

**Job Management Partner 1/Integrated
Management - Manager
Administration Guide**

3020-3-R78-01(E)

■ 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.

For Windows Server 2003 and Windows XP Professional:

P-242C-6H97 Job Management Partner 1/Integrated Management - View 09-00

For Windows Server 2008 and Windows Vista:

P-2A2C-6H97 Job Management Partner 1/Integrated Management - View 09-00

For Windows Server 2003:

P-242C-8E97 Job Management Partner 1/Integrated Management - Manager 09-00

For Windows Server 2008:

P-2A2C-8E97 Job Management Partner 1/Integrated Management - Manager 09-00

For Solaris:

P-9D2C-8E92 Job Management Partner 1/Integrated Management - Manager 09-00

For AIX:

P-1M2C-8E92 Job Management Partner 1/Integrated Management - Manager 09-00

■ Trademarks

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

AIX is a registered trademark of the International Business Machines Corp. in the U.S.

HP-UX is a product name of Hewlett-Packard Company.

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

Itanium is a registered trademark of Intel Corporation or its subsidiaries in the United States and other countries.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and other countries.

Microsoft is a registered trademark of Microsoft Corp. in the U.S. and other countries.

Microsoft Internet Information Services is a product name of Microsoft Corp.

Netscape is a registered trademark of Netscape Communications Corporation in the United States and other countries.

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.

RSA, BSAFE are either registered trademarks or trademarks of RSA Security Inc. in the United States and/or other countries.

RSA Security Inc. All rights reserved.

Solaris is a trademark or registered trademark of Sun Microsystems, Inc. in the United States and other countries.

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

VMware is a registered trademark or trademark of VMware, Inc. in the United States and/or other jurisdictions.

Windows is a registered trademark of Microsoft Corp. in the U.S. and other countries.

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

Windows Vista is a registered 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.

The following program product contains some parts whose copyrights are reserved by Sun Microsystems, Inc.: P-9D2C-8E92.

The following program product contains some parts whose copyrights are reserved by UNIX System Laboratories, Inc.: P-9D2C-8E92.

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

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

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

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

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

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

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

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



This product includes RSA BSAFE(R) Cryptographic software from RSA Security Inc.

HITACHI
Inspire the Next

 Hitachi, Ltd.



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.

■ 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.

Printed in Japan.

■ Edition history

Edition 1 (3020-3-R78-01(E)): November 2009

■ Copyright

All Rights Reserved. Copyright (C) 2009, Hitachi, Ltd.

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* is abbreviated as *JP1*, and *JP1/Integrated Management* is abbreviated as *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, system development managers, and operators who wish to:

- Apply centralized monitoring of the events that occur in a system, and take appropriate action in response to those events.
- 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. Troubleshooting

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

Related publications

This manual is part of a related set of manuals. The manuals in the set are listed below (with the manual numbers):

Manuals related to JP1/IM

- *Job Management Partner 1/Integrated Management - Manager Quick Reference*

(3020-3-R75(E))

- *Job Management Partner 1/Integrated Management - Manager Overview and System Design Guide (3020-3-R76(E))*
- *Job Management Partner 1/Integrated Management - Manager Configuration Guide (3020-3-R77(E))*
- *Job Management Partner 1/Integrated Management - Manager GUI Reference (3020-3-R79(E))*
- *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference (3020-3-R80(E))*
- *Job Management Partner 1/Integrated Management - Manager Messages (3020-3-R81(E))*
- *Job Management Partner 1/Integrated Management - Event Gateway for Network Node Manager i Description, User's Guide and Reference (3020-3-R82(E))*
- *Job Management Partner 1/Integrated Management - Rule Operation System Configuration and User's Guide (3020-3-K10(E))*
- *Job Management Partner 1/Integrated Management - Rule Operation GUI Reference (3020-3-K11(E))*

Manuals related to JPI

- *Job Management Partner 1/Base User's Guide (3020-3-R71(E))*
- *Job Management Partner 1/Base Messages (3020-3-R72(E))*
- *Job Management Partner 1/Base Function Reference (3020-3-R73(E))*

Conventions: Abbreviations

This manual uses the following abbreviations for Hitachi program products and other products:

Abbreviation		Full name or meaning
AIX		AIX(R) 5L 5.2
		AIX(R) 5L 5.3
		AIX(R) 6.1
Cosminexus	Cosminexus Application Server	uCosminexus Application Server Standard
		uCosminexus Application Server Enterprise
		uCosminexus Web Redirector

Abbreviation		Full name or meaning
		uCosminexus Service Platform
HNTRLib		Hitachi Network Objectplaza Trace Library
HNTRLib2		Hitachi Network Objectplaza Trace Library 2
HP-UX	HP-UX (IPF)	HP-UX 11i V2(IPF)
		HP-UX 11i V3(IPF)
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 newer
JP1/AJS	JP1/AJS2 - Advanced Manager	Job Management Partner 1/Automatic Job Management System 2 - Advanced Manager
	JP1/AJS - Agent	Job Management Partner 1/Automatic Job Management System 2 - Agent
		Job Management Partner 1/Automatic Job Management System 3 - Agent
	JP1/AJS - Manager	Job Management Partner 1/Automatic Job Management System 2 - Manager
		Job Management Partner 1/Automatic Job Management System 3 - Manager
	JP1/AJS - View	Job Management Partner 1/Automatic Job Management System 2 - View
		Job Management Partner 1/Automatic Job Management System 3 - View
	JP1/AJS2 - Scenario Operation View	
JP1/AJS2 - View for Mainframe		Job Management Partner 1/Automatic Job Management System 2 - View for Mainframe
JP1/Base		Job Management Partner 1/Base
JP1/Cm2/ESA		Job Management Partner 1/Cm2/Extensible SNMP Agent
		Job Management Partner 1/Cm2/Extensible SNMP Agent for Extension Mib Runtime

Abbreviation		Full name or meaning	
JP1/FTP		Job Management Partner 1/File Transmission Server/FTP	
JP1/Integrated Management or JP1/IM	<i>Version 7 products:</i>		
	JP1/IM - Central Console or JP1/IM - CC	Job Management Partner 1/Integrated Manager - Central Console	
	JP1/IM - Central Console Upgrade or JP1/IM - CC Upgrade	Job Management Partner 1/Integrated Manager - Central Console Upgrade	
	JP1/IM - View	Job Management Partner 1/Integrated Manager - View	
	<i>Version 8 products:</i>		
	JP1/IM - Manager	Job Management Partner 1/Integrated Management - Manager	
	JP1/IM - Rule Operation or JP1/IM - RL [#]	Job Management Partner 1/Integrated Management - Rule Operation	
	JP1/IM - View	Job Management Partner 1/Integrated Management - View	
	<i>Version 9 products:</i>		
	JP1/IM - Event Gateway for Network Node Manager i or JP1/IM - EG for NNMi [#]	Job Management Partner 1/Integrated Management - Event Gateway for Network Node Manager i	
	JP1/IM - Manager	Job Management Partner 1/Integrated Management - Manager	
	JP1/IM - View	Job Management Partner 1/Integrated Management - View	
	JP1/PAM	JP1/PA - Adaptor	Job Management Partner 1/Performance Analysis - Adaptor
			Job Management Partner 1/Performance Management - Analysis Adaptor
JP1/PA - Manager		Job Management Partner 1/Performance Analysis - Manager	
		Job Management Partner 1/Performance Management - Analysis Manager	

Abbreviation		Full name or meaning
	JP1/PA - View	Job Management Partner 1/Performance Analysis - View
		Job Management Partner 1/Performance Management - Analysis View
JP1/PFM	JP1/PFM - Agent	Agent product group, such as Job Management Partner 1/Performance Management - Agent for Platform
	JP1/PFM - Manager	Job Management Partner 1/Performance Management - Manager
	JP1/PFM - View	Job Management Partner 1/Performance Management - View
	JP1/PFM - Web Console	Job Management Partner 1/Performance Management - Web Console
JP1/SES		Job Management Partner 1/System Event Service
JP1/Software Distribution		Job Management Partner 1/Software Distribution Manager
		Job Management Partner 1/Software Distribution SubManager
		Job Management Partner 1/Software Distribution Client
NNM	HP NNM	HP Network Node Manager Software Version 6 or earlier
		HP Network Node Manager Starter Edition Software Version 7.5 or earlier
NNMi	HP NNMi	HP Network Node Manager i Software v8.10
Solaris		Solaris 9
		Solaris 10
VMware		VMware(R) ESX 3.5
Windows 2000		Microsoft(R) Windows(R) 2000 Advanced Server Operating System
		Microsoft(R) Windows(R) 2000 Professional Operating System

Abbreviation		Full name or meaning
		Microsoft(R) Windows(R) 2000 Server Operating System
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 (IPF)	Microsoft(R) Windows Server(R) 2003, Enterprise Edition for Itanium-based Systems
	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	
		Microsoft(R) Windows Server(R) 2008 Standard
Windows Server 2008 (IPF)		Microsoft(R) Windows Server(R) 2008 for Itanium-based Systems
Windows Vista		Microsoft(R) Windows Vista(R) Business
		Microsoft(R) Windows Vista(R) Enterprise
		Microsoft(R) Windows Vista(R) Ultimate
Windows XP Professional		Microsoft(R) Windows(R) XP Professional Operating System

#: This manual includes descriptions of only those JP1/IM - Rule Operation and JP1/IM - Event Gateway for Network Node Manager i functions that relate to JP1/IM - Manager and JP1/IM - View.

- In this manual, *Windows 2000*, *Windows XP Professional*, *Windows Server 2003*, *Windows Vista*, *Windows Server 2008*, and *Windows Server 2008 (IPF)* are generally referred to collectively as *Windows*.
- In this manual, *HP-UX*, *Solaris*, and *AIX* are generally referred to collectively as *UNIX*.

This manual also uses the following abbreviations:

Abbreviation	Full name or meaning
ASCII	American Standard Code for Information Interchange
CMT	Container-Managed Transaction
CRLF	Carriage Return/Line Feed
CSV	Comma Separated Value
DB	Database
DBMS	Database Management System
DNS	Domain Name System
FQDN	Fully Qualified Domain Name
GMT	Greenwich Mean Time
GUI	Graphical User Interface
HTML	Hyper Text Markup Language
HTTP	HyperText Transfer Protocol
IP	Internet Protocol
IPF	Itanium(R) Processor Family
ISAM	Indexed Sequential Access Method
J2EE	Java™ 2 Platform Enterprise Edition
Java VM	Java™ Virtual Machine
JDBC	Java™ DataBase Connectivity
LAN	Local Area Network
NAT	Network Address Translator
NIC	Network Interface Card
NTP	Network Time Protocol

Abbreviation	Full name or meaning
OTS	Object Transaction Service
POSIX	Portable Operating System Interface for UNIX
SFO	Session Fail Over
SNMP	Simple Network Management Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TXT	Text
UAC	User Account Control
UCS	Universal Multiple-Octet Coded Character Set
UNC	Universal Naming Convention
URL	Uniform Resource Locator
UTC	Universal Time Coordinated
UTF	UCS Transformation Format
WAN	Wide Area Network
WWW	World Wide Web

Conventions: Diagrams

This manual uses the following conventions in diagrams:

- Computer (terminal)



- Computer



- Disk device, file



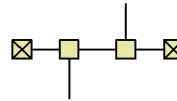
- Screen



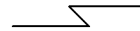
- WAN



- Network



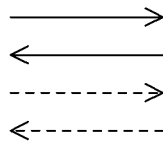
- Communication channel



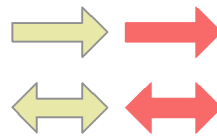
- Program



- 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: <ul style="list-style-type: none"> • From the File menu, choose Open. • Click the Cancel button. • In the Enter name entry box, type your name.
<i>Italics</i>	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: <ul style="list-style-type: none"> • Write the command as follows: <i>copy source-file target-file</i> • Do <i>not</i> 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: <ul style="list-style-type: none"> • At the prompt, enter <code>dir</code>. • Use the <code>send</code> command to send mail. • The following message is displayed: <code>The password is incorrect.</code>

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:

```
StoreDatabase [temp|perm] (database-name . . .)
```

The following table lists the conventions used in syntax explanations:

Example font or symbol	Convention
<code>StoreDatabase</code>	Code-font characters must be entered exactly as shown.
<i>database-name</i>	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.

Example font or symbol	Convention
[]	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	<i>View-path</i>	<i>system-drive:\Program Files\HITACHI\JP1CoView</i>
JP1/IM - Manager	<i>Manager-path</i>	<i>system-drive:\Program Files\HITACHI\JP1IMM</i>

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

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

For Windows Server 2008 and Windows Vista, the *system-drive:\Program Files* part is determined at installation by an OS environment variable, and may therefore vary depending on the environment.

Conventions: KB, MB, GB, and TB

This manual uses the following conventions:

- 1 KB (kilobyte) is 1,024 bytes.
- 1 MB (megabyte) is 1,024² bytes.
- 1 GB (gigabyte) is 1,024³ bytes.
- 1 TB (terabyte) is 1,024⁴ bytes.

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*.

Administrator permissions

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.

Online manuals

JP1/IM provides an HTML version of this manual that can be viewed by using one of the following Web browsers:

- Microsoft Internet Explorer 6.0 or later
- Windows Internet Explorer 7 or later

The contents of the online manual and of this printed manual are identical.

To display the table of contents for this online manual:

- In JP1/IM - View, choose **Help** and then **Help Contents**. Alternatively, from the **Start** menu, choose **Programs, JP1_Integrated Management - View**, and then **Help**.

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

Preface	i
Intended readers	i
Organization of this manual	i
Related publications	i
Conventions: Abbreviations	ii
Conventions: Diagrams	ix
Conventions: Fonts and symbols	ix
Conventions: Installation folders for the Windows version of JP1/IM and JP1/Base	xi
Conventions: KB, MB, GB, and TB	xii
Conventions: Version numbers	xii
Administrator permissions	xii
Online manuals	xiii

PART 1: Administration

1. JP1/IM System Maintenance	1
1.1 Managing the configuration information	2
1.1.1 Backup (in Windows)	2
1.1.2 Recovery (in Windows)	6
1.1.3 Backup (in UNIX)	6
1.1.4 Recovery (in UNIX)	10
1.2 Managing the databases	11
1.2.1 Database reorganization	11
1.2.2 Database backup and recovery	12
1.2.3 Re-creating a database and changing its settings	17
1.3 Managing the disk capacity	26
1.4 Using historical reports	29
1.4.1 Outputting events to a CSV file	29
1.4.2 Correlation event generation history	29
1.5 Migrating the configuration information and databases	31
2. Changing the Configuration of JP1/IM	33
2.1 Changing the JP1/IM settings information	34
2.2 Changing the settings of the host on which JP1/IM runs	35
2.2.1 Effects of a host name change and the necessary tasks	35
2.2.2 Effects of an IP address change and the necessary tasks	37

2.2.3	Tasks that become necessary as a result of a system date/time change.....	38
-------	---	----

PART 2: Operation

3.	Starting and Stopping JP1/IM - Manager	41
3.1	Starting JP1/IM - Manager.....	42
3.1.1	In Windows.....	42
3.1.2	In UNIX.....	43
3.1.3	Operations in a cluster system.....	44
3.2	Stopping JP1/IM - Manager.....	45
3.2.1	In Windows.....	45
3.2.2	In UNIX.....	45
3.2.3	Operations in a cluster system.....	45
3.3	Notes on starting and stopping.....	47
4.	JP1/IM - Manager Logon and Logoff	49
4.1	Logging on to JP1/IM - Manager.....	50
4.1.1	Using the GUI to log on to JP1/IM - Manager.....	50
4.1.2	Using a command to log on to JP1/IM - Manager.....	52
4.2	Logging off from JP1/IM - Manager.....	54
5.	System Monitoring from Central Console	55
5.1	Monitoring the system based on JP1 events.....	56
5.1.1	Viewing JP1 events.....	56
5.1.2	Displaying detailed JP1 event information.....	62
5.1.3	Displaying extended attributes of JP1 events.....	64
5.1.4	Displaying the response status of JP1 events.....	68
5.1.5	Displaying only severe events.....	69
5.1.6	Displaying consolidated events and repeated events.....	70
5.1.7	Displaying and handling correlation events.....	75
5.1.8	Displaying events by specifying a time period.....	78
5.1.9	Displaying events by specifying time.....	79
5.1.10	Checking the rule startup request status and making a rule startup request (JP1/IM - Rule Operation linkage).....	80
5.2	Setting the response status of severe events.....	85
5.3	Changing the severity level of events.....	87
5.4	Editing memo entries.....	89
5.5	Searching for JP1 events.....	90
5.5.1	Search method.....	90
5.5.2	Displaying the search results.....	93
5.5.3	Setting a response status for an event search.....	96
5.6	Opening a monitor window for the application that issued JP1 events.....	98
5.7	Enabling a view filter.....	99

5.8	Switching the event acquisition filter	100
5.8.1	Making a switch from the System Environment Settings window or Event Acquisition Conditions List window of JP1/IM - View	100
5.8.2	Making the switch using the jcochfilter command	103
5.9	Outputting the information displayed in JP1/IM - View to a CSV file	108
5.9.1	Outputting an events list to a CSV file.....	108
5.9.2	Outputting the content of the integrated monitoring database to a CSV file	109
5.9.3	Copying JP1 event information and action execution results to the clipboard	110
6.	System Monitoring from Central Scope	111
6.1	Monitoring from the Monitoring Tree window	112
6.1.1	Changing the status of monitoring nodes	113
6.1.2	Changing the monitoring status of monitoring nodes	114
6.1.3	Searching for monitoring nodes	114
6.1.4	Searching for status-change events	115
6.1.5	Displaying the attributes of monitoring nodes	116
6.1.6	Displaying guide information.....	117
6.1.7	Opening the Visual Monitoring window	117
6.1.8	Displaying a login user list.....	118
6.1.9	Saving the information in the Monitoring Tree window on the local host ..	118
6.2	Monitoring from the Visual Monitoring window	119
6.2.1	Opening the Monitoring Tree window from the Visual Monitoring window.....	120
6.2.2	Changing the status of monitoring nodes.....	120
6.2.3	Changing the monitoring status of monitoring nodes	121
6.2.4	Searching for monitoring nodes	122
6.2.5	Searching for status-change events	122
6.2.6	Displaying the attributes of monitoring nodes	123
6.2.7	Displaying guide information.....	123
7.	System Operation Using JP1/IM	125
7.1	Executing commands on a remote host	126
7.1.1	Executing a command	126
7.1.2	User that executes commands	127
7.1.3	Checking command execution status and deleting a command.....	128
7.2	Executing automated actions and taking necessary steps.....	129
7.2.1	Checking the execution status of an automated action	129
7.2.2	Checking the execution results of automated actions	131
7.2.3	Checking the operating status of the automated action function	138
7.3	Opening other application windows from the Tool Launcher	139
7.3.1	Operations in the Tool Launcher window	140
7.3.2	Functions that can be operated from the Tool Launcher window	141

8. Managing the System Hierarchy using IM Configuration Management	143
8.1 Managing hosts	144
8.1.1 Registering a host	144
8.1.2 Deleting a host	144
8.1.3 Collecting information from hosts	145
8.1.4 Changing the host information	146
8.1.5 Displaying a host list	147
8.2 Managing the system hierarchy	148
8.2.1 Collecting system hierarchy information	148
8.2.2 Displaying the system hierarchy	149
8.2.3 Verifying the system hierarchy	149
8.2.4 Editing the system hierarchy	150
8.2.5 Applying the system hierarchy	153
8.2.6 Synchronizing system hierarchies	153
8.3 Managing profiles	155
8.3.1 Collecting profiles	155
8.3.2 Collecting a profile list	157
8.3.3 Displaying profiles	158
8.3.4 Editing configuration files	159
8.3.5 Applying the edited content of the configuration file	161
8.4 Managing service operation status	164
8.4.1 Collecting service operation information	164
8.4.2 Service operation information display	165
8.5 Importing and exporting management information of IM Configuration Management	167
8.5.1 Exporting management information of IM Configuration Management ...	167
8.5.2 Importing management information of IM Configuration Management ...	170
8.5.3 Applying the imported management information of IM Configuration Management to a system	174
8.6 Managing the configuration of a virtual system	176
8.6.1 Registering a virtual system host	176
8.6.2 Displaying host information in a virtual system	177
8.6.3 Exporting the configuration information of a virtual system	178

PART 3: Troubleshooting

9. Troubleshooting	179
9.1 Troubleshooting procedure	180
9.2 Log information types	181
9.2.1 Common message log	181
9.2.2 Integrated trace log	181
9.2.3 Process-by-process trace log	184
9.2.4 Log files and directory list	184

9.3 Data that needs to be collected when a problem occurs.....	209
9.3.1 In Windows	209
9.3.2 In UNIX.....	224
9.4 Collecting data.....	236
9.4.1 In Windows	236
9.4.2 In UNIX.....	242
9.5 Corrective actions	247

Index	285
--------------	------------

Chapter

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
- 1.2 Managing the databases
- 1.3 Managing the disk capacity
- 1.4 Using historical reports
- 1.5 Migrating the configuration information and databases

1.1 Managing the configuration information

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

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 stopped. If you must make a backup while these services are running, note the following points:

- 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.

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(5) <i>Copying the common definition information</i> in the <i>Job Management Partner 1/Integrated Management - Manager Configuration Guide</i>	Common definition information backup file ^{#1}
JP1/IM - Manager	JP1/IM - Central Console	<i>Console-path</i> \conf\jplco_env.conf	IM environment definition file
		<i>Console-path</i> \conf\jplco_param.conf	IM parameter definition file

Product name	File name	Description
	<i>Console-path</i> \conf\jp1co_param_v7.conf	IM parameter definition file
	<i>Console-path</i> \conf\jp1co_service.conf	Extended startup process definition file
	<i>Console-path</i> \conf\jp1co_system.conf	IM server system environment settings file
	<i>Console-path</i> \conf\action\actdef.conf	Automated action definition file
	<i>Console-path</i> \conf\console\actprofile\actprofile_ <i>JP1-user-name</i>	Action profile
	<i>Console-path</i> \conf\console\actprofile\actprofile2_ <i>JP1-user-name</i>	
	<i>Console-path</i> \conf\console\attribute*.conf	Definition file for extended event attributes
	<i>Console-path</i> \conf\console\filter*.conf	Filter definition file
	<i>Console-path</i> \conf\console\mapping\mapping.conf	Event information mapping definition file
	<i>Console-path</i> \conf\console\monitor*.conf	Definition file for opening monitor windows
	<i>Console-path</i> \conf\console\object_type*	Definition file for object types
	<i>Console-path</i> \conf\console\profile\.system	System profile
	<i>Console-path</i> \conf\console\profile\defaultUser	JP1/IM - View user profile (default)
	<i>Console-path</i> \conf\console\profile\profile_ <i>user-name</i>	JP1/IM - View user profile
	<i>Console-path</i> \www\console.html ^{#2}	Web-based operation definition file
	<i>Console-path</i> \default\console.conf ^{#2}	Communication environment definition file

1. JP1/IM System Maintenance

Product name	File name	Description
	<i>Console-path</i> \conf\console\correlation\view_cor_use r-name.conf	Settings file for the consolidated display of repeated events
	<i>Console-path</i> \conf\health\jcohc.conf	Health check definition file
	<i>Console-path</i> \conf\action\actnotice.conf	Automatic action notification definition file
	<i>Console-path</i> \conf\processupdate\processupdate.conf	Status event definition file
	<i>Console-path</i> \conf\guide\jco_guide.txt	Event guide information file
	<i>user-selected-folder</i> \user-selected-file-name	Event guide message file
	All files under <i>Console-path</i> \conf\evgen\	Definition files for correlation event generation
	<i>user-selected-folder</i> \file-name.conf	Correlation event generation definition file
	<i>Console-path</i> \conf\action\attr_list\attr_list.conf	File that defines which items are displayed for event conditions
	<i>Console-path</i> \conf\chsev\jcochsev.conf	Severity changing definition file
JP1/IM - Central Scope	<i>Scope-path</i> \conf\jcs_guide.txt	Guide information file
	<i>Scope-path</i> \conf\jcs_hosts	Host information file
	<i>Scope-path</i> \conf\action_complete_on.conf	Settings file for completed-action linkage function
	<i>Scope-path</i> \conf\action_complete_off.conf	
	<i>user-selected-folder</i> \user-selected-file-name	Definition file for automatic delete mode of status change event

Product name	File name	Description
	<i>user-selected-folder\user-selected-file-name</i>	Definition file for monitoring object initialization mode
	<i>Scope-path\conf\auto_dbbackup_on.conf</i>	Backup recovery settings file for monitored object database
	<i>Scope-path\conf\auto_dbbackup_off.conf</i>	
	<i>Scope-path\conf\evhist_warn_event_on.conf</i>	Settings file for the maximum number of status change events
	<i>Scope-path\conf\evhist_warn_event_off.conf</i>	
	<i>user-selected-folder\user-selected-file-name</i>	Guide message file
	<i>user-selected-folder\user-selected-file-name</i>	Definition file for on memory mode of status change condition
JP1/IM - View	<i>View-path\conf\webdata\en*.html</i>	Web page call definition file
	<i>View-path\conf\tuning.conf</i>	IM - View settings file
	<i>View-path\default\view.conf.update</i>	Communication environment definition file
	<i>View-path\default\tree_view.conf.update</i>	
	<i>View-path\conf\sovtoolexec\en\!JP1_CS_APP0.conf</i>	Start program definition file
	<i>View-path\conf\sovtoolitem\en\!JP1_CS_FTOOL0.conf</i>	Toolbar definition file
	<i>View-path\conf\sovtoolitem\en\!JP1_CS_FTREE0.conf</i>	Icon operation definition file
	<i>View-path\conf\appexecute\en*.conf</i>	Definition file for executing applications
	<i>View-path\conf\function\en*.conf</i>	Definition file for the tool launcher
	<i>user-selected-folder\user-selected-file-name</i>	Configuration file for monitoring tree
	Files under <i>View-path\image\icon\</i>	Icon file

Product name	File name	Description
	Files under <i>View-path</i> \image\visual\	Visual icon file ^{#3}
	<i>View-path</i> \conf\jcfview\jcfview.conf	Operation definition file for IM Configuration Management - View
	<i>View-path</i> \conf\jrmview\jrmview.conf	Operation definition file for Rule Operation - View ^{#4}
	<i>View-path</i> \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.

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 while the JP1/IM daemons are stopped. If you must make a backup while these daemons are running, note the following points:

- 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.

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(5) <i>Copying the common definition information</i> in the <i>Job Management Partner 1/Integrated Management - Manager Configuration Guide</i>	Common definition information backup file ^{#1}
JP1/IM - Manager	JP1/IM - Central Console	<code>/etc/opt/jp1cons/conf/jp1co_env.conf</code>	IM environment definition file
		<code>/etc/opt/jp1cons/conf/jp1co_param.conf</code>	IM parameter definition file
		<code>/etc/opt/jp1cons/conf/jp1co_param_V7.conf</code>	IM parameter definition file
		<code>/etc/opt/jp1cons/conf/jp1co_service.conf</code>	Extended startup process definition file
		<code>/etc/opt/jp1cons/conf/jp1co_spm�.conf</code>	IM process management definition file

1. JP1/IM System Maintenance

Product name	File name	Description
	/etc/opt/jplcons/conf/jplco_system.conf	IM server system environment settings file
	/etc/opt/jplcons/conf/action/actdef.conf	Automated action definition file
	/etc/opt/jplcons/conf/console/actprofile/actprofile_ <i>JP1-user-name</i>	Action profile
	/etc/opt/jplcons/conf/console/actprofile/actprofile2_ <i>JP1-user-name</i>	
	/etc/opt/jplcons/conf/console/attribute/*.conf	Definition file for extended event attributes
	/etc/opt/jplcons/conf/console/filter/*.conf	Filter definition file
	/etc/opt/jplcons/conf/console/mapping/mapping.conf	Event information mapping definition file
	/etc/opt/jplcons/conf/console/monitor/*.conf	Definition file for opening monitor windows
	/etc/opt/jplcons/conf/console/object_type/*	Definition file for object types
	/etc/opt/jplcons/conf/console/profile/.system	System profile
	/etc/opt/jplcons/conf/console/profile/defaultUser	JP1/IM - View user profile (default)
	/etc/opt/jplcons/conf/console/profile/profile_ <i>user-name</i>	JP1/IM - View user profile
	/opt/jplcons/www/console.html ^{#2}	Web-based operation definition file
	/etc/opt/jplcons/default/console.conf ^{#2}	Communication environment definition file
	/etc/opt/jplcons/conf/console/correlation/view_cor_ <i>user-name</i> .conf	Settings file for the consolidated display of repeated events

Product name	File name	Description
	<code>/etc/opt/jplcons/conf/health/jcohc.conf</code>	Health check definition file
	<code>/etc/opt/jplcons/conf/action/actnotice.conf</code>	Automatic action notification definition file
	<code>/etc/opt/jplcons/conf/processupdate/processupdate.conf</code>	Status event definition file
	<code>/etc/opt/jplcons/conf/guide/jco_guide.txt</code>	Event guide information file
	<i>user-selected-directory/user-selected-file-name</i>	Event guide message file
	All files under <code>/etc/opt/jplcons/conf/evgen/</code>	Definition files for correlation event generation
	<i>user-selected-directory/file-name.conf</i>	Correlation event generation definition file
	<code>/etc/opt/jplcons/conf/chsev/jcochsev.conf</code>	Severity changing definition file
JP1/IM - Central Scope	<code>/etc/opt/jplscope/conf/jcs_guide.txt</code>	Guide information file
	<code>/etc/opt/jplscope/conf/jcs_hosts</code>	Host information file
	<code>/etc/opt/jplscope/conf/action_complete_on.conf</code> <code>/etc/opt/jplscope/conf/action_complete_off.conf</code>	Settings file for completed-action linkage function
	<i>user-selected-directory/user-selected-file-name</i>	Definition file for automatic delete mode of status change event
	<i>user-selected-directory/user-selected-file-name</i>	Definition file for monitoring object initialization mode
	<code>/etc/opt/jplscope/conf/auto_dbbackup_on.conf</code> <code>/etc/opt/jplscope/conf/auto_dbbackup_off.conf</code>	Backup recovery settings file for monitored object database

Product name	File name	Description
	/etc/opt/jplscope/conf/evhist_warn_event_on.conf	Settings file for the maximum number of status change events
	/etc/opt/jplscope/conf/evhist_warn_event_off.conf	
	<i>user-selected-directory/user-selected-file-name</i>	Guide message file
	<i>user-selected-directory/user-selected-file-name</i>	Definition file for on memory mode of status change condition

#: 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.

