/jp1cons/log/console/jp1bizGroupDef{1|2}.log	10 MB	5 MB
	shared-directory/jp1cons/log/console/evtcon_exe{1|2|3}.log	256 KB **x 3**	256 KB
	shared-directory/jp1cons/log/console/jp1cmdButtonDef{1|2|3|4|5}.log	25 MB	5 MB
Automated action trace log[1]	/var/opt/jp1cons/log/action/JCAMAIN{1|2|3|4|5}.log[4]	25,600 KB	5,120 KB

Log type	Default file name and folder name	Maximum disk usage	File-switching timing
	shared-directory/jp1cons/log/action/ JCAMAIN{1|2|3|4|5}.log[#4]	25,600 KB	5,120 KB
Action information file[#1]	/var/opt/jp1cons/log/action/ actinf.log	626 KB[#5]	No switching
		For Linux (IPF) 1,094 KB[#5]	
	shared-directory/jp1cons/log/action/ actinf.log	626 KB[#5]	No switching
		For Linux (IPF) 1,094 KB [#5]	
Action host name file[#1]	/var/opt/jp1cons/log/action/acttxt{1| 2}.log	48.9 MB[#6]	When the action information file wraps around
	shared-directory/jp1cons/log/action/ acttxt{1|2}.log	48.9 MB[#6]	When the action information file wraps around
Action re-execution file[#1]	/var/opt/jp1cons/log/action/ actreaction	300 MB	When system switching occurs
	shared-directory/jp1cons/log/action/ actreaction	300 MB	When system switching occurs
jcochafmode, jcochstat, and jcoevtreport command trace logs[#1,#7]	/var/opt/jp1cons/log/command/CMD{1|2| 3}.log	3,072 KB	1,024 KB
	/var/opt/jp1cons/log/command/ jp1cons_cmd{1|2}.log	12,288 KB	6,144 KB
	/var/opt/jp1cons/log/command/ jp1consM_cmd{1|2}.log	12,288 KB	6,144 KB
Plug-in log[#1]	/var/opt/jp1cons/log/command/ jcoplugin{1|2|3}.log	3 MB	1 MB
Reporting status storage file[#1]	/var/opt/jp1cons/log/notice/ notice_stat.dat	72B	No switching
	shared-directory/jp1cons/log/notice/ notice_stat.dat	72B	No switching
Action definition backup file[#1]	/var/opt/jp1cons/log/action/ actdefbk.conf	2,048 KB	No switching
	shared-directory/jp1cons/log/action/ actdefbk.conf	2,048 KB	No switching
Event base trace log[#1]	/var/opt/jp1cons/log/evflow/EVFLOW{1| 2|3|4|5|6|7|8|9|10}.log	100 MB	10 MB
	/var/opt/jp1cons/log/evflow/ jp1evflowM{1|2...|20}.log	100 MB	5 MB
	/var/opt/jp1cons/log/evflow/ jp1actDef{1|2|3|4|5}.log	25 MB	5 MB
	/var/opt/jp1cons/log/evflow/ jp1chsevDef{1|2|3|4|5}.log	25 MB	5 MB

Log type	Default file name and folder name	Maximum disk usage	File-switching timing
	`/var/opt/jp1cons/log/evflow/` `jp1hostmapDef{1|2|3|4|5}.log`	25 MB	5 MB
	`/var/opt/jp1cons/log/evflow/` `evflow_exe{1|2|3}.log`	256 KB **x** 3	256 KB
	shared-directory`/jp1cons/log/evflow/` `EVFLOW{1|2|3|4|5|6|7|8|9|10}.log`	100 MB	10 MB
	shared-directory`/jp1cons/log/evflow/` `jp1evflowM{1|2...|20}.log`	100 MB	5 MB
	shared-directory`/jp1cons/log/evflow/` `jp1actDef{1|2|3|4|5}.log`	25 MB	5 MB
	shared-directory`/jp1cons/log/evflow/` `jp1chsevDef{1|2|3|4|5}.log`	25 MB	5 MB
	shared-directory`/jp1cons/log/evflow/` `jp1hostmapDef{1|2|3|4|5}.log`	25 MB	5 MB
	shared-directory`/jp1cons/log/evflow/` `evflow_exe{1|2|3}.log`	256 KB **x** 3	256 KB
Matching information file[1]	`/var/opt/jp1cons/log/evflow/` `evflowinf.log`	12B	No switching
		For Linux (IPF) 24 MB	No switching
	shared-directory`/jp1cons/log/evflow/` `evflowinf.log`	12B	No switching
		For Linux (IPF) 24 MB	No switching
Event base error log[1]	`/var/opt/jp1cons/log/evflow/` `jp1evflow{1|2|3|4}.log`	20,480 KB	5,120 KB
	shared-directory`/jp1cons/log/evflow/` `jp1evflow{1|2|3|4}.log`	20,480 KB	5,120 KB
Automated action error log[1]	`/var/opt/jp1cons/log/action/jp1act{1|` `2|3}.log`	15,360 KB	5,120 KB
	shared-directory`/jp1cons/log/action/` `jp1act{1|2|3}.log`	15,360 KB	5,120 KB
Correlation event generation history file[1]	`/var/opt/jp1cons/operation/evgen/` `egs_discrim{1|2|3}.log`[9]	30 MB[9]	10 MB[9]
	shared-directory`/jp1cons/operation/evgen/` `egs_discrim{1|2|3}.log`[9]	30 MB[9]	10 MB[9]
Correlation event generation trace log [1]	`/var/opt/jp1cons/log/evgen/EVGEN{1|2|` `3}.log`	15 MB	5 MB
	`/var/opt/jp1cons/log/evgen/` `evgen_exe{1|2|3}.log`	256 KB **x** 3	256 KB
	shared-directory`/jp1cons/log/evgen/` `EVGEN{1|2|3}.log`	15 MB	5 MB
	shared-directory`/jp1cons/log/evgen/` `evgen_exe{1|2|3}.log`	256 KB **x** 3	256 KB

Log type	Default file name and folder name	Maximum disk usage	File-switching timing
Correlation event generation individual log (for Event Generation Service)[#1]	`/var/opt/jp1cons/log/evgen/jp1egs{1|2}.log`	20 MB	10 MB
	`/var/opt/jp1cons/log/evgen/jp1egsM{1|2}.log`	20 MB	10 MB
	shared-directory`/jp1cons/log/evgen/jp1egs{1|2}.log`	20 MB	10 MB
	shared-directory`/jp1cons/log/evgen/jp1egsM{1|2}.log`	20 MB	10 MB
Correlation event generation individual log (for commands)[#1]	`/var/opt/jp1cons/log/evgen/jp1egs_cmd{1|2|3|4}.log`	20 MB	5 MB
	`/var/opt/jp1cons/log/evgen/jp1egsM_cmd{1|2|3|4}.log`	20 MB	5 MB
Correlation event generation stack trace log[#1,#8]	`/var/opt/jp1cons/log/evgen/javalog0{1|2|3|4}.log`	1 MB	At startup or 256 KB
	shared-directory`/jp1cons/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/jp1cons/log/evgen/egs_discrim_info{1|2|3|4}.dat`	312 MB[#10]	At termination
	shared-directory`/jp1cons/log/evgen/egs_discrim_info{1|2|3|4}.dat`	312 MB[#10]	At termination
Correlation event generation definition application log[#1]	`/var/opt/jp1cons/log/evgen/jp1egsDefine{1|2}.log`	10 MB	5 MB
	shared-directory`/jp1cons/log/evgen/jp1egsDefine{1|2}.log`	10 MB	5 MB
File for accumulated response-waiting events[#1, #11]	`/var/opt/jp1cons/log/response/resevent.dat`	40 MB	No switching
	shared-directory`/jp1cons/log/response/resevent.dat`	40 MB	No switching
Backup file for accumulated response-waiting events[#1, #11]	`/var/opt/jp1cons/log/response/resevent.dat.dump`	40 MB	No switching
	shared-directory`/jp1cons/log/response/resevent.dat.dump`	40 MB	No switching
Integrated monitoring database application log[#1]	`/var/opt/jp1cons/log/evflow/EVFLOW_DBAPI{1|2...|16}.log`	200 MB	12.5 MB
	`/var/opt/jp1cons/log/console/EVCONS_DBAPI{1|2|3|4|5}.log`	50 MB	10 MB
	`/var/opt/jp1cons/log/command/CMD_DBAPI{1|2|3|4|5}.log`	50 MB	10 MB
	shared-directory`/jp1cons/log/evflow/EVFLOW_DBAPI{1|2...|16}.log`	200 MB	12.5 MB
	shared-directory`/jp1cons/log/console/EVCONS_DBAPI{1|2|3|4|5}.log`	50 MB	10 MB

Log type	Default file name and folder name	Maximum disk usage	File-switching timing
API log for the IM Configuration Management database[1]	`/var/opt/jp1cons/log/evflow/` `EVFLOW_CFDBAPI{1|2|3|4|5}.log`	30 MB	10 MB
	`/var/opt/jp1cons/log/console/` `EVCONS_CFDBAPI{1|2|3}.log`	30 MB	10 MB
	`/var/opt/jp1cons/log/command/` `CMD_CFDBAPI{1|2|3}.log`	30 MB	10 MB
	shared-directory`/jp1cons/log/evflow/` `EVFLOW_CFDBAPI{1|2|3|4|5}.log`	30 MB	10 MB
	shared-directory`/jp1cons/log/console/` `EVCONS_CFDBAPI{1|2|3}.log`	30 MB	10 MB
`jcodbsetup` command log[1]	`/var/opt/jp1cons/log/imdb/` `jcodbsetup{1|2}.log`	512 KB	256 KB
`jcodbunsetup` command log[1]	`/var/opt/jp1cons/log/imdb/` `jcodbunsetup{1|2}.log`	512 KB	256 KB
Command execution history directory[1]	`/var/opt/jp1base/log/COMMAND/`	See the *Job Management Partner 1/Base User's Guide*.	
	shared-directory`/jp1base/log/COMMAND`		
Remote command log[1]	`/var/opt/jp1base/log/JCOCMD/` `jcocmd_result{1|2|3}.log`		
	`/var/opt/jp1base/log/JCOCMD/` `jcocmdapi{1|2|3}.log`		
	`/var/opt/jp1base/log/JCOCMD/` `jcocmdapi_trace{1|2|3}.log`		
	`/var/opt/jp1base/log/JCOCMD/` `jcocmdcmc{1|2|3}.log`		
	`/var/opt/jp1base/log/JCOCMD/` `jcocmdcmc_trace{1|2|3}.log`		
	`/var/opt/jp1base/log/JCOCMD/` `jcocmdcom{1|2|3}.log`		
	`/var/opt/jp1base/log/JCOCMD/` `jcocmdcom_trace{1|2|3}.log`		
	`/var/opt/jp1base/log/JCOCMD/` `jcocmdexe{1|2|3}.log`		
	`/var/opt/jp1base/log/JCOCMD/` `jcocmdexe_trace{1|2|3}.log`		
	`/var/opt/jp1base/log/JCOCMD/` `jcocmdrouter{1|2|3}.log`		
	`/var/opt/jp1base/log/JCOCMD/` `jcocmdrouter_trace{1|2|3}.log`		
	`/var/opt/jp1base/log/JCOCMD/` `JCOCMDCMD{1|2|3}.log`		
	shared-directory`/jp1base/log/JCOCMD/` `jcocmd_result{1|2|3}.log`		

Log type	Default file name and folder name	Maximum disk usage	File-switching timing
	shared-directory/jp1base/log/JCOCMD/ jcocmdapi{1|2|3}.log		
	shared-directory/jp1base/log/JCOCMD/ jcocmdapi_trace{1|2|3}.log		
	shared-directory/jp1base/log/JCOCMD/ jcocmdcmc{1|2|3}.log		
	shared-directory/jp1base/log/JCOCMD/ jcocmdcmc_trace{1|2|3}.log		
	shared-directory/jp1base/log/JCOCMD/ jcocmdcom{1|2|3}.log		
	shared-directory/jp1base/log/JCOCMD/ jcocmdcom_trace{1|2|3}.log		
	shared-directory/jp1base/log/JCOCMD/ jcocmdexe{1|2|3}.log		
	shared-directory/jp1base/log/JCOCMD/ jcocmdexe_trace{1|2|3}.log		
	shared-directory/jp1base/log/JCOCMD/ jcocmdrouter{1|2|3}.log		
	shared-directory/jp1base/log/JCOCMD/ jcocmdrouter_trace{1|2|3}.log		
	shared-directory/jp1base/log/JCOCMD/ JCOCMDCMD{1|2|3}.log		
Configuration management log[1]	/var/opt/jp1base/log/route/JBSRT{1|2|3}.log		
	shared-directory/jp1base/log/route/ JBSRT{1|2|3}.log		
Trace log file[1]	/var/opt/jp1base/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)* (*2. Definition Files*) in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.

#5: You can set this value to be from 1 to 4,096 kilobytes (For Linux (IPF), from 1 to 7,168 kilobytes) as described in *Automated action environment definition file (action.conf.update)* (*2. Definition Files*) in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.

#6: This is the value when the size of the action information file is the default value (626 kilobytes). You can use the following estimation formula to estimate the maximum disk usage by this file. Each time an action is performed, the size increases by 5 kilobytes.

((*action information file size* / 64 bytes) - 1) **x** 5 kilobytes

#7: The files are output to the jcochstat and jcochafmode command trace logs on the physical host in a cluster operation system as well.

#8: This log is not output in Solaris.

#9: You can change the file count and file size as described in *Correlation event generation environment definition file* (*2. Definition Files*) in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.

#10: 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.

#11: This file is created when you start JP1/IM - Manager after enabling the response-waiting event management function.

Table 10–9: JP1/IM - Manager (JP1/IM - Central Scope) log files and folders (UNIX)

Log type	Default file name and folder name	Maximum disk usage	File-switching timing
Central Scope trace log#	`/var/opt/jp1scope/log/jcsmain{1|2|3}.log`	6 MB	2 MB
	`/var/opt/jp1scope/log/jcsmain_trace{1|2|3}.log`	6 MB	2 MB
	shared-directory`/jp1scope/log/jcsmain{1|2|3}.log`	6 MB	2 MB
	shared-directory`/jp1scope/log/jcsmain_trace{1|2|3}.log`	6 MB	2 MB
Communication trace log	`/var/opt/jp1scope/log/jcsmain_trace_com{1|2|3}.log`	6 MB	2 MB
	shared-directory`/jp1scope/log/jcsmain_trace_com{1|2|3}.log`	6 MB	2 MB
	`/var/opt/jp1scope/log/jcsmain_trace_ping{1|2|3}.log`	6 MB	2 MB
	shared-directory`/jp1scope/log/jcsmain_trace_ping{1|2|3}.log`	6 MB	2 MB
Database operation API trace log	`/var/opt/jp1scope/log/jcsmain_trace_db{1|2|3}.log`	6 MB	2 MB
	shared-directory`/jp1scope/log/jcsmain_trace_db{1|2|3}.log`	6 MB	2 MB
`jcshostsexport` command log	`/var/opt/jp1scope/log/jcshostsexport{1|2|3}.log`	6 MB	2 MB
	shared-directory`/jp1scope/log/jcshostsexport{1|2|3}.log`	6 MB	2 MB
`jcshostsimport` command log	`/var/opt/jp1scope/log/jcshostsimport{1|2|3}.log`	6 MB	2 MB
	shared-directory`/jp1scope/log/jcshostsimport{1|2|3}.log`	6 MB	2 MB
`jcsdbsetup` command log	`/var/opt/jp1scope/log/jcsdbsetup{1|2|3}.log`	6 MB	2 MB
	shared-directory`/jp1scope/log/jcsdbsetup{1|2|3}.log`	6 MB	2 MB
`jcschstat` command log	`/var/opt/jp1scope/log/jcschstat{1|2|3}.log`	6 MB	2 MB
	shared-directory`/jp1scope/log/jcschstat{1|2|3}.log`	6 MB	2 MB
`jcsdbimport` command log	`/var/opt/jp1scope/log/jcsdbimport{1|2|3}.log`	6 MB	2 MB

Log type	Default file name and folder name	Maximum disk usage	File-switching timing
	shared-directory/jp1scope/log/ jcsdbimport{1|2|3}.log	6 MB	2 MB
jcsdbexport command log	/var/opt/jp1scope/log/jcsdbexport{1|2|3}.log	6 MB	2 MB
	shared-directory/jp1scope/log/ jcsdbexport{1|2|3}.log	6 MB	2 MB
Setup log	/var/opt/jp1scope/log/JCS_SETUP/ jcs_setup.log	100 KB	During installation
	/var/opt/jp1scope/log/jcs_setup/*logical-host-name*/jcs_setup.log	100 KB	During installation
	/var/opt/jp1scope/log/jcs_setup/*logical-host-name*/reg.txt	100 KB	During installation
	/var/opt/*jp1scope/log/jcs_setup/logical-host-name*/reg_def.txt	100 KB	During installation

#: This log is a process-by-process trace log. The process-by-process trace log is the log information that is output by each function of JP1/IM. It is output to a different log file depending on the function that is being used. Since the process-by-process trace log contains product information, its content is not made public.

