

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

**Overview and System Design Guide**

3020-3-R76-01(E)

## ■ Relevant program products

For details about the supported operating system versions and prerequisite service packs and patches for Job Management Partner 1/Integrated Management - Manager and Job Management Partner 1/Integrated Management - View, see the *Release Notes* accompanying each program product.

P-242C-6H97 Job Management Partner 1/Integrated Management - View 09-00 (for Windows Server 2003 and Windows XP Professional)

P-2A2C-6H97 Job Management Partner 1/Integrated Management - View 09-00 (for Windows Server 2008 and Windows Vista)

P-242C-8E97 Job Management Partner 1/Integrated Management - Manager 09-00 (for Windows Server 2003)

P-2A2C-8E97 Job Management Partner 1/Integrated Management - Manager 09-00 (for Windows Server 2008)

P-9D2C-8E92 Job Management Partner 1/Integrated Management - Manager 09-00 (for Solaris)

P-1M2C-8E92 Job Management Partner 1/Integrated Management - Manager 09-00 (for AIX)

## ■ 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/pcrc/

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-R76-01(E)): November 2009

#### ■ Copyright

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





---

# Preface

---

This manual provides an overview and describes the functionality and system design of 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*.

The JP1/IM series includes a number of other program products, which are mentioned in this manual as outlined in the table below. For further details, see the documentation accompanying the product.

Product name	Contents covered in this manual
JP1/IM - Rule Operation	<ul style="list-style-type: none"><li>• The role of JP1/IM - Rule Operation within the JP1/IM series</li><li>• An overview of the JP1/IM - Rule Operation linkage function</li></ul>
JP1/IM - Event Gateway for Network Node Manager i	<ul style="list-style-type: none"><li>• The role of JP1/IM - Event Gateway for Network Node Manager i within the JP1/IM series</li></ul>

## Intended readers

This manual is intended for those responsible for managing and operating the management infrastructure for an open-platform system using JP1/IM. Specifically, this manual is intended for:

- System administrators, system designers, and operators who want to centrally manage the events occurring in the system and take some form of action to resolve them.
- System administrators, system designers, and operators who want to centrally monitor the system management infrastructure by associating its status with events occurring in the system.

## Organization of this manual

This manual is organized into the following parts:

### *PART 1: Overview*

This part provides an overview of the JP1/IM series and JP1/IM - Manager.

### *PART 2: Functionality*

This part describes the functionality of JP1/IM.

### *PART 3: Design*

This part describes the requirements for the monitoring tasks supported by JP1/IM and the system requirements for achieving those objectives.

## **Related publications**

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

### JP1/IM-related

- *Job Management Partner 1/Integrated Management - Manager Quick Reference* (3020-3-R75(E))
- *Job Management Partner 1/Integrated Management - Manager Configuration Guide* (3020-3-R77(E))
- *Job Management Partner 1/Integrated Management - Manager Administration Guide* (3020-3-R78(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))

### JP1-related

- *Job Management Partner 1/Performance Management Planning and Configuration Guide* (3020-3-R31(E))
- *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))
- *Job Management Partner 1/Automatic Job Management System 3 Linkage Guide* (3020-3-S12(E))

- *Job Management Partner 1/Automatic Job Management System 2 Linkage Guide*  
(3020-3-K27(E))

## Conventions: Abbreviations

This manual uses the following abbreviations for the names of Hitachi 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
		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 later
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

Abbreviation		Full name or meaning
	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		Job Management Partner 1/Automatic Job Management System 2 - 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
JP1/FTP		Job Management Partner 1/File Transmission Server/FTP
JP1/Integrated Management or JP1/IM	Version 7 products	
	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
	Version 8 products	
	JP1/IM - Manager	Job Management Partner 1/Integrated Management - Manager
	JP1/IM - Rule Operation or JP1/IM - RL <sup>#</sup>	Job Management Partner 1/Integrated Management - Rule Operation
	JP1/IM - View	Job Management Partner 1/Integrated Management - View
	Version 9 products	

Abbreviation		Full name or meaning
	JP1/IM - Event Gateway for Network Node Manager i or JP1/IM - EG for NNMi <sup>#</sup>	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
	JP1/PA - View	Job Management Partner 1/Performance Analysis - View
		Job Management Partner 1/Performance Management - Analysis View
JP1/PFM	JP1/PFM - Agent	Job Management Partner 1/Performance Management - Agent for Platform, and other agent product names
	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

Abbreviation		Full name or meaning
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
		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 Enterprise

Abbreviation	Full name or meaning
	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

#: In this manual, only the JP1/IM - Rule Operation and JP1/IM - Event Gateway for Network Node Manager i functionality related to JP1/IM - Manager and JP1/IM - View is described in broad outline.

- *Windows* is sometimes used generically, referring to Windows 2000, Windows XP Professional, Windows Server 2003, Windows Vista, Windows Server 2008, and Windows Server 2008 (IPF).
- *UNIX* is sometimes used generically, referring to HP-UX, Solaris, and AIX.