1.2 Managing the databases

The JP1/IM system uses the following databases:

- Command execution log
- Monitored object database
- Host information database
- Event database
- IM database

The monitored object database and the host information database are used when the Central Scope functions are used. 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 IM database

This subsection explains the procedure for reorganizing the IM database.

When data is repeatedly added or deleted, fragmented free spaces are created in the IM database. This condition may prevent new registration even before the number of hosts or properties reaches its upper limit, or you may find that registration, updating, and deletion take an excessively long time.

To prevent such things from happening, reorganize the IM database at a time such as the following:

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

If new registration is prevented even before the number of hosts or properties has reached its upper limit, or if you find that registration, updating, and deletion are taking an excessively long time, use the following procedure 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.
2. Using the `jimdbroorg` command, reorganize the database.

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

3. Start the JP1/IM - Manager service.

(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.
2. Using the `jimdbroorg` command, reorganize the database.

For details about the `jimdbroorg` command, see *jimdbroorg (I. 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.

1.2.2 Database backup and recovery

(1) Command execution log backup and recovery procedures

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

(a) Backup procedure

To back up the command execution log:

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

For details about which files to back up, see (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.

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

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

In UNIX:

Table 1-4: Files to back up (UNIX)

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

For details about the command execution log file, see the *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 <i>Scope-path</i> \database\jcsdb\
		All files under <i>shared-folder</i> \jplscope\database\jcsdb\
UNIX	Monitored object database	All files under /var/opt/jplscope/database/jcsdb/

OS	Information type	Files to back up
		All files under <i>shared-directory</i> /jplscope/database/jcsdb/

3. Start JP1/IM - Manager.

(b) Recovery procedure

To recover the monitored object database:

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

(3) Host information database backup and recovery procedures

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

(a) Backup procedure

To back up the host information database:

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

The table below shows the files to back up.

Table 1-6: Files to back up

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

3. Start JP1/IM - Manager.

(b) Recovery procedure

To recover the host information database:

1. JP1/IM System Maintenance

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) *Command execution log backup and recovery procedures*.

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) 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.

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

To recover the IM database on a physical host:

1. Stop the JP1/IM - Manager service.

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. Start the JP1/IM - Manager service.

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

To recover the IM database in a cluster environment:

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

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 1-7: Files to delete (Windows)

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

In UNIX:

Table 1-8: Files to delete (UNIX)

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

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

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

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

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

1. Stop JP1/IM - Manager.
2. Back up the files.
Back up the *Scope-path*\database\ folder.

3. Re-create the monitored object database.

Executing the `jcsdbsetup -f` command deletes the existing monitored object database, and then re-creates the object database.

4. Re-create the host information database.

First, delete the files from the `Scope-path\database\jcshosts\` folder, and then execute the following command:

```
jcshostsimport -r host-information-file (jcs_hosts)
```

5. Start JP1/IM - Manager.

(3) Procedure for re-creating the event database

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

(a) Manager and Agent (JP1/Base 07-51 or later)

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 *Job Management Partner 1/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.

(b) 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.

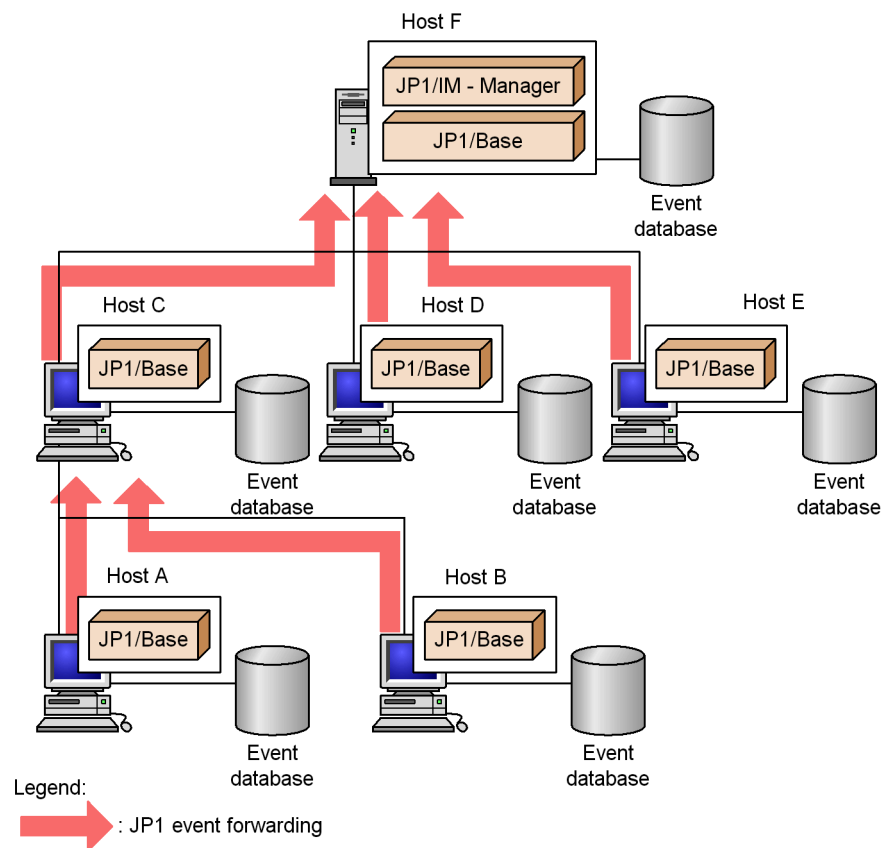
For details about the `jevexport` command, see the chapter on commands in the *Job Management Partner 1/Base User's Guide*.

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) 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

To expand the IM database size on a physical host:

1. Switch the database being used by Central Console.

During database size extension, if you need to continue system monitoring via Central Console (although its functionality is somewhat more limited), switch the database being used by Central Console to the JP1/Base event database.

1. JP1/IM System Maintenance

2. Stop the JP1/IM - Manager service.

If you switched the database being used by Central Console to the JP1/Base event database of JP1/Base, there is no need to stop the JP1/IM - Manager service.

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 both the integrated monitoring database and the IM Configuration Management database.

Unset up only those databases that have been set up.

5. Edit the setup information file.

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

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 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 JP1/IM - Manager service.

If you switched from the integrated monitoring database to the JP1/Base event database in Step 1, switch the database to be used to the integrated monitoring database.

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

To expand the IM database size in a cluster environment:

1. Switch the database being used by Central Console.

During database size extension, if you need to continue system monitoring via Central Console (although its functionality is somewhat more limited), switch the database being used by Central Console to the JP1/Base event database.

2. Stop the JP1/IM - Manager service and the cluster database service.
If you switched the database being used by Central Console to the JP1/Base event database in Step 1, there is no need to stop the JP1/IM - Manager service.
Additionally, 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 both the cluster database service and the JP1/IM - Manager service.
Start the cluster database service and the JP1/IM - Manager service that were stopped in Step 2.
If you switched from the integrated monitoring database to the JP1/Base event database in Step 1, switch the database to be used to the integrated monitoring database.

(5) Procedure for changing the IM database port

To change the IM database port:

1. Stop JP1/IM - Manager.

1. JP1/IM System Maintenance

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.

(6) Procedure for rebuilding the IM database following a host name change

After you change the host name of a physical or logical host, you need to rebuild the IM database. The rebuilding procedure is described below. 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 following a host name change:

1. Stop JP1/IM - Manager.

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 JP1/IM - Manager host name.
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.

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.

1.3 Managing the disk capacity

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

(1) Managing the database capacity

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.

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 1-9: 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*.

(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.

(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.

1. JP1/IM System Maintenance

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 *9. 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 `jvlexport` command, you can output the content of the event database managed by JP1/Base to a CSV file. If you wish to use as historical or statistical information JP1 events that need not be forwarded to the manager, such as normal termination of JP1/AJS jobs, you can use the `jvlexport` command to output the content of the agent's event database to a CSV file.

For details about the `jvlexport` command, see the chapter that explains commands in the *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.

1. JP1/IM System Maintenance

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

This section explains the tasks that are necessary for migrating the configuration information and databases of JP1/IM to JP1/IM to another machine that has a different host name or IP address.

(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 - View*

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

(4) *IM database*

For details about migrating the IM database, see *1.2.3(6) Procedure for rebuilding the IM database following a host name change*.

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

Chapter

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

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

2.1 Changing the JP1/IM settings information

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

To change the operating environment, refer to the manual *Job Management Partner 1/Integrated Management - Manager Overview and System Design Guide* and identify your reasons for changing the operating environment as well as the setting tasks that will be required as a result. Then, carry out the setting tasks by referring to the manual *Job Management Partner 1/Integrated Management - Manager Configuration Guide* and the manual *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 effects of changing the host name, IP address, and system date/time of the host on which JP1/IM is running, and the tasks that are required when you make these changes. When it is necessary to accommodate a change in the network configuration, for example, perform the necessary tasks based on the explanations given in this section.

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.

(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 *1.10 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(6) Procedure for rebuilding the IM database following a host name change*.

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

In UNIX:

For details about how to delete a logical host, see *6.3.5 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* in the *Job Management Partner 1/Integrated Management - Manager Configuration Guide*.

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*

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.

(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

Steps 7 and 8 are required only if you are using the Central Scope functions.

To reset the date/time back to the original date/time:

1. Stop JP1/IM - Manager.
2. Stop JP1/Base.
3. Reset the system date/time to the current date/time.
4. Delete the action information file, action hosts file, event database, and command execution log file.

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

In Windows:

Table 2-1: Files to delete (Windows)

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

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

In UNIX:

Table 2-2: Files to delete (UNIX)

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

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

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

2. Changing the Configuration of JP1/IM

7. From JP1/IM - View, log on to JP1/IM - Manager (JP1/IM - Central Scope).
8. 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 delete both the event database of the JP1/Base on the applicable host and the event database of the JP1/Base 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.

Chapter

3. Starting and Stopping JP1/IM - Manager

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

- 3.1 Starting JP1/IM - Manager
- 3.2 Stopping JP1/IM - Manager
- 3.3 Notes on starting and stopping

3.1 Starting JP1/IM - Manager

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

Before you start JP1/IM - Manager, start Event Service of JP1/Base. To use the IM database, you must also start the IM database when you start JP1/IM - Manager.

Furthermore, if you restart Event Service of JP1/Base, you must also restart JP1/IM - Manager. 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.

3.1.1 In Windows

In Windows, the startup method differs depending on whether the IM database is being used.

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.

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.

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

For details about how to set the automatic startup script, see 2.17.2 *Setting automatic startup and automatic stop* 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, you must start Event Service of JP1/Base. If Event Service of JP1/Base is not started, you cannot start JP1/IM - Manager.

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.

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 I/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.

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 startup script, see *2.17.2 Setting automatic startup and automatic stop* in the *Job Management Partner I/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 I/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

3. Starting and Stopping JP1/IM - Manager

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.

3. Starting and Stopping JP1/IM - Manager

- 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.

Chapter

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

4.2 Logging 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 the GUI to log on to JP1/IM - Manager and use JP1/IM - View:

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 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. 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 the GUI to log on to JP1/IM - Manager and use the IM Configuration Management - View:

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 *1.19.2 Setting up 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 - Manager (JP1/IM - Central Console). If you specify only the `-s` argument, you will be logged on to JP1/IM - Manager (JP1/IM - Central Scope). If both the `-c` and `-s` arguments are omitted, you will be logged on to JP1/IM - Manager (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 specify each argument, 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 specify each argument, 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.

Chapter

5. System Monitoring from Central Console

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

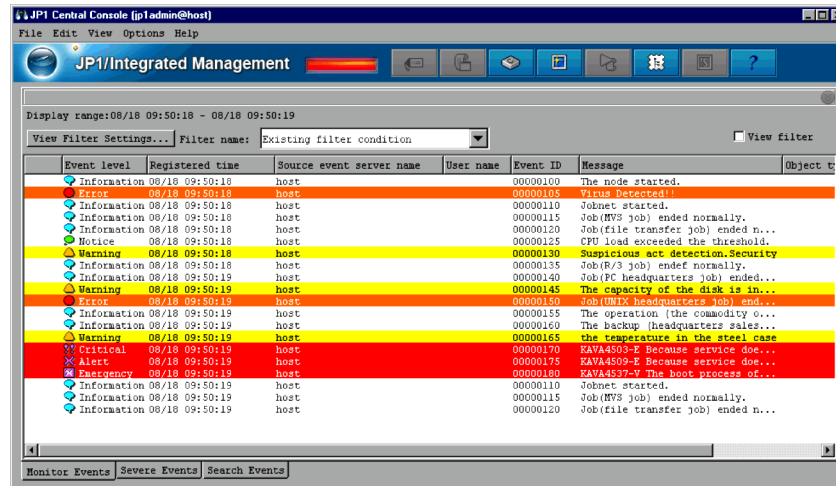
- 5.1 Monitoring the system based on JP1 events
- 5.2 Setting the response status of severe events
- 5.3 Changing the severity level of events
- 5.4 Editing memo entries
- 5.5 Searching for JP1 events
- 5.6 Opening a monitor window for the application that issued JP1 events
- 5.7 Enabling a view filter
- 5.8 Switching the event acquisition filter
- 5.9 Outputting the information displayed in JP1/IM - View to a CSV file

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** 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 *4.9 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 *2.16 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 the displayed items, see *2.16 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, displayed only when the consolidated display of repeated events function is used, shows the number of times the consolidated event is repeated. 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.

5. System Monitoring from Central Console

Attribute	Explanation
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.
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 <code>JOB</code> and <code>JOBNET</code> , 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. When the consolidated display of repeated events function is being used and if 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.
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.

Attribute	Explanation
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.
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*.

(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 consolidated display of repeated events function, information

(Processed, Processing, Held, or Unprocessed) that indicates the response status of JP1 events is automatically displayed. If 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

A plus sign (+) indicating a repetition count or consolidation in progress is displayed in **Display most significant status**.

For details about displaying and operating consolidated events, see 5.1.6 *Displaying consolidated events and repeated events*.

- Correlation events

The icon  or  is displayed in **Type**.

For details about displaying and operating correlation events, see 5.1.7 *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 I/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*.

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 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.
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.

Display name	Description
Occurrence	Event that occurred for the object indicated for for the object name.
Start time	Execution start time or re-execution start time.
End time	Execution end time.
Termination 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 <code>KAVB1588-I</code> is displayed.
Associated serial numbers	Serial numbers of correlation source events, delimited by spaces and displayed in the following format: <i>serial-number</i> Δ <i>serial-number</i> Δ <i>serial-number</i> . . .
Correlation event generation condition name	Approved correlation event generation condition name.
Severity (before change)	When the integrated monitoring database is used and when a severity level is changed using the severity changing function, the urgency of the JP1 event before the change is displayed. The urgency level can take one of the following values (listed in descending order): Emergency, Alert, Critical, Error, Warning, Notice, Information, and Debug.
Memo	When the integrated monitoring database is used and the function for setting memo entries is enabled, memo entries are displayed.

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

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 permissions.

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.

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 "# ".

When a severity filter or user filter is used, you can specify a mapped extended attribute and filter JP1 events.

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 *3.8 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	
Processing	
Held	
Unprocessed	(No icon)
Different response status [#]	!

#

When the consolidated display of repeated events function is used, this symbol indicates a situation in which the response status of a consolidated event is different from the response status of 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` permissions or `JP1_Console_Operator` permissions.

- 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 the consolidated display of repeated events function is used, this symbol indicates a situation in which the response status of a consolidated event is different from the response status of 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*.

5.1.6 Displaying consolidated events and repeated events

When you use the consolidated display of repeated events function, you can consolidate JP1 events that have the same content and occur consecutively over a short time period, and you can display them on the **Monitor Events** page or **Severe Events** page in the Event Console window.

To determine whether JP1 events have the same content, use their severity levels as a guide. Use the severity levels that have been changed via the event severity changing function, and not the ones before the changes are made.

You can display the consolidated repeated events in the Related Events (Summary) window, which is displayed from the **Monitor Events** page or **Severe Events** page of the Event Console window.

When the consolidated display of repeated events function is used, an event that consolidates JP1 events having the same content into a single event is called a *consolidated event*. There are two types of consolidated events: an event for which consolidation is continuing (*event being consolidated*) and an event that has been consolidated (*consolidation completion event*).

Of the JP1 events that have the same content, the first JP1 event received by JP1/IM - View is called the *consolidation start event*. JP1 events that are received thereafter, and that have the same content as the consolidation start event, are called *repeated events*. An event for which no consolidation occurs because there are no repeated events is

called a *non-consolidation event*.

Set up the consolidated display of repeated events function in the Preferences window. For details about the setup method, see *4.10 Setting JP1/IM - View for each login user* in the *Job Management Partner 1/Integrated Management - Manager Configuration Guide*.

(1) **Displaying consolidated events and repeated events**

This subsection explains how to use the consolidated display of repeated events function to display consolidated events, non-consolidation events, and repeated events.

Displaying consolidated events and non-consolidation events:

You can display consolidated events and non-consolidation events on the **Monitor Events** page or **Severe Events** page of the Event Console window.

Furthermore, as is the case when you are not using the consolidated display of repeated events function, you can open the Event Details window from the Event Console window and display detailed attribute information of consolidated events and non-consolidation events. The Event Details window opens when you select an event in the Event Console window and choose **Event Details** from the **View** menu. In the integrated monitoring database, even when consolidated display of repeated events is enabled, you cannot apply consolidated display if you specify a display start position.

Displaying repeated events:

You can display individual repeated events in the Related Events (Summary) window. Individual events are not displayed on the **Monitor Events** page or **Severe Events** page of the Event Console window.

To open the Related Events (Summary) window, from the Event Console window, select a consolidated event, and then choose the **View** menu and **Display Related Event List**.

In the Related Events (Summary) window, you can change the response status as on the **Monitor Events** page of the Event Console window. You can also display detailed attribute information of repeated events in the Event Details window. To open the Event Details window, select an event in the Related Events (Summary) window and choose **Event Details** from the popup menu that opens when you right-click the mouse.

To change a response status, you need JP1_Console_Admin permissions or JP1_Console_Operator permissions.

In the following cases, you cannot select a menu item:

- Multiple events have been selected on the **Monitor Events** page or **Severe Events** page.

- A non-consolidation event has been selected.

The following table shows which events are displayed in each window.

Table 5-7: Events displayed in each window

Window name (page name)	Event type			
	Event being consolidated	Consolidation completion event	Repeated event	Non-consolidation event
Event Console window (Monitor Events page)	C	C	×	N
Event Console window (Severe Events page)	C	C	×	N
Event Console window (Search Events page)	N	N	N	N
Related Events (Summary) window	N	N	N	--

Legend:

C: Consolidated display

N: Non-consolidated display

×: No display

--: No function

(2) How to view the consolidated display

When the consolidated display of repeated events function is enabled, the **Monitor Events** page and the **Severe Events** page of the Event Console window show the following consolidated display:

Figure 5-2: Consolidated display of repeated events example

The screenshot shows the JP1 Central Console interface. At the top, it displays 'JP1/Integrated Management'. Below that, there's a filter section with 'Filter name: Existing filter condition'. The main area is a table of events. The first row in the table has a 'Summary status' of '11'. A red arrow points from this cell to a separate, larger view of the 'Summary status' cell, which shows the number '11' on a yellow background.

Summary status	Type	Event level	Action	Registered time	Source event server name	User name	Event ID	Message
11		Error		08/21 12:24:55	host		00000140	A 10
		Warning		08/21 12:24:56	host		00000410	The
		Notice		08/21 12:24:56	host		00000300	CPU
		Critical		08/21 12:24:56	host		00000123	An
		Warning		08/21 12:24:56	host		00000420	the
		Critical		08/21 12:24:56	host		00000127	An

The consolidated display of repeated events displays the following items.

Summary Status

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

- For consolidation completion events

A repetition count is displayed. The repetition count to be displayed is from 1 to 100.

Summary status	Event level
16	Warning

- 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.

Summary status	Event level
12+	Warning

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.

Summary status	Event level
11+ Del	 Emergency

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

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.

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.

	Summary status	Event level
 !	16	 Warning

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 5-8: Action suppression status

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

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

Summary status	Event level	Action
 ! 16	 Warning	 !

(3) Changing the response status

You can change the response status of consolidated events and repeated events in the same way as when you are not using the consolidated display of repeated events function.

When the response status of consolidated events is changed:

If you change the response status of consolidated events on the **Monitor Events** page or **Severe Events** page of the Event Console window, the response status of all repeated events that have been received up to that point is also changed to the same response status.

The response status is not changed for repeated events that are received after you change the response status. As a result, those repeated events have a different response status, and ! is displayed in the response status display.

When the response status of repeated events is changed:

If you change the response status of repeated events in the Related Events (Summary) window, the response status is not changed for consolidated events that represent the consolidation of repeated events. However, because consolidated events contain repeated events whose response status is different, ! is displayed in the response status display.


5.1.7 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 *2.16 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:


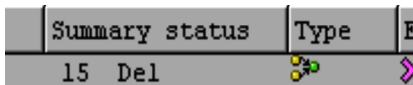

1. Select one correlation event on each of the following pages of the Event Console window:
 - **Monitor Events** page
 - **Severe Events** page
 - **Search Events** page
2. From the **View** menu, choose **Display Related Event List**. Alternatively, from the popup menu, choose **Display Related Event List**.

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

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

Table 5-9: Consolidated display of correlation events example

Display example	Explanation						
<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 33%;">Summary status</th> <th style="width: 33%;">Type</th> <th style="width: 33%;">Event</th> </tr> </thead> <tbody> <tr> <td style="text-align: center;">24</td> <td style="text-align: center;"></td> <td style="text-align: center;"> Err</td> </tr> </tbody> </table>	Summary status	Type	Event	24		 Err	Correlation events have been consolidated.
Summary status	Type	Event					
24		 Err					

Display example	Explanation
	Correlation events are being consolidated.
	Correlation events that have been consolidated are deleted.
	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 *5.1.6 Displaying consolidated events and repeated events*.

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.

5.1.8 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.

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. Under **Specified display event period**, select the **Display** check box.
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.

5.1.9 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 view filter is applied only on the **Monitor Events** page. 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 is the base time of the day when you logged on to Central Console.

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.

5.1.10 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 *4.3.3 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` permissions or `JP1_Console_Operator` permissions.

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 *4.9 Setting the severity changing function* in the *Job Management Partner 1/Integrated Management - Manager Configuration Guide*.

To change the severity level of an event:

1. Make sure that the severity changing function is enabled for the event.

If it is not enabled, use the `jcoimdef` command and enable the severity changing function. Turning on the `-chsev` option enables the severity changing function for the event. By default, the function is not enabled. 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=1
def severity-change-1
  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 service or execute the `jco_spmc_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 service.

For details about the `jco_spmc_reload` command, see *jco_spmc_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.

5.4 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 *4.5 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` permissions or `JP1_Console_Operator` permissions.

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 *3.5 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 *2.17 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 (2) *Event search direction*.

- Specify a condition group

To differentiate between various event search conditions, names are assigned to condition groups.

You can specify multiple condition groups, and condition groups are *ORed*.

To specify condition groups, you must first click the **Show List** button to show the **List** area.

Adding a condition group: Clicking the **Add** button adds 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.

Items that can be specified are 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, and extended attribute. If the memo function is disabled, the memo item cannot be specified.

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, and extended attribute. For details about using a regular expression to specify search conditions, see (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 *2.16 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 5-10: 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:

When **Past direction** is specified in **Search direction** in the Event Search

Conditions window, the latest set of 20 JP1 events registered in the event database events list are displayed chronologically.

Figure 5-4: The latest set of 20 events are acquired and displayed chronologically

```

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)
2000 07/01 00:39:00 Event 39
2000 07/01 01:40:00 Event 40
2000 07/01 00:41:00 Event 41
2000 07/01 00:42:00 Event 42
      (Omitted)
2000 07/01 00:59:00 Event 59
2000 07/01 01:00:00 Event 60

```

} Added

Example 2:

When **Future direction** is specified in **Search direction** in the Event Search Conditions window, the earliest set of 20 JP1 events registered in the event database events list are displayed chronologically.

Figure 5-6: The earliest set of 20 events are acquired and displayed chronologically

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)	
2000	07/01	00:39:00	Event 39
2000	07/01	00:40:00	Event 40

} Added

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 permissions or JP1_Console_Operator permissions.

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.

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 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 *4.12 Setting monitor startup for linked products* in the *Job Management Partner 1/Integrated Management - Manager Configuration Guide*.

5.7 Enabling a view filter

To enable a view filter for the JP1 events being displayed on the **Monitor Events** page 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** page 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` permissions.

(1) Making the switch from the System Environment Settings window

(a) Switching an event acquisition filter

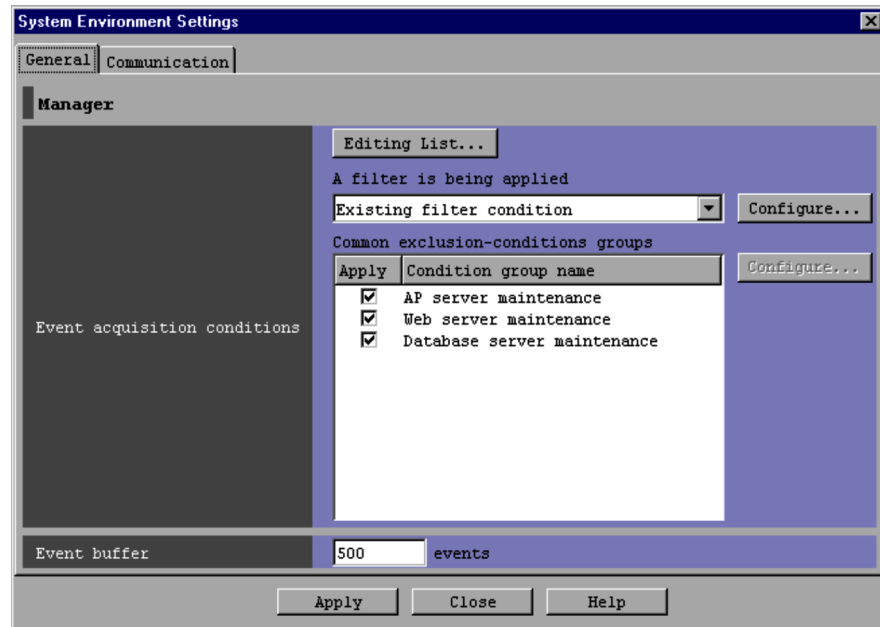
If the name of the event acquisition filter to be switched is clear, select that event acquisition filter from the System Environment Settings window, and then execute the switch.

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.

Figure 5-8: Switching the event acquisition filter from the System Environment Settings window



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:

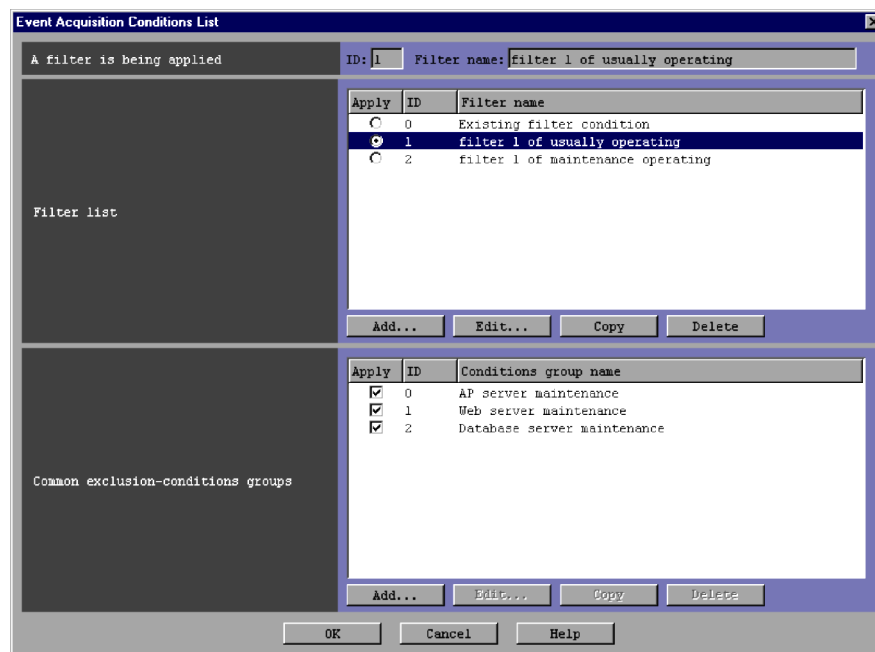
1. In the Event Console window, choose **Options** and then **System Environment Settings**.

The System Environment Settings window opens.

2. In **Event acquisition conditions**, click the **Editing list** button.

The Event Acquisition Conditions List window opens.

Figure 5-9: Switching the event acquisition filter from the Event Acquisition Conditions List window



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 5-10: 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. Enter the `jcochfilter -e` command and enable the common exclusion-conditions group.

Specify all common exclusion-conditions group IDs that you wish to enable. Those common exclusion-conditions groups that you do not specify become disabled.

Examples follow of enabling and disabling a common exclusion condition on a physical host and a logical host.