Table 10–10: JP1/IM - Manager (IM Configuration Management) log files and folders (UNIX)

Log type	Default file name and folder name	Maximum disk usage	File-switching timing
IM Configuration Management trace log	/var/opt/jp1imm/log/imcf/ jcfallogtrap{1|2|3|4|5|6|7|8|9|10}.log	20 MB	2 MB
	/var/opt/jp1imm/log/imcf/ jcfallogtrap_VM_trace{1|2|3}.log	3 MB	1 MB
	/var/opt/jp1imm/log/imcf/ jcfallogtrap_trace_auth{1|2|3|4|5|6|7|8|9|10}.log	20 MB	2 MB
	/var/opt/jp1imm/log/imcf/jcfmain{1|2|3|4|5|6|7|8|9|10}.log	20 MB	2 MB
	/var/opt/jp1imm/log/imcf/ jcfmain_trace{1|2|3|4|5|6|7|8|9|10}.log	20 MB	2 MB
	/var/opt/jp1imm/log/imcf/ jcfmain_VM_trace{1|2|3}.log	3 MB	1 MB
	shared-directory/jp1imm/log/imcf/ jcfallogtrap{1|2|3|4|5|6|7|8|9|10}.log	20 MB	2 MB
	shared-directory/jp1imm/log/imcf/ jcfallogtrap_VM_trace{1|2|3}.log	3 MB	1 MB
	shared-directory/jp1imm/log/imcf/ jcfallogtrap_trace_auth{1|2|3|4|5|6|7|8|9|10}.log	20 MB	2 MB
	shared-directory/jp1imm/log/imcf/ jcfmain{1|2|3|4|5|6|7|8|9|10}.log	20 MB	2 MB

Log type	Default file name and folder name	Maximum disk usage	File-switching timing
	shared-directory/jp1imm/log/imcf/ jcfmain_trace{1|2|3|4|5|6|7|8|9| 10}.log	20 MB	2 MB
	shared-directory/jp1imm/log/imcf/ jcfmain_VM_trace{1|2|3}.log	3 MB	1 MB
Communication trace log	/var/opt/jp1imm/log/imcf/ jcfmain_trace_com{1|2|3|4|5|6|7|8|9| 10}.log	20 MB	2 MB
	/var/opt/jp1imm/log/imcf/ jcfmain_ping{1|2|3|4|5|6|7|8|9| 10}.log	20 MB	2 MB
	shared-directory/jp1imm/log/imcf/ jcfmain_trace_com{1|2|3|4|5|6|7|8|9| 10}.log	20 MB	2 MB
	shared-directory/jp1imm/log/imcf/ jcfmain_ping{1|2|3|4|5|6|7|8|9| 10}.log	20 MB	2 MB
Authentication trace log	/var/opt/jp1imm/log/imcf/ jcfmain_trace_auth{1|2|3|4|5|6|7|8|9| 10}.log	20 MB	2 MB
	shared-directory/jp1imm/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/jp1imm/log/imcf/ jcfmain_trace_db{1|2|3|4|5|6|7|8|9| 10}.log	20 MB	2 MB
	shared-directory/jp1imm/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/jp1imm/log/imcf/ jcfcommand{1|2|3}.log	3 MB	1 MB
	shared-directory/jp1imm/log/imcf/ jcfcommand{1|2|3}.log	3 MB	1 MB
jcfallogstart command log	/var/opt/jp1imm/log/imcf/ jcfallogstart{1|2|3}.log	9 MB	3 MB
	/var/opt/jp1imm/log/imcf/ jcfallogstart_VM_trace{1|2|3}.log	3 MB	1 MB
	shared-directory/jp1imm/log/imcf/ jcfallogstart{1|2|3}.log	9 MB	3 MB
	shared-directory/jp1imm/log/imcf/ jcfallogstart_VM_trace{1|2|3}.log	3 MB	1 MB
jcfallogstat command log	/var/opt/jp1imm/log/imcf/ jcfallogstat{1|2|3}.log	9 MB	3 MB
	/var/opt/jp1imm/log/imcf/ jcfallogstat_VM_trace{1|2|3}.log	3 MB	1 MB
	shared-directory/jp1imm/log/imcf/ jcfallogstat{1|2|3}.log	9 MB	3 MB

10. Troubleshooting

Log type	Default file name and folder name	Maximum disk usage	File-switching timing
	shared-directory/jp1imm/log/imcf/ jcfallogstat_VM_trace{1|2|3}.log	3 MB	1 MB
jcfallogstop command log	/var/opt/jp1imm/log/imcf/ jcfallogstop{1|2|3}.log	9 MB	3 MB
	/var/opt/jp1imm/log/imcf/ jcfallogstop_VM_trace{1|2|3}.log	3 MB	1 MB
	shared-directory/jp1imm/log/imcf/ jcfallogstop{1|2|3}.log	9 MB	3 MB
	shared-directory/jp1imm/log/imcf/ jcfallogstop_VM_trace{1|2|3}.log	3 MB	1 MB
jcfallogreload command log	/var/opt/jp1imm/log/imcf/ jcfallogreload{1|2|3}.log	9 MB	3 MB
	/var/opt/jp1imm/log/imcf/ jcfallogreload_VM_trace{1|2|3}.log	3 MB	1 MB
	shared-directory/jp1imm/log/imcf/ jcfallogreload{1|2|3}.log	9 MB	3 MB
	shared-directory/jp1imm/log/imcf/ jcfallogreload_VM_trace{1|2|3}.log	3 MB	1 MB
jcfallogdef command log	/var/opt/jp1imm/log/imcf/ jcfallogdef{1|2|3}.log	9 MB	3 MB
	/var/opt/jp1imm/log/imcf/ jcfallogdef_VM_trace{1|2|3}.log	3 MB	1 MB
	shared-directory/jp1imm/log/imcf/ jcfallogdef{1|2|3}.log	9 MB	3 MB
	shared-directory/jp1imm/log/imcf/ jcfallogdef_VM_trace{1|2|3}.log	3 MB	1 MB
jcfcolvmesx command log	*Manager-path*\log\imcf \jcfcolvmesx_trace{1|2|3}.log	3 MB	1 MB
jcfcolvmvirtage command log	*Manager-path*\log\imcf \jcfcolvmvirtage_trace{1|2|3}.log	3 MB	1 MB
jcfcolvmvc command log	*Manager-path*\log\imcf \jcfcolvmvc_trace{1|2|3}.log	3 MB	1 MB
jcfcolvmkvm command log	*Manager-path*\log\imcf \jcfcolvmkvm_trace{1|2|3}.log	3 MB	1 MB
jcfcolvmhcsm command log	*Manager-path*\log\imcf \jcfcolvmhcsm_trace{1|2|3}.log	3 MB	1 MB
jcfexport command log	/var/opt/jp1imm/log/imcf/ jcfexport_VM_trace{1|2|3}.log	3 MB	1 MB
	shared-directory/jp1imm/log/imcf/ jcfexport_VM_trace{1|2|3}.log	3 MB	1 MB
jcfimport command log	/var/opt/jp1imm/log/imcf/ jcfimport_VM_trace{1|2|3}.log	3 MB	1 MB
	shared-directory/jp1imm/log/imcf/ jcfimport_VM_trace{1|2|3}.log	3 MB	1 MB

Log type	Default file name and folder name	Maximum disk usage	File-switching timing
`jcfmkhostsdata` command log	`/var/opt/jp1imm/log/imcf/` `jcfmkhostsdata_trace{1|2|3}.log`	3 MB	1 MB
Stack trace log	`/var/opt/jp1imm/log/imcf/javalog0{1|` `2|3|4}.log`	1 MB	At startup or 256 KB
Setup log	`/var/opt/jp1imm/log/imcf/JCF_SETUP/` `jcf_setup.log`	100 KB	During installation
	`/var/opt/jp1imm/log/imcf/JCF_SETUP/` *logical-host-name*`/jcf_setup.log`	100 KB	During installation

Note: The logs above are process-by-process trace logs. The process-by-process trace log is the log information that is output by each function of JP1/IM. It is output to a different log file depending on the function that is being used. Since the process-by-process trace log contains product information, its content is not made public.

10.3 Data that needs to be collected when a problem occurs

This section describes the data that needs to be collected when a problem occurs.

Note that JP1 provides *data collection tools* for batch-collecting the necessary data. The data that can be collected using a data collection tool is the OS system information and JP1 information. The following subsections explain data collection in Windows and UNIX.

10.3.1 In Windows

(1) OS system information

You need to collect the OS-related information listed in the table below. These types of information can be collected using data collection tools.

The two data collection tools (the `jim_log.bat` command and the `jcoview_log.bat` command) collect different types of data. When the `jim_log.bat` command is executed, all of the data listed in the table below is collected. The data that can be collected by executing the `jcoview_log.bat` command is indicated in the far-right column.

Table 10–11: OS system information (Windows)

Information type	Collected data	File name[#1]	View
Data collection date/time	• `date /t` execution result • `time /t` execution result	`date.log`	Y
Hitachi integrated installer log file	Files under *Windows-installation-folder*`\Temp\HCDINST\`	Copies of the files indicated at left	Y
JP1/IM - Manager installation/uninstallation log file	*Windows-installation-folder*`\Temp\HITACHI_JP1_INST_LOG\jp1imm_inst{1|2|3|4|5}.log`	`jp1imm_inst{1|2|3|4|5}.log`	Δ
JP1/IM - View installation/uninstallation log file	*Windows-installation-folder*`\Temp\HITACHI_JP1_INST_LOG\jp1coview_inst{1|2|3|4|5}.log`	`jp1coview_inst{1|2|3|4|5}.log`	Y
JP1/Base installation/uninstallation log file	*Windows-installation-folder*`\Temp\HITACHI_JP1_INST_LOG\jp1base_inst{1|2|3|4|5}.log`	`jp1base_inst{1|2|3|4|5}.log`	Δ
Product information log file	Files under *Windows-installation-folder*`\Temp\jp1common\`	Copies of the files indicated at left	Y
Host name settings that are set in the machine	*system-root-folder*`\system32\drivers\etc\hosts`	`hosts`	Y
Service port settings that are set in the machine	*system-root-folder*`\system32\drivers\etc\services`	`services`	Y
NIC installation status	`ipconfig /all` execution result	`ipconfig.log`	Y
Startup service list	`net start` execution result	`netstart.log`	Y
Network statistical information	`netstat -na` execution result	`netstat.log`	Y

Information type	Collected data	File name[#1]	View
Machine's environment variable	`set` execution result	`set.log`	Y
Machine's system information	`msinfo32 /report-file-name` execution result	`msinfo32.log`	Y
Registry information	Content of the registry `HKEY_LOCAL_MACHINE\SOFTWARE\HITACHI` or `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\HITACHI` collected by the `regedit` command	`hitachi_reg.txt`	Y
Product information file	Files under *system-drive*:`Program Files\jp1common\`	Copies of the files indicated at left	Y
JP1/IM - Manager installation information	*system-drive*:`Program Files\InstallShield Installation Information\{BB5D25EC-537C-4794-BD7A-C7E22CC4AD30}\setup.ini`	`imm_setup.ini`	Δ
JP1/IM - Manager installation log file	*system-drive*:`Program Files\InstallShield Installation Information\{BB5D25EC-537C-4794-BD7A-C7E22CC4AD30}\setup.ilg`	`imm_setup.ilg`	Δ
JP1/Base installation information	*system-drive*:`Program Files\InstallShield Installation Information\{F8C71F7C-E5DE-11D3-A21E-006097C00EBC}\setup.ini`	`base_setup.ini`	Δ
JP1/Base installation log file	*system-drive*:`Program Files\InstallShield Installation Information\{F8C71F7C-E5DE-11D3-A21E-006097C00EBC}\setup.ilg`	`base_setup.ilg`	Δ
JP1/IM - View installation information	*system-drive*:`Program Files\InstallShield Installation Information\{6C01AA81-B45B-4AA6-ACE9-AC9A86B19F1F}\setup.ini`	`imv_setup.ini`	Y
JP1/IM - View installation log file	*system-drive*:`Program Files\InstallShield Installation Information\{6C01AA81-B45B-4AA6-ACE9-AC9A86B19F1F}\setup.ilg`	`imv_setup.ilg`	Y
JP1/Base access permission information (installation folder)	`cacls` *Base-path* execution result	`cacls_jp1base.log`	Δ
	`cacls` *shared-folder*`\JP1Base` execution result[#2]	`cacls_jp1base.log`	--
JP1/Base access permission information (log folder)	`cacls` *Base-path*`\log` execution result	`cacls_jp1base_log.log`	Δ
	`cacls` *shared-folder*`\JP1Base\log` execution result[#2]	`cacls_jp1base_log.log`	--

Information type	Collected data	File name[1]	View
JP1/Base access permission information (command execution history folder)	cacls *Base-path*\log\COMMAND execution result	cacls_jp1base_log_COMMAND.log	Δ
	cacls *shared-folder*\JP1Base\log\COMMAND execution result[2]	cacls_jp1base_log_COMMAND.log	--
JP1/Base access permission information (event database folder)	cacls *Base-path*\sys execution result	cacls_jp1base_sys.log	Δ
JP1/Base access permission information (event database folder)	cacls *Base-path*\sys\event execution result	cacls_jp1base_sys_event.log	Δ
	cacls *shared-folder*\JP1Base\event execution result[2]	cacls_jp1base_event.log	--
JP1/Base access permission information (event database folder)	cacls *Base-path*\sys\event\servers execution result	cacls_jp1base_sys_event_servers.log	Δ
JP1/Base access permission information (event database folder)	cacls *Base-path*\sys\event\servers\default execution result	cacls_jp1base_sys_event_servers_default.log	Δ
JP1/IM - Manager (JP1/IM - Central Console) access permission information (installation folder)	cacls *Console-path* execution result	cacls_jp1cons.log	Δ
	cacls *shared-folder*\JP1Cons execution result[2]	cacls_jp1cons.log	--
JP1/IM - Manager (JP1/IM - Central Console) access permission information (log folder)	cacls *Console-path*\log execution result	cacls_jp1cons_log.log	Δ
	cacls *shared-folder*\JP1Cons\log execution result[2]	cacls_jp1cons_log.log	--
JP1/IM - Manager (JP1/IM - Central Console) access permission information (correlation history folder)	cacls *Console-path*\operation execution result	cacls_jp1cons_operation.log	Δ
	cacls *shared-folder*\JP1Cons\operation execution result[2]	cacls_jp1cons_operation.log	--
JP1/IM - Manager (JP1/IM - Central Console) access permission information (correlation event generation history folder)	cacls *Console-path*\operation\evgen execution result	cacls_jp1cons_operation_evgen.log	Δ
	cacls *shared-folder*\JP1Cons\operation\evgen execution result[2]	cacls_jp1cons_operation_evgen.log	--
JP1/IM - View access permission information (installation folder)	cacls *View-path* execution result	cacls_jp1coview.log	Y
JP1/IM - View access permission information (log folder)	For Windows other than Windows 8.1, Windows 8, Windows Server 2012,Windows 7, Windows Server 2008, and Windows Vista cacls *View-path*\log execution result	cacls_jp1coview_log.log	Y
	For Windows 8.1, Windows 8, Windows Server 2012, Windows 7, Windows Server 2008, and Windows Vista cacls *system-drive*:\ProgramData\Hitachi\jp1\jp1_default\JP1CoView\log execution result	cacls_programdata_jp1coview_log.log	Y