- Enabling a common exclusion condition on a physical host that has a common exclusion-conditions group ID of 3

Enter the command as follows.

```
jcochfilter -e 3
```

- Enabling a common exclusion condition on logical host `hostA`, which has a common exclusion-conditions group ID of 3

Enter the command as follows.

```
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 the information that can be output in the CSV format, see *3.9.2 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 the information that can be copied to the clipboard in the CSV format and the windows in which this function can be used, see *3.9.3 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**.

Chapter

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

6.2 Monitoring from the Visual Monitoring window

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.

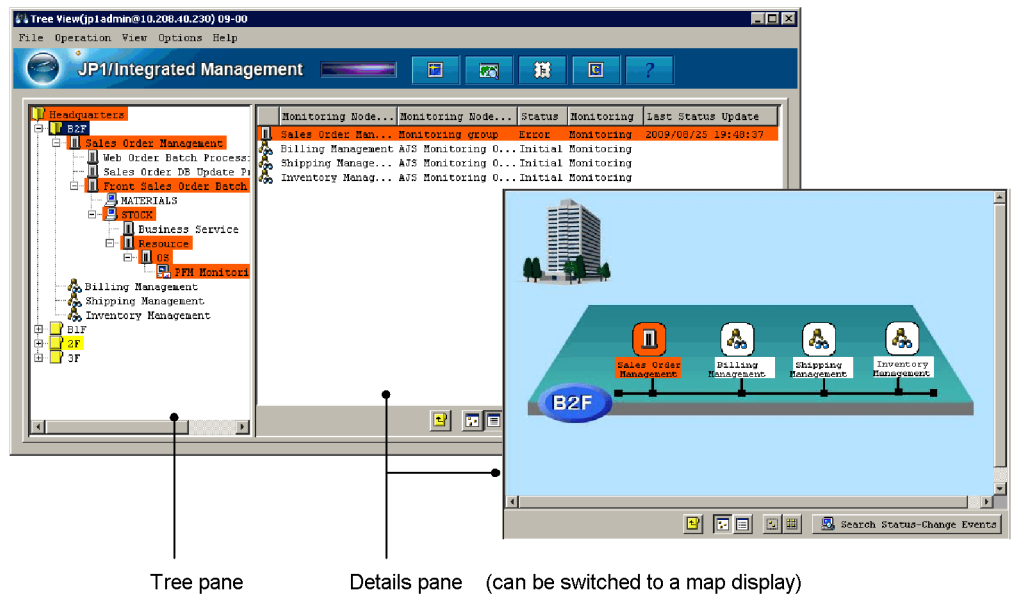
When the monitoring range settings of the monitoring tree are enabled, the monitoring tree displays only the monitoring nodes that are set for the JP1 resource group of the logged-on JP1 user. In this case, a virtual root node is displayed as the highest-order node. If there is no monitoring node that 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` permissions, 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



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` permissions. 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` permissions. 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` permissions 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).

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.

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` permissions 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 *4.7 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 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` permissions, all monitoring nodes are displayed.

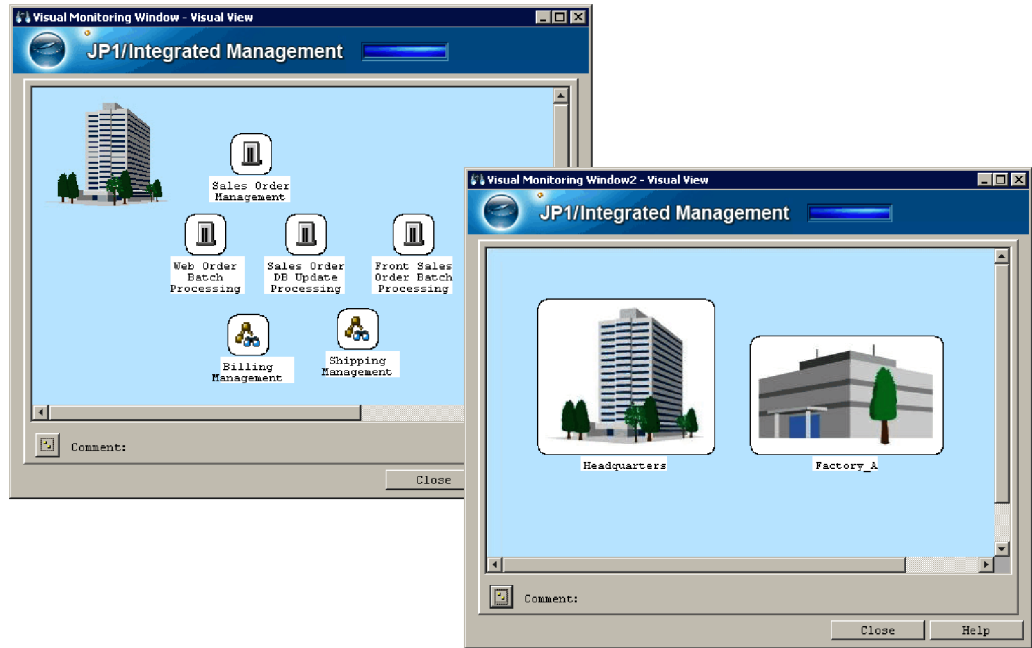
To open the Visual Monitoring window:

1. Use either of the following methods to open the Open Visual Monitoring Window window.
 - From the menu bar in the Monitoring Tree window, choose **View** and then **Visual Monitoring**.
 - Click the  icon in the toolbar of the Monitoring Tree window.
2. Select a Visual Monitoring window name displayed in the Open Visual Monitoring Window window and click **OK**.

When the monitoring range settings of the monitoring tree are enabled, if a visual monitoring window does not contain any monitoring node that can be displayed, it is not displayed in the list in the Open Visual Monitoring Window window.

A Visual Monitoring window display example follows.

Figure 6-2: Visual Monitoring window display example



6.2.1 Opening the Monitoring Tree window from the Visual Monitoring window

To open the Monitoring Tree window from the Visual Monitoring window:

1. Select a monitoring node and double-click it.

The Monitoring Tree window opens with the monitoring node selected that you double-clicked in the Visual Monitoring window.

6.2.2 Changing the status of monitoring nodes

This subsection explains how to change the status of a monitoring node displayed in the Visual Monitoring window. The status that can be changed and the action that occurs at the time of the change differ depending on the monitoring node type (monitoring group or monitored object). For details, see *4.2.2 Statuses of monitoring nodes* in the *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` permissions. 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` permissions 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` permissions. 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` permissions 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**.

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.

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` permissions 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 *4.7 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*.

Chapter

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 commands on a remote host
- 7.2 Executing automated actions and taking necessary steps
- 7.3 Opening other application windows from the Tool Launcher

7.1 Executing commands on a remote host


You can execute commands on a remote host. You can use this function when you are connected to JP1/IM - Manager (JP1/IM - Central Console) from JP1/IM - View.

7.1.1 Executing a command

The operation method is described below. To execute a command on a remote host, you need `JP1_Console_Admin` permissions or `JP1_Console_Operator` permissions.

To execute a command:

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. 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.

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*.

3. 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

4. Click the **Execute** button.

The command is executed on the host specified in **Target host**. When the command is executed, the execution time, host name, and message are displayed in **Log**.

If the JP1/Base of the host is stopped while the command is being executed, CMD.EXE and the executing command (in Windows) or a shell and the executing command (in UNIX) may still remain. In such a case, either manually stop the command or restart the host.

Furthermore, if the JP1/Base of the host is stopped while the command is being executed, commands inside the queue are discarded.

7.1.2 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.

For details about user mapping definitions, see the *Job Management Partner 1/Base User's Guide*.

7.1.3 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.

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*. An action can be executed at the host on which an automated action definition is saved as well as on a remote host.

For details about how to define automated actions, see the following sections:

- For setting up automated actions (using the GUI)
See *2.24 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. Or, 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 2.24 *Action Parameter Definitions window* in the manual *Job Management Partner 1/Integrated Management - Manager GUI Reference*.

See 2.25.1 *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 permissions or JP1_Console_Operator permissions.

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**.

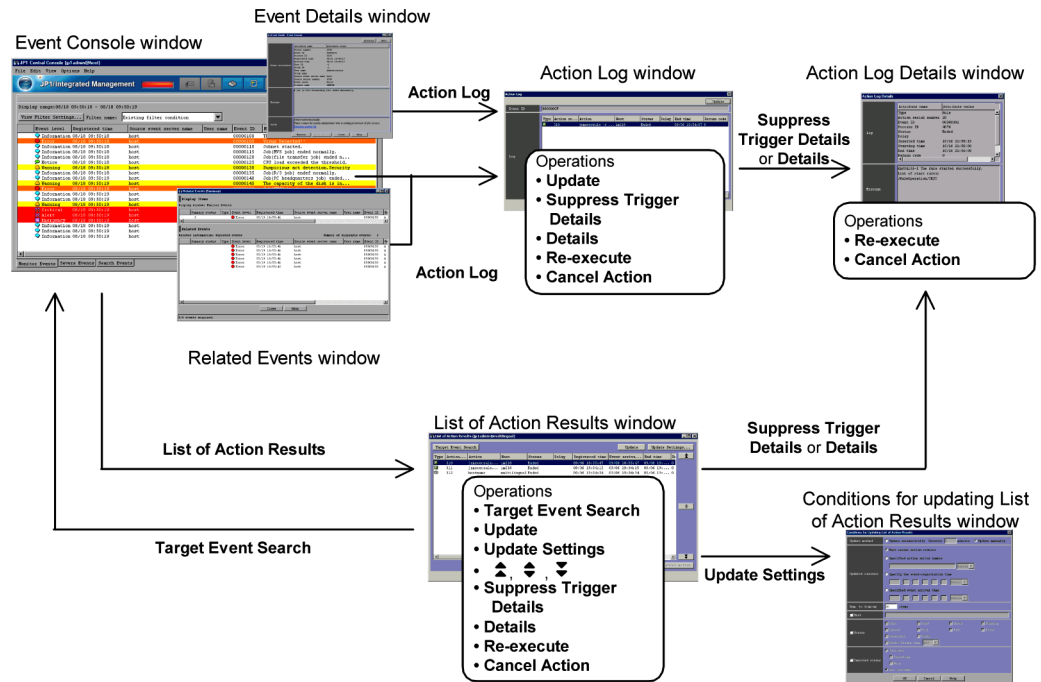
Clicking **Yes** releases the notification suppression, enabling the monitoring function again.

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.

■ **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 *2.29 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.

■ 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 *2.31 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 *2.29 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.

■ 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` permissions or `JP1_Console_Operator` permissions.

Note:

The procedure described here can be used only when the version of JP1/Base on the action execution host is 07-51 or later. This procedure cannot be used if the JP1/Base version is 07-00 or earlier.

■ 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 *(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.

■ **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 *(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.

■ **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 *(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 permissions or JP1_Console_Operator permissions.

■ 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 *(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.

■ 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 *(1) Checking the execution results of automated actions*.
2. Click the **Re-execute** button.
The re-execution request confirmation dialog box opens.
3. Click **OK**.
The request to re-execute the selected automated action has been accepted.
4. To check the status following the re-execution, click the **Close** button to return to the Action Log window or the List of Action Results window, and then click the **Update** button.

7.2.3 Checking the operating status of the automated action function

If the automated action function is not running, no automated action is executed even if an event that triggers automated action is registered in the JP1/Base of the manager. You can use the `jcstatus` command to check the operating status of the automated action function.

When the `jcstatus` command is executed, information indicating a status (`RUNNING`, `STANDBY`, or `STOP`) is output to standard output according to the operating status (running, standby, or stopped). If the operating status is `RUNNING`, the automated action function is running. If the operating status is `STANDBY`, the automated action function is not running and therefore the automated action is not executed. To change the status to `RUNNING`, you need to execute the `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 `jcstatus` command and the display format

*See `jcstatus` (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

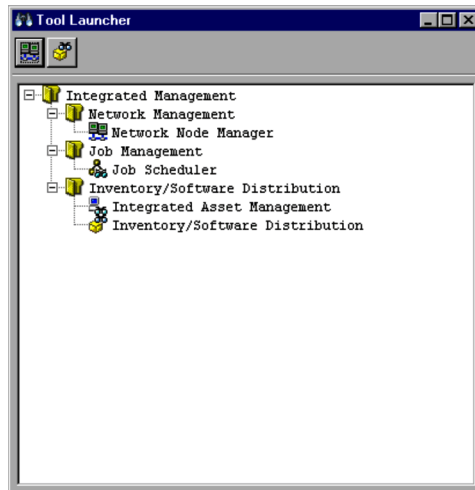
When an application on the system provides a Web page, you can display that Web page. When you select a program from the Tool Launcher, a Web browser starts and displays the Web page.

To use these functions, you must set the URL of the Web page in advance.

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.

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 Vista and the Windows Server 2008 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.

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
Network Management	--	Network Node Manager	Web page	HP NNM
Availability Management	--	Performance Analysis	Application window	JP1/PFM - Analysis View
Job Management	--	Job Scheduler	Application window	JP1/AJS2 or JP1/AJS3
	File Transmission	Transmission Regist. & Exe.	Application window	JP1/FTP
		Log Information	Application window	
Auto-Start Program Registration	Application window			
Inventory/ Software Distribution	--	Integrated Asset Management	Web page	JP1/Asset Information Manager
	--	Inventory/Software Distribution [#]	Web page	JP1/Software Distribution Manager
	Remote Controller	Windows Remote Controller	Application window	JP1/Remote Control Manager
Automated Notification	--	Notification Rule Setting	Application window	TELstaff

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**

7. System Operation Using JP1/IM

icon is not displayed.

Chapter

8. Managing the System Hierarchy using IM Configuration Management

This chapter explains how to use IM Configuration Management to manage the system hierarchy. 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
- 8.2 Managing the system hierarchy
- 8.3 Managing profiles
- 8.4 Managing service operation status
- 8.5 Importing and exporting management information of IM Configuration Management
- 8.6 Managing the configuration of a virtual system

8.1 Managing hosts

This section explains how to use IM Configuration Management - View to manage the information related to the hosts managed by IM Configuration Management.

8.1.1 Registering a host

This subsection explains how to register a new host in the IM Configuration Management database. To register a new host, use the Register Host window, which is opened from the IM Configuration Management window.

To open the Register Host window from the IM Configuration Management window:

1. In the IM Configuration Management window, click the **Host List** tab.
The **Host List** page opens.
2. Use either of the following methods to open the Register Host window:
 - From the tree pane, choose **Host List**, and then from the menu bar, choose **Edit** and then **Register Host**.
 - From the tree pane, choose **Host List**, and then from the popup menu that opens when you right-click the mouse, choose **Register Host**.
3. Specify the items displayed in the Register Host window to register a new host.
For details about the items displayed in the Register Host window, see *4.2 Register Host window* in the manual *Job Management Partner 1/Integrated Management - Manager GUI Reference*.
4. Click the **OK** button.

8.1.2 Deleting a host

This subsection explains how to delete a host registered in the IM Configuration Management database. You can delete a host registered in the IM Configuration Management database on the **Host List** page of the IM Configuration Management window.

To delete a host 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 appears.
2. Select a host from the tree pane.
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 delete the host(s):
 - From the menu bar, choose **Edit** and then **Delete Host**.
 - From the popup menu that opens when you right-click the mouse, choose **Delete Host**.

When a message confirming deletion of the selected host is issued, click **Yes**.

The selected host is deleted from the IM Configuration Management database. If the deletion operation fails, an error message is issued.

8.1.3 Collecting information from hosts

This subsection explains how to collect host information from the IM Configuration Management database.

You can collect information from the specified host. Execute host information collection immediately after a host has been registered, or when information about the host itself or about software installed on the host has been updated in any of the following circumstances:

- OS change
- IP address change
- Software change
 - Software installation or uninstallation
 - Software version upgrade

When you execute host information collection, the profile list is cleared. After you have collected host information, collect the latest profile list when you open the Display/Edit Profiles window.

You can collect host information from the **Host List** page or **IM Configuration** page of the IM Configuration Management window.

To collect host information from the **Host List** page or **IM Configuration** page of the IM Configuration Management window:

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 the 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 is issued confirming collection of information from the selected host, click **Yes**. Information is collected from the selected host. If multiple hosts were selected, you can check the execution results in the Log window.

After the execution of host information collection, you can check the status of the host on the **Host List** page. If the collection option failed, the host icon in the tree pane on the **Host List** page is displayed in gray. You can view the details by clicking the **Basic Information** button in the node information display area of the **Host List** page.

8.1.4 Changing the host information

This subsection explains how to change the host information registered in the IM Configuration Management database. To change the host information registered in the IM Configuration Management database, invoke the Edit Host Properties window from the IM Configuration Management window.

If you edit the host name registered in the system hierarchy, you must re-apply the system hierarchy. For details about the procedure for applying the system hierarchy, see *8.2.5 Applying the system hierarchy*.

To change the host information in the Edit Host Properties 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.
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.
3. Use either of the following methods to open the Edit Host Properties window:
 - From the menu bar, choose **Edit** and then **Edit Host Properties**.
 - From the popup menu that opens when you right-click the mouse, choose **Edit Host Properties**.
4. Change the host information by changing the specification of the item displayed in the Edit Host Properties window.

For details about the items displayed in the Edit Host Properties window, see *4.3 Edit Host Properties window* in the manual *Job Management Partner 1/ Integrated Management - Manager GUI Reference*.

5. Click **OK**.

8.1.5 Displaying a host list

This subsection explains how to display the list of hosts registered in the IM Configuration Management database. To display the host list, use the **Host List** page of the IM Configuration Management window.

To display the host list 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.

For details about the **Host List** page, see *4.1.1 Host List page* in the manual *Job Management Partner 1/Integrated Management - Manager GUI Reference*.

2. Select a host list.

When you select a host list from the tree pane, a host list is displayed as lower-order host information in the node information display area.

To view the host information, perform one of the following operations.

To display basic information:

When you select a host from the tree pane or the node information display area and click the **Basic Information** button, the node information display area displays the basic information and detailed information.

To display product information:

When you select a host from the tree pane or the node information display area and click the **Product Information** button, the node information display area displays the product information and detailed information.

To display service information:

When you select a host from the tree pane or the node information display area and click the **Service Information** button, the node information display area displays the service information and detailed information.

8.2 Managing the system hierarchy

This section explains how to use IM Configuration Management - View to manage the system hierarchy.

8.2.1 Collecting system hierarchy information

This subsection explains how to collect system configuration definition information from all hosts that comprise a system. To collect the configuration definition information, use the **Host List** page or **IM Configuration** page of the IM Configuration Management window.

To collect the configuration definition information on the **Host List** page or **IM Configuration** page of the IM Configuration Management window:

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 menu bar, choose **Operation** and then **Collect IM Configuration**.

When a message confirming collection of the configuration definition information is issued, click **Yes**. The collected configuration definition information is saved in the manager on which IM Configuration Management is running.

- If the collected configuration definition information includes a host that is not registered in IM Configuration Management, it is automatically registered in the IM Configuration Management database. However, no host information is collected. To collect host information, you need to use the **Host List** page or **IM Configuration** page of the IM Configuration Management window.
- If the collected configuration definition information contains the same host name more than once, an error message is displayed and these hosts are not applied in the configuration definition information held by the IM Configuration Management database.
- If the collected configuration definition information contains the same host name more than once, the collected configuration definition information is discarded and the IM configuration tree is displayed in gray on the **IM Configuration** page.
- If the collected configuration definition information does not match the configuration definition information held by the IM Configuration Management database, the system hierarchy is displayed in gray on the **IM Configuration** page.

- If the configuration definition information held by the JP1/Base of the manager on which IM Configuration Management is running has been deleted, the message KNAN20230-Q IM configuration does not exist. Do you want to delete the IM configuration maintained in the Server? is issued.

If you click **Yes**, the configuration definition information held by the IM Configuration Management database is deleted. If you click **No**, the configuration definition information held by the IM Configuration Management database is not deleted, and the system hierarchy is displayed in gray on the **IM Configuration** page.

8.2.2 Displaying the system hierarchy

This subsection explains how to display the system hierarchy. To display the system hierarchy, use the **IM Configuration** page of the IM Configuration Management window.

To display the system hierarchy 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.

For details about the **IM Configuration** page, see *4.1.2 IM Configuration page* in the manual *Job Management Partner 1/Integrated Management - Manager GUI Reference*.

2. Click the **Lower Host Information** button.

When you select a host from the tree pane and click the **Lower Host Information** button, the node information display area displays the lower-order host information.

8.2.3 Verifying the system hierarchy

This subsection explains how to verify whether the content of the configuration definition information that can be collected from all hosts comprising the system matches the content of the configuration definition information held 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.

To verify the configuration definition information from the **Host List** page or **IM Configuration** page of the IM Configuration Management window:

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 menu bar, choose **Operation** and then **Verify IM Configuration**.

When a message confirming verification of the configuration definition information is issued, click **Yes**.

When you execute the verification of the configuration definition information, the configuration definition information of the selected host is collected and compared with the content of the configuration definition information held by IM Configuration Management.

If the configuration definition information held by the JP1/Base of the manager on which IM Configuration Management is running does not match the content of the configuration definition information held by the IM Configuration Management database, an icon indicating an error status is displayed as the host icon in the tree pane of the **IM Configuration** page of the IM Configuration Management window.

If the verification fails, an icon indicating an error status is displayed as the host icon in the tree pane of the **IM Configuration** page of the IM Configuration Management window.

If the installation of JP1/Base running on the host is Version 9 or earlier, it does not support system hierarchy verification. Therefore, an icon indicating an unknown configuration status is displayed as the host icon in the tree pane of the **IM Configuration** page in the IM Configuration Management window of IM Configuration Management - View.

If the manager's configuration definition information does not exist or if the configuration definition information is damaged, the manager verification ends in an error and the process is terminated.

8.2.4 Editing the system hierarchy

This subsection explains how to edit the system's configuration definition information. By editing the configuration definition information, you can add, move, and delete hosts. To edit the configuration definition information, invoke the Edit IM Configuration window from the IM Configuration Management window.

(1) Adding hosts

To add hosts to the system hierarchy:

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 menu bar, choose **Edit** and then **Edit IM Configuration**.

The Edit IM Configuration window opens.

3. In the tree pane of the Edit IM Configuration window, select the higher-order host

of the host to be added.

Information on the hosts that are under the selected host is displayed in **Lower Host Information**. Information on the hosts that can be added to the selected host is displayed under **Host List**.

4. Use one of the following methods to register the hosts:
 - From **Host List** in the Edit IM Configuration window, select the hosts to be added and then drag and drop them into the tree pane.
 - From the menu bar in the Edit IM Configuration window, choose **Edit** and then **Add Host**.

The Select Hosts window opens. From the host list displayed in **Select host(s)**, select the host(s) to be added and add them to the **Selected host(s)** list. Once you have selected the host(s), click **OK**.

- In the tree pane of the Edit IM Configuration window, from the popup menu that opens when you right-click the mouse, choose **Add Host**.

The Select Hosts window opens. From the host list displayed in **Select host(s)**, select the host(s) to be added and add them to the **Selected host(s)** list. Once you have selected the host(s), click **OK**.

For details about the Edit IM Configuration window, see *4.5 Edit IM Configuration window* in the manual *Job Management Partner 1/Integrated Management - Manager GUI Reference*. For details about the Select Hosts window, see *4.4 Select Hosts window* in the manual *Job Management Partner 1/Integrated Management - Manager GUI Reference*.

(2) Moving hosts

To move a host from the system hierarchy:

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 menu bar, choose **Edit** and then **Edit IM Configuration**.

The Edit IM Configuration window opens.

3. In the tree pane of the Edit IM Configuration window, select the host to be moved.
4. Use one of the following methods to move the host:
 - Drag and drop the host selected in the tree pane of the Edit IM Configuration window to another hierarchy in the tree pane.
 - From the menu bar in the Edit IM Configuration window, choose **Edit** and then **Cut**, and then from the tree pane, select the higher-order host at the

moving destination and choose **Edit** and then **Paste**.

- In the tree pane of the Edit IM Configuration window, from the popup menu that opens when you right-click the mouse, choose **Cut**, and then select the higher-order host at the moving destination from the tree pane. Finally, from the popup menu that opens when you right-click the mouse, choose **Paste**.

Moving a higher-order host also moves the lower-order hosts at the same time.

The type of host selected limits the host at the moving destination. For details about the range of hosts that can be selected, see *6.2.5 Editing the system hierarchy* in the *Job Management Partner 1/Integrated Management - Manager Overview and System Design Guide*.

For details about the Edit IM Configuration window, see *4.5 Edit IM Configuration window* in the manual *Job Management Partner 1/Integrated Management - Manager GUI Reference*.

(3) Deleting hosts

To delete a host, invoke the Edit IM Configuration window from the IM Configuration Management window.

To delete a host:

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 menu bar, choose **Edit** and then **Edit IM Configuration**.

The Edit IM Configuration window opens.

3. In the tree pane of the Edit IM Configuration window, select the host you want to delete.

4. Use one of the following methods to delete the host:

- From the tree pane of the Edit IM Configuration window, select the host you want to delete, and then drag and drop it under **Host List**.
- From the menu bar in the Edit IM Configuration window, choose **Edit** and then **Delete Host**.
- In the tree pane of the Edit IM Configuration window, from the popup menu that opens when you right-click the mouse, choose **Delete Host**.

The selected host is deleted from the configuration definition information of JP1/IM.

Deleting a higher-order host also deletes the lower-order hosts at the same time.

8.2.5 Applying the system hierarchy

This subsection explains how to apply the configuration definition information edited in the Edit IM Configuration window to all hosts comprising the system. To apply the configuration definition information, use the Edit IM Configuration window.

To invoke the Edit IM Configuration window from the IM Configuration Management window and use the Edit IM Configuration window to apply the configuration definition 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 menu bar, choose **Edit** and then **Edit IM Configuration**.

The Edit IM Configuration window opens.

3. In the Edit IM Configuration window, check the **Acquire update right** check box.

You can now apply the JP1/IM system configuration. While one user is editing the configuration definition after having acquired update rights, other users cannot edit the configuration of the JP1/IM system.

4. From the menu bar in the Edit IM Configuration window, choose **Operation** and then **Update Host Information**.

The host information is updated to the content displayed in the Edit IM Configuration window, and the configuration definition information is updated.

5. From the menu bar in the Edit IM Configuration window, choose **Operation** and then **IM configuration application**.

The latest configuration definition information that is set by IM Configuration Management is applied to all hosts comprising the system, overwriting the existing information.

The results of system hierarchy application are displayed in a dialog. You can also check the system hierarchy after the application on the **IM Configuration** page of the IM Configuration Management window. If the application operation fails, an icon indicating an error status is displayed as the host icon in the tree pane of the **IM Configuration** page. You can view the details by clicking the **Basic Information** button in the node information display area of the **IM Configuration** page.

8.2.6 Synchronizing system hierarchies

This subsection explains how to synchronize the configuration definition information between the integrated manager and the site managers. To synchronize the configuration definition information, use the **IM Configuration** page of the IM

Configuration Management window.

To synchronize the configuration definition information from the **IM Configuration** page of the IM Configuration Management window:

1. In IM Configuration Management window, click the **Host List** or **IM Configuration** tab.

The **Host List** page or **IM Configuration** page opens.

2. From the menu bar, choose **Operation** and then **Synchronize IM Configuration**.

The configuration definition information is synchronized between the integrated manager and the site managers.

If no site manager is defined under the integrated manager, synchronization of the configuration definition information is not executed.

8.3 Managing profiles

This section explains how to use IM Configuration Management - View to manage the profile of the JP1/Base running on each host.

A JP1/Base profile consists of the following two types of information:

- Valid configuration information

This is the configuration information currently being used by each service of an agent. This information is updated by the agent when a service starts normally. Each service runs based on this valid configuration information.

- Configuration file content

This is the configuration file saved in the agent. Individual services do not necessarily run using the configuration information described in this configuration file. For example, after the definition file information is edited, the update may not be applied to the services. Consequently, the valid configuration information may differ from the content of the configuration file.

8.3.1 Collecting profiles

In profile collection, profile information is collected after profile lists are collected from agents.

Two methods are available for collecting JP1/Base profiles from agents, depending on how you want to collect the profiles. These two methods are explained below.

(1) *Batch-collecting profiles*

This subsection explains how to batch-collect JP1/Base profiles from all hosts defined in the system hierarchy. To batch-collect profiles, use the **Host List** page or **IM Configuration** page of the IM Configuration Management window.

Profiles cannot be batch-collected in the following cases:

- A configuration file exists for which another user has acquired exclusive editing rights.
- Another user is batch-collecting profiles.
- Another user is batch-applying the edited content of the configuration file.

To batch-collect profiles:

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 menu bar, choose **Operation** and then **Batch Collect Profiles**.

Batch collection of profiles is executed. The execution result is output to the Log window.

When a message confirming batch collection of profiles is issued, click **Yes**. Profile collection is executed and the collected profiles are saved in the manager on which IM Configuration Management is running.

In the Display/Edit Profiles window, you can check the status of profiles after the execution of batch collection. If there are any profiles that could not be collected, **Configuration file contents** in the node information display area becomes inactive and the status of the profile(s) is displayed in **Status**.

On the **IM Configuration** page of the IM Configuration Management window, you can check the status of hosts after the batch collection of profiles is executed. If there are any profiles that could not be collected, an icon indicating an error status is displayed as the host icon in the tree pane of the **IM Configuration** page. You can view the details by clicking the **Basic Information** button in the node information display area of the **IM Configuration** page.

(2) Collecting profiles from hosts individually

This subsection explains how to collect JP1/Base profiles from hosts individually.

This function targets hosts on which JP1/Base Version 9 is running. To collect profiles from hosts individually, use the Display/Edit Profiles window.

If a configuration file exists for which another user has acquired exclusive editing rights, profiles cannot be collected from hosts individually.

To collect profiles from hosts individually:

1. In the IM Configuration Management window, click the **IM Configuration** tab. The **IM Configuration** page opens.
2. In the tree pane, select the host from which to collect a profile.
3. Use either of the following methods to open the Display/Edit Profiles window:
 - From the menu bar, choose **Display** and then **Display Profiles**.
 - From the popup menu that opens when you right-click the mouse, choose **Display Profiles**.
4. From the tree pane, select a JP1 product name (JP1/Base), and use either of the following methods to acquire exclusive editing rights:
 - From the menu bar, choose **Edit** and then **Exclusive Editing Settings**.
 - From the popup menu that opens when you right-click the mouse, choose **Exclusive Editing Settings**.

You can then acquire exclusive editing rights to the JP1 product (JP1/Base of the target host).

5. Click the **Configuration File** button.

The **Configuration File** page opens.

If the configuration file has never been edited, clicking the **Configuration File** button automatically collects the configuration file.

6. From the tree pane, select the profile to be collected and use either of the following methods to collect the profile.
 - From the menu bar, choose **Operation** and then **Collect Profiles**.
 - From the popup menu that opens when you right-click the mouse, choose **Collect Profiles**.

When a message confirming collection of the target profile from the agent is issued, click **Yes**. Profiles are collected and saved in the manager on which IM Configuration Management is running.

8.3.2 Collecting a profile list

You can collect a profile list managed by IM Configuration Management from the agent. The collected information is displayed in the tree pane of the Display/Edit Profiles window.

When any of the following operations is executed, a profile list becomes unregistered:

- Initial startup of IM Configuration Management
- Host information collection
- System hierarchy application
- `jcfimport` command execution

To collect a profile list:

1. In the IM Configuration Management window, click the **IM Configuration** tab. The **IM Configuration** page opens.
2. Use either of the following methods to open the Display/Edit Profiles window:
 - From the menu bar, choose **Display** and then **Display Profiles**.
 - From the popup menu that opens when you right-click the mouse, choose **Display Profiles**.
3. From the tree pane, select a JP1 product name (JP1/Base), and use either of the following methods to update the profile list:
 - From the menu bar, choose **Operation** and then **Rebuild Profile Tree**.

- From the popup menu that opens when you right-click the mouse, choose **Rebuild Profile Tree**.

The profile tree is rebuilt and the profile list is updated. When you restart the agent or the JP1/Base of the agent, rebuild the profile tree before editing the profile or applying the editing results.

4. From the menu bar in the IM Configuration Management window, choose **Operation** and then **Batch Collect Profiles**.

The profile list managed by IM Configuration Management is collected from the agent.

Note:

- If profile tree rebuilding fails, an error message is displayed and the profile tree that existed before the execution of the rebuilding operation is displayed. In this case, operations can be executed on the profile tree that existed before the execution of the rebuilding operation, and profiles that have the same information as the agent, but have subsequent operations, may be adversely affected. Therefore, after removing the error cause, re-execute rebuilding of the profile tree.
- If multiple event log traps have been started using the same action definition file, or if event log traps have been started using action definition files that have the same name but are in different directories, profile list collection fails.

8.3.3 Displaying profiles

Two methods are available for displaying JP1/Base profiles, depending on the information to be displayed. This subsection explains these two methods.

(1) *Displaying the valid configuration information*

This subsection explains how to display the valid configuration information of JP1/Base for each host. This function targets hosts on which JP1/Base Version 9 is running. To display the valid configuration information of JP1/Base for each host, use the Display/Edit Profiles window.

To display the valid configuration information in the Display/Edit Profiles window:

1. In the IM Configuration Management window, click the **IM Configuration** tab.
The **IM Configuration** page opens.
2. In the tree pane, select the host whose valid configuration information you want to display.
3. Use either of the following methods to open the Display/Edit Profiles window:
 - From the menu bar, choose **Display** and then **Display Profiles**.

- From the popup menu that opens when you right-click the mouse, choose **Display Profiles**.
4. From the tree pane of the Display/Edit Profiles window, select the items for which you want to display valid configuration information.
 5. Click the **Valid configuration information** button.

The content of the valid configuration information that is displayed differs depending on the display items selected in the tree pane of the Display/Edit Profiles window. For details, see *4.6.1 Valid Configuration Information page* in the manual *Job Management Partner 1/Integrated Management - Manager GUI Reference*.

(2) **Displaying the configuration file**

This subsection explains how to display the configuration file of JP1/Base for each host. To display the configuration file of JP1/Base for each host, use the Display/Edit Profiles window.

To display the configuration file in the Display/Edit Profiles window:

1. In the IM Configuration Management window, click the **IM Configuration** tab. The **IM Configuration** page opens.
2. In the tree pane, select the host whose configuration file you want to display.
3. Use either of the following methods to open the Display/Edit Profiles window:
 - From the menu bar, choose **Display** and then **Display Profiles**.
 - From the popup menu that opens when you right-click the mouse, choose **Display Profiles**.
4. From the tree pane of the Display/Edit Profiles window, select the display item whose configuration file you want to display.
5. Click the **Configuration File** button.

The content of the configuration file that is displayed differs depending on the display items selected in the tree pane of the Display/Edit Profiles window. For details, see *4.6.2 Configuration File page* in the manual *Job Management Partner 1/Integrated Management - Manager GUI Reference*.

Some of the items displayed in configuration files can be edited, but others cannot. For details about how to edit configuration files, see *8.3.4 Editing configuration files*.

8.3.4 Editing configuration files

This subsection explains how to edit and save collected configuration files of JP1/Base. For details about how to collect configuration files, see *8.3.1 Collecting profiles*. To edit and save configuration files, use the Display/Edit Profiles window.

The profile types that can be edited in a configuration file are event forwarding settings information, log file trap information, event log trap information, and local action information.

To edit and save a configuration file in the Display/Edit Profiles window:

1. In the IM Configuration Management window, click the **IM Configuration** tab. The **IM Configuration** page opens.
2. In the tree pane, select the host whose configuration file you want to edit.
3. Use either of the following methods to open the Display/Edit Profiles window:
 - From the menu bar, choose **Display** and then **Display Profiles**.
 - From the popup menu that opens when you right-click the mouse, choose **Display Profiles**.
4. From the tree pane, select a JP1 product name (JP1/Base), and use either of the following methods to acquire exclusive editing rights:[#]
 - From the menu bar, choose **Edit** and then **Exclusive Editing Settings**.
 - From the popup menu that opens when you right-click the mouse, choose **Exclusive Editing Settings**.
5. In the tree pane of the Display/Edit Profiles window, select the configuration file you want to edit.
6. In the node information display area of the Display/Edit Profiles window, click the **Configuration File** button.

The contents of the configuration file for the profile to be edited and saved on the manager on which IM Configuration Management is running is displayed. For details about the items that can be edited, see *4.6.2 Configuration File page* in the manual *Job Management Partner 1/Integrated Management - Manager GUI Reference*.

7. When the editing is finished, from the menu bar, choose **Operation**, and then from the **Save/Apply Profiles** menu, choose **Save on the Server**.

The content of the edited configuration file is saved in the manager on which IM Configuration Management is running.

Note, however, that the content of the configuration file saved in the manager on which IM Configuration Management is running is not forwarded to the host. When the configuration file is applied, it is automatically saved. For details about how to forward the configuration file to the host and apply it, see *8.3.5 Applying the edited content of the configuration file*.

#

- To cut or paste a character string in the configuration file, you need to execute Step 4 and acquire exclusive editing rights.
- If you are only copying a character string in the configuration file, there is no need to execute Step 4.
- If you have already acquired exclusive editing rights, there is no need to execute Step 4.

If you collect a profile from a host after you have saved the content of the configuration file in the manager on which IM Configuration Management is running, the saved content will be overwritten by the collected content.

8.3.5 Applying the edited content of the configuration file

Two methods are available for applying the edited content of the configuration file, depending on how you want to apply the content. These two methods are explained below.

If an attempt to apply the configuration file fails when JP1/Base Version 9 is used, the configuration file of the agent is rolled back to the original configuration file.

(1) *Batch-applying the edited content of the configuration file*

This subsection explains how to batch-apply the edited content of the configuration file to all hosts registered in the system hierarchy. To batch-apply the edited content of the configuration file, use the **Host List** page or **IM Configuration** page of the IM Configuration Management window.

The profile types that can be batch-applied in the configuration file are event forwarding settings information, event log trap information, and local action information.

The edited content of the configuration file cannot be batch-applied in the following cases:

- A configuration file exists for which another user has acquired exclusive editing rights.
- Another user is batch-collecting profiles.
- Another user is batch-applying the edited content of the configuration file.

To batch-apply the edited content of the configuration file:

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 menu bar, choose **Operation** and then **Batch Reflect Profiles**.

Batch application of profiles is executed. The execution result is output to the Log

window.

When a message confirming batch application of the configuration file is issued, click **Yes**. The content of the configuration file that has been saved in the manager on which IM Configuration Management is running is applied to all hosts.

In the Display/Edit Profiles window, you can check the status of the configuration file after the execution of batch application. If there are any configuration files for which application failed, or if there are any configuration files whose status is `Saved on the server`, the icon for the configuration file(s) in the tree pane indicates that editing is in progress.

On the **IM Configuration** page of IM Configuration Management - View's IM Configuration Management window, you can check the status of hosts after the batch application is executed. If there are any configuration files for which application failed, or if there are any configuration files whose status is `Saved on the server`, an icon indicating an error status is displayed as the host icon in the tree pane of the **IM Configuration** page. You can view the details by clicking the **Basic Information** button in the node information display area of the **IM Configuration** page.

(2) Applying the edited content of the configuration file to hosts individually

This subsection explains how to apply the edited content of the configuration file to hosts individually. To apply the edited content of the configuration file to hosts individually, use the Display/Edit Profiles window.

The profile types of the configuration file that can be applied to hosts individually are event forwarding settings information, log file trap information, event log trap information, and local action information.

To apply the edited content of the configuration file:

1. In the IM Configuration Management window, click the **IM Configuration** tab.^{#1}
The **IM Configuration** page opens.
2. In the tree pane, select a host to which you want to apply the configuration file.^{#1}
3. Use either of the following methods to open the Display/Edit Profiles window:^{#1}
 - From the menu bar, choose **Display** and then **Display Profiles**.
 - From the popup menu that opens when you right-click the mouse, choose **Display Profiles**.
4. From the tree pane, select a JP1 product name (JP1/Base), and use either of the following methods to acquire exclusive editing rights:^{#1}
 - From the menu bar, choose **Edit** and then **Exclusive Editing Settings**.
 - From the popup menu that opens when you right-click the mouse, choose

Exclusive Editing Settings.

5. From the tree pane, select the profiles you want to apply and click the **Configuration File** button.^{#2}

The **Configuration File** page opens.

6. From the menu bar, choose **Operation**, and then from the **Profile application** menu, choose **Apply by Reloading**.

Profile application is executed.

When a message confirming application of the edited content of the configuration file is issued, click **Yes**.

#1

If you have already acquired exclusive editing rights, there is no need to execute Steps 1 through 4.

#2

If you have edited the configuration file of the profile to be applied, there is no need to execute Step 5.

8.4 Managing service operation status

This chapter explains how to use IM Configuration Management - View to manage the status of service operations on each host.

8.4.1 Collecting service operation information

This subsection explains how to collect the operating information of services that are running on each host from the system hierarchy. To collect service operation information on each host, use the **Host List** page or **IM Configuration** page of the IM Configuration Management window. However, the procedure differs depending on 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 *6.4.2 Collecting service activity information in the Job Management Partner I/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 6.4.2 *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.

8.4.2 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, see 8.4.1 *Collecting service operation information*.

The information on services in the IM Configuration Management window displays the following types of operation information:

Table 8-1: Operation information that is displayed for each service

Product name	Service name	Operating status
JP1/Base	JP1/Base	The operating status of the service is displayed as one of the following: <ul style="list-style-type: none"> • Running • Stopped • Partially running • Collection failed
	Event Service	
	Log file trap	
JP1/IM - Manager	JP1/IM - Manager	

Detailed Information in the IM Configuration Management window displays the execution results of the commands that collect information from individual services as follows:

Table 8-2: Service-collection commands

Service name	Collection command
JP1/Base	jbs_spm�_status
Event Service	jevstat
Log file trap	jevlogstat ALL
JP1/IM - Manager	jco_spm�_status

8.5 Importing and exporting management information of IM Configuration Management

This section explains how to execute commands to import and export the management information of IM Configuration Management.

8.5.1 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.

(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.

The name of the host input information file is `host_input_data.csv`. You can edit and import the host input information file.

The table below shows the types of information output to the host input information file.

Table 8-3: Host information that is exported (host input information file)

Line	Output item	Output value
First line (header information)	Product name	JP1/IM-CF
	File format version	File format version Example: 090000
	Character code	Character code

Line	Output item	Output value
Second line (header information)	Host name	Host_name
	IP address	IPAddress
	List of host names	Host_list
	Comment	Comment
	Host type	Host_type
	Active host	Running_host_name
	Standby host	Standby_host_name
	VMM host	VMM_host_name
Third and subsequent lines	Host name	Name of the host that was registered in the system hierarchy
	IP address	IP address of the host that was registered in the system hierarchy (if there are multiple IP addresses, they must be delimited by commas and the entire string must be enclosed in double quotation marks).
	List of host names	List of host names registered on a host (if there are multiple hosts, they must be delimited by commas and the entire string must be enclosed in double quotation marks).
	Comment	Comment registered in the host
	Host type	Host type (physical, logical, virtual, or unknown)
	Active host	Name of the active host
	Standby host	Name of the standby host (if there are multiple standby hosts, they must be delimited by commas and the entire string must be enclosed in double quotation marks).
	VMM host	Name of the host on which the virtual machine monitor is running

The name of the collected host information file is `host_collect_data.csv`. You cannot edit or import the collected host information file.

The table below shows the types of information output to the collected host information file.

Table 8-4: Host information that is exported (collected host information file)

Row	Output item	Output value
First line (header information)	Product name	JP1/IM-CF
	File format version	File format version Example: 090000
	Character code	Character code
Second line (header information)	Real host name	Real_host_name
	OS name	OS_name
	Product name	JP1_product_name
	Product module	JP1_product_id
	Version	JP1_product_version
	Installation path	Install_path
	Environment settings file storage folder	Conf_dir
	Update date/time	Date
	Update date/time (GMT)	Total_time
Third and subsequent lines	Real host name	Real host name of the host
	OS name	Name of the OS running on the host
	Product name	Name of the product running on the host
	Product module	Product module name
	Version	Product version
	Installation path	Installation path for the product
	Environment settings file storage folder	Folder that stores the product's environment settings file
	Update date/time	YYYY/MM/DD hh:mm:ss
	Update date/time (GMT)	GMT

(2) System hierarchy information

The system hierarchy information is exported to a file. The name of the file that is exported is `system_tree_information.txt`. You can edit the exported file and import it.

The table below shows the system hierarchy information that is output to this file.

Table 8-5: JP1/IM's system hierarchy information that is exported

Output item	Description of output value
<i>[managing-host]</i>	<ul style="list-style-type: none"> Indicates the integrated manager, a site manager, or a relay manager that manages JP1/Base hosts. The first managing host that is defined is the integrated manager, and the managing hosts subsequently defined are either site managers or relay managers. Hosts are treated as managed hosts until the next host in square brackets [] appears. If the system hierarchy is divided and defined, the host name is preceded by an asterisk (*).
<i>managed-host</i>	<ul style="list-style-type: none"> A JP1/Base host that is managed by a managing host. A site manager or relay manager is defined as a host managed by the integrated manager. If the system hierarchy is divided and defined, the host name is preceded by an asterisk (*).

(3) Profile information

The profile information of the JP1/Base that is running on the host is exported. The table below shows the profile information that is exported.

Table 8-6: Export file names of profile information that is exported

Profile information	Export file name
Event forwarding settings file	<code>forward</code>
Event log-trap action definition file	<code>nthevent.conf</code>
Local action execution definition file	<code>jbslact.conf</code>

8.5.2 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.

(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 8-7: 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 and the hyphen (-), excluding control codes.	Required [#]	--
Host name list	A maximum of four host names may be input. Permitted characters are alphanumeric characters and the hyphen (-), excluding control codes.	Optional	Blank
Comment	A character string of up to 80 bytes may be input.	Optional	Blank
Host type	<code>physical</code> , <code>logical</code> , <code>virtual</code> , or <code>unknown</code> may be input.	Optional	<code>physical</code>
Active host	A character string of up to 255 bytes may be input. Permitted characters are alphanumeric characters and the hyphen (-), excluding control codes.	Optional	Blank
Standby host	A maximum of four host names may be input. For each host name, a character string of up to 255 bytes may be input. Permitted characters are alphanumeric characters 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 and the hyphen (-), excluding control codes.	Optional	Blank

Legend:

--: There is no default value.

#

If the required item is not specified, an error occurs. If an optional item is not specified, the default value is imported.

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.

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 (`system_tree_information.txt`) for the system hierarchy information is imported.

If any of the conditions listed below applies to the content of the export file (`system_tree_information.txt`) 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 (`system_tree_information.txt`) for the system hierarchy information is edited, the host name specified in the export file (`system_tree_information.txt`) for the system hierarchy information may not be specified in the export file (`host_input_data.csv`) for host information (manually entered-information) in some cases. In such cases, after the export file (`system_tree_information.txt`) 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 (`system_tree_information.txt`) for the system hierarchy information does not exist, an error message is displayed and the importing operation is halted.

(3) Profile information

The content of the export files for the profile information is imported. The table below shows the export files for the profile information that is imported.

Table 8-8: Export files for the profile information that is imported

Profile information	Export file name
Event Forwarding Settings File	<code>forward</code>
Event Log-Trap Action Definition File	<code>ntevent.conf</code>
Local Action Execution Definition File	<code>jbslcact.conf</code>

When profile information is imported, its 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.

8.5.3 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*

Merely importing the management information of IM Configuration Management does not apply the system hierarchy information to the actual system. When you click

the **IM Configuration** tab in the IM Configuration Management window, the tree is displayed in gray.

To apply the system hierarchy 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 menu bar, choose **Edit** and then **Edit IM Configuration**.

The Edit IM Configuration window opens.

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. In the Edit IM Configuration window, check the **Acquire update right** check box.

You can now edit the JP1/IM system configuration.

5. From the menu bar in the Edit IM Configuration window, choose **Operation** and then **IM configuration application**.

The system hierarchy information is applied to the actual system.

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 *8.3.5 Applying the edited content of the configuration file*.

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 profiles, see *8.3.1 Collecting profiles*.

8.6 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.

To manage a virtual configuration, you need VMware ESX.

8.6.1 Registering a virtual system host

This subsection explains how to register a virtual host in the system hierarchy. To register a new virtual host, you can either invoke the Register Host window from the IM Configuration Management window, or import the virtualization configuration information of VMware ESX.

(1) Registering from the Register Host window

To register a new virtual host by invoking the Register Host window from the IM Configuration Management window:

1. In the IM Configuration Management window, click the **Host List** tab to open the **Host List** page.
2. Use either of the following methods to open the Register Host window:
 - In the tree pane, select **Host List**, and from the menu bar, choose **Edit** and then **Register Host**.
 - In the tree pane, select **Host List**, and from the popup menu that opens when you right-click the mouse, choose **Register Host**.
3. Specify the items displayed in the Register Host window and register the new host.

Select `virtual host` for the host type, and specify for the VMM host the name of a host on which the virtual machine monitor is running.

(2) Importing the virtualization configuration information

If you are using VMware ESX as the virtual machine monitor, register the new virtual host by exporting the virtualization configuration information of VMware ESX and merging it with the exported configuration information of IM Configuration Management. Then, import the merged result into IM Configuration Management. The procedure follows.

1. Execute the `jcfexport -m` command.

This step exports the host list that IM Configuration Management has.
2. Execute the `jcfcolvmesx` command.

This step acquires the virtual host name from VMware ESX and outputs it to a file.

3. Change the `host_input_data.csv` file name.
Change the name of the `host_input_data.csv` file that was output by the `jcfexport` command to a different name.
4. Execute the `jcfmkhostsdata` command.
Merge the file that was output in Step 2 with the file whose name was changed in Step 3, and then output the result to the directory exported in Step 1 as the `host_input_data.csv` file.
5. Execute the `jcfimport -a` command.
Specify the directory exported in Step 1 and import the `host_input_data.csv` file, and then register it in the host list.

When you use the `jcfimport` command to import the virtualization configuration information, three types of information that IM Configuration Management has, namely host, system hierarchy, and profile, are deleted. To manage profiles, you need to collect these three types of information after importation. The procedure follows.

1. In the IM Configuration Management window, open the **Host List** page.
2. From the tree pane, select **Host List**, and then select all hosts displayed in **Lower Host Information**.
3. From the menu bar, choose **Operation** and then **Collect Host Information**.
4. From the menu bar, choose **Operation** and then **Collect IM Configuration**.
5. From the menu bar, choose **Operation** and then **Batch Collect Profiles**.

Batch collection of profiles is executed.

8.6.2 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.

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.

8.6.3 Exporting the configuration information of a virtual system

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.

Chapter

9. Troubleshooting

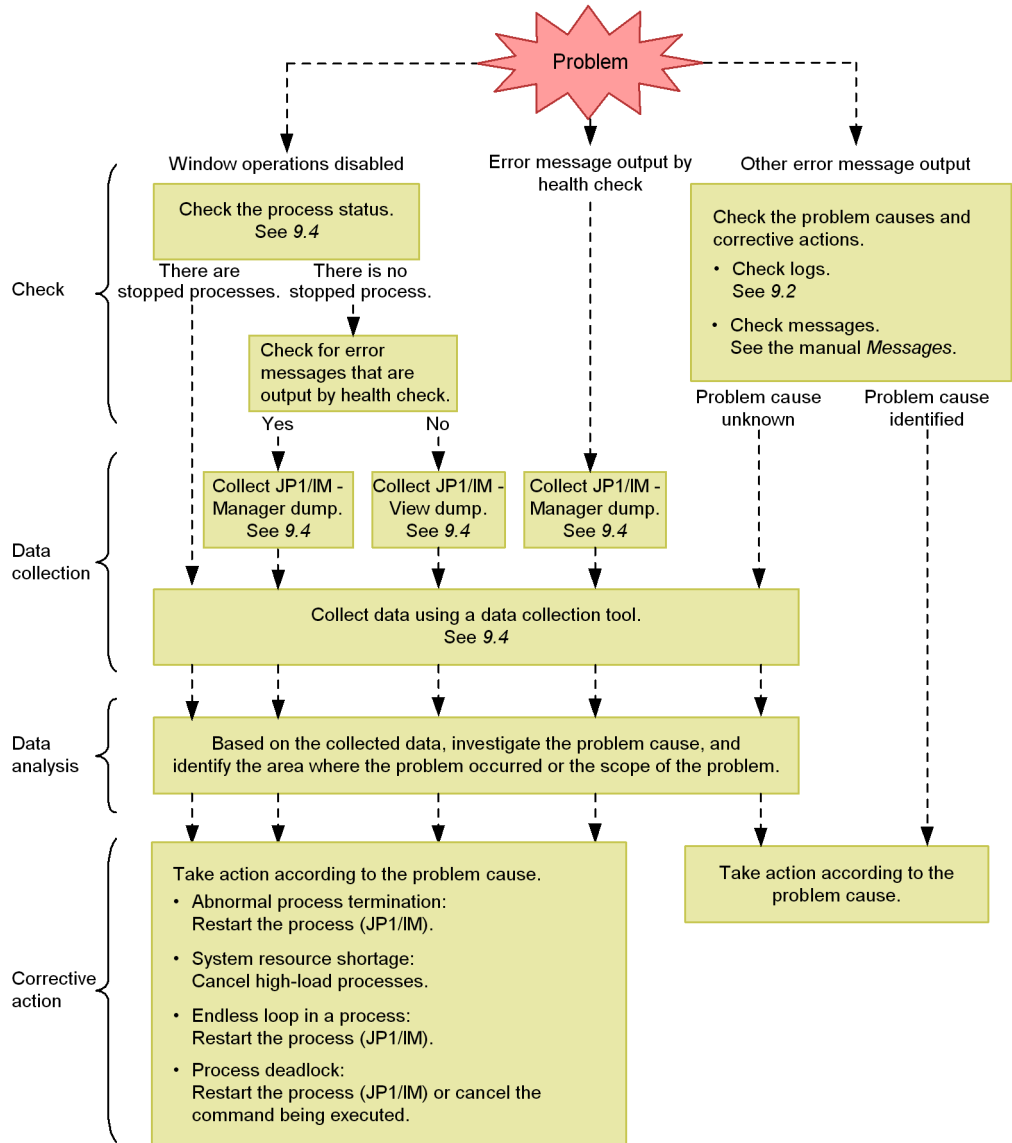
This chapter explains how to handle problems if they occur in JP1/IM. It also explains items that tend to cause problems.

- 9.1 Troubleshooting procedure
- 9.2 Log information types
- 9.3 Data that needs to be collected when a problem occurs
- 9.4 Collecting data
- 9.5 Corrective actions

9.1 Troubleshooting procedure

The figure below shows the procedure to follow when a problem occurs in JP1/IM.

Figure 9-1: Troubleshooting procedure



9.2 Log information types

The following three types of logs are output by JP1/IM:

- Common message log
- Integrated trace log
- Process-by-process trace log

This section explains these three types of log information.

9.2.1 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)

Note:

In UNIX, when a message is being output to the syslog file, the message may be incomplete.

9.2.2 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
```

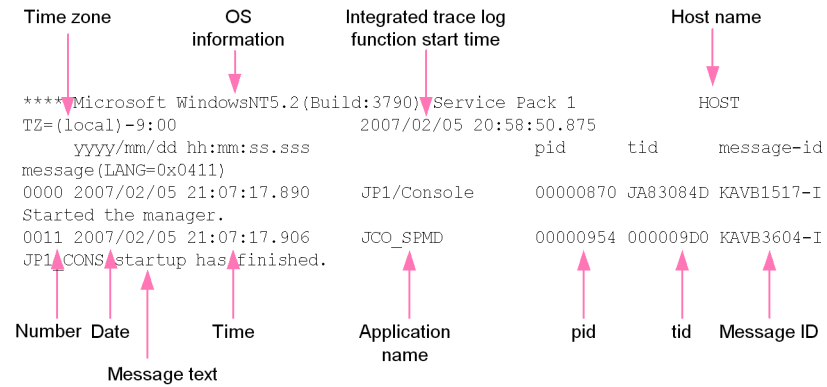
In UNIX:

```
/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 9-2: 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 9-1: 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 9-2: 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)

Output items	Explanation
AP name (16 bytes or shorter)	<p>Name that identifies an application (application identifier)</p> <p>The following AP names are output by JP1/IM - Manager:</p> <ul style="list-style-type: none"> • JP1/IM-Manager Service JP1/IM-Manager • Event Base Service evflow • Automatic Action Service jcmain • Event Generation Service evgen • Central Scope Service jcsmain • IM Configuration Management Service jcfmain • Process management JCO_SPMD • jcochstat command jcochngstat • Other commands <i>command-name</i> <p>The following AP names are output by JP1/IM - View:</p> <ul style="list-style-type: none"> • Central Console - View JP1/IM-View • Central Scope - View JP1/IM-View • IM Configuration Management - View JP1/IM-View • Edit Tree window JP1/IM-Edit
pid	Process ID assigned by the OS
tid	Thread ID for identifying a thread
Message ID	Message ID explained in the message output format. Message ID used by this product.
Message text	Message text that is output to the integrated trace log. Message text that is output from this product.

The log time that is output to the integrated trace log is formatted according to the time zone of the process that output the log.

Consequently, if a user who has changed the environment variable *TZ* starts a service or executes a command, a time that is different from the time zone that is set in the OS may be output.

9.2.3 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.

9.2.4 Log files and directory list

This subsection explains the types of log information that are output by JP1/IM, default file names, and directory names.

Note that the files explained here are output for product maintenance purposes. Therefore, there is no need for the user to view or modify these files. If a problem such as a system error occurs, the user may be asked to temporarily retain these files on site for the purpose of collecting data.

(1) In Windows

The tables below show the default log files and folders that are output by the Windows version of JP1/IM.

The *Log type* column lists the log types that are output by JP1/IM.

The *Default file name and folder name* column describes log file names as absolute paths when JP1/IM - Manager, JP1/IM - View, or JP1/Base is installed in the default mode. *Default file name and folder name* in a cluster operation system describes the log file names of shared folders as absolute paths.

The *Maximum disk usage* column shows the maximum disk space used by each log file. When there are multiple log files, the combined total is given.

The *File-switching timing* column shows how JP1/IM times output destination log file switching. When the file reaches the size shown in this column or when the event shown in this column occurs, the output destination is switched. If there are multiple log files and if the maximum disk usage is reached, files are overwritten, beginning with the ones that have the oldest update dates.

Table 9-3: 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	<i>Console-path</i> \log\JCO_SPMD{1 2 3}.log	384 KB	128 KB
	<i>Console-path</i> \log\JCO_SPMD_COMMAND{1 2 3}.log	384 KB	128 KB

Log type	Default file name and folder name	Maximum disk usage	File-switching timing
	<i>shared-folder</i> \jplcons\log\JCO_SPMD{1 2 3}.log	384 KB	128 KB
	<i>shared-folder</i> \jplcons\log\JCO_SPMD_COMMAND{1 2 3}.log	384 KB	128 KB
Stack trace log	<i>Console-path</i> \log\javalog0{1 2 3 4}.log	1 MB	At startup or 256 KB
	<i>shared-folder</i> \jplcons\log\javalog0{1 2 3 4}.log	1 MB	At startup or 256 KB
	<i>View-path</i> \log\jrmjavalog0{1 2}.log	512 KB	At startup or 256 KB
Logical host settings program log	<i>Console-path</i> \log\jplhassetup.{log log.old}	2,000 KB	1,000 KB
Installation log	<i>Console-path</i> \log\command\comdef[_old].log	512 KB	256 KB
Event console log	<i>Console-path</i> \log\console\EVCONS{1 2 3}.log	30,720 KB	10,240 KB
	<i>Console-path</i> \log\console\jplcons{1 2 3 4}.log	20,480 KB	5,120 KB ^{#1}
	<i>Console-path</i> \log\console\evtcon_exe{1 2 3}.log	256 KB x 3	256 KB
	<i>Console-path</i> \log\console\jplconsM{1 2... 20}.log	100 MB	5 MB ^{#1}
	<i>Console-path</i> \log\console\jplfilterDef{1 2}.log	10 MB	5 MB
	<i>shared-folder</i> \jplcons\log\console\EVCONS{1 2 3}.log	30,720 KB	10,240 KB
	<i>shared-folder</i> \jplcons\log\console\jplcons{1 2 3 4}.log	20,480 KB	5,120 KB ^{#1}
	<i>shared-folder</i> \jplcons\log\console\evtcon_exe{1 2 3}.log	256 KB x 3	256 KB
	<i>shared-folder</i> \jplcons\log\console\jplconsM{1 2... 20}.log	100 MB	5 MB ^{#1}
	<i>shared-folder</i> \jplcons\log\console\jplfilterDef{1 2}.log	10 MB	5 MB

9. Troubleshooting

Log type	Default file name and folder name	Maximum disk usage	File-switching timing
Automated action trace log	<i>Console-path</i> \log\action\JCAMAIN{1 2 3 4 5}.log	25,600 KB ^{#2}	5,120 KB
	<i>shared-folder</i> \jplcons\log\action\JCAMAIN{1 2 3 4 5}.log	25,600 KB ^{#2}	5,120 KB
Product information log	<i>Console-path</i> \log\hliclib\hliclibtrc{1 2 3 4 5}.log	5 MB	1 MB
	<i>Console-path</i> \log\hliclib\hlicliberr{1 2 3 4 5}.log	5 MB	1 MB
	<i>Console-path</i> \log\hliclib\hliclibmgrtrc{1 2 3 4 5}.log	5 MB	1 MB
	<i>Console-path</i> \log\hliclib\hliclibmgrerr{1 2 3 4 5}.log	5 MB	1 MB
	<i>shared-folder</i> \jplcons\log\hliclib\hliclibtrc{1 2 3 4 5}.log	5 MB	1 MB
	<i>shared-folder</i> \jplcons\log\hliclib\hlicliberr{1 2 3 4 5}.log	5 MB	1 MB
	<i>shared-folder</i> \jplcons\log\hliclib\hliclibmgrtrc{1 2 3 4 5}.log	5 MB	1 MB
	<i>shared-folder</i> \jplcons\log\hliclib\hliclibmgrerr{1 2 3 4 5}.log	5 MB	1 MB
Action information file	<i>Console-path</i> \log\action\actinf.log	626 KB ^{#3}	No switching
	<i>shared-folder</i> \jplcons\log\action\actinf.log	626 KB ^{#3}	No switching
Action host name file	<i>Console-path</i> \log\action\acttxt{1 2}.log	48.9 MB ^{#4}	When the action information file wraps around
	<i>shared-folder</i> \jplcons\log\action\acttxt{1 2}.log	48.9 MB ^{#4}	When the action information file wraps around
Action re-execution file	<i>Console-path</i> \log\action\actreaction	300 MB	When system switching occurs
	<i>shared-folder</i> \jplcons\log\action\actreaction	300 MB	When system switching occurs

Log type	Default file name and folder name	Maximum disk usage	File-switching timing
jcochafmode, jcochstat, and jcoevtreport command trace logs ^{#5}	<i>Console-path</i> \log\command\CMD{1 2 3}.log	3,072 KB	1,024 KB
	<i>Console-path</i> \log\command\jplcons_cmd{1 2}.log	12,288 KB	6,144 KB
	<i>Console-path</i> \log\command\jplconsM_cmd{1 2}.log	12,288 KB	6,144 KB
Plug-in log	<i>Console-path</i> \log\command\jcoplugin{1 2 3}.log	3 MB	1 MB
Reporting status storage file	<i>Console-path</i> \log\notice\notice_stat.dat	72B	No switching
	<i>shared-folder</i> \jplcons\log\notice\notice_stat.dat	72B	No switching
Action definition backup file	<i>Console-path</i> \log\action\actdefbk.conf	2,048 KB	No switching
	<i>shared-folder</i> \jplcons\log\action\actdefbk.conf	2,048 KB	No switching
Event base trace log	<i>Console-path</i> \log\evflow\EVFLOW{1 2 3 4 5 6 7 8 9 10}.log	100 MB	10 MB
	<i>Console-path</i> \log\evflow\jplevflowM{1 2... 20}.log	100 MB	5 MB
	<i>Console-path</i> \log\evflow\jplactDef{1 2}.log	10 MB	5 MB
	<i>Console-path</i> \log\evflow\jplchsevDef{1 2}.log	10 MB	5 MB
	<i>Console-path</i> \log\evflow\evflow_exe{1 2 3}.log	256 KB x 3	256 KB
	<i>shared-folder</i> \jplcons\log\evflow\EVFLOW{1 2 3 4 5 6 7 8 9 10}.log	100 MB	10 MB
	<i>shared-folder</i> \jplcons\log\evflow\jplevflowM{1 2... 20}.log	100 MB	5 MB
	<i>shared-folder</i> \jplcons\log\evflow\jplactDef{1 2}.log	10 MB	5 MB

Log type	Default file name and folder name	Maximum disk usage	File-switching timing
	<i>shared-folder</i> \jplcons\log\evflow\jplchsevDef{1 2}.log	10 MB	5 MB
	<i>shared-folder</i> \jplcons\log\evflow\evflow_exe{1 2 3}.log	256 KB x 3	256 KB
Matching information file	<i>Console-path</i> \log\evflow\evflowinf.log	12B	No switching
	<i>shared-folder</i> \jplcons\log\evflow\evflowinf.log	12B	No switching
Event base error log	<i>Console-path</i> \log\evflow\jpl-evflow{1 2 3 4}.log	20,480 KB	5,120 KB
	<i>shared-folder</i> \jplcons\log\evflow\jpl-evflow{1 2 3 4}.log	20,480 KB	5,120 KB
Event base stack trace	<i>Console-path</i> \log\evflow\javalog0{1 2 3 4}.log	1 MB	At startup or 256 KB
	<i>shared-folder</i> \jplcons\log\evflow\javalog0{1 2 3 4}.log	1 MB	At startup or 256 KB
Automated action error log	<i>Console-path</i> \log\action\jplact{1 2 3}.log	15,360 KB	5,120 KB
	<i>shared-folder</i> \jplcons\log\action\jplact{1 2 3}.log	15,360 KB	5,120 KB
Correlation event generation history file	<i>Console-path</i> \operation\evgen\egs_discrim{1 2 3}.log ^{#6}	30 MB ^{#6}	10 MB ^{#6}
	<i>shared-folder</i> \jplcons\operation\evgen\egs_discrim{1 2 3}.log ^{#6}	30 MB ^{#6}	10 MB ^{#6}
Correlation event generation trace log	<i>Console-path</i> \log\evgen\EVGEN{1 2 3}.log	15 MB	5 MB
	<i>Console-path</i> \log\evgen\evgen_exe{1 2 3}.log	256 KB x 3	256 KB
	<i>shared-folder</i> \jplcons\log\evgen\EVGEN{1 2 3}.log	15 MB	5 MB
	<i>shared-folder</i> \jplcons\log\evgen\evgen_exe{1 2 3}.log	256 KB x 3	256 KB

Log type	Default file name and folder name	Maximum disk usage	File-switching timing
Correlation event generation individual log	<i>Console-path</i> \log\evgen\jplegs{1 2}.log	20 MB	10 MB
	<i>Console-path</i> \log\evgen\jplegsM{1 2}.log	20 MB	10 MB
	<i>shared-folder</i> \jplcons\log\evgen\jplegs{1 2}.log	20 MB	10 MB
	<i>shared-folder</i> \jplcons\log\evgen\jplegsM{1 2}.log	20 MB	10 MB
Correlation event generation individual log (for commands)	<i>Console-path</i> \log\evgen\jplegs_cmd{1 2 3 4}.log	20 MB	5 MB
	<i>Console-path</i> \log\evgen\jplegsM_cmd{1 2 3 4}.log	20 MB	5 MB
	<i>shared-folder</i> \jplcons\log\evgen\jplegs_cmd{1 2 3 4}.log	20 MB	5 MB
	<i>shared-folder</i> \jplcons\log\evgen\jplegsM_cmd{1 2 3 4}.log	20 MB	5 MB
Correlation event generation stack trace log	<i>Console-path</i> \log\evgen\javalog0{1 2 3 4}.log	1 MB	At startup or 256 KB
	<i>shared-folder</i> \jplcons\log\evgen\javalog0{1 2 3 4}.log	1 MB	At startup or 256 KB
Correlation event generation process inheriting definition file	<i>Console-path</i> \log\evgen\egs_discrim_info{1 2 3 4}.dat	312 MB ^{#7}	At termination
	<i>shared-folder</i> \jplcons\log\evgen\egs_discrim_info{1 2 3 4}.dat	312 MB ^{#7}	At termination
Correlation event generation definition application log	<i>Console-path</i> \log\evgen\jplegsDefine{1 2}.log	10 MB	5 MB
	<i>shared-folder</i> \jplcons\log\evgen\jplegsDefine{1 2}.log	10 MB	5 MB

Log type	Default file name and folder name	Maximum disk usage	File-switching timing
Severity definition update log	<i>Console-path</i> \log\evflow\jplchsevDef{1 2}.log	100 MB	5 MB
	<i>shared-folder</i> \jplcons\log\evflow\jplchsevDef{1 2}.log	100 MB	5 MB
Command execution history folder	<i>Base-path</i> \log\COMMAND\ 	See the <i>Job Management Partner 1/Base User's Guide</i> .	
	<i>shared-folder</i> \jplbase\log\COMMAND\ 		
Remote command log	<i>Base-path</i> \log\JCOCMD\jco cmd_result{1 2 3}.log		
	<i>Base-path</i> \log\JCOCMD\jco cmdapi{1 2 3}.log		
	<i>Base-path</i> \log\JCOCMD\jco cmdapi_trace{1 2 3}.log		
	<i>Base-path</i> \log\JCOCMD\jco cmdcom{1 2 3}.log		
	<i>Base-path</i> \log\JCOCMD\jco cmdcom_trace{1 2 3}.log		
	<i>Base-path</i> \log\JCOCMD\jco cmdexe{1 2 3}.log		
	<i>Base-path</i> \log\JCOCMD\jco cmdexe_trace{1 2 3}.log		
	<i>Base-path</i> \log\JCOCMD\jco cmdrouter{1 2 3}.log		
	<i>Base-path</i> \log\JCOCMD\jco cmdrouter_trace{1 2 3}.log		
	<i>Base-path</i> \log\JCOCMD\JCOCMDCMD{1 2 3}.log		
	<i>shared-folder</i> \jplbase\log\JCOCMD\jco cmd_result{1 2 3}.log		
	<i>shared-folder</i> \jplbase\log\JCOCMD\jco cmdapi{1 2 3}.log		
	<i>shared-folder</i> \jplbase\log\JCOCMD\jco cmdapi_trace{1 2 3}.log		

Log type	Default file name and folder name	Maximum disk usage	File-switching timing
	<i>shared-folder\jplbase\log\JCOCMD\jcmdcom{1 2 3}.log</i>		
	<i>shared-folder\jplbase\log\JCOCMD\jcmdcom_trace{1 2 3}.log</i>		
	<i>shared-folder\jplbase\log\JCOCMD\jcmdexe{1 2 3}.log</i>		
	<i>shared-folder\jplbase\log\JCOCMD\jcmdexe_trace{1 2 3}.log</i>		
	<i>shared-folder\jplbase\log\JCOCMD\jcmdrouter{1 2 3}.log</i>		
	<i>shared-folder\jplbase\log\JCOCMD\jcmdrouter_trace{1 2 3}.log</i>		
	<i>shared-folder\jplbase\log\JCOCMD\JCOCMDCMD{1 2 3}.log</i>		
Configuration management log	<i>Base-path\log\route\JBSRT{1 2 3}.log</i>		
	<i>shared-folder\jplbase\log\route\JBSRT{1 2 3}.log</i>		
Integrated monitoring database application log	<i>Console-path\log\evflow\EVFLOW_DBAPI{1 2... 16}.log</i>	200 MB	12.5 MB
	<i>Console-path\log\console\EVCONS_DBAPI{1 2 3 4 5}.log</i>	50 MB	10 MB
	<i>Console-path\log\command\CMD_DBAPI{1 2 3 4 5}.log</i>	50 MB	10 MB
	<i>shared-folder\jplcons\log\evflow\EVFLOW_DBAPI{1 2... 16}.log</i>	200 MB	12.5 MB
	<i>shared-folder\jplcons\log\console\EVCONS_DBAPI{1 2 3 4 5}.log</i>	50 MB	10 MB
jcodbsetup command log	<i>Console-path\log\imdb\jcodbsetup{1 2}.log</i>	512 KB	256 KB
jcodbunsetup command log	<i>Console-path\log\imdb\jcodbunsetup{1 2}.log</i>	512 KB	256 KB

#1: The file size may be dozens of kilobytes larger than this value.

#2: You can set this value to be from 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.

$((\text{action information file size}/64 \text{ bytes}) - 1) \times 5 \text{ kilobytes}$

#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.

Table 9-4: 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
Process-by-process trace log	<i>Scope-path</i> \log\jcsmain{1 2 3}.log	6 MB	2 MB
	<i>Scope-path</i> \log\jcsmain_trace{1 2 3}.log	6 MB	2 MB
	<i>shared-folder</i> \JP1Scope\log\jcsmain{1 2 3}.log	6 MB	2 MB
	<i>shared-folder</i> \JP1Scope\log\jcsmain_trace{1 2 3}.log	6 MB	2 MB
Communication trace log	<i>Scope-path</i> \log\jcsmain_trace_com{1 2 3}.log	6 MB	2 MB
	<i>shared-folder</i> \JP1Scope\log\jcsmain_trace_com{1 2 3}.log	6 MB	2 MB

Log type	Default file name and folder name	Maximum disk usage	File-switching timing
	<i>Scope-path</i> \log\jcsmain_trace_ping{1 2 3}.log	6 MB	2 MB
	<i>shared-folder</i> \JP1Scope\log\jcsmain_trace_ping{1 2 3}.log	6 MB	2 MB
Logical host settings program log	<i>Scope-path</i> \log\jcp1hassetup.{log log.old}	2,000 KB	1,000 KB
Database operation API trace log	<i>Scope-path</i> \log\jcsmain_trace_db{1 2 3}.log	6 MB	2 MB
	<i>shared-folder</i> \JP1Scope\log\jcsmain_trace_db{1 2 3}.log	6 MB	2 MB
jcshostsexport command log	<i>Scope-path</i> \log\jcshostsexport{1 2 3}.log	6 MB	2 MB
	<i>shared-folder</i> \JP1Scope\log\jcshostsexport{1 2 3}.log	6 MB	2 MB
jcshostsimport command log	<i>Scope-path</i> \log\jcshostsimport{1 2 3}.log	6 MB	2 MB
	<i>shared-folder</i> \JP1Scope\log\jcshostsimport{1 2 3}.log	6 MB	2 MB
jcsdbsetup command log	<i>Scope-path</i> \log\jcsdbsetup{1 2 3}.log	6 MB	2 MB
	<i>shared-folder</i> \JP1Scope\log\jcsdbsetup{1 2 3}.log	6 MB	2 MB
jcschstat command log	<i>Scope-path</i> \log\jcschstat{1 2 3}.log	6 MB	2 MB
	<i>shared-folder</i> \JP1Scope\log\jcschstat{1 2 3}.log	6 MB	2 MB
jcsdbexport command log	<i>Scope-path</i> \log\jcsdbexport{1 2 3}.log	6 MB	2 MB
	<i>shared-folder</i> \JP1Scope\log\jcsdbexport{1 2 3}.log	6 MB	2 MB
jcsdbimport command log	<i>Scope-path</i> \log\jcsdimport{1 2 3}.log	6 MB	2 MB
	<i>shared-folder</i> \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
jcsdbconvert command log	<i>Scope-path</i> \log\jcsdbconvert{1 2 3}.log	6 MB	2 MB
	<i>shared-folder</i> \JP1Scope\log\jcsdbconvert{1 2 3}.log	6 MB	2 MB
jp1csverup command log	<i>Scope-path</i> \log\jp1csverup_front{1 2 3}.log	6 MB	2 MB
jp1cshaverup command log	<i>shared-folder</i> \JP1Scope\log\jp1cshaverup_front{1 2 3}.log	6 MB	2 MB

Table 9-5: 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
Process-by-process trace log	<i>Manager-path</i> \log\imcf\jcfmain{1 2 3}.log	3 MB	1 MB
	<i>Manager-path</i> \log\imcf\jcfmain_trace{1 2 3}.log	3 MB	1 MB
	<i>Manager-path</i> \log\imcf\jcfmain_VM_trace{1 2 3}.log	3 MB	1 MB
	<i>shared-folder</i> \JP1IMM\log\imcf\jcfmain{1 2 3}.log	3 MB	1 MB
	<i>shared-folder</i> \JP1IMM\log\imcf\jcfmain_trace{1 2 3}.log	3 MB	1 MB
	<i>shared-folder</i> \JP1IMM\log\imcf\jcfmain_VM_trace{1 2 3}.log	3 MB	1 MB
Communication trace log	<i>Manager-path</i> \log\imcf\jcfmain_trace_com{1 2 3}.log	3 MB	1 MB
	<i>Manager-path</i> \log\imcf\jcfmain_ping{1 2 3}.log	3 MB	1 MB
	<i>shared-folder</i> \JP1IMM\log\imcf\jcfmain_trace_com{1 2 3}.log	3 MB	1 MB
	<i>shared-folder</i> \JP1IMM\log\imcf\jcfmain_ping{1 2 3}.log	3 MB	1 MB
Logical host settings program log	<i>Manager-path</i> \log\imcf\jp1hassetup.{log log.old}	2,000 KB	1,000 KB

Log type	Default file name and folder name	Maximum disk usage	File-switching timing
Database operation API trace log	<i>Manager-path</i> \log\imcf\jcfmain_trace_db{1 2 3}.log	3 MB	1 MB
	<i>shared-folder</i> \JP1IMM\log\imcf\jcfmain_trace_db{1 2 3}.log	3 MB	1 MB
Command common log	<i>Manager-path</i> \log\imcf\jcfcommand{1 2 3}.log	3 MB	1 MB
	<i>shared-folder</i> \JP1IMM\log\imcf\jcfcommand{1 2 3}.log	3 MB	1 MB
jcfcolvmesx command log	<i>Manager-path</i> \log\imcf\jcfcolvmesx_trace{1 2 3}.log	3 MB	1 MB
jcfexport command log	<i>Manager-path</i> \log\imcf\jcfexport_VM_trace{1 2 3}.log	3 MB	1 MB
	<i>shared-folder</i> \JP1IMM\log\imcf\jcfexport_VM_trace{1 2 3}.log	3 MB	1 MB
jcfimport command log	<i>Manager-path</i> \log\imcf\jcfimport_VM_trace{1 2 3}.log	3 MB	1 MB
	<i>shared-folder</i> \JP1IMM\log\imcf\jcfimport_VM_trace{1 2 3}.log	3 MB	1 MB
jcfmkhostsdata command log	<i>Manager-path</i> \log\imcf\jcfmkhostsdata_trace{1 2 3}.log	3 MB	1 MB
Stack trace log	<i>Manager-path</i> \log\imcf\javalog{1 2 3 4}.log	1 MB	At startup or 256 KB

Table 9-6: 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	<i>View-path</i> \log\VIEW{1 2 3}.log	30,720 KB	10,240 KB
	<i>View-path</i> \log\jplconv{1 2 3 4}.log	1,000,000 KB	5,000 KB ^{#1}
	<i>View-path</i> \log\jplconvM{1 2... 20}.log	1,000,000 KB	5,000 KB ^{#1}
	<i>View-path</i> \log\jplcsov[_old].log	6,144 KB	3,072 KB ^{#1}
	<i>View-path</i> \log\jplcsovM[_old].log	6,144 KB	3,072 KB ^{#1}

Log type	Default file name and folder name	Maximum disk usage	File-switching timing
	<i>View-path</i> \log\imrm\jp1rmJP1-IM-RM View{1 2 3}.log ^{#2}	3,072 KB	1,024 KB
	<i>View-path</i> \log\imrm\jp1rmJP1-IM-RM View_dbg{1 2 3}.log ^{#2}	3,072 KB	1,024 KB
	<i>View-path</i> \log\jrmview\view{1 2 3}.log ^{#2}	3,072 KB	1,024 KB
Stack trace log	<i>View-path</i> \log\javalog0{1 2}.log	512 KB	At startup or 256 KB
Integrated trace log	system-drive:\Program Files\Hitachi\HNTRLib2\spool\hntr 2{1 2 3 4}.log	1,024 KB	256 KB
Product information log	<i>View-path</i> \log\hliclib\hliclibtrc{1 2 3 4 5}.log	5 MB	1 MB
	<i>View-path</i> \log\hliclib\hlicliberr{1 2 3 4 5}.log	5 MB	1 MB
	<i>View-path</i> \log\hliclib\hliclibmgrtrc{1 2 3 4 5}.log	5 MB	1 MB
	<i>View-path</i> \log\hliclib\hliclibmgrerr{1 2 3 4 5}.log	5 MB	1 MB

Note: In Windows Vista or Windows Server 2008, replace *View-path*\log\ with *system-drive*:\ProgramData\HITACHI\JP1\JP1_DEFAULT\JP1CoView\log\.

#1: The file size may be dozens of kilobytes larger than this value.

#2: This log is output only when JP1/IM - Rule Operation is linked.

Table 9-7: JP1/IM - IM Configuration Management - View log files and folders

Log type	Default file name and folder name	Maximum disk usage	File-switching timing
Process-by-process trace log	<i>Manager-path</i> \log\jcfview\VIEW{1 2 3}.log	30 MB	10 MB
Stack trace log	<i>Manager-path</i> \log\jcfjavalog{1 2}.log	512 KB	At startup or 256 KB
Integrated trace log	system-drive:\Program Files\Hitachi\HNTRLib2\spool\hntr 2{1 2 3 4}.log	1,024 KB	256 KB

Note: In Windows Vista or Windows Server 2008, replace *Manager-path\log* with *system-drive:\ProgramData\HITACHI\JP1\JP1_DEFAULT\JP1CoView\log*.

(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 9-8: 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	/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	/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

Log type	Default file name and folder name	Maximum disk usage	File-switching timing
JP1/IM startup log	/var/opt/jp1cons/log/ jco_start.log[.old]	1 KB	At startup
	<i>shared-directory</i> /jp1cons/log/ jco_start_logical-host-name.log[.old]	1 KB	At startup
JP1/IM kill log ^{#1}	<i>shared-directory</i> /jp1cons/log/ jco_killall.cluster{none 1 2 3 4}	2 KB	When the jco_killall. cluster command is executed
Installation log	/var/opt/jp1cons/log/JCO_SETUP/ jco_setup.log	100 KB	During installation
	/var/opt/jp1cons/log/JCO_SETUP/ jco_inst.log	100 KB	During installation
	/var/opt/jp1cons/log/jco_setup/ logical-host-name/jco_setup.log	100 KB	During installation
	/var/opt/jp1cons/log/jco_setup/ logical-host-name/reg.txt	100 KB	During installation
	/var/opt/jp1cons/log/jco_setup/ logical-host-name/reg_def.txt	100 KB	During installation
	/var/opt/jp1cons/log/command/ comdef[_old].log	512 KB	256 KB
Event console log	/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 ^{#2}
	/var/opt/jp1cons/log/console/ jp1consM{1 2... 20}.log	100 MB	5 MB ^{#2}
	/var/opt/jp1cons/log/console/ jp1filterDef{1 2}.log	10 MB	5 MB
	/var/opt/jp1cons/log/console/ evtcon_exe{1 2 3}.log	256 KB x 3	256 KB
	<i>shared-directory</i> /jp1cons/log/console/ EVCONS{1 2 3}.log	30,720 KB	10,240 KB
	<i>shared-directory</i> /jp1cons/log/console/ jp1cons{1 2 3 4}.log	20,480 KB	5,120 KB ^{#2}

Log type	Default file name and folder name	Maximum disk usage	File-switching timing
	<i>shared-directory/jplcons/log/console/jplconsM{1 2}.log</i>	100 MB	5 MB ^{#2}
	<i>shared-directory/jplcons/log/console/jplfilterDef{1 2}.log</i>	10 MB	5 MB
	<i>shared-directory/jplcons/log/console/evtcon_exe{1 2 3}.log</i>	256 KB x 3	256 KB
Automated action trace log	<i>/var/opt/jplcons/log/action/JCAMAIN{1 2 3 4 5}.log^{#3}</i>	25,600 KB	5,120 KB
	<i>shared-directory/jplcons/log/action/JCAMAIN{1 2 3 4 5}.log^{#3}</i>	25,600 KB	5,120 KB
Action information file	<i>/var/opt/jplcons/log/action/actinf.log</i>	626 KB ^{#4}	No switching
	<i>shared-directory/jplcons/log/action/actinf.log</i>	626 KB ^{#4}	No switching
Action host name file	<i>/var/opt/jplcons/log/action/acttxt{1 2}.log</i>	48.9 MB ^{#5}	When the action information file wraps around
	<i>shared-directory/jplcons/log/action/acttxt{1 2}.log</i>	48.9 MB ^{#5}	When the action information file wraps around
Action re-execution file	<i>/var/opt/jplcons/log/action/actreaction</i>	300 MB	When system switching occurs
	<i>shared-directory/jplcons/log/action/actreaction</i>	300 MB	When system switching occurs
jcochafmode, jcochstat, and jcoevtreport command trace logs ^{#6}	<i>/var/opt/jplcons/log/command/CMD{1 2 3}.log</i>	3,072 KB	1,024 KB
	<i>/var/opt/jplcons/log/command/jplcons_cmd{1 2}.log</i>	12,288 KB	6,144 KB
	<i>/var/opt/jplcons/log/command/jplconsM_cmd{1 2}.log</i>	12,288 KB	6,144 KB
Plug-in log	<i>/var/opt/jplcons/log/command/jcoplugin{1 2 3}.log</i>	3 MB	1 MB

Log type	Default file name and folder name	Maximum disk usage	File-switching timing
Reporting status storage file	/var/opt/jplcons/log/notice/notice_stat.dat	72B	No switching
	<i>shared-directory</i> /jplcons/log/notice/notice_stat.dat	72B	No switching
Action definition backup file	/var/opt/jplcons/log/action/actdefbk.conf	2,048 KB	No switching
	<i>shared-directory</i> /jplcons/log/action/actdefbk.conf	2,048 KB	No switching
Event base trace log	/var/opt/jplcons/log/evflow/EVFLOW{1 2 3 4 5 6 7 8 9 10}.log	100 MB	10 MB
	/var/opt/jplcons/log/evflow/jplevflowM{1 2... 20}.log	100 MB	5 MB
	/var/opt/jplcons/log/evflow/jplactDef{1 2}.log	10 MB	5 MB
	/var/opt/jplcons/log/evflow/jplchsevDef{1 2}.log	10 MB	5 MB
	/var/opt/jplcons/log/evflow/evflow_exe{1 2 3}.log	256 KB x 3	256 KB
	<i>shared-directory</i> /jplcons/log/evflow/EVFLOW{1 2 3 4 5 6 7 8 9 10}.log	100 MB	10 MB
	<i>shared-directory</i> /jplcons/log/evflow/jplevflowM{1 2... 20}.log	100 MB	5 MB
	<i>shared-directory</i> /jplcons/log/evflow/jplactDef{1 2}.log	10 MB	5 MB
	<i>shared-directory</i> /jplcons/log/evflow/jplchsevDef{1 2}.log	10 MB	5 MB
	<i>shared-directory</i> /jplcons/log/evflow/evflow_exe{1 2 3}.log	256 KB x 3	256 KB
	Matching information file	/var/opt/jplcons/log/evflow/evflowinf.log	12B
<i>shared-directory</i> /jplcons/log/evflow/evflowinf.log		12B	No switching
Event base error log	/var/opt/jplcons/log/evflow/jplevflow{1 2 3 4}.log	20,480 KB	5,120 KB

Log type	Default file name and folder name	Maximum disk usage	File-switching timing
	<i>shared-directory</i> /jplcons/log/evflow/jplevflow{1 2 3 4}.log	20,480 KB	5,120 KB
Automated action error log	/var/opt/jplcons/log/action/jplact{1 2 3}.log	15,360 KB	5,120 KB
	<i>shared-directory</i> /jplcons/log/action/jplact{1 2 3}.log	15,360 KB	5,120 KB
Correlation event generation history file	/var/opt/jplcons/operation/evgen/egs_discrim{1 2 3}.log ^{#8}	30 MB ^{#8}	10 MB ^{#8}
	<i>shared-directory</i> /jplcons/operation/evgen/egs_discrim{1 2 3}.log ^{#8}	30 MB ^{#8}	10 MB ^{#8}
Correlation event generation trace log	/var/opt/jplcons/log/evgen/EVGEN{1 2 3}.log	15 MB	5 MB
	/var/opt/jplcons/log/evgen/evgen_exe{1 2 3}.log	256 KB x 3	256 KB
	<i>shared-directory</i> /jplcons/log/evgen/EVGEN{1 2 3}.log	15 MB	5 MB
	<i>shared-directory</i> /jplcons/log/evgen/evgen_exe{1 2 3}.log	256 KB x 3	256 KB
Correlation event generation individual log (for Event Generation Service)	/var/opt/jplcons/log/evgen/jplegs{1 2}.log	20 MB	10 MB
	/var/opt/jplcons/log/evgen/jplegsM{1 2}.log	20 MB	10 MB
	<i>shared-directory</i> /jplcons/log/evgen/jplegs{1 2}.log	20 MB	10 MB
	<i>shared-directory</i> /jplcons/log/evgen/jplegsM{1 2}.log	20 MB	10 MB
Correlation event generation individual log (for commands)	/var/opt/jplcons/log/evgen/jplegs_cmd{1 2 3 4}.log	20 MB	5 MB
	/var/opt/jplcons/log/evgen/jplegsM_cmd{1 2 3 4}.log	20 MB	5 MB

9. Troubleshooting

Log type	Default file name and folder name	Maximum disk usage	File-switching timing