Information type	Collected data	File name[#1]	View
JP1/IM - Manager access permission information (installation folder)	`cacls` *Manager-path* execution result	`cacls_jp1imm.log`	Δ
JP1/IM - Manager access permission information (log folder)	`cacls` *Manager-path*`\log` execution result	`cacls_jp1imm_log.log`	Δ
JP1/IM - Manager (JP1/IM - Central Scope) access permission information (installation folder)	`cacls` *Scope-path* execution result	`cacls_jp1scope.log`	Δ
	`cacls` *shared-folder*`\JP1Scope` execution result[#2]	`cacls_jp1scope.log`	--
JP1/IM - Manager (JP1/IM - Central Scope) access permission information (log folder)	`cacls` *Scope-path*`\log` execution result	`cacls_jp1scope_log.log`	Δ
	`cacls` *shared-folder*`\JP1Scope\log` execution result[#2]	`cacls_jp1scope_log.log`	--
JP1/IM - Manager (JP1/IM - Central Scope) access permission information (database folder)	`cacls` *Scope-path*`\database` execution result	`cacls_jp1scope_database.log`	Δ
	`cacls` *shared-folder*`\JP1Scope\database` execution result[#2]	`cacls_jp1scope_database.log`	--
JP1/IM - Manager (JP1/IM - Central Scope) access permission information (database folder)	`cacls` *Scope-path*`\database\event` execution result	`cacls_jp1scope_database_event.log`	Δ
	`cacls` *shared-folder*`\JP1Scope\database\event` execution result[#2]	`cacls_jp1scope_database_event.log`	--
JP1/IM - Manager (JP1/IM - Central Scope) access permission information (database folder)	`cacls` *Scope-path*`\database\jcsdb` execution result	`cacls_jp1scope_database_jcsdb.log`	Δ
	`cacls` *shared-folder*`\JP1Scope\database\jcsdb` execution result[#2]	`cacls_jp1scope_database_jcsdb.log`	--
JP1/IM - Manager (JP1/IM - Central Scope) access permission information (database folder)	`cacls` *Scope-path*`\database\jcsdb\event` execution result	`cacls_jp1scope_database_jcsdb_event.log`	Δ
	`cacls` *shared-folder*`\JP1Scope\database\jcsdb\event` execution result[#2]	`cacls_jp1scope_database_jcsdb_event.log`	--
JP1/IM - Manager (JP1/IM - Central Scope) access permission information (database folder)	`cacls` *Scope-path*`\database\jcsdb\pw` execution result	`cacls_jp1scope_database_jcsdb_pw.log`	Δ
	`cacls` *shared-folder*`\JP1Scope\database\jcsdb\pw` execution result[#2]	`cacls_jp1scope_database_jcsdb_pw.log`	--
JP1/IM - Manager (JP1/IM - Central Scope) access permission information (database folder)	`cacls` *Scope-path*`\database\jcsdb\tree` execution result	`cacls_jp1scope_database_jcsdb_tree.log`	Δ
	`cacls` *shared-folder*`\JP1Scope\database\jcsdb\tree` execution result[#2]	`cacls_jp1scope_database_jcsdb_tree.log`	--
JP1/IM - Manager (JP1/IM - Central Scope) access permission information (database folder)	`cacls` *Scope-path*`\database\jcshosts` execution result	`cacls_jp1scope_database_jcshosts.log`	Δ
	`cacls` *shared-folder*`\JP1Scope\database\jcshosts` execution result[#2]	`cacls_jp1scope_database_jcshosts.log`	--

Information type	Collected data	File name[#1]	View
JP1/Base file list	dir *Base-path* /s execution result	dir_jp1base.log	Δ
	dir *shared-folder*\JP1Base /s execution result[#2]	dir_*logical-host-name*_jp1base.log	--
JP1/IM - Manager (JP1/IM - Central Console) file list	dir *Console-path* /s execution result	dir_jp1cons.log	Δ
	dir *shared-folder*\JP1Cons /s execution result[#2]	dir_*logical-host-name*_jp1cons.log	--
JP1/IM - View file list	dir *View-path* /s execution result	dir_jp1coview.log	Y
	Only for Windows 8.1, Windows 8, Windows Server 2012, Windows 7, Windows Server 2008, and Windows Vista dir *system-drive*:\ProgramData \Hitachi\jp1\jp1_default \JP1CoView /s execution result	dir_programdata_jp1coview.log	Y
JP1/IM - Manager file list	dir *Manager-path* /s execution result	dir_jp1imm.log	Δ
JP1/IM - Manager (JP1/IM - Central Scope) file list	dir *Scope-path* /s execution result	dir_jp1scope.log	Δ
	dir *shared-folder*\JP1Scope /s execution result[#2]	dir_*logical-host-name*_jp1scope.log	--
Host name for resolving network address	jbsgethostbyname execution result	• jbsgethostbyname.log (standard output) • jbsgethostbyname_err.log (standard error)	Δ
	jbsgethostbyname *logical-host-name* execution result[#2]	• jbsgethostbyname.log (standard output) • jbsgethostbyname_err.log (standard error)	--
Health check	jbshcstatus -debbug -a execution result	• jbshcstatus.log (standard output) • jbshcstatus_err.log (standard error)	Δ
	jbshcstatus -debbug -a -h *logical-host-name* execution result[#2]	• jbshcstatus.log (standard output) • jbshcstatus_err.log (standard error)	--
Process operation status of Event Service	jevstat execution result	• jevstat.log (standard output) • jevstat_err.log (standard error)	Δ
Process operation status of items other than Event Service	jbs_spmd_status execution result	• jbs_spmd_status.log (standard output) • jbs_spmd_status_err.log (standard error)	Δ
	jbs_spmd_status -h *logical-host-name* execution result[#2]	• jbs_spmd_status.log (standard output) • jbs_spmd_status_err.log (standard error)	--
Automated action execution result	jcashowa execution result	• jcashowa.log (standard output) • jcashowa_err.log (standard error)	Δ
	jcashowa -h *logical-host-name* execution result[#2]	• jcashowa.log (standard output) • jcashowa_err.log (standard error)	--
Automated action status	jcastatus execution result	• jcastatus.log (standard output) • jcastatus_err.log (standard error)	Δ

Information type	Collected data	File name[#1]	View
	`jcastatus -h` *logical-host-name* execution result[#2]	• `jcastatus.log` (standard output) • `jcastatus_err.log` (standard error)	--
Automated action definition file content	`jcastatus -d` execution result	• `jcastatus_d.log` (standard output) • `jcastatus_d_err.log` (standard error)	Δ
	`jcastatus -d -h` *logical-host-name* execution result[#2]	• `jcastatus_d.log` (standard output) • `jcastatus_d_err.log` (standard error)	--
Event Generation Service status	`jcoegsstatus` execution result	• `jcoegsstatus.log` (standard output) • `jcoegsstatus_err.log` (standard error)	Δ
	`jcoegsstatus -h` *logical-host-name* execution result[#2]	• `jcoegsstatus.log` (standard output) • `jcoegsstatus_err.log` (standard error)	--
Process operation status	`jco_spmd_status` execution result	• `jco_spmd_status.log` (standard output) • `jco_spmd_status_err.log` (standard error)	Δ
	`jco_spmd_status -h` *logical-host-name* execution result[#2]	• `jco_spmd_status.log` (standard output) • `jco_spmd_status_err.log` (standard error)	--
Data collection command execution result	`jim_log.bat` command execution result	`jim_log_result.log`	Y
Windows event log	• Application: *system-root-folder*`\system32\config\AppEvent.Evt` • System: *system-root-folder*`\system32\config\SysEvent.Evt`	• `AppEvent(Backup).evt` • `AppEvent(Backup).txt` • `SysEvent(Backup).evt` • `SysEvent(Backup).txt`	Y
Crash dump[#3]	*user-specified-folder*`\user.dmp`	`user.dmp`	Y[#4]
Watson (Dr. Watson) log[#3]	*user-specified-folder*`\drwtsn32.log`	`drwtsn32.log`	Y

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)* (*1. Commands*) in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*

- *jcoview_log.bat (Windows only)* (*1. Commands*) in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*

#2: Can be collected when data in a logical host (cluster) environment is being collected.

#3: The output destination must be specified in advance. (See *1.19.2(1) Preparations for collecting data in the event of a failure* in the *Job Management Partner 1/Integrated Management - Manager Configuration Guide*.)

#4: JP1/IM - View and JP1/IM - Manager for Windows 8.1, Windows 8, Windows Server 2012, Windows 7, Windows Server 2008, and Windows Vista do not collect crash dumps.

(2) JP1 information

You need to collect the JP1-related information listed in the table below. These types of information can be collected using a data collection tool. If a network connection problem has occurred, you must also collect files from the machine at the connection destination.

The two data collection tools (the `jim_log.bat` command and the `jcoview_log.bat` command) collect different types of data. When the `jim_log.bat` command is executed, all of the data listed in the table below is collected. The data that can be collected by executing the `jcoview_log.bat` command is indicated in the far-right column.

Table 10–12: JP1 information (Windows)

Information type		Collected data	File name[1]	View
Common to JP1/IM and JP1/Base	Integrated trace log	*system-drive*:`Program Files` `\Hitachi\HNTRLib2\spool`	The following files in the default mode: `hntr2[1|2|3|4].log`	Y
JP1/IM - Manager (common to components)	Patch information	*Manager-path*`\PATCHLOG.TXT`	`Patchlog_jp1imm.txt`	--
	Settings and definition file	Files under *Manager-path*`\conf\`	Copies of the files indicated at left	--
	Log file	Files under *Manager-path*`\log\`	Copies of the files indicated at left	--
JP1/IM - Manager (JP1/IM - Central Console)	Settings and definition file	Files under *Console-path*`\conf\`	Copies of the files indicated at left	--
		Files under *shared-folder*`\JP1Cons\conf` `\`[2]	Copies of the files indicated at left	--
	Common definition information	Files under *Console-path*`\default\`	Copies of the files indicated at left	--
	Log file	Files under *Console-path*`\log\`	Copies of the files indicated at left	--
		Files under *shared-folder*`\JP1Cons\log` `\`[2]	Copies of the files indicated at left	--
	File for accumulated response-waiting events[3]	Files under *Console-path*`\log\response` `\`	Copies of the files indicated at left	--
		Files under *shared-folder*`\jp1cons\log` `\response\`	Copies of the files indicated at left	--
	Correlation event generation history file	Files under *Console-path*`\operation` `\evgen\`	Copies of the files indicated at left	--
		Files under *shared-folder*`\JP1Cons` `\operation\evgen\`[2]	Copies of the files indicated at left	--
JP1/IM - Manager (JP1/IM - Central Scope)	Settings and definition file	Files under *Scope-path*`\conf\`	Copies of the files indicated at left	--
		Files under *shared-folder*`\JP1Scope` `\conf\`[2]	Copies of the files indicated at left	--
	Common definition information	Files under *Scope-path*`\default\`	Copies of the files indicated at left	--

Information type		Collected data	File name[1]	View
	Log file	Files under *Scope-path*\log\	Copies of the files indicated at left	--
		Files under *shared-folder*\JP1Scope\log\[2]	Copies of the files indicated at left	--
	Database information	Files under *Scope-path*\database\	Copies of the files indicated at left	--
		Files under *shared-folder*\JP1Scope\database\[2]	Copies of the files indicated at left	--
JP1/IM - Manager (IM Configuration Management)	Settings and definition file	Files under *Manager-path*\conf\imcf\	Copies of the files indicated at left	--
		Files under *shared-folder*\jp1imm\conf\imcf\[2]	Copies of the files indicated at left	--
	Common definition information	Files under *Manager-path*\system\default\new\imcf\	Copies of the files indicated at left	--
	Log file	Files under *Manager-path*\log\imcf\	Copies of the files indicated at left	--
		Files under *shared-folder*\jp1imm\log\imcf\[2]	Copies of the files indicated at left	--
JP1/IM - View	Patch information	*View-path*\Patchlog.txt	Patchlog_jp1coview.txt	Y
	Settings and definition file	Files under *View-path*\conf\	Copies of the files indicated at left	Y
		Only for Windows 8.1, Windows 8, Windows Server 2012, Windows 7, Windows Server 2008, and Windows Vista Files under *system-drive*:\ProgramData\Hitachi\jp1\jp1_default\JP1CoView\conf\	Copies of the files indicated at left	Y
	Common definition information	Files under *View-path*\default\	Copies of the files indicated at left	Y
	Log file	For Windows other than Windows 8.1, Windows 8, Windows Server 2012, Windows 7, Windows Server 2008, and Windows Vista Files under *View-path*\log\	Copies of the files indicated at left	Y
		For Windows 8.1, Windows 8, Windows Server 2012, Windows 7, Windows Server 2008, and Windows Vista Files under *system-drive*:\ProgramData\Hitachi\jp1\jp1_default\JP1CoView\log\	Copies of the files indicated at left	Y
JP1/Base	Patch information	*Base-path*\PatchLog.txt	Patchlog_jp1base.txt	--
	Settings and definition file	Files under *Base-path*\conf\	Copies of the files indicated at left	--

Information type		Collected data	File name[1]	View
		Files under *shared-folder*\JP1Base\conf\[2]	Copies of the files indicated at left	--
	Common definition information	Files under *Base-path*\default\	Copies of the files indicated at left	--
	Log file	Files under *Base-path*\log\	All files under the folder indicated at left, excluding COMMAND	--
		Files under *shared-folder*\JP1Base\log\[2]	All files under the folder indicated at left, excluding COMMAND	--
	Plug-in service settings file	Files under *Base-path*\plugin\conf\	Copies of the files indicated at left	--
	Log and temporary file	Files under *Base-path*\sys\tmp\	Copies of the files indicated at left	--
		shared-folder\JP1Base\event[2]	All files under the folder indicated at left, excluding IMEvent*.*	--
	Command execution log file	Files under *Base-path*\log\COMMAND\	Copies of the files indicated at left	--
		Files under *shared-folder*\JP1Base\log\COMMAND\[2]	Copies of the files indicated at left	--
	Event database	Files under *Base-path*\sys\event\servers\default\	Copies of the files indicated at left	--
		shared-folder\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)* (*1. Commands*) in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*

- *jcoview_log.bat (Windows only)* (*1. Commands*) in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*

#2: Can be collected when data in a logical host (cluster) environment is being collected.

#3: The file for accumulated response-waiting events is created when you enable the response-waiting event management function. You can prevent the jim_log.bat command from collecting this file by specifying a command option. For details, see *9.5.2 jim_log.bat (Windows only)*.

(3) Operation content

You need the following types of information related to the operation that was being performed when the problem occurred:

- Operation content details

- Time of problem occurrence

- Machine configuration (version of each OS, host name, and Central Console configuration)

- Reproducibility

- Login user name that was used to log in from JP1/IM - View

(4) Error information on the screen

Collect a hard copy of the following:

- Error dialog box (and the content displayed by the **Details** button, if available)

(5) Information related to the Web version of JP1/IM - View

If a problem occurs while you are using the Web version of JP1/IM - View, you need to collect the following data.

View side

- Java stack trace log

  Before you can collect a Java stack trace log, you must set up the system such that the Java Console window can be opened. For details, see *4.16.4 Specifying display settings for the Java Console window* in the *Job Management Partner 1/Integrated Management - Manager Configuration Guide*.

- Java trace file of Java^{TM} Plug-in

  The Java trace file is located in the following directory:

  Java^{TM} Plug-in 1.4.2:

  > *system-drive*:`\Documents and Settings\`*login-user-name*`\Application Data\Sun\Java \Deployment\log\`

Manager side

- HTTP server error log
- HTTP server access log

(6) User dump (Only for Windows 8.1, Windows 8, Windows Server 2012, Windows 7, Windows Server 2008, and Windows Vista)

If a JP1/IM - View process stops due to an application error in Windows 8.1, Windows 8, Windows Server 2012, Windows 7, Windows Server 2008, or Windows Vista, collect a user dump.

(7) Problem report (Only for Windows Server 2008$^{\#}$ and Windows Vista)

If a JP1/IM - View process stops due to an application error in Windows Server 2008$^{\#}$ or Windows Vista, obtain a problem report.

#:

Windows Server 2008 R2 (x64) or later is excepted.

10.3.2 In UNIX

(1) OS system information

You need to collect the OS-related information listed in the table below. These types of information can be collected using data collection tools.