	<i>shared-directory</i> /jplcons/log/evgen/jplegs_cmd{1 2 3 4}.log	20 MB	5 MB
	<i>shared-directory</i> /jplcons/log/evgen/jplegsM_cmd{1 2 3 4}.log	20 MB	5 MB
Correlation event generation stack trace log ^{#7}	/var/opt/jplcons/log/evgen/javalog0{1 2 3 4}.log	1 MB	At startup or 256 KB
	<i>shared-directory</i> /jplcons/log/evgen/javalog0{1 2 3 4}.log	1 MB	At startup or 256 KB
Correlation event generation process inheriting definition file	/var/opt/jplcons/log/evgen/egs_discrim_info{1 2 3 4}.dat	312 MB ^{#9}	At termination
	<i>shared-directory</i> /jplcons/log/evgen/egs_discrim_info{1 2 3 4}.dat	312 MB ^{#9}	At termination
Correlation event generation definition application log	/var/opt/jplcons/log/evgen/jplegsDefine{1 2}.log	10 MB	5 MB
	<i>shared-directory</i> /jplcons/log/evgen/jplegsDefine{1 2}.log	10 MB	5 MB
Integrated monitoring database application log	/var/opt/jplcons/log/evflow/EVFLOW_DBAPI{1 2... 16}.log	200 MB	12.5 MB
	/var/opt/jplcons/log/console/EVCONS_DBAPI{1 2 3 4 5}.log	50 MB	10 MB
	/var/opt/jplcons/log/command/CMD_DBAPI{1 2 3 4 5}.log	50 MB	10 MB
	<i>shared-directory</i> /jplcons/log/evflow/EVFLOW_DBAPI{1 2... 16}.log	200 MB	12.5 MB
	<i>shared-directory</i> /jplcons/log/console/EVCONS_DBAPI{1 2 3 4 5}.log	50 MB	10 MB
jcodbsetup command log	/var/opt/jplcons/log/imdb/jcodbsetup{1 2}.log	512 KB	256 KB
jcodbunsetup command log	/var/opt/jplcons/log/imdb/jcodbunsetup{1 2}.log	512 KB	256 KB

Log type	Default file name and folder name	Maximum disk usage	File-switching timing
Command execution history directory	/var/opt/jp1base/log/COMMAND/	See the <i>Job Management Partner 1/Base User's Guide</i> .	
	<i>shared-directory</i> /jp1base/log/COMMAND		
Remote command log	/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		
	<i>shared-directory</i> /jp1base/log/JCOCMD/jcocmd_result{1 2 3}.log		
	<i>shared-directory</i> /jp1base/log/JCOCMD/jcocmdapi{1 2 3}.log		
	<i>shared-directory</i> /jp1base/log/JCOCMD/jcocmdapi_trace{1 2 3}.log		

Log type	Default file name and folder name	Maximum disk usage	File-switching timing
	<i>shared-directory</i> /jplbase/log/JCOCMD/jcocmdcmc{1 2 3}.log		
	<i>shared-directory</i> /jplbase/log/JCOCMD/jcocmdcmc_trace{1 2 3}.log		
	<i>shared-directory</i> /jplbase/log/JCOCMD/jcocmdcom{1 2 3}.log		
	<i>shared-directory</i> /jplbase/log/JCOCMD/jcocmdcom_trace{1 2 3}.log		
	<i>shared-directory</i> /jplbase/log/JCOCMD/jcocmdexe{1 2 3}.log		
	<i>shared-directory</i> /jplbase/log/JCOCMD/jcocmdexe_trace{1 2 3}.log		
	<i>shared-directory</i> /jplbase/log/JCOCMD/jcocmdrouter{1 2 3}.log		
	<i>shared-directory</i> /jplbase/log/JCOCMD/jcocmdrouter_trace{1 2 3}.log		
	<i>shared-directory</i> /jplbase/log/JCOCMD/JCOCMDCMD{1 2 3}.log		
Configuration management log	/var/opt/jplbase/log/route/JBSRT{1 2 3}.log		
	<i>shared-directory</i> /jplbase/log/route/JBSRT{1 2 3}.log		

#1: This log is created only in a cluster environment.

#2: The file size may be dozens of kilobytes larger than this value.

#3: 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*.

#4: 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*.

#5: This is the value when the size of the action information file is the default value (626 kilobytes). You can use the following estimation formula to estimate the maximum disk usage by this file. Each time an action is performed, the size increases

by 5 kilobytes.

$((\text{action information file size}/64 \text{ bytes}) - 1) \times 5 \text{ kilobytes}$

#6: The files are output to the `jcochstat` and `jcochafmode` command trace logs on the physical host in a cluster operation system as well.

#7: This log is not output in Solaris.

#8: 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*.

#9: This file is used to output the memory information for inheriting data during correlation event generation, and therefore its size varies depending on the correlation event generation condition and the correlation-source event. For details about estimating the size of this file, see the JP1/IM - Manager release notes.

Table 9-9: 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
Process-by-process trace log	<code>/var/opt/jp1scope/log/jcsmain{1 2 3}.log</code>	6 MB	2 MB
	<code>/var/opt/jp1scope/log/jcsmain_trace{1 2 3}.log</code>	6 MB	2 MB
	<code>shared-directory/jp1scope/log/jcsmain{1 2 3}.log</code>	6 MB	2 MB
	<code>shared-directory/jp1scope/log/jcsmain_trace{1 2 3}.log</code>	6 MB	2 MB
Communication trace log	<code>/var/opt/jp1scope/log/jcsmain_trace_com{1 2 3}.log</code>	6 MB	2 MB
	<code>shared-directory/jp1scope/log/jcsmain_trace_com{1 2 3}.log</code>	6 MB	2 MB
	<code>/var/opt/jp1scope/log/jcsmain_trace_ping{1 2 3}.log</code>	6 MB	2 MB
	<code>shared-directory/jp1scope/log/jcsmain_trace_ping{1 2 3}.log</code>	6 MB	2 MB
Database operation API trace log	<code>/var/opt/jp1scope/log/jcsmain_trace_db{1 2 3}.log</code>	6 MB	2 MB
	<code>shared-directory/jp1scope/log/jcsmain_trace_db{1 2 3}.log</code>	6 MB	2 MB

9. Troubleshooting

Log type	Default file name and folder name	Maximum disk usage	File-switching timing
jcshostsexport command log	/var/opt/jplscope/log/ jcshostsexport{1 2 3}.log	6 MB	2 MB
	<i>shared-directory</i> /jplscope/log/ jcshostsexport{1 2 3}.log	6 MB	2 MB
jcshostsimport command log	/var/opt/jplscope/log/ jcshostsimport{1 2 3}.log	6 MB	2 MB
	<i>shared-directory</i> /jplscope/log/ jcshostsimport{1 2 3}.log	6 MB	2 MB
jcldbsetup command log	/var/opt/jplscope/log/ jcldbsetup{1 2 3}.log	6 MB	2 MB
	<i>shared-directory</i> /jplscope/log/ jcldbsetup{1 2 3}.log	6 MB	2 MB
jcschstat command log	/var/opt/jplscope/log/ jcschstat{1 2 3}.log	6 MB	2 MB
	<i>shared-directory</i> /jplscope/log/ jcschstat{1 2 3}.log	6 MB	2 MB
jcldbimport command log	/var/opt/jplscope/log/ jcldbimport{1 2 3}.log	6 MB	2 MB
	<i>shared-directory</i> /jplscope/log/ jcldbimport{1 2 3}.log	6 MB	2 MB
jcldbexport command log	/var/opt/jplscope/log/ jcldbexport{1 2 3}.log	6 MB	2 MB
	<i>shared-directory</i> /jplscope/log/ jcldbexport{1 2 3}.log	6 MB	2 MB
Installation log	/var/opt/jplscope/log/JCS_SETUP/ jcs_setup.log	100 KB	During installation
	/var/opt/jplscope/log/jcs_setup/ <i>logical-host-name</i> /jcs_setup.log	100 KB	During installation
	/var/opt/jplscope/log/jcs_setup/ <i>logical-host-name</i> /reg.txt	100 KB	During installation
	/var/opt/jplscope/log/jcs_setup/ <i>logical-host-name</i> /reg_def.txt	100 KB	During installation

Table 9-10: 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
Process-by-process trace log	/var/opt/jplimm/log/imcf/jcfmain{1 2 3}.log	3 MB	1 MB
	/var/opt/jplimm/log/imcf/jcfmain_trace{1 2 3}.log	3 MB	1 MB
	/var/opt/jplimm/log/imcf/jcfmain_VM_trace{1 2 3}.log	3 MB	1 MB
	shared-directory/jplimm/log/imcf/jcfmain{1 2 3}.log	3 MB	1 MB
	shared-directory/jplimm/log/imcf/jcfmain_trace{1 2 3}.log	3 MB	1 MB
	shared-directory/jplimm/log/imcf/jcfmain_VM_trace{1 2 3}.log	3 MB	1 MB
Communication trace log	/var/opt/jplimm/log/imcf/jcfmain_trace_com{1 2 3}.log	3 MB	1 MB
	/var/opt/jplimm/log/imcf/jcfmain_ping{1 2 3}.log	3 MB	1 MB
	shared-directory/jplimm/log/imcf/jcfmain_trace_com{1 2 3}.log	3 MB	1 MB
	shared-directory/jplimm/log/imcf/jcfmain_ping{1 2 3}.log	3 MB	1 MB
Database operation API trace log	/var/opt/jplimm/log/imcf/jcfmain_trace_db{1 2 3}.log	3 MB	1 MB
	shared-directory/jplimm/log/imcf/jcfmain_trace_db{1 2 3}.log	3 MB	1 MB
Command common log	/var/opt/jplimm/log/imcf/\jcfcommand{1 2 3}.log	3 MB	1 MB
	shared-directory/jplimm/log/imcf/jcfcommand{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
jcfexport command log	/var/opt/jplimm/log/imcf/jcfexport_VM_trace{1 2 3}.log	3 MB	1 MB

9. Troubleshooting

Log type	Default file name and folder name	Maximum disk usage	File-switching timing
	<i>shared-directory</i> /jplimm/log/imcf/jcfexport_VM_trace{1 2 3}.log	3 MB	1 MB
jcfimport command log	/var/opt/jplimm/log/imcf/jcfimport_VM_trace{1 2 3}.log	3 MB	1 MB
	<i>shared-directory</i> /jplimm/log/imcf/jcfimport_VM_trace{1 2 3}.log	3 MB	1 MB
jcfmkhostsdata command log	/var/opt/jplimm/log/imcf/jcfmkhostsdata_trace{1 2 3}.log	3 MB	1 MB
Stack trace log	/var/opt/jplimm/log/imcf/javalog{1 2 3 4}.log	1 MB	At startup or 256 KB
Installation log	/var/opt/jplimm/log/imcf/JCF_SETUP/jcf_setup.log	100 KB	During installation
	/var/opt/jplimm/log/imcf/JCF_SETUP/ <i>logical-host-name</i> /jcf_setup.log	100 KB	During installation

9.3 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.

9.3.1 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 9-11: OS system information (Windows)

Information type	Collected data	File name#1	View
Data collection date/time	<ul style="list-style-type: none"> date /t execution result time /t execution result 	date.log	Y
Hitachi integrated installer log file	Files under <i>Windows-installation-folder</i> \Temp\HCDINST\	Copies of the files indicated at left	Y
JP1/IM - Manager installation/uninstallation log file	<i>Windows-installation-folder</i> \Temp\HITACHI_JP1_INST_LOG\jplimm_inst{1 2 3 4 5}.log	jplimm_inst{1 2 3 4 5}.log	Δ
JP1/IM - View installation/uninstallation log file	<i>Windows-installation-folder</i> \Temp\HITACHI_JP1_INST_LOG\jplcoview_inst{1 2 3 4 5}.log	jplcoview_inst{1 2 3 4 5}.log	Y
JP1/Base installation/uninstallation log file	<i>Windows-installation-folder</i> \Temp\HITACHI_JP1_INST_LOG\jplbase_inst{1 2 3 4 5}.log	jplbase_inst{1 2 3 4 5}.log	Δ
Product information log file	Files under <i>Windows-installation-folder</i> \Temp\jplcommon\	Copies of the files indicated at left	Y

9. Troubleshooting

Information type	Collected data	File name#1	View
Host name settings that are set in the machine	<i>system-root-folder</i> \system32\drivers\etc\hosts	hosts	Y
Service port settings that are set in the machine	<i>system-root-folder</i> \system32\drivers\etc\services	services	Y
NIC installation status	ipconfig /all execution result	ipconfig.log	Y
Startup service list	net start execution result	netstart.log	Y
Network statistical information	netstat -na execution result	netstat.log	Y
Machine's environment variable	set execution result	set.log	Y
Machine's system information	msinfo32 /report-file-name execution result	msinfo32.log	Y
Registry information	Content of the registry HKEY_LOCAL_MACHINE\SOFTWARE\HITACHI or HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\HITACHI collected by the regedit command	hitachi_reg.txt	Y
Product information file	Files under <i>system-drive</i> :Program Files\jplcommon\	Copies of the files indicated at left	Y
JP1/IM - Manager installation information	<i>system-drive</i> :Program Files\InstallShield Installation Information\{BB5D25EC-537C-4794-BD7A-C7E22CC4AD30}\setup.ini	imm_setup.ini	▲
JP1/IM - Manager installation log file	<i>system-drive</i> :Program Files\InstallShield Installation Information\{BB5D25EC-537C-4794-BD7A-C7E22CC4AD30}\setup.ilg	imm_setup.ilg	▲

Information type	Collected data	File name ^{#1}	View
JP1/Base installation information	<i>system-drive</i> :Program Files\InstallShield Installation Information\{F8C71F7C-E5DE-11D3-A21E-006097C00EBC}\setup.ini	base_setup.ini	△
JP1/Base installation log file	<i>system-drive</i> :Program Files\InstallShield Installation Information\{F8C71F7C-E5DE-11D3-A21E-006097C00EBC}\setup.ilg	base_setup.ilg	△
JP1/IM - View installation information	<i>system-drive</i> :Program Files\InstallShield Installation Information\{6C01AA81-B45B-4AA6-ACE9-AC9A86B19F1F}\setup.ini	imv_setup.ini	Y
JP1/IM - View installation log file	<i>system-drive</i> :Program Files\InstallShield Installation Information\{6C01AA81-B45B-4AA6-ACE9-AC9A86B19F1F}\setup.ilg	imv_setup.ilg	Y
JP1/Base access permission information (installation folder)	cacls <i>Base-path</i> execution result	cacls_jp1base.log	△
	cacls <i>shared-folder</i> \JP1Base execution result ^{#2}	cacls_jp1base.log	--
JP1/Base access permission information (log folder)	cacls <i>Base-path</i> \log execution result	cacls_jp1base_log.log	△
	cacls <i>shared-folder</i> \JP1Base\log execution result ^{#2}	cacls_jp1base_log.log	--
JP1/Base access permission information (command execution history folder)	cacls <i>Base-path</i> \log\COMMAND execution result	cacls_jp1base_log_COMMAND.log	△

Information type	Collected data	File name ^{#1}	View
	cacls <i>shared-folder</i> \JP1Base\log\COMMAND execution result ^{#2}	cacls_jp1base_log_COMMAND.log	--
JP1/Base access permission information (event database folder)	cacls <i>Base-path</i> \sys execution result	cacls_jp1base_sys.log	▲
JP1/Base access permission information (event database folder)	cacls <i>Base-path</i> \sys\event execution result	cacls_jp1base_sys_event.log	▲
	cacls <i>shared-folder</i> \JP1Base\event execution result ^{#2}	cacls_jp1base_event.log	--
JP1/Base access permission information (event database folder)	cacls <i>Base-path</i> \sys\event\servers execution result	cacls_jp1base_sys_event_servers.log	▲
JP1/Base access permission information (event database folder)	cacls <i>Base-path</i> \sys\event\servers\default execution result	cacls_jp1base_sys_event_servers_default.log	▲
JP1/IM - Manager (JP1/IM - Central Console) access permission information (installation folder)	cacls <i>Console-path</i> execution result	cacls_jp1cons.log	▲
	cacls <i>shared-folder</i> \JP1Cons execution result ^{#2}	cacls_jp1cons.log	--
JP1/IM - Manager (JP1/IM - Central Console) access permission information (log folder)	cacls <i>Console-path</i> \log execution result	cacls_jp1cons_log.log	▲
	cacls <i>shared-folder</i> \JP1Cons\log execution result ^{#2}	cacls_jp1cons_log.log	--

Information type	Collected data	File name ^{#1}	View
JP1/IM - Manager (JP1/IM - Central Console) access permission information (correlation history folder)	cacls <i>Console-path</i> \operation execution result	cacls_jp1cons_operation.log	Δ
	cacls <i>shared-folder</i> \JP1Cons\operation execution result ^{#2}	cacls_jp1cons_operation.log	--
JP1/IM - Manager (JP1/IM - Central Console) access permission information (correlation event generation history folder)	cacls <i>Console-path</i> \operation\evgen execution result	cacls_jp1cons_operation_evgen.log	Δ
	cacls <i>shared-folder</i> \JP1Cons\operation\evgen execution result ^{#2}	cacls_jp1cons_operation_evgen.log	--
JP1/IM - View access permission information (installation folder)	cacls <i>View-path</i> execution result	cacls_jp1coview.log	Y
JP1/IM - View access permission information (log folder)	When the OS is not Windows Vista or Windows Server 2008: cacls <i>View-path</i> \log execution result	cacls_jp1coview_log.log	Y
	When the OS is Windows Vista or Windows Server 2008: cacls <i>system-drive</i> : \ProgramData\HITACHI\JP1\JP1_DEFAULT\JP1CoView\log execution result	cacls_programdata_jp1coview_log.log	Y
JP1/IM - Manager access permission information (installation folder)	cacls <i>Manager-path</i> execution result	cacls_jp1imm.log	Δ

9. Troubleshooting

Information type	Collected data	File name ^{#1}	View
JP1/IM - Manager access permission information (log folder)	cacls <i>Manager-path</i> \log execution result	cacls_jp1imm_log.log	▲
JP1/IM - Manager (JP1/IM - Central Scope) access permission information (installation folder)	cacls <i>Scope-path</i> execution result	cacls_jp1scope.log	▲
	cacls <i>shared-folder</i> \JP1Scope execution result ^{#2}	cacls_jp1scope.log	--
JP1/IM - Manager (JP1/IM - Central Scope) access permission information (log folder)	cacls <i>Scope-path</i> \log execution result	cacls_jp1scope_log.log	▲
	cacls <i>shared-folder</i> \JP1Scope\log execution result ^{#2}	cacls_jp1scope_log.log	--
JP1/IM - Manager (JP1/IM - Central Scope) access permission information (database folder)	cacls <i>Scope-path</i> \database execution result	cacls_jp1scope_database.log	▲
	cacls <i>shared-folder</i> \JP1Scope\database execution result ^{#2}	cacls_jp1scope_database.log	--
JP1/IM - Manager (JP1/IM - Central Scope) access permission information (database folder)	cacls <i>Scope-path</i> \database\event execution result	cacls_jp1scope_database_event.log	▲
	cacls <i>shared-folder</i> \JP1Scope\database\event execution result ^{#2}	cacls_jp1scope_database_event.log	--

Information type	Collected data	File name#1	View
JP1/IM - Manager (JP1/IM - Central Scope) access permission information (database folder)	cacls <i>Scope-path</i> \database\jcsdb execution result	cacls_jp1scope_database_jcsdb. log	▲
	cacls <i>shared-folder</i> \JP1Scope\datab ase\jcsdb execution result#2	cacls_jp1scope_database_jcsdb. log	--
JP1/IM - Manager (JP1/IM - Central Scope) access permission information (database folder)	cacls <i>Scope-path</i> \database\jcsdb\ev ent execution result	cacls_jp1scope_database_jcsdb_ event.log	▲
	cacls <i>shared-folder</i> \JP1Scope\datab ase\jcsdb\event execution result#2	cacls_jp1scope_database_jcsdb_ event.log	--
JP1/IM - Manager (JP1/IM - Central Scope) access permission information (database folder)	cacls <i>Scope-path</i> \database\jcsdb\p w execution result	cacls_jp1scope_database_jcsdb_ pw.log	▲
	cacls <i>shared-folder</i> \JP1Scope\datab ase\jcsdb\pw execution result#2	cacls_jp1scope_database_jcsdb_ pw.log	--
JP1/IM - Manager (JP1/IM - Central Scope) access permission information (database folder)	cacls <i>Scope-path</i> \database\jcsdb\t ree execution result	cacls_jp1scope_database_jcsdb_ tree.log	▲
	cacls <i>shared-folder</i> \JP1Scope\datab ase\jcsdb\tree execution result#2	cacls_jp1scope_database_jcsdb_ tree.log	--

9. Troubleshooting

Information type	Collected data	File name#1	View
JP1/IM - Manager (JP1/IM - Central Scope) access permission information (database folder)	cacls <i>Scope-path</i> \database\jcshosts execution result	cacls_jp1scope_database_jcshosts.log	▲
	cacls <i>shared-folder</i> \JP1Scope\database\jcshosts execution result#2	cacls_jp1scope_database_jcshosts.log	--
JP1/Base file list	dir <i>Base-path</i> /s execution result	dir_jplbase.log	▲
	dir <i>shared-folder</i> \JP1Base /s execution result#2	dir_logical-host-name_jplbase.log	--
JP1/IM - Manager (JP1/IM - Central Console) file list	dir <i>Console-path</i> /s execution result	dir_jplcons.log	▲
	dir <i>shared-folder</i> \JP1Cons /s execution result#2	dir_logical-host-name_jplcons.log	--
JP1/IM - View file list	dir <i>View-path</i> /s execution result	dir_jplcoview.log	Y
	Windows Vista and Windows Server 2008 only: dir <i>system-drive</i> : \ProgramData\HITACHI\JP1\JP1_DEFAULT\JP1CoView /s execution result	dir_programdata_jplcoview.log	Y
JP1/IM - Manager file list	dir <i>Manager-path</i> /s execution result	dir_jplimm.log	▲
JP1/IM - Manager (JP1/IM - Central Scope) file list	dir <i>Scope-path</i> /s execution result	dir_jp1scope.log	▲
	dir <i>shared-folder</i> \JP1Scope /s execution result#2	dir_logical-host-name_jp1scope.log	--
Host name for resolving network address	jbsgethostbyname execution result	<ul style="list-style-type: none"> jbsgethostbyname.log (standard output) jbsgethostbyname_err.log (standard error) 	▲

Information type	Collected data	File name ^{#1}	View
	<code>jbsgethostbyname</code> <i>logical-host-name</i> execution result ^{#2}	<ul style="list-style-type: none"> <code>jbsgethostbyname.log</code> (standard output) <code>jbsgethostbyname_err.log</code> (standard error) 	--
Health check	<code>jbshcstatus -debug -a</code> execution result	<ul style="list-style-type: none"> <code>jbshcstatus.log</code> (standard output) <code>jbshcstatus_err.log</code> (standard error) 	▲
	<code>jbshcstatus -debug -a -h</code> <i>logical-host-name</i> execution result ^{#2}	<ul style="list-style-type: none"> <code>jbshcstatus.log</code> (standard output) <code>jbshcstatus_err.log</code> (standard error) 	--
Process operation status of Event Service	<code>jevstat</code> execution result	<ul style="list-style-type: none"> <code>jevstat.log</code> (standard output) <code>jevstat_err.log</code> (standard error) 	▲
Process operation status of items other than Event Service	<code>jbs_spm�_status</code> execution result	<ul style="list-style-type: none"> <code>jbs_spm�_status.log</code> (standard output) <code>jbs_spm�_status_err.log</code> (standard error) 	▲
	<code>jbs_spm�_status -h</code> <i>logical-host-name</i> execution result ^{#2}	<ul style="list-style-type: none"> <code>jbs_spm�_status.log</code> (standard output) <code>jbs_spm�_status_err.log</code> (standard error) 	--
Automated action execution result	<code>jcashowa</code> execution result	<ul style="list-style-type: none"> <code>jcashowa.log</code> (standard output) <code>jcashowa_err.log</code> (standard error) 	▲
	<code>jcashowa -h</code> <i>logical-host-name</i> execution result ^{#2}	<ul style="list-style-type: none"> <code>jcashowa.log</code> (standard output) <code>jcashowa_err.log</code> (standard error) 	--
Automated action status	<code>jcastatus</code> execution result	<ul style="list-style-type: none"> <code>jcastatus.log</code> (standard output) <code>jcastatus_err.log</code> (standard error) 	▲
	<code>jcastatus -h</code> <i>logical-host-name</i> execution result ^{#2}	<ul style="list-style-type: none"> <code>jcastatus.log</code> (standard output) <code>jcastatus_err.log</code> (standard error) 	--
Automated action definition file content	<code>jcastatus -d</code> execution result	<ul style="list-style-type: none"> <code>jcastatus_d.log</code> (standard output) <code>jcastatus_d_err.log</code> (standard error) 	▲

Information type	Collected data	File name ^{#1}	View
	<code>jcastatus -d -h</code> <i>logical-host-name</i> execution result ^{#2}	<ul style="list-style-type: none"> <code>jcastatus_d.log</code> (standard output) <code>jcastatus_d_err.log</code> (standard error) 	--
Event Generation Service status	<code>jcoegsstatus</code> execution result	<ul style="list-style-type: none"> <code>jcoegsstatus.log</code> (standard output) <code>jcoegsstatus_err.log</code> (standard error) 	Δ
	<code>jcoegsstatus -h</code> <i>logical-host-name</i> execution result ^{#2}	<ul style="list-style-type: none"> <code>jcoegsstatus.log</code> (standard output) <code>jcoegsstatus_err.log</code> (standard error) 	--
Process operation status	<code>jco_spm�_status</code> execution result	<ul style="list-style-type: none"> <code>jco_spm�_status.log</code> (standard output) <code>jco_spm�_status_err.log</code> (standard error) 	Δ
	<code>jco_spm�_status -h</code> <i>logical-host-name</i> execution result ^{#2}	<ul style="list-style-type: none"> <code>jco_spm�_status.log</code> (standard output) <code>jco_spm�_status_err.log</code> (standard error) 	--
Data collection command execution result	<code>jim_log.bat</code> command execution result	<code>jim_log_result.log</code>	Y
Windows event log	<ul style="list-style-type: none"> Application: <i>system-root-folder</i>\system32\config\AppEvent.Evt System: <i>system-root-folder</i>\system32\config\SysEvent.Evt 	<ul style="list-style-type: none"> <code>AppEvent (Backup).evt</code> <code>AppEvent (Backup).txt</code> <code>SysEvent (Backup).evt</code> <code>SysEvent (Backup).txt</code> 	Y
Crash dump ^{#3}	<i>user-specified-folder</i> \user.dmp	<code>user.dmp</code>	Y ^{#4}
Watson (Dr. Watson) log ^{#3}	<i>user-specified-folder</i> \drwtsn32.log	<code>drwtsn32.log</code>	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 *1.18.2(1) Preparations for collecting data in the event of a failure* in the *Job Management Partner 1/Integrated Management - Manager Configuration Guide*.)

#4: A crash dump is not collected in the Windows Vista or Windows Server 2008 version of JP1/IM - View or JP1/IM - Manager.

(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 9-12: JP1 information (Windows)

Information type		Collected data	File name ^{#1}	View
Common to JP1/IM and JP1/Base	Integrated trace log	<i>system-drive</i> :Program Files\Hitachi\HNTRLib2\spool	The following files in the default mode: hntr2 [1 2 3 4] .log	Y
JP1/IM - Manager (common to components)	Patch information	<i>Manager-path</i> \PATCHLOG.TXT	Patchlog_jp1imm.txt	--
	Settings and definition file	Files under <i>Manager-path</i> \conf\	Copies of the files indicated at left	--
	Log file	Files under <i>Manager-path</i> \log\	Copies of the files indicated at left	--

9. Troubleshooting

Information type		Collected data	File name#1	View
JP1/IM - Manager (JP1/IM - Central Console)	Settings and definition file	Files under <i>Console-path</i> \conf\	Copies of the files indicated at left	--
		Files under <i>shared-folder</i> \JP1Cons\conf\#2	Copies of the files indicated at left	--
	Common definition information	Files under <i>Console-path</i> \default\	Copies of the files indicated at left	--
	Log file	Files under <i>Console-path</i> \log\	Copies of the files indicated at left	--
		Files under <i>shared-folder</i> \JP1Cons\log\#2	Copies of the files indicated at left	--
	Correlation event generation history file	Files under <i>Console-path</i> \operation\evgen\	Copies of the files indicated at left	--
		Files under <i>shared-folder</i> \JP1Cons\operation\evgen\#2	Copies of the files indicated at left	--
	JP1/IM - Manager (JP1/IM - Central Scope)	Settings and definition file	Files under <i>Scope-path</i> \conf\	Copies of the files indicated at left
Files under <i>shared-folder</i> \JP1Scope\conf\#2			Copies of the files indicated at left	--
Common definition information		Files under <i>Scope-path</i> \default\	Copies of the files indicated at left	--
Log file		Files under <i>Scope-path</i> \log\	Copies of the files indicated at left	--
		Files under <i>shared-folder</i> \JP1Scope\log\#2	Copies of the files indicated at left	--
Database information		Files under <i>Scope-path</i> \database\	Copies of the files indicated at left	--
		Files under <i>shared-folder</i> \JP1Scope\database\#2	Copies of the files indicated at left	--

Information type		Collected data	File name#1	View
JP1/IM - Manager (IM Configuration Management)	Settings and definition file	Files under <i>Manager-path</i> \conf\imcf\	Copies of the files indicated at left	--
		Files under <i>shared-folder</i> \jp1imm\conf\imcf\#2	Copies of the files indicated at left	--
	Common definition information	Files under <i>Manager-path</i> \system\default\new\imcf\	Copies of the files indicated at left	--
	Log file	Files under <i>Manager-path</i> \log\imcf\	Copies of the files indicated at left	--
		Files under <i>shared-folder</i> \jp1imm\log\imcf\#2	Copies of the files indicated at left	--
JP1/IM - View	Patch information	<i>View-path</i> \Patchlog.txt	Patchlog_jp1coview.txt	Y
	Settings and definition file	Files under <i>View-path</i> \conf\	Copies of the files indicated at left	Y
		Windows Vista and Windows Server 2008 only: Files under <i>system-drive</i> :\ProgramData\HITACHI\JP1\JP1_DEFAULT\JP1Coview\conf\	Copies of the files indicated at left	Y
	Common definition information	Files under <i>View-path</i> \default\	Copies of the files indicated at left	Y
	Log file	For OSs other than Windows Vista and Windows Server 2008: Files under <i>View-path</i> \log\	Copies of the files indicated at left	Y
		For Windows Vista and Windows Server 2008: Files under <i>system-drive</i> :\ProgramData\HITACHI\JP1\JP1_DEFAULT\JP1Coview\log\	Copies of the files indicated at left	Y
JP1/Base	Patch information	<i>Base-path</i> \PatchLog.txt	Patchlog_jp1base.txt	--

Information type		Collected data	File name#1	View
	Settings and definition file	Files under <i>Base-path</i> \conf\	Copies of the files indicated at left	--
		Files under <i>shared-folder</i> \JP1Base\conf\#2	Copies of the files indicated at left	--
	Common definition information	Files under <i>Base-path</i> \default\	Copies of the files indicated at left	--
	Log file	Files under <i>Base-path</i> \log\	All files under the folder indicated at left, excluding COMMAND	--
		Files under <i>shared-folder</i> \JP1Base\log\#2	All files under the folder indicated at left, excluding COMMAND	--
	Plug-in service settings file	Files under <i>Base-path</i> \plugin\conf\	Copies of the files indicated at left	--
	Log and temporary file	Files under <i>Base-path</i> \sys\tmp\	Copies of the files indicated at left	--
		<i>shared-folder</i> \JP1Base\event#2	All files under the folder indicated at left, excluding IMEvent*.*	--
	Command execution log file	Files under <i>Base-path</i> \log\COMMAND\	Copies of the files indicated at left	--
		Files under <i>shared-folder</i> \JP1Base\log\COMMAND\#2	Copies of the files indicated at left	--
	Event database	Files under <i>Base-path</i> \sys\event\servers\default\	Copies of the files indicated at left	--
		<i>shared-folder</i> \JP1Base\event#2	IMEvent*.*	--

Legend:

Y: Collected by the jcoview_log.bat command.

--: Not collected by the jcoview_log.bat command.

#1: Indicates the storage destination file name after a data collection tool is used. For details about the storage destination, see the following sections:

- *jim_log.bat (Windows only) (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) 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 *4.14.4 Specifying display settings for the Java Console window* in the *Job Management Partner 1/Integrated Management - Manager Configuration Guide*.

- Java trace file of Java™ Plug-in

The Java trace file is located in the following directory:

Java™ Plug-in 1.4.2:

system-drive:\Documents and
Settings*login-user-name*\Application
Data\Sun\Java\Deployment\log\

Manager side

- HTTP server error log
- HTTP server access log

(6) User dump (Windows Vista and Windows Server 2008 only)

If an application error causes a JP1/IM - View process to stop in Windows Vista or Windows Server 2008, collect a user dump.

(7) Problem report (Windows Vista and Windows Server 2008 only)

If an application error causes a JP1/IM - View process to stop in Windows Vista or Windows Server 2008, collect a problem report.

9.3.2 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 9-13: OS system information (UNIX)

Information type	Collected data	File name#1
Installed Hitachi product information	/etc/.hitachi/pplistd/ pplistd	<ul style="list-style-type: none"> • jp1_default_imm_1st.tar.{Z gz} • pplistd
Hitachi PP Installer installation log file	/etc/.hitachi/.install.log*	<ul style="list-style-type: none"> • jp1_default_imm_1st.tar.{Z gz} • .install.log*
Hitachi PP Installer uninstallation log file	/etc/.hitachi/ .uninstall.log*	<ul style="list-style-type: none"> • jp1_default_imm_1st.tar.{Z gz} • .uninstall.log*
Common definition information	Files under /opt/jp1/hcclibcnf/	<ul style="list-style-type: none"> • jp1_default_imm_1st.tar.{Z gz} • Copies of the files indicated at left
JP1/IM - Manager (JP1/IM - Central Console) core analysis information (back trace)	Analysis result from seraph /var/opt/jp1cons	<ul style="list-style-type: none"> • jp1_default_imm_1st.tar.{Z gz} • core_module-name.log
	Analysis result from seraph shared-directory/jp1cons/log#2	<ul style="list-style-type: none"> • logical-host-name_imm_1st.tar.{Z gz} • core_module-name.log

Information type	Collected data	File name#1
JP1/IM - Manager (JP1/IM - Central Scope) core analysis information (back trace)	Analysis result from seraph /var/opt/jp1scope	<ul style="list-style-type: none"> • jp1_default_imm_1st.tar.{Z gz} • core_module-name.log
	Analysis result from seraph shared-directory/jp1scope/log#2	<ul style="list-style-type: none"> • logical-host-name_imm_1st.tar.{Z gz} • core_module-name.log
JP1/Base installation log file	/tmp/HITACHI_JP1_INST_LOG/ jp1base_inst{1 2 3 4 5}.log	<ul style="list-style-type: none"> • jp1_default_imm_1st.tar.{Z gz} • jp1base_inst{1 2 3 4 5}.log
JP1/IM - Manager installation log file	/tmp/HITACHI_JP1_INST_LOG/ jp1imm_inst{1 2 3 4 5}.log	<ul style="list-style-type: none"> • jp1_default_imm_1st.tar.{Z gz} • jp1imm_inst{1 2 3 4 5}.log
File list	<ul style="list-style-type: none"> • ls -lRa /opt/jp1imm execution result • ls -lRa /var/opt/jp1imm execution result • ls -lRa /opt/jp1cons execution result • ls -lRa /etc/opt/jp1cons execution result • ls -lRa /var/opt/jp1cons execution result • ls -lRa /opt/jp1scope execution result • ls -lRa /etc/opt/jp1scope execution result • ls -lRa /var/opt/jp1scope execution result • ls -lRa /opt/jp1base execution result • ls -lRa /etc/opt/jp1base execution result • ls -lRa /var/opt/jp1base execution result 	<ul style="list-style-type: none"> • jp1_default_imm_1st.tar.{Z gz} • inst_dir.log
	<ul style="list-style-type: none"> • 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 	<ul style="list-style-type: none"> • logical-host-name_imm_1st.tar.{Z gz} • share_dir.log

9. Troubleshooting

Information type	Collected data	File name#1
Data collection date/ time	date execution result	<ul style="list-style-type: none"> • jp1_default_imm_1st.tar.{Z gz} • jp1_default_imm_2nd.tar.{Z gz} • <i>logical-host-name</i>_imm_1st.tar.{Z gz} • <i>logical-host-name</i>_imm_2nd.tar.{Z gz} • date.log
Disk information	df -k execution result	<ul style="list-style-type: none"> • jp1_default_imm_1st.tar.{Z gz} • df.log
Machine's environment variable	env execution result	<ul style="list-style-type: none"> • jp1_default_imm_1st.tar.{Z gz} • env.log
Host name settings that are set in the machine	<ul style="list-style-type: none"> • /etc/inet/hosts (Solaris) • /etc/hosts (AIX) 	<ul style="list-style-type: none"> • jp1_default_imm_1st.tar.{Z gz} • hosts
Status of shared memory for inter-process communication	ipcs -ma execution result	<ul style="list-style-type: none"> • jp1_default_imm_1st.tar.{Z gz} • ipcs.log
Host name for resolving network address	jbsgethostbyname execution result	<ul style="list-style-type: none"> • jp1_default_imm_1st.tar.{Z gz} • jbsgethostbyname.log (standard output) • jbsgethostbyname_err.log (standard error)
	jbsgethostbyname <i>logical-host-name</i> execution result#2	<ul style="list-style-type: none"> • <i>logical-host-name</i>_imm_1st.tar.{Z gz} • jbsgethostbyname_<i>logical-host-name</i>.log
Health check	jbshcstatus -debug -a execution result	<ul style="list-style-type: none"> • jp1_default_imm_1st.tar.{Z gz} • jbshcstatus.log (standard output) • jbshcstatus_err.log (standard error)
	jbshcstatus -debug -a -h <i>logical-host-name</i> execution result#2	<ul style="list-style-type: none"> • <i>logical-host-name</i>_imm_1st.tar.{Z gz} • jbshcstatus.log (standard output) • jbshcstatus_err.log (standard error)
Process operation status of Event Service	jevstat execution result	<ul style="list-style-type: none"> • 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_spm�_status execution result	<ul style="list-style-type: none"> • jp1_default_imm_1st.tar.{Z gz} • jbs_spm�_status.log (standard output) • jbs_spm�_status_err.log (standard error)

Information type	Collected data	File name#1
	<code>jbs_spm�_status -h</code> <i>logical-host-name</i> execution result#2	<ul style="list-style-type: none"> • <i>logical-host-name_imm_1st.tar</i>.{Z gz} • <i>jbs_spm�_status.log</i> (standard output) • <i>jbs_spm�_status_err.log</i> (standard error)
Automated action execution result	<code>jcashowa</code> execution result	<ul style="list-style-type: none"> • <i>jp1_default_imm_1st.tar</i>.{Z gz} • <i>jcashowa.log</i> (standard output) • <i>jcashowa_err.log</i> (standard error)
	<code>jcashowa -h</code> <i>logical-host-name</i> execution result#2	<ul style="list-style-type: none"> • <i>logical-host-name_imm_1st.tar</i>.{Z gz} • <i>jcashowa.log</i> (standard output) • <i>jcashowa_err.log</i> (standard error)
Automated action function status	<code>jcastatus</code> execution result	<ul style="list-style-type: none"> • <i>jp1_default_imm_1st.tar</i>.{Z gz} • <i>jcastatus.log</i> (standard output) • <i>jcastatus_err.log</i> (standard error)
	<code>jcastatus -h</code> <i>logical-host-name</i> execution result#2	<ul style="list-style-type: none"> • <i>logical-host-name_imm_1st.tar</i>.{Z gz} • <i>jcastatus.log</i> (standard output) • <i>jcastatus_err.log</i> (standard error)
Automated action definition file content	<code>jcastatus -d</code> execution result	<ul style="list-style-type: none"> • <i>jp1_default_imm_1st.tar</i>.{Z gz} • <i>jcastatus_d.log</i> (standard output) • <i>jcastatus_d_err.log</i> (standard error)
	<code>jcastatus -d -h</code> <i>logical-host-name</i> execution result#2	<ul style="list-style-type: none"> • <i>logical-host-name_imm_1st.tar</i>.{Z gz} • <i>jcastatus_d.log</i> (standard output) • <i>jcastatus_d_err.log</i> (standard error)
Event Generation Service status	<code>jcoegsstatus</code> execution result	<ul style="list-style-type: none"> • <i>jp1_default_imm_1st.tar</i>.{Z gz} • <i>jcoegsstatus.log</i> (standard output) • <i>jcoegsstatus_err.log</i> (standard error)
	<code>jcoegsstatus -h</code> <i>logical-host-name</i> execution result#2	<ul style="list-style-type: none"> • <i>logical-host-name_imm_1st.tar</i>.{Z gz} • <i>jcoegsstatus.log</i> (standard output) • <i>jcoegsstatus_err.log</i> (standard error)
Process operation status	<code>jco_spm�_status</code> execution result	<ul style="list-style-type: none"> • <i>jp1_default_imm_1st.tar</i>.{Z gz} • <i>jco_spm�_status.log</i> (standard output) • <i>jco_spm�_status_err.log</i> (standard error)

9. Troubleshooting

Information type	Collected data	File name#1
	<code>jco_spm�_status -h</code> <i>logical-host-name</i> execution result#2	<ul style="list-style-type: none"> • <i>logical-host-name_imm_1st.tar.Z gz</i> • <code>jco_spm�_status.log</code> (standard output) • <code>jco_spm�_status_err.log</code> (standard error)
Data collection command execution result	<code>jim_log.sh</code> command execution result	<ul style="list-style-type: none"> • <code>jp1_default_imm_1st.tar.{Z gz}</code> • <code>jim_log_result.log</code>
NIC installation status	<code>netstat -i</code> execution result	<ul style="list-style-type: none"> • <code>jp1_default_imm_1st.tar.{Z gz}</code> • <code>netstat_i.log</code>
Network statistical information	<code>netstat -na</code> execution result	<ul style="list-style-type: none"> • <code>jp1_default_imm_1st.tar.{Z gz}</code> • <code>netstat_na.log</code>
List of users that are set in the machine	<code>/etc/passwd</code>	<ul style="list-style-type: none"> • <code>jp1_default_imm_1st.tar.{Z gz}</code> • <code>passwd</code>
Process list	<code>ps -elfa</code> execution result	<ul style="list-style-type: none"> • <code>jp1_default_imm_1st.tar.{Z gz}</code> • <code>ps.log</code>
Service port settings that are set in the machine	<ul style="list-style-type: none"> • <code>/etc/inet/services</code> (Solaris) • <code>/etc/services</code> (AIX) 	<ul style="list-style-type: none"> • <code>jp1_default_imm_1st.tar.{Z gz}</code> • <code>services</code>
Memory information	<ul style="list-style-type: none"> • <code>swap -l</code> execution result (Solaris) • <code>lspcs -s</code> execution result (AIX) 	<ul style="list-style-type: none"> • <code>jp1_default_imm_1st.tar.{Z gz}</code> • <code>swapinfo.log</code>
System diagnostic information	<ul style="list-style-type: none"> • <code>dmesg</code> execution result (Solaris) • <code>alog -o -t boot</code> execution result (AIX) 	<ul style="list-style-type: none"> • <code>jp1_default_imm_1st.tar.{Z gz}</code> • <code>sys_info.log</code>
Syslog (<code>syslog</code>)	<ul style="list-style-type: none"> • <code>/var/adm/messages</code> (Solaris) • <code>/var/adm/messages</code> (AIX) 	<ul style="list-style-type: none"> • <code>jp1_default_imm_1st.tar.{Z gz}</code> • <code>syslog.log</code>
JP1/IM - Manager (JP1/IM - Central Console) core analysis information (back trace) output by the <code>jcogencore</code> command	Analysis result from <code>seraph</code> <code>/var/opt/jp1cons</code>	<ul style="list-style-type: none"> • <code>jp1_default_imm_1st.tar.{Z gz}</code> • <code>trace_module-name.log</code>
	Analysis result from <code>seraph</code> <code>shared-directory/jp1cons/log</code> (core output by <code>jcogencore</code>)#2	<ul style="list-style-type: none"> • <i>logical-host-name_imm_1st.tar.{Z gz}</i> • <code>trace_module-name.log</code>

Information type	Collected data	File name#1
OS version information	uname -a execution result	<ul style="list-style-type: none"> • jpl_default_imm_1st.tar.{Z gz} • uname_a.log
Kernel parameter information	In Solaris: <ul style="list-style-type: none"> • sysdef -i execution result • ulimit -a execution result In AIX: <ul style="list-style-type: none"> • lsattr -E -l sys0 execution result • ulimit -a execution result • /etc/security/limits execution result 	<ul style="list-style-type: none"> • jpl_default_imm_1st.tar.{Z gz} In Solaris: <ul style="list-style-type: none"> • sysdef.log • ulimit.log In AIX: <ul style="list-style-type: none"> • isattr.log • ulimit.log • limits
Page size information	<ul style="list-style-type: none"> • pagesize execution result (Solaris) • pagesize execution result (AIX) 	<ul style="list-style-type: none"> • jpl_default_imm_1st.tar.{Z gz} • pagesize.log
OS patch application information	In Solaris: <ul style="list-style-type: none"> • showrev -a execution result In AIX: <ul style="list-style-type: none"> • instfix -a -icv execution result • lslpp -l -a execution result 	<ul style="list-style-type: none"> • jpl_default_imm_1st.tar.{Z gz} In Solaris: <ul style="list-style-type: none"> • showrev.log In AIX: <ul style="list-style-type: none"> • instfix.log • lslpp.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 the .tar.Z format.

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 9-14: JP1 information (UNIX)

Information type		Collected data	File name#1
Common to JP1/IM and JP1/Base	Integrated trace log	All files under <code>/var/opt/hitachi/HNTRLlib2/spool/</code>	<ul style="list-style-type: none"> <code>jp1_default_imm_1st.tar.{Z gz}</code> The following files in the default mode: <code>hntr2[1 2 3 4].log</code>
	Patch application history	<code>/opt/jp1imm/patch_history</code>	<ul style="list-style-type: none"> <code>jp1_default_imm_1st.tar.{Z gz}</code> <code>patch_history</code>
JP1/IM - Manager (common to components)	Patch log information	<code>/opt/jp1imm/update.log</code>	<ul style="list-style-type: none"> <code>jp1_default_imm_1st.tar.{Z gz}</code> <code>update.log</code>
	Automatic startup and automatic termination script	Files under <code>/etc/opt/jp1cons/</code>	<ul style="list-style-type: none"> <code>jp1_default_imm_1st.tar.Z</code> Copies of the files indicated at left
JP1/IM - Manager (JP1/IM - Central Console)	Settings and definition file	Files under <code>/etc/opt/jp1cons/conf/</code>	<ul style="list-style-type: none"> <code>jp1_default_imm_1st.tar.{Z gz}</code> Copies of the files indicated at left
		Files under <i>shared-directory</i> / <code>jp1cons/conf/#2</code>	<ul style="list-style-type: none"> <code>logical-host-name_imm_1st.tar.{Z gz}</code> Copies of the files indicated at left
	Common definition information	Files under <code>/etc/opt/jp1cons/default/</code>	<ul style="list-style-type: none"> <code>jp1_default_imm_1st.tar.{Z gz}</code> Copies of the files indicated at left
	Log file	Files under <code>/var/opt/jp1cons/log/</code>	<ul style="list-style-type: none"> <code>jp1_default_imm_1st.tar.{Z gz}</code> Copies of the files indicated at left
		Files under <i>shared-directory</i> / <code>jp1cons/log/#2</code>	<ul style="list-style-type: none"> <code>logical-host-name_imm_1st.tar.{Z gz}</code> Copies of the files indicated at left
	Core analysis information (CAR file) output by the <code>jcogencore</code> command	<code>car</code> command result <code>/var/opt/jp1cons/log</code> (core output by <code>jcogencore</code>)	<ul style="list-style-type: none"> <code>jp1_default_imm_2nd.tar.{Z gz}</code> <code>car_module-name.tar.Z</code>

Information type	Collected data	File name ^{#1}	
	car command result <i>shared-directory</i> /jplcons/ log (core output by jcgencore) ^{#2}	<ul style="list-style-type: none"> • <i>logical-host-name_imm_2nd.tar</i>.{Z gz} • <i>car_module-name.tar.Z</i> 	
Core analysis information (CAR file)	car command result /var/opt/jplcons/log	<ul style="list-style-type: none"> • <i>jpl_default_imm_2nd.tar</i>.{Z gz} • <i>core_module-name_car.tar.Z</i> 	
	car command result <i>shared-directory</i> /jplcons/ log ^{#2}	<ul style="list-style-type: none"> • <i>logical-host-name_imm_2nd.tar</i>.{Z gz} • <i>core_module-name_car.tar.Z</i> 	
Correlation event generation history file	Files under /var/opt/ jplcons/operation/evgen/	<ul style="list-style-type: none"> • <i>jpl_default_imm_2nd.tar</i>.{Z gz} • Copies of the files indicated at left 	
	<i>shared-directory</i> /jplcons/ operation/evgen ^{#2}	<ul style="list-style-type: none"> • <i>logical-host-name_imm_2nd.tar</i>.{Z gz} • Copies of the files indicated at left 	
JP1/IM - Manager (JP1/IM - Central Scope)	Settings and definition file	Files under /etc/opt/ jplscope/conf/	<ul style="list-style-type: none"> • <i>jpl_default_imm_1st.tar</i>.{Z gz} • Copies of the files indicated at left
		Files under <i>shared-directory</i> / jplscope/conf/ ^{#2}	<ul style="list-style-type: none"> • <i>logical-host-name_imm_1st.tar</i>.{Z gz} • Copies of the files indicated at left
	Common definition information	Files under /etc/opt/ jplscope/default/	<ul style="list-style-type: none"> • <i>jpl_default_imm_1st.tar</i>.{Z gz} • Copies of the files indicated at left
	Log file	Files under /var/opt/ jplscope/log/	<ul style="list-style-type: none"> • <i>jpl_default_imm_1st.tar</i>.{Z gz} • Copies of the files indicated at left
		Files under <i>shared-directory</i> / jplscope/log/ ^{#2}	<ul style="list-style-type: none"> • <i>logical-host-name_imm_1st.tar</i>.{Z gz} • Copies of the files indicated at left
Core analysis information (CAR file)	car command result /var/opt/jplscope/log	<ul style="list-style-type: none"> • <i>jpl_default_imm_2nd.tar</i>.{Z gz} • <i>core_module-name_car.tar.Z</i> 	

Information type	Collected data	File name ^{#1}	
	car command result <i>shared-directory</i> /jplscope/ log ^{#2}	<ul style="list-style-type: none"> • <i>logical-host-name_Imm_2nd.tar.</i>{Z gz} • <i>core_module-name_car.tar.Z</i> 	
	Database information	Files under /var/opt/ jplscope/database/	<ul style="list-style-type: none"> • <i>jpl_default_Imm_2nd.tar.</i>{Z gz} • Copies of the files indicated at left
		Files under <i>shared-directory</i> / jplscope/database/ ^{#2}	<ul style="list-style-type: none"> • <i>logical-host-name_Imm_2nd.tar.</i>{Z gz} • Copies of the files indicated at left
JP1/IM - Manager (IM Configuration Management)	Settings and definition files	Files under /etc/opt/ jplimm/conf/imcf/	<ul style="list-style-type: none"> • <i>jpl_default_Imm_1st.tar.</i>{Z gz} • <i>./etc/opt/lplimm/conf/imcf</i> • Copies of the files indicated at left
		Files under <i>shared-directory</i> / jplimm/conf/imcf/ ^{#2}	<ul style="list-style-type: none"> • <i>logical-host-name_Imm_1st.tar.</i>{Z gz} • <i>./shared-directory/jplimm/conf/imcf</i> • Copies of the files indicated at left
	Common definition information	Files under /etc/opt/ jplimm/default/imcf/	<ul style="list-style-type: none"> • <i>jpl_default_Imm_1st.tar.</i>{Z gz} • <i>./etc/opt/jplimm/default/imcf</i> • Copies of the files indicated at left
	Log file	Files under /var/opt/ jplimm/log/imcf/	<ul style="list-style-type: none"> • <i>jpl_default_Imm_1st.tar.</i>{Z gz} • <i>./var/opt/jplimm/log/imcf</i> • Copies of the files indicated at left
		Files under <i>shared-directory</i> / jplimm/log/imcf/ ^{#2}	<ul style="list-style-type: none"> • <i>logical-host-name_Imm_1st.tar.</i>{Z gz} • <i>./shared-directory/jplimm/log/imcf</i> • Copies of the files indicated at left
	Core analysis information(CAR file)	car command result /var/opt/jplimm/log	<ul style="list-style-type: none"> • <i>jpl_default_Imm_2nd.tar.</i>{Z gz} • <i>./var/opt/jplimm/log/_jpl_default/core/core_module-name_car.tar.Z</i>

Information type	Collected data	File name ^{#1}	
	car command result <i>shared-directory</i> /jplimm/ log ^{#2}	<ul style="list-style-type: none"> • <i>logical-host-name_imm_2nd.tar.</i>{Z gz} • <i>./var/opt/jplimm/log/_logical-host-name/core/core_module-name_car.tar.Z</i> 	
JP1/Base	Automatic startup and automatic termination script	Files under <i>/etc/opt/jplbase/</i> <ul style="list-style-type: none"> • <i>jpl_default_imm_1st.tar.</i>{Z gz} • Copies of the files indicated at left 	
	Settings and definition file	Files under <i>/etc/opt/jplbase/conf/</i>	<ul style="list-style-type: none"> • <i>jpl_default_imm_1st.tar.</i>{Z gz} • Copies of the files indicated at left
		Files under <i>shared-directory/jplbase/conf/#2</i>	<ul style="list-style-type: none"> • <i>logical-host-name_imm_1st.tar.</i>{Z gz} • Copies of the files indicated at left
	Common definition information	Files under <i>/etc/opt/jplbase/default/</i>	<ul style="list-style-type: none"> • <i>jpl_default_imm_1st.tar.</i>{Z gz} • Copies of the files indicated at left
	Plug-in service settings file	Files under <i>/opt/jplbase/conf/plugin/</i>	<ul style="list-style-type: none"> • <i>jpl_default_imm_1st.tar.</i>{Z gz} • Copies of the files indicated at left
	Patch application history	<i>/opt/jplbase/PatchInfo</i>	<ul style="list-style-type: none"> • <i>jpl_default_imm_1st.tar.</i>{Z gz} • <i>PatchInfo</i>
	Patch log information	<i>/opt/jplbase/PatchLog</i>	<ul style="list-style-type: none"> • <i>jpl_default_imm_1st.tar.</i>{Z gz} • <i>PatchLog</i>
	Log file	<i>/var/opt/jplbase/log</i>	<ul style="list-style-type: none"> • <i>jpl_default_imm_1st.tar.</i>{Z gz} • All files under the directory indicated at left, except <i>COMMAND</i>
		<i>shared-directory/jplbase/log#2</i>	<ul style="list-style-type: none"> • <i>logical-host-name_imm_1st.tar.</i>{Z gz} • All files under the directory indicated at left, except <i>COMMAND</i>
Log and temporary file	Files under <i>/var/opt/jplbase/sys/tmp/</i>	<ul style="list-style-type: none"> • <i>jpl_default_imm_1st.tar.</i>{Z gz} • Copies of the files indicated at left 	

Information type	Collected data	File name ^{#1}
	<i>shared-directory/event</i> ^{#2}	<ul style="list-style-type: none"> <i>logical-host-name_imm_1st.tar.</i>{Z gz} All files under the directory indicated at left, except <i>IMEvent*</i>
SES settings file	<ul style="list-style-type: none"> <i>/tmp/.Jp1_SEs*</i> <i>/usr/tmp/jp1_ses</i> <i>/usr/lib/jp1_ses/log</i> <i>/usr/lib/jp1_ses/sys</i> <i>/usr/bin/jp1_ses/jp*</i> <i>/var/opt/jp1_ses</i> 	<ul style="list-style-type: none"> <i>jp1_default_imm_2nd.tar.</i>{Z gz} Copies of the files indicated at left
Command execution history file	Files under <i>/var/opt/jp1base/log/COMMAND/</i>	<ul style="list-style-type: none"> <i>jp1_default_imm_2nd.tar.</i>{Z gz} Copies of the files indicated at left
	Files under <i>shared-directory/jp1base /log/COMMAND/</i> ^{#2}	<ul style="list-style-type: none"> <i>logical-host-name_imm_2nd.tar.</i>{Z gz} Copies of the files indicated at left
Event database	Files under <i>/var/opt/jp1base/sys/event/servers/default/</i>	<ul style="list-style-type: none"> <i>jp1_default_imm_2nd.tar.</i>{Z gz} Copies of the files indicated at left
	<i>shared-directory/event</i> ^{#2}	<ul style="list-style-type: none"> <i>logical-host-name_imm_2nd.tar.</i>{Z gz} <i>IMEvent*.*</i>

#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 the `.tar.z` format.

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) 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 *4.14.4 Specifying display settings for the Java Console window* in the *Job Management Partner 1/Integrated Management - Manager Configuration Guide*.

- Java trace file of Java™ 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

9.4 Collecting data

This section explains how to collect data when a problem occurs.

9.4.1 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 9-15: JP1/IM - Manager processes (Windows)

Parent process name	Function	Child process name	Function
jco_spm�.exe (1)	JP1/IM - Manager process management	jcmain.exe (1)	Automatic Action Service (Process management display name: jcmain)
		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	--	--

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.

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
jcmain	4088
evtcon	4236
jcsmain	4668
jcfmain	4950
evgen	5624