Table 10–13: OS system information (UNIX)

Information type	Collected data	File name[1]
Installed Hitachi product information	`/etc/.hitachi/pplistd/pplistd`	• `jp1_default_imm_1st.tar.{Z|gz}` • `pplistd`
Hitachi PP Installer installation log file	`/etc/.hitachi/.install.log*`	• `jp1_default_imm_1st.tar.{Z|gz}` • `.install.log*`
Hitachi PP Installer uninstallation log file	`/etc/.hitachi/.uninstall.log*`	• `jp1_default_imm_1st.tar.{Z|gz}` • `.uninstall.log*`
Common definition information	Files under `/opt/jp1/hcclibcnf/`	• `jp1_default_imm_1st.tar.{Z|gz}` • Copies of the files indicated at left
JP1/IM - Manager (JP1/IM - Central Console) core analysis information (back trace)	Analysis result from `seraph` `/var/opt/jp1cons`	• `jp1_default_imm_1st.tar.{Z|gz}` • `core_module-name.log`
	Analysis result from `seraph` *shared-directory*`/jp1cons/log`[2]	• *logical-host-name*`_imm_1st.tar.{Z|gz}` • `core_module-name.log`
JP1/IM - Manager (JP1/IM - Central Scope) core analysis information (back trace)	Analysis result from `seraph` `/var/opt/jp1scope`	• `jp1_default_imm_1st.tar.{Z|gz}` • `core_module-name.log`
	Analysis result from `seraph` *shared-directory*`/jp1scope/log`[2]	• *logical-host-name*`_imm_1st.tar.{Z|gz}` • `core_module-name.log`
JP1/Base installation log file	`/tmp/HITACHI_JP1_INST_LOG/` `jp1base_inst{1|2|3|4|5}.log`	• `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`	• `jp1_default_imm_1st.tar.{Z|gz}` • `jp1imm_inst{1|2|3|4|5}.log`
File list	• `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	• `jp1_default_imm_1st.tar.{Z|gz}` • `inst_dir.log`

Information type	Collected data	File name[1]
	• `ls -lRa /etc/opt/jp1base` execution result • `ls -lRa /var/opt/jp1base` execution result	
	• `ls -lRa` *shared-directory*`/jp1cons` execution result[2] • `ls -lRa` *shared-directory*`/jp1scope` execution result[2] • `ls -lRa` *shared-directory*`/jp1base` execution result[2] • `ls -lRa` *shared-directory*`/event` execution result[2]	• *logical-host-name*`_imm_1st.tar.{Z｜gz}` • `share_dir.log`
Data collection date/time	`date` execution result	• `jp1_default_imm_1st.tar.{Z｜gz}` • `jp1_default_imm_2nd.tar.{Z｜gz}` • *logical-host-name*`_imm_1st.tar.{Z｜gz}` • *logical-host-name*`_imm_2nd.tar.{Z｜gz}` • `date.log`
Disk information	`df -k` execution result	• `jp1_default_imm_1st.tar.{Z｜gz}` • `df.log`
Machine's environment variable	`env` execution result	• `jp1_default_imm_1st.tar.{Z｜gz}` • `env.log`
Host name settings that are set in the machine	• `/etc/inet/hosts` (Solaris) • `/etc/hosts` (AIX) • `/etc/hosts`(Linux)	• `jp1_default_imm_1st.tar.{Z｜gz}` • `hosts`
Status of shared memory for inter-process communication	`ipcs -ma` execution result	• `jp1_default_imm_1st.tar.{Z｜gz}` • `ipcs.log`
Host name for resolving network address	`jbsgethostbyname` execution result	• `jp1_default_imm_1st.tar.{Z｜gz}` • `jbsgethostbyname.log` (standard output) • `jbsgethostbyname_err.log` (standard error)
	`jbsgethostbyname` *logical-host-name* execution result[2]	• *logical-host-name*`_imm_1st.tar.{Z｜gz}` • `jbsgethostbyname`*logical-host-name*`.log`
Health check	`jbshcstatus -debbug -a` execution result	• `jp1_default_imm_1st.tar.{Z｜gz}` • `jbshcstatus.log` (standard output) • `jbshcstatus_err.log` (standard error)
	`jbshcstatus -debbug -a -h` *logical-host-name* execution result[2]	• *logical-host-name*`_imm_1st.tar.{Z｜gz}` • `jbshcstatus.log` (standard output) • `jbshcstatus_err.log` (standard error)
Process operation status of Event Service	`jevstat` execution result	• `jp1_default_imm_1st.tar.{Z｜gz}` • `jevstat.log` (standard output) • `jevstat_err.log` (standard error)
Process operation status of items other than Event Service	`jbs_spmd_status` execution result	• `jp1_default_imm_1st.tar.{Z｜gz}` • `jbs_spmd_status.log` (standard output) • `jbs_spmd_status_err.log` (standard error)

Information type	Collected data	File name[1]
	`jbs_spmd_status -h` *logical-host-name* execution result[2]	• *logical-host-name*`_imm_1st.tar.{Z|gz}` • `jbs_spmd_status.log` (standard output) • `jbs_spmd_status_err.log` (standard error)
Automated action execution result	`jcashowa` execution result	• `jp1_default_imm_1st.tar.{Z|gz}` • `jcashowa.log` (standard output) • `jcashowa_err.log` (standard error)
	`jcashowa -h` *logical-host-name* execution result[2]	• *logical-host-name*`_imm_1st.tar.{Z|gz}` • `jcashowa.log` (standard output) • `jcashowa_err.log` (standard error)
Automated action function status	`jcastatus` execution result	• `jp1_default_imm_1st.tar.{Z|gz}` • `jcastatus.log` (standard output) • `jcastatus_err.log` (standard error)
	`jcastatus -h` *logical-host-name* execution result[2]	• *logical-host-name*`_imm_1st.tar.{Z|gz}` • `jcastatus.log` (standard output) • `jcastatus_err.log` (standard error)
Automated action definition file content	`jcastatus -d` execution result	• `jp1_default_imm_1st.tar.{Z|gz}` • `jcastatus_d.log` (standard output) • `jcastatus_d_err.log` (standard error)
	`jcastatus -d -h` *logical-host-name* execution result[2]	• *logical-host-name*`_imm_1st.tar.{Z|gz}` • `jcastatus_d.log` (standard output) • `jcastatus_d_err.log` (standard error)
Event Generation Service status	`jcoegsstatus` execution result	• `jp1_default_imm_1st.tar.{Z|gz}` • `jcoegsstatus.log` (standard output) • `jcoegsstatus_err.log` (standard error)
	`jcoegsstatus -h` *logical-host-name* execution result[2]	• *logical-host-name*`_imm_1st.tar.{Z|gz}` • `jcoegsstatus.log` (standard output) • `jcoegsstatus_err.log` (standard error)
Process operation status	`jco_spmd_status` execution result	• `jp1_default_imm_1st.tar.{Z|gz}` • `jco_spmd_status.log` (standard output) • `jco_spmd_status_err.log` (standard error)
	`jco_spmd_status -h` *logical-host-name* execution result[2]	• *logical-host-name*`_imm_1st.tar.Z{Z|gz}` • `jco_spmd_status.log` (standard output) • `jco_spmd_status_err.log` (standard error)
Data collection command execution result	`jim_log.sh` command execution result	• `jp1_default_imm_1st.tar.{Z|gz}` • `jim_log_result.log`
NIC installation status	`netstat -i` execution result	• `jp1_default_imm_1st.tar.{Z|gz}` • `netstat_i.log`
Network statistical information	`netstat -na` execution result	• `jp1_default_imm_1st.tar.{Z|gz}` • `netstat_na.log`
List of users that are set in the machine	`/etc/passwd`	• `jp1_default_imm_1st.tar.{Z|gz}` • `passwd`
Process list	`ps -elfa` execution result	• `jp1_default_imm_1st.tar.{Z|gz}`

Information type	Collected data	File name[1]
		• `ps.log`
Service port settings that are set in the machine	• `/etc/inet/services` (Solaris) • `/etc/services` (AIX) • `/etc/services` (Linux)	• `jp1_default_imm_1st.tar.{Z|gz}` • `services`
Memory information	• `swap -l` execution result (Solaris) • `lsps -s` execution result (AIX) • `cat /proc/meminfo` (Linux)	• `jp1_default_imm_1st.tar.{Z|gz}` • `swapinfo.log`
System diagnostic information	• `dmesg` execution result (Solaris) • `alog -o -t boot` execution result (AIX) • `dmesg` execution result (Linux)	• `jp1_default_imm_1st.tar.{Z|gz}` • `sys_info.log`
Syslog (`syslog`)	• `/var/adm/messages` (Solaris) • `/var/adm/messages` (AIX) • `/var/log/messages` (Linux)	• `jp1_default_imm_1st.tar.{Z|gz}` • `syslog.log`
JP1/IM - Manager (JP1/IM - Central Console) core analysis information (back trace) output by the `jcogencore` command	Analysis result from `seraph` `/var/opt/jp1cons`	• `jp1_default_imm_1st.tar.{Z|gz}` • `trace_module-name.log`
	Analysis result from `seraph` *shared-directory*`/jp1cons/log` (core output by `jcogencore`)[2]	• *logical-host-name*`_imm_1st.tar.{Z|gz}` • `trace_module-name.log`
OS version information	`uname -a` execution result	• `jp1_default_imm_1st.tar.{Z|gz}` • `uname_a.log`
Kernel parameter information	In Solaris: • `sysdef -i` execution result • `ulimit -a` execution result In AIX: • `lsattr -E -l sys0` execution result • `ulimit -a` execution result • `/etc/security/limits` execution result In Linux: • `sysctl -a` execution result • `ulimit -a` execution result	• `jp1_default_imm_1st.tar.{Z|gz}` In Solaris: • `sysdef.log` • `ulimit.log` In AIX: • `isattr.log` • `ulimit.log` • `limits` In Linux: • `sysctl.log` • `ulimit.log`
Page size information	• `pagesize` execution result (Solaris) • `pagesize` execution result (AIX) • Nothing (Linux)	• `jp1_default_imm_1st.tar.{Z|gz}` • `pagesize.log`
OS patch application information	In Solaris 10: • `showrev -a` execution result In Solaris 11: • `pkg info entire` execution result • `pkg list` execution result In AIX: • `instfix -a -icv` execution result • `lslpp -l -a` execution result In Linux:	• `jp1_default_imm_1st.tar.{Z|gz}` In Solaris 10 • `showrev.log` In Solaris 11 • `pkg.log` In AIX: • `instfix.log` • `lslpp.log` In Linux:

Information type	Collected data	File name[1]
	• rpm -qa execution result	• rpm.log

#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, Solaris, and AIX, and created in .tar.gz format for Linux.

For details about the internal directory configuration of the compressed file, see *jim_log.sh (UNIX only)* (*1. Commands*) in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.

#2: Can be collected when data in a logical host (cluster) environment is being collected.

(2) JP1 information

You need to collect the JP1-related information listed in the table below. These types of information can be collected using a data collection tool. If a network connection problem has occurred, you must also collect files from the machine at the connection destination.

Table 10–14: JP1 information (UNIX)

Information type		Collected data	File name[1]
Common to JP1/IM and JP1/Base	Integrated trace log	All files under /var/opt/hitachi/HNTRLib2/spool/	• jp1_default_imm_1st.tar.{Z|gz} • The following files in the default mode: hntr2[1|2|3|4].log
JP1/IM - Manager (common to components)	Patch application history	/opt/jp1imm/patch_history	• jp1_default_imm_1st.tar.{Z|gz} • patch_history
	Patch log information	/opt/jp1imm/update.log	• jp1_default_imm_1st.tar.{Z|gz} • update.log
JP1/IM - Manager (JP1/IM - Central Console)	Automatic startup and automatic termination script	Files under /etc/opt/jp1cons/	• jp1_default_imm_1st.tar.Z • Copies of the files indicated at left
	Settings and defintion file	Files under /etc/opt/jp1cons/conf/	• jp1_default_imm_1st.tar.{Z|gz} • Copies of the files indicated at left
		Files under *shared-directory*/jp1cons/conf/[2]	• *logical-host-name*_imm_1st.tar.{Z|gz} • Copies of the files indicated at left
	Common definition information	Files under /etc/opt/jp1cons/default/	• jp1_default_imm_1st.tar.{Z|gz} • Copies of the files indicated at left
	Log file	Files under /var/opt/jp1cons/log/	• jp1_default_imm_1st.tar.{Z|gz} • Copies of the files indicated at left
		Files under *shared-directory*/jp1cons/log/[2]	• *logical-host-name*_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/	• jp1_default_imm_1st.tar.{Z|gz} • Copies of the files indicated at left

Information type	Collected data		File name[1]
		Files under *shared-directory*/ `jp1cons/log/response/`	• `jp1_default_imm_1st.tar.{Z|` `gz}` • Copies of the files indicated at left
	Core analysis information (CAR file) output by the `jcogencore` command	`car` command result `/var/opt/jp1cons/log` (core output by `jcogencore`)	• `jp1_default_imm_2nd.tar.{Z|` `gz}` • `car_module-name.tar.Z`
		`car` command result *shared-directory*/`jp1cons/log` (core output by `jcogencore`)[2]	• *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`	• `jp1_default_imm_2nd.tar.{Z|` `gz}` • `core_module-name_car.tar.Z`
		`car` command result *shared-directory*/`jp1cons/log`[2]	• *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/`	• `jp1_default_imm_2nd.tar.{Z|` `gz}` • Copies of the files indicated at left
		shared-directory/`jp1cons/` `operation/evgen`[2]	• *logical-host-name*`_imm_2nd.tar.{Z|` `gz}` • Copies of the files indicated at left
JP1/IM - Manager (JP1/IM - Central Scope)	Settings and definition file	Files under `/etc/opt/jp1scope/` `conf/`	• `jp1_default_imm_1st.tar.{Z|` `gz}` • Copies of the files indicated at left
		Files under *shared-directory*/ `jp1scope/conf/`[2]	• *logical-host-name*`_imm_1st.tar.{Z|` `gz}` • Copies of the files indicated at left
	Common definition information	Files under `/etc/opt/jp1scope/` `default/`	• `jp1_default_imm_1st.tar.{Z|` `gz}` • Copies of the files indicated at left
	Log file	Files under `/var/opt/` `jp1scope/log/`	• `jp1_default_imm_1st.tar.{Z|` `gz}` • Copies of the files indicated at left
		Files under *shared-directory*/ `jp1scope/log/`[2]	• *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`	• `jp1_default_imm_2nd.tar.{Z|` `gz}` • `core_module-name_car.tar.Z`
		`car` command result *shared-directory*/`jp1scope/log`[2]	• *logical-host-name*`_imm_2nd.tar.{Z|` `gz}` • `core_module-name_car.tar.Z`
	Database information	Files under `/var/opt/jp1scope/` `database/`	• `jp1_default_imm_2nd.tar.{Z|` `gz}` • Copies of the files indicated at left

Information type		Collected data	File name[1]
		Files under *shared-directory*/ `jp1scope/database/`[2]	• *logical-host-name*`_imm_2nd.tar.{Z| gz}` • Copies of the files indicated at left
JP1/IM - Manager (IM Configuration Management)	Settings and defintion files	Files under `/etc/opt/jp1imm/ conf/imcf/`	• `jp1_default_imm_1st.tar.{Z| gz}` • Copies of the files indicated at left
		Files under *shared-directory*/`jp1imm/ conf/imcf/`[2]	• *logical-host-name*`_imm_1st.tar.{Z| gz}` • Copies of the files indicated at left
	Common definition information	Files under `/etc/opt/jp1imm/ default/imcf/`	• `jp1_default_imm_1st.tar.{Z| gz}` • Copies of the files indicated at left
	Log file	Files under `/var/opt/ jp1imm/log/imcf/`	• `jp1_default_imm_1st.tar.{Z| gz}` • Copies of the files indicated at left
		Files under *shared-directory*/ `jp1imm/log/imcf/`[2]	• *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/jp1imm/log`	• `jp1_default_imm_2nd.tar.{Z| gz}` • `./var/opt/jp1imm/log/ _jp1_default/core/core_`*module-name*`_car.tar.Z`
		`car` command result *shared-directory*/`jp1imm/log`[2]	• *logical-host-name*`_imm_2nd.tar.{Z| gz}` • `./var/opt/jp1imm/log/_`*logical-host-name*`/core/core_`*module-name*`_car.tar.Z`
JP1/Base	Automatic startup and automatic termination script	Files under `/etc/opt/jp1base/`	• `jp1_default_imm_1st.tar.{Z| gz}` • Copies of the files indicated at left
	Settings and definition file	Files under `/etc/opt/jp1base/ conf/`	• `jp1_default_imm_1st.tar.{Z| gz}` • Copies of the files indicated at left
		Files under *shared-directory*/ `jp1base/conf/`[2]	• *logical-host-name*`_imm_1st.tar.{Z| gz}` • Copies of the files indicated at left
	Common definition information	Files under `/etc/opt/jp1base/ default/`	• `jp1_default_imm_1st.tar.{Z| gz}` • Copies of the files indicated at left
	Plug-in service settings file	Files under `/opt/jp1base/conf/ plugin/`	• `jp1_default_imm_1st.tar.{Z| gz}` • Copies of the files indicated at left
	Patch application history	`/opt/jp1base/PatchInfo`	• `jp1_default_imm_1st.tar.{Z| gz}` • `PatchInfo`

Information type		Collected data	File name[#1]
	Patch log information	`/opt/jp1base/PatchLog`	• `jp1_default_imm_1st.tar.{Z|gz}` • `PatchLog`
	Log file	`/var/opt/jp1base/log`	• `jp1_default_imm_1st.tar.{Z|gz}` • All files under the directory indicated at left, except `COMMAND`
		shared-directory/`jp1base/log`[#2]	• *logical-host-name*`_imm_1st.tar.{Z|gz}` • All files under the directory indicated at left, except `COMMAND`
	Log and temporary file	Files under `/var/opt/jp1base/sys/tmp/`	• `jp1_default_imm_1st.tar.{Z|gz}` • Copies of the files indicated at left
		shared-directory/`event`[#2]	• *logical-host-name*`_imm_1st.tar.{Z|gz}` • All files under the directory indicated at left, except `IMEvent*`
	SES settings file	• `/tmp/.JP1_SES*` • `/usr/tmp/jp1_ses` • `/usr/lib/jp1_ses/log` • `/usr/lib/jp1_ses/sys` • `/usr/bin/jp1_ses/jp*` • `/var/opt/jp1_ses`	• `jp1_default_imm_2nd.tar.{Z|gz}` • Copies of the files indicated at left
	Command execution history file	Files under `/var/opt/jp1base/log/COMMAND/`	• `jp1_default_imm_2nd.tar.{Z|gz}` • Copies of the files indicated at left
		Files under *shared-directory*/`jp1base /log/COMMAND/`[#2]	• *logical-host-name*`_imm_2nd.tar.{Z|gz}` • Copies of the files indicated at left
	Event database	Files under `/var/opt/jp1base/sys/event/servers/default/`	• `jp1_default_imm_2nd.tar.{Z|gz}` • Copies of the files indicated at left
		shared-directory/`event`[#2]	• *logical-host-name*`_imm_2nd.tar.{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.Z` format for Solaris and AIX, and created in `.tar.gz` format for Linux.

For details about the internal directory configuration of the compressed file, see *jim_log.sh (UNIX only)* (*1. Commands*) in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.

#2: Can be collected when data in a logical host (cluster) environment is being collected.

#3: The file for accumulated response-waiting events is created when you enable the response-waiting event management function. You can prevent the `jim_log.sh` command from collecting this file by specifying a command option. For details, see *9.5.3 jim_log.sh (UNIX only)*.

(3) Operation content

You need the following types of information related to the operation that was being performed when the problem occurred:

- Operation content details
- Time of problem occurrence
- Machine configuration (version of each OS, host name, and Central Console configuration)
- Reproducibility
- Login user name that was used to log in from JP1/IM - View

(4) Error information on the screen

Collect a hard copy of the following:

- Error dialog box

(5) Information related to the Web version of JP1/IM - View

If a problem occurs while you are using the Web version of JP1/IM - View, you need to collect the following data.

View side

- Java stack trace log

  Before you can collect a Java stack trace log, you must set up the system such that the Java Console window can be opened. For details, see *4.16.4 Specifying display settings for the Java Console window* in the *Job Management Partner 1/Integrated Management - Manager Configuration Guide*.
- Java trace file of Java^{TM} Plug-in

  The Java trace file is located in the following directory:

      system-drive:\Documents and Settings*login-user-name*\Application Data\Sun\Java
      \Deployment\log\

Manager side

- HTTP server error log
- HTTP server access log

10.4 Collecting data

This section explains how to collect data when a problem occurs.

10.4.1 In Windows

(1) Checking the process status

Using Windows Task Manager, check the operating status of processes. This subsection shows the processes that are displayed when the programs are running normally.

(a) JP1/IM - Manager

The table below shows the processes of JP1/IM - Manager. The value inside parentheses ( ) indicates the number of processes that execute simultaneously.

Table 10–15: JP1/IM - Manager processes (Windows)

Parent process name	Function	Child process name	Function
`jco_spmd.exe` (1)	JP1/IM - Manager process management	`jcamain.exe` (1)	Automatic Action Service (Process management display name: `jcamain`)
		`evtcon.exe` (1)	Event Console Service (Process management display name: `evtcon`)
		`evflow.exe` (1)	Event Base Service (Process management display name: `evflow`)
		`jcsmain.exe` (1)	Central Scope Service[#2] (Process management display name: `jcsmain`)
		`jcfmain.exe` (1)	IM Configuration Management Service[#2] (Process management display name: `jcfmain`)
		`evgen.exe` (2)[#1, #3]	Event Generation Service[#2] (Process management display name: `evgen`)
`jco_service.exe` (1)	JP1/IM - Manager Windows service control	--	--
`jcfmain.exe` (1)(1)	JP1/IM - Manager IM Configuration Management	--	IM Configuration Management Service
		`jcfallogtrap.exe` (0 to 157)[#4]	Log collection process
`pdservice.exe`	IM database	--	Windows service control
		`pdprcd.exe`	Process server process
`pdprcd.exe`	IM database	--	Process server process

Parent process name	Function	Child process name	Function
(1)		`pdrsvre.exe` (3)	Post-processing that performs recovery processing after a process terminates abnormally
		`pdmlgd.exe` (1)	Message log server process that controls message output
		`pdrdmd.exe` (1)	System manager process that controls unit starting and stopping, and manages connected users
		`pdstsd.exe` (1)	Status server process that controls I/O operations on unit status files
		`pdscdd.exe` (1)	Scheduler process that allocates transactions to single server processes
		`pdtrnd.exe` (1)	Transaction server process that controls transactions
		`pdtrnrvd.exe` (1 to 128)[5]	Transaction recovery process that controls determination processing for and recovery of transactions
		`pdlogd.exe` (1)	Log server process that controls the acquisition of system logs and log-related processes
		`pd_buf_dfw.exe` (1)	Deferred write process that controls background writes to a disk where the database is stored
		`pdlogswd.exe` (1)	Log swapper process that allocates and de-allocates system log-related files, manages I/O operations for system log-related files, and acquires sync-point dumps
		`pdsds.exe` (10 to 128)[6]	Single server process that performs SQL processing
`pdsha.exe` (1)	IM database	--	Service for an embedded HiRDB in a cluster environment

Legend:

--: None

#1: The maximum number is 2, but the normal number is 1. The details are as follows.

- This is a process that is temporarily generated when Event Service is connected. It is generated in the following cases:
  - When Event Generation Service starts
  - When the event acquisition filter is updated

#2: In the default, this service does not run.

#3: This is the service that is used when the integrated monitoring database is not used.

#4: This process does not run at startup. The number of process instances increases with the number of monitored files in remote monitoring. The maximum number of concurrent processes is 157.

#5: Only one process runs at startup. However, this number increases temporarily with each abnormal termination of the `pdsds.exe` process.

#6: Ten instances of this process run at startup, and this number increases with the number of access requests to the IM database. The maximum number of concurrent processes is 32.

When JP1/IM - Manager is running in a cluster system, the above processes are executed on each physical host and on each logical host. The number of processes that execute simultaneously can be obtained by multiplying the number of physical hosts and logical hosts that are running by the number of above processes.

In the table, a process whose parent process is `jco_spmd.exe` is controlled by process management, and you can use the `jco_spmd_status` command to check the process status.

- A display example during normal operations follows.

```
c:\>jco_spmd_status
KAVB3690-I Processing to report the status of JP1_CONS has started.
Shows processes that are running.
Process name Process ID
evflow 3672
jcamain 4088
evtcon 4236
jcsmain#1 4668
jcfmain#2 4950
evgen#3 5624
KAVB3691-I All the processes have started.
```

#1: `jcsmain` is displayed only when the Central Scope is enabled.

#2: `jcfmain` is displayed only when the IM Configuration Management is enabled.

#3: `evgen` is displayed only when the Event Generation Service is enabled.

(b) JP1/IM - View

The table below shows the processes of JP1/IM - View. The value inside parentheses ( ) indicates the number of processes that execute simultaneously.

Table 10–16: JP1/IM - View processes

Parent process name	Function	Child process name	Function
`jcoview.exe` (3+3#)	JP1/IM - View process management	`jcoview_evt.exe` (3)	Sends thread dump output events.
		`java.exe` (3+3#)	Controls the JP1/IM - View window.
`jcfview.exe` (3)	IM Configuration Management - View process management	`jcfview_evt.exe` (3)	Sends thread dump output events
		`java.exe` (3+3#)	Controls the IM Configuration Management - View window.

#: Added when JP1/IM - View (the part linked to JP1/IM - Rule Operation) is running.

(c) JP1/IM - IM Configuration Management - View

The table below shows the processes of JP1/IM - IM Configuration Management - View. The value inside parentheses ( ) indicates the number of processes that execute simultaneously.

Table 10–17: JP1/IM - IM Configuration Management - View processes

Parent process name	Function	Child process name	Function
`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.

(2) Outputting a thread dump for JP1/IM

(a) JP1/IM - View

Follow the procedure described below to output a dump file.

1. Start Task Manager.

2. On the Applications page, select JP1/IM - View, and then from the pop-up menu, choose **Bring To Front**.
   In this way, you can determine whether JP1/IM - View is disabled. If you have identified a disabled JP1/IM - View, proceed to the next step.

3. From the pop-up menu, choose **Go To Process**.
   The display switches to the **Process** page. Since `java.exe` of JP1/IM - View is displayed in the selected state, use this to identify the process ID (PID).[#]
   #: If no PID is displayed, from the menu, choose **Display** and then **Select Columns**, and then, from the Select Columns window, select the **PID (Process Identifier)** check box.

4. Using the process ID that has been identified as the argument, execute the `jcothreaddmp` command.

For details about the `jcothreaddmp` command, see *jcothreaddmp (Windows only)* (*1. Commands*) in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.

(b) JP1/IM - Manager

When the health check function detects an abnormality in Event Console 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* (*1. Commands*) in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.

(3) Collecting information related to the Web version of JP1/IM - View

When a problem occurs in the Web version of JP1/IM - View, collect the following data in addition to the data described in this section.

View side

- Java stack trace log

The collection procedure follows.

1. Choose the Java Console window and enter `v`.

The Java stack trace log is output to the Java Console window.

2. Copy the log and manually paste it to a text file, for example.

3. Save the text file.

- Java trace file of Java[TM] Plug-in

The Java trace file is located in the following directory:

system-drive:`\Documents and Settings\`*login-user-name*`\Application Data\Sun\Java`
`\Deployment\log\`

> **Important note**
>
> The Java trace file of Java[TM] Plug-in is erased when Java[TM] Plug-in restarts. Therefore, if a problem occurs, save the content of this file to another file before restarting.

Manager side

- HTTP server error log
- HTTP server access log

(4) Executing the data collection tool

This subsection describes execution of the data collection tool (`jim_log.bat` or `jcoview_log.bat`).

When you execute the `jim_log.bat` command, which is provided by JP1/IM - Manager, you can collect the data necessary for troubleshooting JP1/IM - Manager and JP1/IM - View on the same host.

If you execute the `jcoview_log.bat` command, which is provided by JP1/IM - View, you can collect the data necessary for troubleshooting JP1/IM - View.

Use one of above commands according to the application that is being used.

Because the total volume of data collected by a data collection tool is massive, you need to estimate it before you execute the command and make sure the machine you are using has sufficient free space.

For the volume of data that will be collected by the `jim_log.bat` command, see the JP1/IM - Manager release notes.

For the volume of data that will be collected by the `jcoview_log.bat` command, see the JP1/IM - View release notes.

A tool execution example follows.

`C:\>"C:\Program Files\Hitachi\JP1IMM\tools\jim_log.bat" -f` *data-storage-folder*

Specify the data storage folder as an absolute path. If the data storage folder path contains a space, enclose the path in double quotation marks.

When you execute the tool, the `jp1_default` folder is created under the folder specified as the data storage folder, and the collected data is copied into this folder. Use a data-compression tool to compress the collected data.

(5) Checking the operation content

Check the content of the operation that was taking place when the problem occurred, and record it. The following types of information must be checked:

- Operation content details
- Time of problem occurrence
- Reproducibility
- Login user name that was used to log in from JP1/IM - View
- Machine configuration (version of each OS, host name, and Central Console configuration)

(6) Collecting the error information on the screen

If an error is displayed on the screen, collect that information as well. Collect a hard copy of the following:

- Error dialog box
  Copy the content displayed by the **Details** button, if available.

(7) Collecting a user dump (Windows 8.1, Windows 8, Windows Server 2012, Windows 7, Windows Server 2008, and Windows Vista only)

When a JP1/IM - View process stops due to an application error in Windows 8.1, Windows 8, Windows Server 2012, Windows 7, Windows Server 2008, or Windows Vista, 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 note**
   >
   > If the error dialog box is closed, a normal dump cannot be collected, and consequently you will not be able to collect a user dump. If you closed the error dialog box by mistake (by clicking **OK**, for example) before collecting a user dump, reproduce the error and then collect a user dump.

(8) Obtaining a problem report (Windows Server 2008[#] and Windows Vista only)

When a JP1/IM - View process stops due to an application error in Windows Server 2008[#] or Windows Vista, use the following procedure to obtain a problem reports.

#:

    Windows Server 2008 R2 (x64) or later is excepted.

1. In the **Run** text box, enter `wercon` and click **OK**.

   The Problem Report and Solution dialog box opens.

2. On the left pane, click **Show Problem History**.

3. Double-click the applicable problem.

   Details of the problem report are displayed.

4. Choose **Copy to Clipboard**.

5. Copy the copied content and save it in a text file.

   Use the saved problem report for troubleshooting.

10.4.2 In UNIX

(1) Checking the process status

The process names that are displayed when the `ps` command is executed are shown below. In UNIX, by using the data collection tool (`jim_log.sh`), you can collect the execution results of the `ps` command along with other data.

(a) JP1/IM - Manager

The table below shows the processes of JP1/IM - Manager. The value inside parentheses ( ) indicates the number of processes that execute simultaneously.

Table 10–18: JP1/IM - Manager processes (UNIX)

Parent process name	Function	Child process name	Function
`jco_spmd` (1)[#1]	Process management	`jcamain` (1)	Automatic Action Service (Process management display name: `jcamain`)
		`evtcon` (1)[#1]	Event Console Service (Process management display name: `evtcon`)
		`evflow` (1)	Event Base Service (Process management display name: `evflow`)
		`jcsmain` (1)	Central Scope Service[#3] (Process management display name: `jcsmain`)
		`jcfmain` (1)	IM Configuration Management Service[#3] (Process management display name: `jcfmain`)
		`evgen` (2)[#2, #4]	Event Generation Service[#3] (Process management display name: `evgen`)

#1: The number of these processes may temporarily increase.

#2: The maximum number is 2, but the normal number is 1. The details are explained below.

- Event Generation Service process core

- This is a process that is temporarily generated when Event Service is connected. It is generated in the following cases:

- When Event Generation Service starts
- When the event acquisition filter is updated

#3: In the default, this service does not run.

#4: This is the service that is used when the integrated monitoring database is not used.

When JP1/IM - Manager is running in a cluster system, the above processes are executed on each physical host and on each logical host. The number of processes that execute simultaneously can be obtained by multiplying the number of physical hosts and logical hosts that are running by the number of above processes. The processes that are running in a cluster system are displayed as follows when the `ps` command is executed (note that `evtcon` and `evgen` are not followed by a logical host name).

`jco_spmd` *logical-host-name*

`evflow` *logical-host-name*

`jcamain` *logical-host-name*

`evtcon`

`evgen`

`jcsmain` *logical-host-name*

`jcfmain` *logical-host-name*

In the table, a process whose parent process is `jco_spmd` is controlled by process management, and you can use the `jco_spmd_status` command to check the process status.

- A display example during normal operations follows.
  ```
  # jco_spmd_status
  KAVB3690-I Processing to report the status of JP1_CONS has started.
  Shows processes that are running.
  Process name Process ID
  evflow 3672
  jcamain 4088
  evtcon 4236
  jcsmain#1 4846
  jcfmain#2 4950
  evgen#3 5624
  KAVB3691-I All the processes have started.
  ```
  #1: `jcsmain` is displayed only when the Central Scope is enabled.

  #2: `jcfmain` is displayed only when the IM Configuration Management is enabled.

  #3: `evgen` is displayed only when the Event Generation Service is enabled.

(2) Outputting a dump file for JP1/IM

(a) JP1/IM - Manager

You only need to output a dump file for JP1/IM - Manager when the health check function detects an abnormality in JP1/IM - Manager. Execute the `jcogencore` command as follows.

```
jcogencore
```

When you execute the `jcogencore` command, a message appears asking you to select the process from which to output a dump file. Select the process that is included in the message information issued by the health check function. If a dump file already exists, an overwrite confirmation message is displayed. If you choose not to overwrite the dump file, choose `n` and terminate the command. Next, save the dump file and then re-execute the `jcogencore` command.

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

(3) Collecting information related to the Web version of JP1/IM - View

When a problem occurs in the Web version of JP1/IM - View, collect the following data in addition to the data described in this section.

View side

- Java stack trace log

  The collection procedure follows.