```
KAVB3691-I All the processes have started.
```

- `jcsmain` is displayed only when Central Scope is enabled.
- `jcfmain` is displayed only when IM Configuration Management is enabled.
- `evgen` is displayed only when 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 9-16: 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.

#: 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 9-17: 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™ 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\
```

Note:

The Java trace file of Java™ Plug-in is erased when Java™ Plug-in restarts. Therefore, if a problem occurs, save the content of this file to another file before restarting.

Manager side

- HTTP server error log
- HTTP server access log

(4) Executing the data collection tool

This subsection describes execution of the data collection tool (`jim_log.bat` or `jcoview_log.bat`).

When you execute the `jim_log.bat` command, which is provided by JP1/IM - Manager, you can collect the data necessary for troubleshooting JP1/IM - Manager and JP1/IM - View on the same host.

If you execute the `jcoview_log.bat` command, which is provided by JP1/IM - View, you can collect the data necessary for troubleshooting JP1/IM - View.

Use one of above commands according to the application that is being used.

Because the total volume of data collected by a data collection tool is massive, you need to estimate it before you execute the command and make sure the machine you are using has sufficient free space.

For the volume of data that will be collected by the `jim_log.bat` command, see the JP1/IM - Manager release notes.

For the volume of data that will be collected by the `jcoview_log.bat` command, see the JP1/IM - View release notes.

A tool execution example follows.

```
C:\>"C:\Program Files\HITACHI\JP1IMM\tools\jim_log.bat" -f  
data-storage-folder
```

Specify the data storage folder as an absolute path. If the data storage folder path contains a space, enclose the path in double quotation marks.

When you execute the tool, the `jp1_default` folder is created under the folder specified as the data storage folder, and the collected data is copied into this folder. Use a data-compression tool to compress the collected data.

(5) **Checking the operation content**

Check the content of the operation that was taking place when the problem occurred, and record it. The following types of information must be checked:

- Operation content details
- Time of problem occurrence
- Reproducibility
- Login user name that was used to log in from JP1/IM - View
- Machine configuration (version of each OS, host name, and Central Console configuration)

(6) **Collecting the error information on the screen**

If an error is displayed on the screen, collect that information as well. Collect a hard copy of the following:

- Error dialog box

Copy the content displayed by the **Details** button, if available.

(7) **Collecting a user dump (Windows Vista and Windows Server 2008 only)**

If an application error causes a JP1/IM - View process to stop in Windows Vista or Windows Server 2008, use the following procedure to collect a user dump, with the error dialog box displayed.

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.

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) Collecting a problem report (Windows Vista and Windows Server 2008 only)

If an application error causes a JP1/IM - View process to stop in Windows Vista or Windows Server 2008, use the following procedure to collect a problem report.

1. In the **Run** text box, enter `wercn` 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.

9.4.2 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 9-18: JP1/IM - Manager processes (UNIX)

Parent process name	Function	Child process name	Function
jco_spm (1) ^{#1}	Process management	jcain (1)	Automatic Action Service (Process management display name: jcain)
		evtcon (1) ^{#1}	Event Console Service (Process management display name: evtcon)
		evflow (1)	Event Base Service (Process management display name: evflow)

Parent process name	Function	Child process name	Function
		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_spmc 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_spmc` is controlled by process

management, and you can use the `jco_spm�_status` command to check the process status.

A display example during normal operations follows.

```
# jco_spm�_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     4846
    jcfmain     4950
    evgen       5624
KAVB3691-I All the processes have started.
```

- `jcsmain` is displayed only when Central Scope is enabled.
- `jcfmain` is displayed only when IM Configuration Management is enabled.
- `evgen` is displayed only when 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™ 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\
```

Note:

The Java trace file of Java™ Plug-in is erased when Java™ Plug-in restarts. Therefore, if a problem occurs, save the content of this file to another file before restarting.

Manager side

- HTTP server error log
- HTTP server access log

(4) Executing the data collection tool

This subsection describes execution of the data collection tool (`jim_log.sh`).

When you execute the `jim_log.sh` command, which is provided by JP1/IM - Manager, you can collect the data necessary for troubleshooting JP1/IM - Manager and JP1/Base on the same host.

Because the total volume of data collected by a data collection tool is massive, you need to estimate it before you execute the command and make sure the machine you are using has sufficient free space. For the volume of data that will be collected by the `jim_log.bat` command, see the JP1/IM - Manager release notes.

A tool execution example follows.