    1. Choose the Java Console window and enter `v`.

    The Java stack trace log is output to the Java Console window.

    2. Copy the log and manually paste it to a text file, for example.

    3. Save the text file.

- Java trace file of Java^{TM} Plug-in

  The Java trace file is located in the following directory:

  system-drive`:\Documents and Settings\`*login-user-name*`\Application Data\Sun\Java`
  `\Deployment\log\`

  > **▌ Important note**
  >
  > The Java trace file of Java^{TM} Plug-in is erased when Java^{TM} Plug-in restarts. Therefore, if a problem occurs, save the content of this file to another file before restarting.

Manager side

- HTTP server error log
- HTTP server access log

(4) Executing the data collection tool

This subsection describes execution of the data collection tool (`jim_log.sh`).

When you execute the `jim_log.sh` command, which is provided by JP1/IM - Manager, you can collect the data necessary for troubleshooting JP1/IM - Manager and JP1/Base on the same host.

Because the total volume of data collected by a data collection tool is massive, you need to estimate it before you execute the command and make sure the machine you are using has sufficient free space. For the volume of data that will be collected by the `jim_log.bat` command, see the JP1/IM - Manager release notes.

A tool execution example follows.

```
# /opt/jp1imm/tools/jim_log.sh -f data-storage-directory
```

When you execute the tool, the collected data is summarized in the `tar` format and output as compressed data.

(5) Checking the operation content

Check the content of the operation that was taking place when the problem occurred, and record it. The following types of information must be checked:

- Operation content details
- Time of problem occurrence
- Reproducibility
- Login user name that was used to log in from JP1/IM - View
- Machine configuration (version of each OS, host name, and Central Console configuration)

(6) Collecting the error information on the screen

If an error is displayed on the screen, collect that information as well. Collect a hard copy of the following:

- Error dialog box
  If the **Details** button is available, copy its content as well.

10.5 Troubleshooting

10.5.1 Dealing with common problems

This section explains how to correct the problems that can generally be anticipated.

(1) Actions to take when you cannot log on 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 on the API settings file (`api`) and the event server settings file (`conf`), see the chapters on these files in the *Job Management Partner 1/Base User's Guide*.

Cause 3

JP1/IM - Manager is running on an IPv6 host.

Corrective action 3

JP1/IM - Manager does not support IPv6 hosts. Therefore, when the monitored host is an IPv6 host, install JP1/IM - Manager on an IPv4/IPv6 host. Follow the instructions in error messages to take corrective action.

(3) Actions to take when the definition menu is not displayed in the Event Console window

In the **Options** menu of the Event Console window, menu-related definitions are disabled.

Cause

The JP1 resource group settings are invalid.

Corrective action

>Make sure that in the JP1 resource group settings, the group name `JP1_Console` is specified for the JP1 resource group of the logged-in JP1 user, and `JP1_Console_Admin` or `JP1_Console_Operator` is specified for the permission level.

(4) Actions to take when the trapped JP1 event message indicates unreadable characters

The following are possible causes:

- The character encoding of the monitored log file does not match the encoding specified on the **Configuration File** page.
- The specified character encoding is not supported on the agent host.

The corrective action to take for each case is described as follows:

The character encoding of the monitored log file does not match the encoding specified on the **Configuration File** *page.*

>Correct the character encoding of monitored log file, and then retry the operation.

>Note that this problem can also occur in remote monitoring.

The specified character encoding is not supported on the agent host.

>Even when the character encoding is supported by JP1/IM - Manager, it might not be specifiable for the version of JP1/Base installed on the agent host. Check the version of JP1/Base installed on the agent host, and set a supported character encoding. Then retry the operation.

(5) Actions to take when you cannot execute a command

In the Execute Command window, the message `KAVB0415-E: The command cannot be executed because the business group or monitoring group specified for the execution host name is not defined. (execution host name = `*execution-host-name*`) is output.*

Cause

>The business group or monitoring group specified for the execution host name is not defined.

Corrective action

>Review the business group or monitoring group, and then re-execute the command. Note that the information in this message cannot be checked by using the `jcocmdshow` command of JP1/Base.

>If you are still unable to execute the command, contact the system administrator and confirm the settings of the business group.

In the Execute Command window, the message `KAVB0416-E: The command cannot be executed because the host specified for the execution host name is not a management target. (execution host name = `*execution-host-name*`) is output.*

Cause

>The host specified for the execution host name is not a managed host.

Corrective action

>Check the type of host and then re-execute the command. Note that the information in this message cannot be checked by using the `jcocmdshow` command of JP1/Base.

>If you are still unable to execute the command, contact the system administrator and check the settings of the business group.

In the Execute Command window, the message `KAVB0417-E: The command cannot be executed because the user does not have the permissions necessary to execute it on the business group specified in the execution host name. (execution host name = execution-host-name)` *is output.*

> Cause
>
>> No permission is required for executing the command for the business group specified for the execution host name.
>
> Corrective action
>
>> Review the business group or monitoring group, and then re-execute the command. Note that the information in this message cannot be checked by using the `jcocmdshow` command of JP1/Base.
>>
>> If you are still unable to execute the command, contact the system administrator and check the settings of the business group.

In the Execute Command window, the message `KAVB0418-E: The command cannot be executed because the user does not have the permissions necessary to execute on the host specified in the execution host name. (execution host name = execution-host-name)` *is output.*

> Cause
>
>> No permission is required for executing the command on the host specified for the execution host name.
>
> Corrective action
>
>> Review the host and then re-execute the command. Note that the information in this message cannot be checked by using the `jcocmdshow` command of JP1/Base.
>>
>> If you are still unable to execute the command, contact the system administrator and check the settings of the business group.

In the Execute Command window, the message `KAVB0419-E: The command cannot be executed because a host group is defined with the same name as the host name specified for the execution host name. (execution host name = execution-host-name)` *is output.*

> Cause
>
>> The host group name specified for the destination host name is the same as the execution host name.
>
> Corrective action
>
>> Confirm that no host group has the same name as the host name specified for the execution host name. If there is such a host group, change either name of the host or of the host group.

In the Execute Command window, the message `KAVB0422-E: A host is not defined for the business group or monitoring group. (group name = group-name)` *is output.*

> Cause
>
>> No host is defined for the business group or monitoring group specified for the execution host name.
>
> Corrective action
>
>> Define a host for the specified business group or monitoring group. Also review the coding of the business group or monitoring group path.

In the Execute Command window, the message `KAVB0423-E: The business group or monitoring group is not defined. (group name = group-name)` *is output.*

> Cause
>
>> The business group or monitoring group specified for the execution host name is not defined.

Corrective action

Define the specified business group or monitoring group. Also review the coding of the business group or monitoring group path.

In the Execute Command window, the message `KAVB2027-E:Cannot execute the command. Failed to simulate the user` *user-name* `environment.` *is output.*

Cause

The user mapping setting is invalid.

Corrective action

Check the user mapping setting. If it is not set, set it. This setting is required in Windows.

When the host specified for the mapping source server name is using DNS, a domain name must be included in the setting. If the host name is correct but the simulation still fails, check whether DNS is being used. For details about the user mapping setting, see the chapter related to user mapping in the *Job Management Partner 1/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 *Job Management Partner 1/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 on to JP1/IM - View, and then re-execute the command.

The execution result from the DOS prompt differs from the execution result in the Execute Command window, or it differs from the execution result of an automated action.

Cause

The OS user environment used for execution is invalid.

Corrective action

Enable the `-loaduserprofile` option of the `jcocmddef` command. For details, see *7.4.4(3)(c) Environment for command execution* in the *Job Management Partner 1/Integrated Management - Manager Overview and System Design Guide*. See also the chapter that explains commands in the *Job Management Partner 1/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, restored 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 -l3 *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 *Job Management Partner 1/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 *Job Management Partner 1/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 *Job Management Partner 1/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 *Job Management Partner 1/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 *Job Management Partner 1/Base User's Guide*.

   In Windows

Table 10–19: Locations of files to be deleted (Windows)

File name	Location
Command execution log file for automated actions	• *Base-path*`\log\COMMAND\ACTISAMLOGV8.DRF` • *Base-path*`\log\COMMAND\ACTISAMLOGV8.K01` • *Base-path*`\log\COMMAND\ACTISAMLOGV8.KDF`
	• *shared-folder*`\jp1base\log\COMMAND\ACTISAMLOGV8.DRF` • *shared-folder*`\jp1base\log\COMMAND\ACTISAMLOGV8.K01` • *shared-folder*`\jp1base\log\COMMAND\ACTISAMLOGV8.KDF`
Action information file	*Console-path*`\log\action\actinf.log`
	shared-folder`\jp1cons\log\action\actinf.log`
Action host name file	*Console-path*`\log\action\acttxt{1|2}.log`
	shared-folder`\jp1cons\log\action\acttxt{1|2}.log`

In UNIX

Table 10–20: Locations of files to be deleted (UNIX)

File name	Location
Command execution log file for automated action	• `/var/opt/jp1base/log/COMMAND/actisamlogv8.DAT` • `/var/opt/jp1base/log/COMMAND/actisamlogv8.K01` • `/var/opt/jp1base/log/COMMAND/actisamlogv8.DEF`
	• *shared-directory*`/jp1base/log/COMMAND/actisamlogv8.DAT` • *shared-directory*`/jp1base/log/COMMAND/actisamlogv8.K01` • *shared-directory*`/jp1base/log/COMMAND/actisamlogv8.DEF`
Action information file	`/var/opt/jp1cons/log/action/actinf.log`
	shared-directory`/jp1cons/log/action/actinf.log`
Action host name file	`/var/opt/jp1cons/log/action/acttxt{1|2}.log`
	shared-directory`/jp1cons/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 *Job Management Partner 1/Base User's Guide*.

In Windows

Table 10–21: Locations of files to be deleted (Windows)

File name	Location
Command execution log file for command execution	• *Base-path*`\log\COMMAND\CMDISAMLOGV8.DRF` • *Base-path*`\log\COMMAND\CMDISAMLOGV8.K01` • *Base-path*`\log\COMMAND\CMDISAMLOGV8.KDF`
	• *shared-folder*`\jp1base\log\COMMAND\CMDISAMLOGV8.DRF` • *shared-folder*`\jp1base\log\COMMAND\CMDISAMLOGV8.K01` • *shared-folder*`\jp1base\log\COMMAND\CMDISAMLOGV8.KDF`

In UNIX

Table 10–22: Locations of files to be deleted (UNIX)

File name	Location
Command execution log file for command execution	• `/var/opt/jp1base/log/COMMAND/cmdisamlogv8.DAT` • `/var/opt/jp1base/log/COMMAND/cmdisamlogv8.K01` • `/var/opt/jp1base/log/COMMAND/cmdisamlogv8.DEF`

File name	Location
	• *shared-directory*/jp1base/log/COMMAND/cmdisamlogv8.DAT • *shared-directory*/jp1base/log/COMMAND/cmdisamlogv8.K01 • *shared-directory*/jp1base/log/COMMAND/cmdisamlogv8.DEF

4. Start JP1/Base.

5. Start JP1/IM - Manager.

(10) Actions to take when Unknown is displayed as the automated action execution status

There may be inconsistencies among the files in which automated action execution results are saved (action information file, action host name file, and command execution log file).

If so, you need to delete the files in which automated action execution results are saved. If you delete these files, you will no longer be able to view past automated action execution results. Therefore, if deletion will cause a problem, back up the files. For details, see *1.2.2 Database backup and recovery*.

The deletion procedure follows.

1. Stop JP1/IM - Manager and then stop JP1/Base.

   In the case of a cluster configuration, operate the cluster software to stop the logical hosts. After you have confirmed that they have stopped, mount a shared disk in the shared directory.

2. Delete the action information file, action host name file, and command execution log file.

   The table below shows the locations of the files to delete.

   In Windows

   Table 10–23: Locations of files to delete (Windows)

File name	Location
Action information file	*Console-path*\log\action\actinf.log
	shared-folder\jp1cons\log\action\actinf.log
Action host name file	*Console-path*\log\action\acttxt{1|2}.log
	shared-folder\jp1cons\log\action\acttxt{1|2}.log
Command execution log file	All files under *Base-path*\log\COMMAND\
	All files under *shared-folder*\jp1base\log\COMMAND\

   In UNIX

   Table 10–24: Locations of files to delete (UNIX)

File name	Location
Action information file	/var/opt/jp1cons/log/action/actinf.log
	shared-directory/jp1cons/log/action/actinf.log
Action host name file	/var/opt/jp1cons/log/action/acttxt{1|2}.log
	shared-directory/jp1cons/log/action/acttxt{1|2}.log

File name	Location
Command execution log file	All files under `/var/opt/jp1base/log/COMMAND/`
	All files under *shared-directory*`/jp1base/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 *7.1.4 Checking command execution status and deleting a command* in this manual, and see *7.4.4(6) Commands for troubleshooting* in the *Job Management Partner 1/Integrated Management - Manager Overview and System Design Guide*.

The message `KAVB2239-E: A network connection with the connected host could not be established.` *is displayed.*

Cause

JP1/Base on the executing host stopped while the command was being executed.

Corrective action

Restart JP1/Base on the executing host.

As a means of monitoring JP1/Base, the JP1/Base health check function is available. For details, see *7.4.8 JP1/Base health check function* in the *Job Management Partner 1/Integrated Management - Manager Overview and System Design Guide*.

There are a large number of commands whose execution status (`STATUS`*) is* `Q`.

Cause

The number of automated actions to be executed is too large.

Corrective action

Check the automated actions being executed and reassess the following:

- Were any unnecessary automated actions set?
- Is it possible to narrow the JP1 events for which automated actions are to be set?

If there are no unnecessary automated actions, use the `jcocmddef` command[#] to increase the number of commands that can be executed simultaneously. For details, see *12.7.6 Command execution environment* in the *Job Management Partner 1/Integrated Management - Manager Overview and System Design Guide*.

[#]

For details about the `jcocmdshow` command, `jcocmddel` command, and `jcocmddef` command, see the chapter explaining commands in the *Job Management Partner 1/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 `Jismlcktr` command.

3. Determine which process has locked the files under *Scope-path*`\database`.

4. Execute the `Jislckfree -p PID` command on the process ID determined in Step 3.

The `Jismlcktr` and `Jislckfree` commands are provided by JP1/Base. For details, see the chapter that explains commands in the *Job Management Partner 1/Base User's Guide*.

(14) Actions to take when KAVB5150-W is displayed in the detailed information (message) for the action result

When the Action Log Details window is opened, the message `KAVB5150-W: There is no applicable data in the Command Executed log file.` *is displayed in the message column.*

Cause

The command execution log file (`ISAM`) may have wrapped. If it has wrapped, automated action execution results cannot be displayed.

Corrective action

If this phenomenon occurs frequently, consider increasing the upper limit for the record count in the command execution log file. Keep in mind, however, that increasing the record count will also use more disk space.

The procedure follows.

Changing the upper limit for the record count

When you increase the upper limit for the record count, you must delete the command execution log file to enable the new setting. When you delete the command execution log file, all history on past automated actions and command execution is lost. Therefore, if deletion will cause a problem, back up the files. For details, see *1.2.2 Database backup and recovery*.

1. Execute the `jcocmddef` command to change the record count in the command execution log file.

2. Stop JP1/IM - Manager and JP1/Base.

   In the case of a cluster configuration, operate the cluster software to stop the logical hosts.

   After you have confirmed that they have stopped, mount a shared disk in the shared directory.

3. Delete the command execution log files.

   This means all files under the command execution log folder. The default command execution log folder is described below.

   In Windows

   Table 10–25: Locations of command execution log files (Windows)

File name	Location
Command execution log file	All files under *Base-path*`\log\COMMAND\`
	All files under *shared-folder*`\jp1base\log\COMMAND\`

   In UNIX

   Table 10–26: Locations of command execution log files (UNIX)

File name	Location
Command execution log file	All files under `/var/opt/jp1base/log/COMMAND/`
	All files under *shared-directory*`/jp1base/log/COMMAND/`

   For details about the command execution log file, see the *Job Management Partner 1/Base User's Guide*.

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

   In the case of a cluster configuration, unmount the shared disk and then operate the cluster software to start the logical hosts.

For details about the `jcocmddef` command, see the chapter that explains commands in the *Job Management Partner 1/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 then 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: *1.19.3(2) Executing the Central Scope upgrade command* in the *Job Management Partner 1/ Integrated Management - Manager Configuration Guide*

  UNIX: *2.18.5(2) Executing the Central Scope upgrade command* in the *Job Management Partner 1/ Integrated Management - Manager Configuration Guide*

- For a logical host

  Windows: *6.2.3 Installing and setting up the logical host (upgrade installation and setup)* in the *Job Management Partner 1/Integrated Management - Manager Configuration Guide*

  UNIX: *6.3.3 Installing and setting up the logical host (upgrade installation and setup)* in the *Job Management Partner 1/Integrated Management - Manager Configuration Guide*

When the version of JP1/IM - Manager is later than the version of JP1/IM - View, and an earlier version of the monitored object database is being used:

Follow the procedure below to upgrade the JP1/IM - View version.