```
# /opt/jplimm/tools/jim_log.sh -f data-storage-directory
```

When you execute the tool, the collected data is summarized in the `tar` format and output as compressed data.

(5) Checking the operation content

Check the content of the operation that was taking place when the problem occurred, and record it. The following types of information must be checked:

- Operation content details
- Time of problem occurrence
- Reproducibility
- Login user name that was used to log in from JP1/IM - View
- Machine configuration (version of each OS, host name, and Central Console configuration)

(6) Collecting the error information on the screen

If an error is displayed on the screen, collect that information as well. Collect a hard copy of the following:

- Error dialog box

If the **Details** button is available, copy its content as well.

9.5 Corrective actions

This section explains how to correct the problems that can generally be anticipated.

Table 9-19: Problems that can generally be anticipated

No.	Problem description
1	You cannot log on from JP1/IM - View.
2	The definition menu is not displayed in the Event Console window.
3	You cannot execute a command.
4	The command execution log file is damaged.
5	Unknown is displayed as the automated action execution status.
6	An automated action is delayed.
7	The monitored object database is damaged.
8	The monitored object database cannot be unlocked.
9	KAVB5150-W is displayed in the detailed information (message) for the action result.
10	Either the JP1/IM - Central Scope version or the JP1/IM - View version is old.
11	Many JP1 events occurred for which correlation events were generated.
12	Correlation events cannot be displayed in JP1/IM - View.
13	The JP1/IM - View window cannot be displayed after you have logged on to JP1/IM - View.
14	Command execution or a batch file executed in an automated action does not terminate normally (Windows only).
15	Processing of JP1 events received by JP1/IM - Manager (JP1/IM - Central Scope) is delayed.
16	No JP1 event is displayed in the Event Console window.
17	Status cannot be changed.
18	An event search cannot be performed.
19	Memo entries cannot be set up.
20	The IM database cannot be terminated.
21	You cannot connect to the IM database.
22	JP1/IM - Manager cannot be uninstalled.

No.	Problem description
23	An error message indicating an invalid port number is issued when the IM database is set up.
24	IM database setup fails.
25	The setup information file is output as invalid during IM database setup.
26	The IM database cannot be started. Or, database-related commands cannot be executed.
27	IM Configuration Management failed to collect host information.
28	IM Configuration Management failed to apply the system hierarchy.
29	IM Configuration Management failed to collect the operation definition file for the log file trap.
30	JP1/IM - View cannot display any of the log file traps that are active.
31	The content of the profile settings file does not match the content of the valid configuration information.
32	Menu items such as Register Host and Edit IM Configuration are disabled in IM Configuration Management - View.

(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 actions

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. *is output.*

Cause

The authentication server that is set at the connection-destination host has not been started.

Corrective action

Start the authentication server.

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: A connection to the specified connection destination host cannot be established. Confirm that the server has started up. *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 connection-target host.

The message KNAN20102-E: A connection to the specified connection destination host cannot be established. is output.

Cause

User authentication failed. The user name or password is invalid.

Corrective action

Make sure the specified user name and password are correct, and then retry the operation.

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 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 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 target host has been started.
- Make sure that there are no communication problems with the target host.

(2) 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.

(3) Actions to take when you cannot execute a command

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.

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. Or, 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*.

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*.

(4) Actions to take when a command execution log file is damaged

If an operation to write data into a command execution log file is interrupted by, for example, a machine stoppage caused by a power failure, the command execution log file for automated actions or the command execution log file for command execution may be damaged.

In such cases, the following messages are issued:

- In the Action Log Details window of JP1/IM - View, or when the `jcashowa` command is executed to display the execution result of an automated action, the message `KAVB5151-W Failed to get data from Command Executed log file.` is displayed as the execution result.

The command execution log file for automated actions may be damaged.

- When the `jcocmdlog` command is executed, the message `KAVB2523-E The command-execution log file for the executed command cannot be opened.` is output.

The command execution log file for command execution may be damaged.

- When the `jcocmdlog` command is executed, the message `KAVB2525-E The command-execution log file for the automatic action cannot be opened.` is output.

The command execution log file for automated actions may be damaged.

- When the `jcocmdlog` command is executed, the message `KAVB2527-E An attempt to read the command-execution log file has failed.` is output.

- If `-act` is specified for the option, the command execution log file for automated actions may be damaged.
- If `-window` is specified for the option, the command execution log file for command execution may be damaged.
- If neither `-act` nor `-window` is specified for the option, the command execution log file for automated actions or command execution may be damaged.
- The message `KAVB2064-E Error in writing execution results to Command execution log.` is output to the integrated trace log.

The command execution log file for automated actions or the command execution log file for command execution may be damaged.

If any of these messages is output, use the following procedure to check the status of the command execution log file.

1. Use the procedure in (a) below to check the file that may have been damaged.
2. If it is not damaged, take the correction action prescribed in each message.
3. If it is damaged, restore it using the procedure described in (b).
4. If the file cannot be restored using the procedure in (b), follow the procedure in (c) to delete the command execution log file.

(a) How to check the command execution log files

Checking the command execution log file for automated actions

■ In Windows

From the command prompt, execute the following commands:

```
cd Base-path\log\COMMAND
```

(For a logical host: `cd shared-folder\jplbase\log\COMMAND`)

```
Jischk -l3 Base-path\log\COMMAND\ACTISAMLOGV8
```

■ In UNIX

Execute the following command:

```
cd /var/opt/jplbase/log/COMMAND
```

(For a logical host: `cd shared-directory/jplbase/log/COMMAND`)

```
/opt/jplbase/bin/Jischk -l3 actisamlogv8
```

Checking the command execution log file for command execution

■ In Windows

From the command prompt, execute the following commands:

```
cd Base-path\log\COMMAND
```

(For a logical host: cd *shared-folder*\jplbase\log\COMMAND)

```
Jischk -l3 Base-path\log\COMMAND\CMDISAMLOGV8
```

- In UNIX

Execute the following command:

```
cd /var/opt/jplbase/log/COMMAND
```

(For a logical host: cd *shared-directory*/jplbase/log/COMMAND)

```
/opt/jplbase/bin/Jischk -l3 cmdisamlogv8
```

If the `Jischk` command does not detect file invalidity, the command execution log file is not damaged. If the `Jischk` command detects file invalidity, follow the procedure described in (b) below to restore the command execution log file.

For details about the `Jischk` command, see the *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*\jplbase\log\COMMAND)

```
Jiscond ACTISAMLOGV8
```

4. From the command prompt, execute the following command to check whether the command execution log file has been normally restored:

```
Jischk -l3 ACTISAMLOGV8
```

If the `Jischk` command detects file invalidity, the command execution log file cannot be restored. If the file cannot be restored, follow the procedure described in (c) below to delete the command execution log file for automated actions.

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

■ In UNIX

Perform the following operations with superuser permissions. Also, for the restoration operation you need free space that is approximately three times the size of `actisamlogv8.DAT`.

1. Stop JP1/IM - Manager.
2. Stop JP1/Base.
3. Execute the commands listed below to restore the command execution log file.

For details about the `Jiscond` command, see the *Job Management Partner I/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 I/Base User's Guide*.

```
cd Base-path\log\COMMAND
```

(For a logical host: `cd shared-folder\jplbase\log\COMMAND`)

```
Jiscond CMDISAMLOGV8
```

4. From the command prompt, execute the following command to check whether the command execution log file has been normally restored:

```
Jischk -l3 CMDISAMLOGV8
```

If the `Jischk` command detects file invalidity, the command execution log file cannot be restored. If the file cannot be restored, follow the procedure described in (c) below to delete the command execution log file for command execution.

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

■ In UNIX

Perform the following operations with superuser permissions. Also, for the restoration operation you need free space that is approximately three times the size of `cmdisamlogv8.DAT`.

1. Stop JP1/IM - Manager.
2. Stop JP1/Base.
3. Execute the following command:

```
cd /var/opt/jplbase/log/COMMAND
```

(For a logical host: `cd shared-directory/jplbase/log/COMMAND`)

```
/opt/jplbase/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/jplbase/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 9-20: Locations of files to be deleted (Windows)

File name	Location
Command execution log file for automated actions	<ul style="list-style-type: none"> • <i>Base-path</i>\log\COMMAND\ACTISAMLOGV8.DRF • <i>Base-path</i>\log\COMMAND\ACTISAMLOGV8.K01 • <i>Base-path</i>\log\COMMAND\ACTISAMLOGV8.KDF
	<ul style="list-style-type: none"> • <i>shared-folder</i>\jplbase\log\COMMAND\ACTISAMLOGV8.DRF • <i>shared-folder</i>\jplbase\log\COMMAND\ACTISAMLOGV8.K01 • <i>shared-folder</i>\jplbase\log\COMMAND\ACTISAMLOGV8.KDF
Action information file	<i>Console-path</i> \log\action\actinf.log
	<i>shared-folder</i> \jplcons\log\action\actinf.log
Action host name file	<i>Console-path</i> \log\action\acttxt{1 2}.log
	<i>shared-folder</i> \jplcons\log\action\acttxt{1 2}.log

In UNIX

Table 9-21: Locations of files to be deleted (UNIX)

File name	Location
Command execution log file for automated action	<ul style="list-style-type: none"> • /var/opt/jplbase/log/COMMAND/actisamlogv8.DAT • /var/opt/jplbase/log/COMMAND/actisamlogv8.K01 • /var/opt/jplbase/log/COMMAND/actisamlogv8.DEF

File name	Location
	<ul style="list-style-type: none"> <i>shared-directory</i>/jplbase/log/COMMAND/actisamlogv8.DAT <i>shared-directory</i>/jplbase/log/COMMAND/actisamlogv8.K01 <i>shared-directory</i>/jplbase/log/COMMAND/actisamlogv8.DEF
Action information file	/var/opt/jplcons/log/action/actinf.log
	<i>shared-directory</i> /jplcons/log/action/actinf.log
Action host name file	/var/opt/jplcons/log/action/acttxt{1 2}.log
	<i>shared-directory</i> /jplcons/log/action/acttxt{1 2}.log

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

Deleting the command execution log file for command execution

When you delete the command execution log file for command execution, all history on past command execution is lost. Therefore, if deletion will cause a problem, back up the files. For details, see *1.2.2 Database backup and recovery*.

1. Stop JP1/IM - Manager.
2. Stop JP1/Base.
3. Delete the command execution log file.

Delete the files listed in the table below if you could not restore the command execution log file for command execution. For details about the command execution log file, see the *Job Management Partner 1/Base User's Guide*.

In Windows

Table 9-22: Locations of files to be deleted (Windows)

File name	Location
Command execution log file for command execution	<ul style="list-style-type: none"> <i>Base-path</i>\log\COMMAND\CMDISAMLOGV8.DRF <i>Base-path</i>\log\COMMAND\CMDISAMLOGV8.K01 <i>Base-path</i>\log\COMMAND\CMDISAMLOGV8.KDF
	<ul style="list-style-type: none"> <i>shared-folder</i>\jplbase\log\COMMAND\CMDISAMLOGV8.DRF <i>shared-folder</i>\jplbase\log\COMMAND\CMDISAMLOGV8.K01 <i>shared-folder</i>\jplbase\log\COMMAND\CMDISAMLOGV8.KDF

In UNIX

Table 9-23: Locations of files to be deleted (UNIX)

File name	Location
Command execution log file for command execution	<ul style="list-style-type: none"> • /var/opt/jp1base/log/COMMAND/cmdisamlogv8.DAT • /var/opt/jp1base/log/COMMAND/cmdisamlogv8.K01 • /var/opt/jp1base/log/COMMAND/cmdisamlogv8.DEF
	<ul style="list-style-type: none"> • <i>shared-directory</i>/jp1base/log/COMMAND/cmdisamlogv8.DAT • <i>shared-directory</i>/jp1base/log/COMMAND/cmdisamlogv8.K01 • <i>shared-directory</i>/jp1base/log/COMMAND/cmdisamlogv8.DEF

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

(5) 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 9-24: Locations of files to delete (Windows)

File name	Location
Action information file	<i>Console-path</i> \log\action\actinf.log
	<i>shared-folder</i> \jp1cons\log\action\actinf.log

File name	Location
Action host name file	<i>Console-path</i> \log\action\acttxt{1 2}.log
	<i>shared-folder</i> \jplcons\log\action\acttxt{1 2}.log
Command execution log file	All files under <i>Base-path</i> \log\COMMAND\
	All files under <i>shared-folder</i> \jplbase\log\COMMAND\

In UNIX

Table 9-25: Locations of files to delete (UNIX)

File name	Location
Action information file	/var/opt/jplcons/log/action/actinf.log
	<i>shared-directory</i> /jplcons/log/action/actinf.log
Action host name file	/var/opt/jplcons/log/action/acttxt{1 2}.log
	<i>shared-directory</i> /jplcons/log/action/acttxt{1 2}.log
Command execution log file	All files under /var/opt/jplbase/log/COMMAND/
	All files under <i>shared-directory</i> /jplbase/log/COMMAND/

3. Start JP1/Base and then start JP1/IM - Manager.

In the case of a cluster configuration, unmount the shared disk and then operate the cluster software to start the logical hosts.

(6) Actions to take when an automated action is delayed

When the automated action status remains Running.

First, use the `jccmdshow` 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 7.1.3 *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*.

(7) 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.

(8) Actions to take when the monitored object database cannot be unlocked

The monitored object database stays locked.

Cause

The following is the possible cause:

- An attempt to acquire a lock on the monitored object database of JP1/IM - Manager failed.

Corrective action

Take the following steps:

1. Execute the `jco_spm�_status` command to make sure the `jcsmain` process is not active.
2. Execute the `Jismlcktr` command.
3. Determine which process has locked the files under *Scope-path*\database.
4. Execute the `Jislckfree -p PID` command on the process ID determined in Step 3.

The `Jismlcktr` and `Jislckfree` commands are provided by JP1/Base.

For details, see the chapter that explains commands in the *Job Management Partner I/Base User's Guide*.

(9) 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 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 9-26: Locations of command execution log files (Windows)*

File name	Location
Command execution log file	All files under <i>Base-path</i> \log\COMMAND\
	All files under <i>shared-folder</i> \jp1base\log\COMMAND\

*In UNIX**Table 9-27: 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 <i>shared-directory</i> /jp1base/log/COMMAND/

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

1. Start JP1/Base and JP1/IM.

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*.

(10) Actions to take when an earlier version of JP1/IM - Central Scope 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 or JP1/IM - Central Scope 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 or JP1/IM - Central Scope is earlier than the version of JP1/IM - View:

Use the following procedure to upgrade the JP1/IM - Manager or JP1/IM - Central Scope 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 or JP1/IM - Central Scope 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 or JP1/IM - Central 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: *1.18.3(2) Executing the Central Scope upgrade command in the Job Management Partner 1/Integrated Management - Manager Configuration Guide*

UNIX: *2.17.5(2) Executing the Central Scope upgrade command in the Job Management Partner 1/Integrated Management - Manager Configuration Guide*

- For a logical host

Windows: *6.2.2(2) Setup during upgrading in the Job Management Partner 1/Integrated Management - Manager Configuration Guide*

UNIX: *6.3.2(2) Setup during upgrading in the Job Management Partner 1/Integrated Management - Manager Configuration Guide*

When the version of JP1/IM - Manager or JP1/IM - Central Scope 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 or JP1/IM - Central Scope.
3. Delete the JP1/IM - Manager or JP1/IM - Central Scope 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 or JP1/IM - Central Scope to the later version.
8. Upgrade JP1/IM - View to the same version as JP1/IM - Manager or JP1/IM - Central Scope.

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 JP1/IM - Central Scope, 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 or JP1/IM - Central Scope.
3. Delete the JP1/IM - Manager or JP1/IM - Central Scope installation directory.
4. Install the JP1/IM - Manager or JP1/IM - Central Scope 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 or JP1/IM - Central Scope to the later version.
8. Upgrade JP1/IM - View to the same version as JP1/IM - Manager or JP1/IM - Central Scope.

(11) 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_spm�_reload` command to enable the startup option setting.

(12) 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.

(13) 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.

(14) 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.

(15) 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*, jplerror = 2001)...

or

...fs_jcsHostsAccessPtr->getHostByAddr() is failed. (host = *IP-address-for-which-name-resolution-failed*, jplerror = 2001)...

Check one of these messages and specify **Host name comparison** as the individual condition. Then, use one of the methods described below to enable name resolution of the host name or IP address specified as the attribute value.

- Register in the host information database the host name or IP address specified as the attribute value of the individual condition.
- Register in `jp1hosts` 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.

(16) 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

(17) 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. Or, 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. Or, 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_spmc_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 JPI 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_spmc_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.

(18) 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 JPI 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 08-00 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_spmc_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_spmc_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 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. Or, 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 08-00 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 08-00 or earlier, execute the search without using an exclusion condition.

(19) 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_spmc_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_spmc_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.

(20) 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.

(21) 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 (I. 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.

(22) 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.

(23) 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

(24) 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 `IMBDDIR` or `SHAREDDIR` 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 IMBDDIR or SHAREDDIR 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?

(25) 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.

(26) 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

(27) Actions to take when IM Configuration Management fails to collect host information

The message KNAN22017-E: Collection of host information failed because a connection could not be established with the host "host-name" . is output and host information collection fails.

Cause

The following are possible causes:

- The target host name is different.
- The target host name has not been resolved.
- The target host has not been started.
- JP1/Base of the target host has not been started.
- An error occurred in communications with the target host.
- The installation of JP1/Base on the target host is earlier than Version 7.

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 JP1/Base of the target host has been started.
- Make sure that there is no problem in communications with the target host.
- Make sure that the installation of JP1/Base on the target host is Version 7 or later.

(28) 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 it 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.

(29) 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.

(30) 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.

(31) 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.

(32) Actions to take when menu items such as Register Host and Edit IM 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

First, upgrade the instance of JP1/Base specified in the authentication server to Version 9 or later. Then, assign IM Configuration Management permissions (JP1_CF_Admin, JP1_CF_Manager, or JP1_CF_User) to the JP1 user, and have the user log in again.

Index

A

abbreviations defined ii

actions to take when

- automated action is delayed 260
- command execution log file is damaged 252
- command execution or batch file executed in automated action does not terminate normally 270
- correlation events cannot be displayed in JP1/IM - View 268
- either JP1/IM - Central Scope or JP1/IM - View is old 264
- event search cannot be executed 273
- IM Configuration Management failed to apply system hierarchy 281
- IM Configuration Management failed to collect host information 281
- IM Configuration Management failed to collect operation definition file for log file trap 282
- IM database cannot be terminated 276
- JP1/IM - View cannot display any log file traps that are active 283
- JP1/IM - View window cannot be displayed after you have logged on 269
- KAVB5150-W is displayed in detailed information for action result 263
- many JP1 events occurred for which correlation events were generated 267
- memo entries cannot be set up 275
- monitored object database cannot be unlocked 262
- monitored object database is damaged 261
- profile settings file does not match valid configuration information 283
- status cannot be changed 272
- unknown is displayed as automated action execution status 259
- you cannot connect to IM database 276

- you cannot execute command 251

automated actions

- canceling 135
- checking execution results of 131
- checking execution status of 129
- checking operating status of 138
- executing 129
- re-executing 136
- setting up 129

B

backing up 12

- command execution log 12
- configuration information (UNIX) 6
- configuration information (Windows) 2
- database 12
- event database 16
- host information database 15
- IM database 16
- monitored object database 14

batch file, terminated abnormally 270

C

canceling automated actions 135

Central Console, monitoring system from 55

Central Scope

- monitoring from Monitoring Tree window 112
- monitoring from Visual Monitoring window 119
- monitoring system from 111

changing

- database settings 17
- JP1/IM settings 34
- monitoring status of monitoring nodes 114, 121
- settings of host on which JP1/IM runs 35
- status of monitoring nodes 113, 120

- checking
 - command execution status 128
 - execution results of automated actions 131
 - execution status of automated actions 129
 - operating status of automated actions 138
 - cluster system, operations in 44, 45
 - command execution log
 - backing up 12
 - procedures for backing up and recovering 12
 - re-creating 17
 - recovering 12
 - reorganizing 11
 - command execution log file is damaged, actions to take when 252
 - command execution status, checking 128
 - commands
 - actions to take when you cannot execute 251
 - deleting 128
 - executing 126
 - executing on remote host 126
 - user who executes 127
 - common exclusion condition, switching using jcochfilter command 105
 - configuration file
 - applying edited content of 161
 - editing 159
 - configuration information
 - managing 2
 - migrating 31
 - consolidated display, viewing 72
 - consolidated events, displaying 70, 71
 - conventions
 - abbreviations ii
 - diagrams ix
 - fonts and symbols ix
 - KB, MB, GB and TB xii
 - mathematical expressions xi
 - version numbers xii
 - correlation event generation history 29
 - correlation events
 - displaying 75
 - handling 75
 - CSV file
 - outputting events to 29
 - outputting information displayed in JP1/IM - View to 108
- D**
- data collection tool
 - executing (UNIX) 245
 - executing (Windows) 240
 - data, collecting 236
 - database capacity, managing 26
 - database management 11
 - backing up command execution log 12
 - backing up event database 16
 - backing up host information database 15
 - backing up IM database 16
 - backing up monitored object database 14
 - changing IM database port 23
 - expanding IM database size 21
 - recovering command execution log 12
 - recovering event database 16
 - recovering host information database 15
 - recovering IM database 16
 - recovering monitored object database 14
 - reorganizing event database 11
 - reorganizing IM database 11
 - databases
 - backing up 12
 - changing settings of 17
 - managing 11
 - migrating 31
 - re-creating 17
 - recovering 12
 - reorganizing 11
 - deleting commands 128
 - diagram conventions ix
 - disk capacity, managing 26
 - displaying
 - attributes of monitoring nodes 116, 123
 - consolidated events 70
 - detailed JP1 event information 62
 - extended attributes of JP1 events 64
 - guide information 117, 123
 - login user list 118
 - repeated events 70
 - response status of JP1 events 68

- search results of JP1 events 93
- severe events only 69

dump files, managing 27

E

- editing memo entries 89
- error information
 - collecting (UNIX) 246
 - collecting (Windows) 241
- event acquisition filter
 - switching 100
 - switching windows 100
 - switching, using jcochfilter command 103, 104
- Event Console window
 - actions to take when definition menu is not displayed in 251
 - actions to take when no JP1 event is displayed in 272
- event database
 - backing up 16
 - procedures for backing up and recovering 16
 - re-creating 19
 - recovering 16
 - reorganizing 11
- event search direction 92
- event search, setting response status for 96
- events
 - changing severity level of 87
 - displayed on screen 60
 - outputting, to CSV file 29
- events list, items displayed in 56
- executing
 - automated actions 129
 - commands 126
 - commands on remote host 126

F

font conventions ix

G

- GB meaning xii
- guide information, displaying 117, 123

H

- historical reports, using 29
- host information database
 - backing up 15
 - procedures for backing up and recovering 15
 - re-creating 18
 - recovering 15
 - reorganizing 11
- host name change
 - effects of 35
 - necessary tasks as a result of 35, 36
- hosts
 - adding 150
 - changing information of 146
 - collecting information from 145
 - deleting 144, 152
 - displaying list of 147
 - managing 144
 - moving 151
 - registering 144

I

- IM Configuration Management
 - applying imported management information of 174
 - collecting information from hosts 145
 - exporting management information of 167
 - importing management information of 170
 - managing hosts 144
 - managing profiles 155
 - managing service operation status 164
 - managing system hierarchy using 143
 - importing/exporting management information of 167
- IM database
 - backing up 16
 - changing port of 23
 - expanding size of 21
 - recovering 16
 - reorganizing 11
- integrated monitoring database, outputting 109
- IP address change
 - effects of 37
 - necessary tasks as a result of 37

J

JP1 event information and action execution results, copying 110

JP1 events

- changing severity level of 87
- displaying 56
- displaying detailed information of 62
- displaying extended attributes of 64
- displaying only severe 69
- displaying response status of 68
- displaying search results of 93
- displaying, by specifying time 79
- displaying, by specifying time period 78
- enabling view filter for 99
- items that can be displayed 57
- method for searching 90
- monitoring system based on 56
- opening monitor window for application that issued 98
- searching for 90
- setting response status for searching 96
- setting response status of severe 85
- using historical information of 29
- viewing 56

JP1/IM

- changing configuration of 33
- changing event severity 87
- collecting data 236
- correcting problems 247
- data that needs to be collected when problem occurs 209
- editing memo entries 89
- enabling view filter 99
- log information types 181
- logging off 54
- logging off from JP1/IM - Manager 54
- logging on 50
- logging on to JP1/IM - Manager 50
- managing configuration information 2
- managing databases 11
- managing disk capacity 26
- monitoring from Monitoring Tree window 112

- monitoring from Visual Monitoring window 119
- monitoring system based on JP1 events 56
- monitoring system from Central Scope 111
- necessary tasks as a result of system date/time change 38
- opening other application windows from Tool Launcher 139
- outputting dump file for (UNIX) 244
- outputting thread dump for (Windows) 238
- runs, changing settings of host on which 35
- searching for JP1 events 90
- setting response status of severe events 85
- settings information, changing 34
- starting 42
- stopping 45
- switching event acquisition filter 100
- system maintenance 1
- system operation using 125
- troubleshooting 179
- troubleshooting procedure 180
- using historical reports 29

JP1/IM - Manager

- log files and folders (IM Configuration Management) (UNIX) 207
- log files and folders (IM Configuration Management) (Windows) 194
- log files and folders (JP1/IM - Central Console) (UNIX) 197
- log files and folders (JP1/IM - Central Console) (Windows) 184
- log files and folders (JP1/IM - Central Scope) (UNIX) 205
- log files and folders (JP1/IM - Central Scope) (Windows) 192
- logging off from 54
- logging on to 50
- logon and logoff 49
- notes on starting 47
- notes on stopping 47
- starting 41, 42, 43
- stopping 41, 45
- using command to log on to 52
- using GUI to log on to 50

JP1/IM - Rule Operation
 checking rule startup request status 80
 displaying Rule Log Details window of 82
 making rule startup request 80

JP1/IM - View
 actions to take when you cannot log on
 from 248
 collecting information related to web version
 of (UNIX) 244
 collecting information related to web version
 of (Windows) 239
 executing commands 126
 log files and folders 195
 opening monitor window for application that
 issued JP1 events 98
 opening other application windows from Tool
 Launcher 139
 outputting events list to CSV file 108
 outputting information displayed in 108
 switching common exclusion condition 101,
 103
 switching event acquisition filter 100, 102
 switching windows of 100
 system operation 125

JP1/IM files for backup 2, 7

K

KAVB0104-E 248
 KAVB0109-E 249
 KAVB1200-E 248
 KAVB2027-E 251
 KAVB2031-E 251
 KAVB2239-E 261
 KAVB7247-E 261
 KAVB7248-E 262
 KB meaning xii
 KNAN20100-E 249
 KNAN20101-E 249
 KNAN20102-E 250
 KNAN20103-E 250
 KNAN20104-E 250

L

log

common message 181
 files and directory list 184
 integrated trace 181
 process-by-process trace 184
 types of information 181

log file size, managing 27
 login user list, displaying 118
 logoff 54
 logon 50
 using GUI 50

M

maintenance 1
 management information, importing and
 exporting 167
 managing
 configuration information 2
 configuration of virtual system 176
 databases 11
 disk capacity 26
 hosts 144
 profiles 155
 service operation status 164
 mathematical expression conventions xi
 MB meaning xii
 memo entries, editing 89
 migrating configuration information and
 databases 31
 monitor window 98
 opening, for application that issued JP1
 events 98
 monitored object database
 backing up 14
 procedures for backing up and recovering 14
 re-creating 18
 recovering 14
 reorganizing 11
 monitoring
 from Monitoring Tree window 112
 from Visual Monitoring window 119
 monitoring nodes
 changing monitoring status of 114, 121
 changing status of 113, 120
 displaying attributes of 116, 123

- searching for 114, 122
 - monitoring system based on JP1 events 56
 - monitoring tree
 - changing monitoring status of monitoring nodes in 114
 - changing status of monitoring nodes in 113
 - displaying attributes of monitoring nodes in 116
 - displaying guide information in 117
 - searching for monitoring nodes in 114
 - searching for status-change events in 115
 - Monitoring Tree window
 - monitoring from 112
 - opening, from Visual Monitoring window 120
 - saving information in 118
- N**
- notes on
 - starting JP1/IM - Manager 47
 - stopping JP1/IM - Manager 47
- O**
- opening
 - monitor window for application 98
 - Monitoring Tree window from Visual Monitoring window 120
 - other application windows from Tool Launcher 139
 - Visual Monitoring window 117
 - operation content
 - checking (UNIX) 246
 - checking (Windows) 241
 - operations
 - changing event severity 87
 - displaying detailed JP1 event information 62
 - displaying extended attributes of JP1 events 64
 - displaying login user list 118
 - enabling view filter 99
 - logoff 54
 - logon 50
 - monitoring system based on JP1 events 56
 - opening monitor window 98
 - opening Visual Monitoring window 117
 - saving information in Monitoring Tree window on local host 118
 - searching for JP1 events 90
 - searching for monitoring nodes 122
 - searching for monitoring nodes from monitoring tree 114
 - setting response status for event search 96
 - starting JP1/IM - Manager 42
 - stopping JP1/IM - Manager 45
 - switching event acquisition filter 100
 - Tool Launcher window 140
 - using command to log on 52
 - using GUI to log on 50
 - outputting information displayed in JP1/IM - View to CSV file 108
- P**
- problem report, collecting 242
 - procedures
 - changing IM database port 23
 - expanding IM database size 21
 - troubleshooting 180
 - process status, checking 236, 242
 - profiles
 - collecting 155
 - collecting list of 157
 - displaying 158
 - managing 155
- R**
- re-creating
 - command execution log 17
 - databases 17
 - event database 19
 - host information database 18
 - monitored object database 18
 - re-executing automated actions 136
 - recovering 12
 - command execution log 12
 - configuration information (UNIX) 10
 - configuration information (Windows) 6
 - database 12
 - event database 16

- host information database 15
- IM database 16
- monitored object database 14
- regular expression, using 93
- remote host, executing commands on 126
- reorganizing 11
 - command execution log 11
 - event database 11
 - host information database 11
 - IM database 11
 - monitored object database 11
- repeated events, displaying 70, 71
- response status of
 - consolidated events, changing 75
 - events, changing 68
 - JP1 events, displaying 68
 - repeated events, changing 75
- rule startup request
 - checking status of 80
 - making 80

S

- saving information in Monitoring Tree window on local host 118
- search method (JP1 events) 90
- search results of JP1 events, displaying 93
- searching
 - JP1 events 90
 - monitoring nodes 114, 122
 - status-change events 122
 - status-change events from monitoring tree 115
- service operation information
 - displaying 165
 - managing 164
- setting response status of severe events 85
- settings information, changing 34
- settings of host on which JP1/IM runs, changing 35
- severe events
 - deleting 85
 - displaying only 69
 - setting response status of 85
- starting
 - JP1/IM - Manager 42

- notes on 47
- status-change events, searching 115, 122
- stopping
 - JP1/IM - Manager 45
 - notes on 47
- symbol conventions ix
- syntax conventions x
- system clock that is slower than current time, setting forward 40
- system date/time
 - change, necessary tasks as a result of 38
 - returning, to past 38
- system hierarchies
 - applying 153
 - collecting information of 148
 - displaying 149
 - editing 150
 - managing 143, 148
 - synchronizing 153
 - verifying 149
- system monitoring from Central Console 55

T

- TB meaning xii
- Tool Launcher
 - functions that can be operated from 141
 - opening other application windows from 139
 - operations in 140
- troubleshooting 179
 - corrective actions 247
 - data collection method 236
 - data that needs to be collected 209
 - log information types 181
 - procedure 180

U

- user dump, collecting 241
- user who executes commands 127

V

- version number conventions xii
- view filter, enabling 99
- virtual host, registering 176

Index

virtual system

- displaying host information in 177
- exporting configuration information of 178
- managing configuration of 176

Visual Monitoring window

- changing monitoring status of monitoring nodes in 121
- changing status of monitoring nodes in 120
- displaying attributes of monitoring nodes from 123
- displaying guide information from 123
- monitoring from 119
- opening 117
- opening Monitoring Tree window from 120
- searching for monitoring nodes in 122
- searching for status-change events in 122

W

Web version of JP1/IM - View 51

Reader's Comment Form

We would appreciate your comments and suggestions on this manual. We will use these comments to improve our manuals. When you send a comment or suggestion, please include the manual name and manual number. You can send your comments by any of the following methods:

- Send email to your local Hitachi representative.
- Send email to the following address:
WWW-mk@itg.hitachi.co.jp
- If you do not have access to email, please fill out the following information and submit this form to your Hitachi representative:

Manual name:	
Manual number:	
Your name:	
Company or organization:	
Street address:	
Comment:	

(For Hitachi use)