1. In the Monitoring Tree (Editing) window, choose **File** and then **Save Tree**, and save the edited monitoring tree in the `csv` file.

2. Uninstall JP1/IM - Manager.

3. Delete the JP1/IM - Manager installation directory.

4. Install the version of JP1/IM - Manager or JP1/IM - Central Scope that matches the version of JP1/IM - View.

5. In the Monitoring Tree (Editing) window, choose **File** and then **Open Tree**, and load the `csv` file that was saved.

6. In the Monitoring Tree (Editing) window, choose **File** and then **Update Server Tree** to update the server tree.

7. Upgrade JP1/IM - Manager to the later version.

8. Upgrade JP1/IM - View to the same version as JP1/IM - Manager.

The message `KAVB6046-E: The user (`*user*`) does not have permission necessary for operations.` *is displayed.*

Cause

The version of JP1/IM - View is earlier than the version of JP1/IM - Manager, or the edited data in JP1/IM - View is from an earlier version.

Corrective action

Follow the procedure below to upgrade the version of JP1/IM - View.

1. In the Monitoring Tree (Editing) window, choose **File** and then **Save Tree**, and save the edited monitoring tree in the `csv` file.

2. Uninstall JP1/IM - Manager.

3. Delete the JP1/IM - Manager installation directory.

4. Install the JP1/IM - Manager version that is the same version as JP1/IM - View.

5. In the Monitoring Tree (Editing) window, choose **File** and then **Open Tree**, and load the `csv` file that was saved.

6. In the Monitoring Tree (Editing) window, choose **File** and then **Update Server Tree** to update the server tree.

7. Upgrade JP1/IM - Manager to the later version.

8. Upgrade JP1/IM - View to the same version as JP1/IM - Manager.

(16) Actions to take when many JP1 events occurred for which correlation events were generated

If an operation such as system maintenance generates a large number of JP1 events for which correlation events are generated, the correlation event generation process may become overloaded.

The following two methods are available for avoiding this situation:

- Pause the correlation event generation process.
- Stop JP1/IM - Manager.

Stop JP1/IM - Manager only if the problem cannot be avoided even after the correlation event generation process has been paused.

Pausing the correlation event generation process

Pause the correlation event generation process, and resume it once the situation has improved.

The procedure follows.

1. Execute the `jcoegsstop` command to pause correlation event generation processing.

Executing the `jcoegsstop` command places Event Generation Service in standby status. This means that JP1 events generated during this period are not processed.

Since the command stops only the processing without actually stopping the service, operations can continue without failover during cluster operation.

2. To resume correlation event generation processing, execute the `jcoegsstart` command.

Stopping JP1/IM - Manager

When you stop JP1/IM - Manager, if the startup option is set to `cold`, there is no need to perform the procedure described below. Perform it only when the startup option is set to `warm`.

The procedure follows.

1. Edit the correlation event generation system profile (`egs_system.conf`) and then change the startup option to `cold`.

2. Restart JP1/IM - Manager.

3. Edit the correlation event generation system profile (`egs_system.conf`) and then change the startup option back to `warm`.

4. Execute the `jco_spmd_reload` command to enable the startup option setting.

(17) Actions to take when correlation events cannot be displayed in JP1/IM - View

The following are possible causes:

- Correlation event generation is not enabled.
- Correlation event generation definition has not been created.
- Correlation events are being filtered.
- The applied correlation event generation definition is damaged.

The action to take in response to each cause is described below.

Correlation event generation is not enabled.

Event Generation Service is an optional function and thus does not start by default. If Event Generation Service is not set to start, execute the `jcoimdef` command to set up the service to start. Event Generation Service will now start when JP1/IM - Manager is restarted.

To check whether the correlation event generation process is running, first restart JP1/IM - Manager and then execute the `jcoegsstatus` command to check whether Event Generation Service is in `RUNNING` status.

A correlation event generation definition has not been created.

Event Generation Service generates correlation events according to the correlation event generation definition. Since the correlation event generation definition is not created by default, correlation events are not generated.

After you have created the correlation event generation definition file, execute the `jcoegschange` command to apply the correlation event generation definition to Event Generation Service. You can use the `jcoegsstatus` command to check the correlation event generation definition that has been applied.

Correlation events are being filtered.

Check whether correlation events are not being filtered by an event acquisition filter, a user filter, a severe event filter, or a view filter.

Like normal JP1 events, correlation events are also filtered by an event acquisition filter, a user filter, a severe event filter, and a view filter. Furthermore, events for which no severity level has been defined are filtered by an event acquisition filter (in the default setting).

The applied correlation event generation definition is damaged.

If the message described below is output to the integrated trace log, the correlation event generation definition that was applied to Event Generation Service by the `jcoegschange` command may have been damaged.

- `KAJV2246-E An incorrect definition was detected because the correlation event generation definition storage file is corrupt. (line = ` *line-number*`, incorrect contents = ` *invalid-content*`)`

If this message is output, execute the `jcoegschange` command and apply the correlation event generation definition again.

(18) Actions to take when the JP1/IM - View window cannot be displayed after you log on to JP1/IM - View

After you log on 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 on 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 from JP1/IM - View.

3. After you log on 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 operates in compatibility mode, or the common exclusion-conditions operate in basic mode.

- The definition file has an error.

- 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, restart JP1/IM - Manager or execute the `jco_spmd_reload` command 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 restart JP1/ IM - Manager or execute the `jco_spmd_reload` command 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 restart JP1/IM - Manager or execute the `jco_spmd_reload` command 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 restart JP1/IM - Manager or execute the `jco_spmd_reload` command 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 restart JP1/IM - Manager or execute the `jco_spmd_reload` command to reload the common-exclusion-conditions auto-input definition file.

(21) Actions to take when processing of JP1 events received by JP1/IM - Manager (JP1/IM - Central Scope) is delayed

Cause

Name resolution of the character string (host name or IP address) specified as an attribute value of the individual condition in the status-change condition settings may have failed.

Corrective action

The host name that could not be resolved is output to the following logs:

In Windows

Scope-path`\log\jcsmain_trace{1|2|3}.log`#

In UNIX

`/var/opt/jp1scope/log/jcsmain_trace{1|2|3}.log`#

\#

Do not specify this log as the monitoring target of the JP1/Base log file trapping function.

If name resolution failed, one of the following messages is output in the aforementioned log file:

`...fs_jcsHostsAccessPtr->getHostByName() is failed. (host = `*host-name-for-which-name-resolution-failed*`,jp1error = 2001)...`

or

`...fs_jcsHostsAccessPtr->getHostByAddr() is failed. (host = `*IP-address-for-which-name-resolution-failed*`,jp1error = 2001)...`

Check one of these messages and specify **Host name comparison** as the individual condition. Then, use one of the methods described below to enable name resolution of the host name or IP address specified as the attribute value.

- Register in the host information database the host name or IP address specified as the attribute value of the individual condition.
- Register in the `jp1hosts` information or the `jp1hosts2` information of JP1/Base the host name or IP address specified as the attribute value of the individual condition.
- Register in `hosts` or DNS the host name or IP address specified as the attribute value of the individual condition.

(22) Actions to take when no response-waiting events are displayed in JP1/IM - View

Cause

The following are possible causes:

- The response-waiting event management function is disabled.
  `OFF` might be specified as the value of the `-resevent` option of the `jcoimdef` command.
- No response-waiting events have been issued.
- Response-waiting events have been issued but were filtered by JP1/IM - Manager.

Corrective action

If the response-waiting event management function is disabled, enable it by executing the `jcoimdef` command with `ON` specified in the `-resevent` option.

If the response-waiting event management function is enabled, follow the steps below to identify the cause of the problem:

1. Check whether response-waiting events are registered in the event database on the JP1/IM - Manager host.

As a JP1 user such as the administrator who is not subject to an event receiver filter, check whether response-waiting events are registered in the event database by conducting an event search.

If there are no response-waiting events registered in the database, investigate further according to Step 2 below.

If there are response-waiting events in the database, a filter (an event acquisition filter or an event receiver filter) is filtering the events in JP1/IM - Manager. In this case, review the filter conditions.

2. Check the log files on the BJEX or JP1/AS host for BJEX errors, JP1/AS errors, or communication errors.

If an error message was output, take action as described in the message. BJEX or JP1/AS might have been set up incorrectly, or a communication error might have occurred.

(23) Actions to take when response-waiting events are displayed in JP1/IM - View but as ordinary JP1 events (the arrow icon does not appear and you cannot enter a response)

Cause

The following are possible causes:

- The response-waiting event management function is disabled.

  OFF might be specified as the value of the -resevent option of the jcoimdef command.

- The JP1/IM - Manager host name is specified incorrectly in the BJEX or JP1/AS configuration.

  An IP address might be specified instead of a host name.

- The response-waiting event was forwarded to a JP1/IM - Manager host other than the one set up in BJEX or JP1/AS.

Corrective action

Take the corrective action that matches the cause.

- Enable the response-waiting event management function.

  Execute the jcoimdef command with ON specified in the -resevent option.

- Specify the correct JP1/IM - Manager host name in the settings of BJEX or JP1/AS.

- To respond to the response-waiting event, log in to the JP1/IM - Manager host specified in the BJEX or JP1/AS settings.

(24) Actions to take when no JP1 event is displayed in the Event Console window

Cause

Because no condition is specified in the exclusion-conditions or valid common exclusion-conditions for a filter, all JP1 events are excluded.

Corrective action

Reassess the exclusion-conditions or valid common exclusion-conditions for the following filters:

- 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 source 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 JP1/IM - Central Scope is used, the match processing might take a long time due to a 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 use JP1/IM - 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 *Job Management Partner 1/Integrated Management - Manager Overview and System Design Guide*.

- When you set `local` as the method for obtaining the event source 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 source host name to `remote`, and then restart JP1/IM - Manager. For details about the method for obtaining the event source host name, see *Automated action environment definition file*

(action.conf.update) in *2. Definition Files* in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*. For details about the `hosts` setting of the OS, see *12.4.1 Host names and IP addresses* in the *Job Management Partner 1/Integrated Management - Manager Overview and System Design Guide*.

- When you use JP1/IM - Central Scope, in addition to the actions above, confirm whether name resolution of the character string (host name or IP address) specified as an attribute value of the individual condition in the status-change condition settings can be performed promptly. For details, see *10.5.1(21) Actions to take when processing of JP1 events received by JP1/IM - Manager (JP1/IM - Central Scope) is delayed*.

  Furthermore, if you use the memory-resident function for the status change condition of the monitoring object, the match processing time for a change of monitoring object status takes less time. When you estimate the memory requirements for securing sufficient memory, we recommend that you set this function. For details about the memory-resident function for the status change condition of the monitoring object, see *4.2.3 Status change conditions* in the *Job Management Partner 1/Integrated Management - Manager Overview and System Design Guide*.

- If the communication type of the `server` parameter is set to `close` in the API settings file (`api`), a temporary port is used each time JP1/IM - Manager receives an event, so temporary ports will run short. As a result, a communication error or delay in receiving events might occur. On the event server to which JP1/IM - Manager connects, in the API settings file (`api`), make sure that you set the communication type of the `server` parameter to `keep-alive`.

(26) Actions to take when a status cannot be changed

The following are possible causes:

- Connection cannot be established between the event console and Central Console. Alternatively, connection cannot be established between the event console and the `jcochstat` command.
- The specified JP1 event was an event that cannot be changed.
- Connection cannot be established between Event Console Service and Event Service.
- Connection cannot be established between Event Console Service and Event Base Service.
- Connection cannot be established between Event Base Service and the IM database service.

The action to take in response to each cause is described below.

Connection cannot be established between the event console and Central Console. Alternatively, connection cannot be established between the event console and the `jcochstat` *command.*

The event console on the manager may not have been started, the system (host or network) may be under a heavy workload, or the network settings may be invalid.

- Corrective action

  Execute the `jco_spmd_status` command to check whether the event console on the manager has started, and then try to change the status again.

  Alternatively, use the `ping` command, for example, to check whether the logged-in host is running normally, and then try to change the status again.

The specified JP1 event was an event that cannot be changed.

- Corrective action

  Reassess the serial number inside the event database and then try to change the status again.

Connection cannot be established between Event Console Service and Event Service.

- Corrective action

Check whether Event Service has started, and then try to change the status again.

Connection cannot be established between Event Console Service and Event Base Service.

Event Base Service may not have been started, or the system (host or network) may be under a heavy workload.

- Corrective action

   Execute the `jco_spmd_status` command to check whether Event Base Service on the manager has started, and then try to change the status again.

Connection cannot be established between the Event Base Service and the IM database service.

The IM database service may not have been started, or the system (host or network) may be under a heavy workload.

- Corrective action

   First start the IM database service, and then try to change the status again.

(27) Actions to take when an event search cannot be performed

The following are possible causes:

- Connection cannot be established between the event console and the viewer.
- Connection cannot be established between Event Base Service and Event Console Service.
- Connection cannot be established between Event Base Service and the integrated monitoring database.
- Connection cannot be established between Event Console Service and Event Service.
- A JP1 event search was performed using an unsupported condition.
- The regular expression specified for performing the event search was invalid.
- When an event search was performed with an exclusion-condition specified, the JP1/Base version of the search host was 08-11 or earlier.

The action to take in response to each cause is described below.

Connection cannot be established between the event console and the viewer.

The event console on the manager may not have been started, the system (host or network) may be under a heavy workload, or the network settings may be invalid.

- Corrective action

   Execute the `jco_spmd_status` command to check whether the event console on the manager has started, and then perform the event search again.

   Alternatively, use the `ping` command, for example, to check whether the logged-in host is running normally, and then perform the event search again.

Connection cannot be established between Event Base Service and Event Console Service.

Event Base Service may not have been started, or the system (host or network) may be under a heavy workload.

- Corrective action

   Execute the `jco_spmd_status` command to check whether Event Base Service has started on the manager, and then perform the event search again.

Connection cannot be established between Event Base Service and the integrated monitoring database.

The integrated monitoring database may not have been started, or the system (host or network) may be under a heavy workload.

- Corrective action

   First start the integrated monitoring database, and then perform the event search again.

Connection cannot be established between Event Console Service and Event Service.

The Event Service instance at the target host may not have been started, the system (host or network) may be under a heavy workload, or the network settings may be invalid.

- Corrective action

    Execute the `jevstat` command to check whether the Event Service instance at the target host has started, and then perform the event search again. For details about the `jevstat` command, see the *Job Management Partner 1/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* (*1. Commands*) in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.

The IM database has not been started.

- Corrective action

    Make sure that the IM database has been started.

The port number setting is invalid.

- Corrective action

    Make sure that the specified port number is not the same as any of the following port numbers:
    - Port number specified during the setup of another logical host
    - Port number described in the `services` file
    - Port number that is used by a HiRDB instance bundled with another product
    - Temporary port number that is used by another product or by the OS, for example

When a logical host in a non-cluster system was set up, standby was specified for the `-c` *option of the* `jcfdbsetup` *or* `jcodbsetup` *command.*

- Corrective action

    When setting up a logical host of a non-cluster system, specify `online` for the `-c` option of the `jcfdbsetup` or `jcodbsetup` command.

(31) Actions to take when JP1/IM - Manager cannot be uninstalled

The message `KAVB9940-E: Unsetup has not been performed for the IM database service on the physical host.` *or* `KAVB9941-E: Unsetup has not been performed for the IM database service on the logical host. (Logical host name: ` *logical-host-name* `)` *is output.*

Cause

    The IM database has not been unset up.

Corrective action

    Make sure that the integrated monitoring database and the IM Configuration Management database have been unset up.

(32) Actions to take when an error message indicating an invalid port number is issued after the IM database has been set up

The message `KNAN11044-E: The setup information file does not exist.` *is output.*

Cause

    The specified port number is the same as a port number being used elsewhere.

Corrective action

    Make sure that the specified port number is not the same as any of the following port numbers:

- Port number specified during the setup of another logical host

- Port number described in the `services` file

- Port number that is used by a HiRDB instance bundled with another product

- Temporary port number that is used by another product or the OS, for example

(33) Actions to take when IM database setup fails

The message `KNAN11084-E: Creation of a database file system area has failed.` *is output.*

The following are possible causes:

- The file system in the path specified in `IMDBDIR` or `SHAREDBDIR` 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* `SHAREDBDIR` *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 of the host onto which the system hierarchy is to be applied has not been started.
  To apply the system hierarchy, all hosts included in the system hierarchy must be active.
- 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 the JP1/Base of the host for which system hierarchy application failed is active, and then retry the operation.

- 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 if from that system hierarchy, and then retry the operation.

- 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 on to IM Configuration Management - View is not assigned IM Configuration Management permissions (`JP1_CF_Admin`, `JP1_CF_Manager`, or `JP1_CF_User`), the only operation that is allowed is viewing. The following are possible causes:

- The instance of JP1/Base specified in the authentication server is Version 8 or earlier.

- After the instance of JP1/Base specified in the authentication server was upgraded from Version 8 or earlier by means of overwrite installation, the JP1 user was not assigned IM Configuration Management permissions (`JP1_CF_Admin`, `JP1_CF_Manager`, or `JP1_CF_User`).

- The JP1 user is not assigned IM Configuration Management permissions (`JP1_CF_Admin`, `JP1_CF_Manager`, or `JP1_CF_User`).

Corrective action

Take the corrective action that matches the cause.

- Upgrade the instance of JP1/Base specified on the authentication server to version 9 or later.

- Set `JP1_Console` for the JP1 resource group name of the JP1 user that logs in, assign one of the IM Configuration Management permissions (`JP1_CF_Admin`, `JP1_CF_Manager`, or `JP1_CF_User`) to the JP1 user, and then have the user log in again.

  The scope of a menu's operations differs according to the permission levels of IM Configuration Management. For details, see *Appendix E.3 Operating permissions required for IM Configuration Management* in the *Job Management Partner 1/Integrated Management - Manager Overview and System Design Guide*.

(41) Actions to take when virtualization system configuration cannot be obtained in IM Configuration Management

The message `KNAN22062-E: Collection of the virtualization configuration failed for the host "host-name" because the communication type is not supported.` *is output.*

Cause

The following are possible causes:

- The destination host name is different from the intended one.
- The name of the destination host has not been resolved.
- The destination host is not running.
- vCenter, JP1/SC/CM, SCVMM, HCSM, or KVM has not been started or set up on the destination host.
- Communication with the destination host failed.

Corrective action

Take the corrective action that matches the cause.

- Make sure that the destination host name is correct.
- Make sure that the destination host is running.
- Make sure that vCenter, JP1/SC/CM, SCVMM, HCSM, or KVM has been started and set up on the destination host.
- Make sure that there are no communication problems with the destination host. If the destination VMM host is a KVM, make sure that the SSH connection is set up correctly.

(42) Actions to take when valid configuration information of a remote monitoring log file trap or a remote monitoring event log trap cannot be viewed in IM Configuration Management

The message `KNAN22422-E: Collection of operation definition information for` *Log File Trapping* `failed. (Detail information: A required service or process is not running.)` *or* `KNAN22422-E Collection of operation definition information for` *Event Log Trapping* `failed. (Detail information: A required service or process is not running.)` *is output.*

Cause

The following are possible causes:

- Because of an error while the remote monitoring log file trap was running, the remote monitoring log file trap stopped.
- Because of an error while the remote monitoring event log trap was running, the remote monitoring event log trap stopped.

Corrective action

A description of the error occurring while the remote monitoring log file trap or the remote monitoring event log trap is running is output to the integrated log. See the corrective action for the error message output to the integrated log and remove the cause of the error. After correcting the error, stop the remote monitoring log file trap or the remote monitoring event log trap and then restart it.

(43) Actions to take if JP1 events are not received even when the remote monitoring log file trap is running in IM Configuration Management

Cause

The following are possible causes:

- The specification of the filter (`filter` to `end-filter`) in the remote-monitoring log file trap action-definition file is incorrect.

- Because the monitoring interval of the remote monitoring log file trap is long, differences occurring in log files have not been monitored.

- Although the remotely monitored host or monitored log file is invalid, an error does not occur because, on the **Valid Configuration Information** page in the Display/Edit Profiles window, you selected the sequence **Log File Trapping - Startup Options** and then enabled **Retry specification for opening a log file [-r]** or because you executed the `jcfallogstart` command with the `-r` option specified.

- Because the filter specification of the startup option for the remote monitoring log file trap is incorrect, the monitored log file data was not transferred from the monitored host.

Corrective action

- Check whether the specification of the filter (`filter` to `end-filter`) in the remote-monitoring log file trap action-definition file is correct.

- Check whether JP1 events still cannot be received even when a time greater than the file monitoring interval specified by the `-t` option of the `jcfallogstart` command has passed.

- If the remotely monitored host is a Windows host, check whether the NetBIOS (NetBIOS over TCP/IP) settings for monitoring logs on the remotely monitored host are correct. For details about the NetBIOS (NetBIOS over TCP/IP) settings, see *1.18.2 NetBIOS setting (NetBIOS over TCP/IP)* in the *Job Management Partner 1/Integrated Management - Manager Configuration Guide*.

- If the remotely monitored host is UNIX, check whether the SSH settings for monitoring logs on the remotely monitored host are correct. For details about the SSH settings, see *2.17.1 Configuring SSH* in the *Job Management Partner 1/Integrated Management - Manager Configuration Guide*.

- Make sure that the monitored log file is in a readable state.

- When the `stty`, `tty`, `tset`, or `script` command, which requires interactive operation, is coded in the login script of an SSH-connection user, log files might not be able to be read. In such cases, create a new SSH-connection user for remote monitoring, or change the login script of the SSH-connection user so that these commands are not executed.

- Check whether the filter specification of the startup option for the remote monitoring log file trap is correct. If the filter specification is correct, check whether users who use SSH connection on the remotely monitored host can execute the following command:

  For Linux:

  `/bin/grep -E '`*regular-expression-character-string-specified-in-filter*`'` *path-to-monitored-log-file*

  For Solaris:

  `/usr/xpg4/bin/grep -E '`*regular-expression-character-string-specified-in-filter*`'` *path-to-monitored-log-file*

  For OSs other than Linux and Solaris:

  `/usr/bin/grep -E '`*regular-expression-character-string-specified-in-filter*`'` *path-to-monitored-log-file*

  Furthermore, check whether the data in a monitored log file is excluded because of the filter specification.

- If you specify `-r` as an additional option, check the items listed below.

See *10.5.1(50) Actions to take when the remote monitored log file name is incorrect*, and then check whether the path is specified correctly.

- Make sure that the file access permission is set correctly.
- Operation of the log file trap without the `-r` option is effective when you check for errors.

- If none of the above actions resolves the problem, use the data collection tool to collect data on the JP1/IM - Manager host and the monitored host. The following table shows data that needs to be collected on the monitored host.

OS on monitored host	Data to be collected	Method
Windows	System information	1. Choose **Run** from the start menu. 2. Enter `msinfo32` 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	1. In Event Viewer, select the relevant event log. 2. Select **Save Log File As**, and specify `evt` 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 *10.3.2 In UNIX*.

(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	1. Choose **Run** from the start menu. 2. Enter `msinfo32` in the text box and then click the **OK** button. 3. In the System Information window, select **File** and then **Export** to save the system information in a text file.

Data to be collected	Method
Windows application and system event logs	1. Select the target event log from Event Viewer. 2. Select **Save Log File As**, and specify `evt` 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, 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.

- JP1/Base holds no configuration definition information because the `jbsrt_del` command was executed.

- 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 *Job Management Partner 1/ Integrated Management - Manager Configuration Guide* has not been performed.

Corrective action

Take the corrective action that matches the cause.

- If the agent configuration has not been applied, execute **Apply Agent Configuration** in IM Configuration Management - View.

- Execute **Collect IM Configuration** in IM Configuration Management - View. When the configuration is not the configuration you expect from the operation, execute **Apply Agent Configuration**.

(47) Actions to take when the same JP1 event is received redundantly in the remote monitoring log file trap of IM Configuration Management

Cause

- When a log is output during log processing, the same log might be trapped twice.

Corrective action

- No action is required. You can safely ignore the redundant JP1 events.

(48) Actions to take when an attempt to start the profile of a remote monitoring log file trap fails in IM Configuration Management

The message `KNAN26039-E: The specified remote log-file trap failed to start. (Host name:` *Host-name,* `Monitoring-target-name:` *monitoring-target-name,* `Details:` *message*) *is output, and an attempt to start the profile fails.*

See the actions for *KNAN26039-E* in *2.13 Messages related to IM Configuration Management (KNAN22000 to KNAN26999)* in the manual *Job Management Partner 1/Integrated Management - Manager Messages*.

If you are still unable to resolve the problem, take action as follows.

How you handle the problem depends on the detailed information.

Cannot connect to the monitored host.

Cause

- A connection to the monitored host has not been established.

Corrective action

- See *10.5.1(51) Actions to take when you cannot connect to the remotely monitored host* to check connectivity with the remotely monitored host.

Cannot access the log file of the monitoring target.

Cause

- The path to the log file is not set correctly.

Corrective action

- See *10.5.1(50) Actions to take when the remote monitored log file name is incorrect* to check correct setting of the path.

(49) Notes applying before starting a remote monitoring log file trap by using IM Configuration Management

Note:

- Make sure that the file type of the log file is correct.
- Make sure that the size of the log file is not too large.
- Make sure that the header size of the log file is not too large.

- Make sure that the JP1/Base LogTrap service does not stop.

(50) Actions to take when the remote monitored log file name is incorrect

Check whether items are set correctly.

To do so, see *Table 4-31 Items additionally displayed on the Configuration File page (when an item under Log File Trapping selected)* in *4.9.2 Configuration File page* in the manual *Job Management Partner 1/Integrated Management - Manager GUI Reference*.

The following are examples of mistakes that are easy to make:

- When the remotely monitored host is a Windows host, the path is not set in *\shared-folder-name\file-name* format.
- When the remotely monitored host is a UNIX host, the full path is not set as the path.
- The path indicates a folder.

(51) Actions to take when you cannot connect to the remotely monitored host

Check whether the following items are set correctly.

When the JP1/IM - Manager host is a Windows host:

See the following subsections in the *Job Management Partner 1/Integrated Management - Manager Configuration Guide*:

- *1.18.1 Configuring WMI*
- *1.18.2 NetBIOS setting (NetBIOS over TCP/IP)*
- *1.18.3 Configuring SSH*

When the JP1/IM - Manager host is a UNIX host:

2.17.1 Configuring SSH in the *Job Management Partner 1/Integrated Management - Manager Configuration Guide*

Check for the following problems:

- The monitored host is not running.
- Name resolution of the monitored host cannot be performed from the JP1/IM - Manager host.

(52) Actions to take when an attempt to collect host information in IM Configuration Management fails

How you resolve the problem depends on the message type.

The message `KNAN22017-E:Collection of host information failed because a connection could not be established with the host "host-name".` *is output, and an attempt to collect host information fails.*

Cause

The following are possible causes:

- The destination host name is different from the intended one.
- The name of the destination host has not been resolved.
- The destination host is not running.

- JP1/Base on the destination host is not running.

- Communication with the destination host failed.

- The version of JP1/Base on the destination host is earlier than 07-00.

Corrective action

Take the corrective action that matches the cause.

- Execute the command below on the JP1/IM - Manager host to check whether the name of the host registered in IM Configuration Management can be resolved, and whether communication with the host registered in IM Configuration Management is possible. If the system operates in an IPv6 environment, check whether the IPv6 address is the primary IP address (whether the IPv6 address is first address displayed in Resolved Host List that is displayed by executing the following command), and whether communication is possible using the IPv6 address.

  - `jp1ping` *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 `20306` (IP address)

  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 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_spmd_status` (for a logical host: `jbs_spmd_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.

  - `jp1ping` *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.

- The monitored host does not exist.

- The collection of log files timed out.

- Authentication processing failed.

- The private key does not exist.

- The creation of the remote monitoring process failed.

Corrective action

Take the corrective action that matches the cause.

- Set remote communication on the monitored host, and then retry the operation.

- Check the connection with the remotely monitored host. For details about the method, see *10.5.1(51) Actions to take when you cannot connect to the remotely monitored host*.

- Check the following:

  When the OS of the host of the monitored host name is a Windows host:

  - Whether communication with the host that has the monitored host name is possible

  - Whether the password of the user who logs in to the monitored host has expired

  - Whether the remote communication type of the host that has the monitored host name is set correctly

  - Whether the WMI service is running

  At this point, if there is no problem, check whether the WMI connection is set normally.

  When the OS of the host of the monitored host name is a UNIX host:

  - Whether communication with the host that has the monitored host name is possible

  - Whether the remote communication type of the host that has the monitored host name is set correctly

  - Whether the SSH server is running on the host that has the monitored host name

At this point, if there is no problem, check whether the SSH connection is set correctly.

- Check the following:

  When the OS of the host of the monitored host name is a Windows host:

  - Whether the user name, password, and domain name in the System Common Settings window or the Remote Monitoring Settings window are set correctly

  - Whether DCOM is set correctly on the host that has the monitored host name

  - Whether DCOM is set correctly on the JP1/IM - Manager host

  At this point, if there is no problem, check whether the WMI connection is set correctly.

  When the OS of the host of the monitored host name is a UNIX host:

  - Whether the SSH authentication settings are correct

  At this point, if there is no problem, check whether the SSH connection is set correctly.

- Check whether the private key exists.

- Check the settings on the **IM Host Account** page in the System Common Settings window.

(53) Actions to take when the source host name is different from the host name registered in IM Configuration Management

Corrective action

Take corrective action according to the version. For details, see *12.3.11(2)(b) Changing JP1 event attributes (Setting for JP1/IM - Manager)* in the *Job Management Partner 1/Integrated Management - Manager Overview and System Design Guide*.

- For a new installation or an overwrite installation of JP1/IM - Manager, perform the following steps:

1. Check the content of the common definition configuration file for changes in the JP1 event attributes.

2. Execute the `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 *10.5.1(53) Actions to take when the source host name is different from the host name registered in IM Configuration Management*.

(55) Actions to take when JP1/IM - Manager does not start, or JP1/IM - View cannot be operated after the OS starts or the network settings are changed in Windows

Cause

The following are possible causes:

- After OS startup, JP1/IM - Manager startup processing started before the network became available.

  The time from OS startup until the network becomes available depends on the environment. In an environment in which teaming is used, a few minutes might be needed before the network becomes available. Also, in a

teaming environment, JP1/IM - Manager startup processing might start before the network becomes available (for example, when JP1/IM - Manager is started automatically by the startup control function of JP1/Base).

- The network settings (such as the teaming settings) were changed during JP1/IM - Manager startup.

Corrective action

On the physical host and all logical hosts, terminate JP1/IM - Manager, JP1/IM - View, JP1/Base, and any programs that require JP1/Base. Execute `jp1ping` *local-host-name* to make sure that the local host name can be resolved to the intended IP address, and then start JP1/IM - Manager, JP1/IM - View, JP1/Base, and the programs requiring JP1/Base.

The following describes the appropriate actions to be taken in each case.

- After OS startup, JP1/IM - Manager startup processing starts before the network became available

  To automatically start JP1/IM - Manager when the OS starts, use the startup control function of JP1/Base. To do so, configure the settings so that the timing of startup of the JP1/IM - Manager service is delayed to postpone JP1/IM - Manager startup until after the network becomes available. For details about the settings, see the chapter related to the explanation for setting the timing of the startup of services in the *Job Management Partner 1/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 JP1events 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 *Job Management Partner 1/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
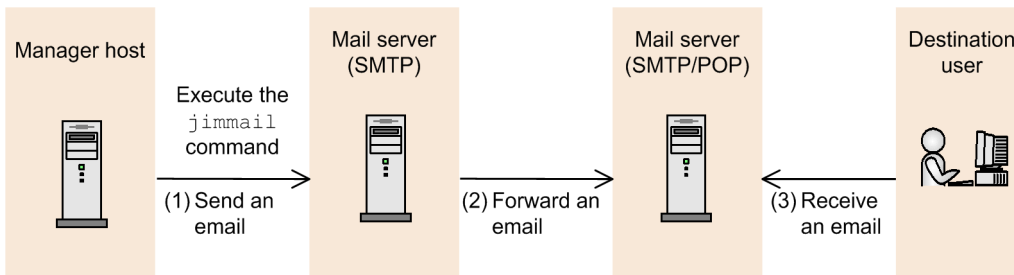
JP1/IM - Manager

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 *2. List of Messages* in the manual *Job Management Partner 1/Integrated Management - Manager Messages*.

- The mail server (SMTP) is running.

- No error occurs in the mail server (SMTP) log.

- Transit through a port in the firewall is allowed.

- Host name resolution for the mail server (SMTP) is enabled.

- The authentication account and password in the email environment definition file is correct.

Index

L

M

N

O

P

R