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

<b>Abbreviation</b>	<b>Full name or meaning</b>
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
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: Default installation folders of the Windows version of JP1/IM and JP1/Base

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

Product name	Installation folder notation	Default installation folder <sup>#</sup>
JP1/IM - View	<i>view-path</i>	<i>system-drive</i> : \Program Files\HITACHI\JP1CoView
JP1/IM - Manager	<i>manager-path</i>	<i>system-drive</i> : \Program Files\HITACHI\JP1IMM
	<i>console-path</i>	<i>system-drive</i> : \Program Files\HITACHI\JP1Cons
	<i>scope-path</i>	<i>system-drive</i> : \Program Files\HITACHI\JP1Scope
JP1/Base	<i>base-path</i>	<i>system-drive</i> : \Program Files\HITACHI\JP1Base

<sup>#</sup>: Represents the installation folder when the product is installed in the default location.

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

## Conventions: Diagrams

This manual uses the following conventions in diagrams:

● Computer



● Server



● File



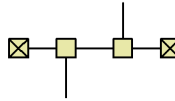
● Window



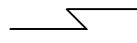
● Network



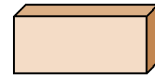
● LAN



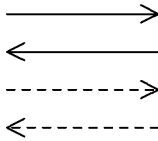
● Communication line



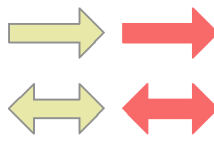
● Program



● Flow of control



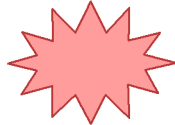
● Flow of data



● 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
<b>Bold</b>	Bold type indicates text on a window, other than the window title. Such text includes menus, menu options, buttons, radio box options, or explanatory labels. For example, bold is used in sentences such as the following: <ul style="list-style-type: none"> <li>From the <b>File</b> menu, choose <b>Open</b>.</li> <li>Click the <b>Cancel</b> button.</li> <li>In the <b>Enter name</b> entry box, type your name.</li> </ul>
<i>Italics</i>	Italics are used to indicate a placeholder for some actual text provided by the user or system. Italics are also used for emphasis. For example: <ul style="list-style-type: none"> <li>Write the command as follows: <i>copy source-file target-file</i></li> <li>Do <i>not</i> delete the configuration file.</li> </ul>
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"> <li>At the prompt, enter <code>dir</code>.</li> <li>Use the <code>send</code> command to send mail.</li> <li>The following message is displayed: <code>The password is incorrect.</code></li> </ul>

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.
<b>SD</b>	Bold code-font characters indicate the abbreviation for a command.
<u>perm</u>	Underlined characters indicate the default value.
[ ]	Square brackets enclose an item or set of items whose specification is optional.

Example font or symbol	Convention
	Only one of the options separated by a vertical bar can be specified at the same time.
...	An ellipsis (...) indicates that the item or items enclosed in ( ) or [ ] immediately preceding the ellipsis may be specified as many times as necessary.
( )	Parentheses indicate the range of items to which the vertical bar ( ) or ellipsis (...) is applicable.
{ }	One of the items enclosed in curly brackets and separated by a vertical bar must be specified.

## Conventions: KB, MB, GB and TB

This manual uses the following conventions:

- 1 KB (kilobyte) is 1,024 bytes.
- 1 MB (megabyte) is 1,024<sup>2</sup> bytes.
- 1 GB (gigabyte) is 1,024<sup>3</sup> bytes.
- 1 TB (terabyte) is 1,024<sup>4</sup> bytes.

## Conventions: Mathematical expressions

This manual uses the following symbols in mathematical expressions:

Symbol	Meaning
x	Multiplication sign
/	Division sign

## Conventions: Meaning of "Administrators permissions"

In this manual, *Administrators permissions* refers to Administrators permissions for the local PC. The local user, domain user, or user of the Active Directory environment can perform tasks requiring Administrators permissions if granted Administrators permissions for the local PC.

## Conventions: Version numbers

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

- Version 1.00 (or 1.0) is written as 01-00.
- Version 2.05 is written as 02-05.

- Version 2.50 (or 2.5) is written as 02-50.
- Version 12.25 is written as 12-25.

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

## Online manual

JP1/IM comes with an HTML manual that you can read in either of the following Web browsers:

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

The HTML manual has the same contents as this manual.

To view the HTML manual:

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

*Note:*

- Depending on the OS settings, the HTML manual might appear in the active window when opened from the **Start** menu.



---

# Contents

---

<b>Preface</b>	<b>i</b>
Intended readers .....	i
Organization of this manual .....	i
Related publications .....	ii
Conventions: Abbreviations .....	iii
Conventions: Default installation folders of the Windows version of JP1/IM and JP1/Base .....	ix
Conventions: Diagrams .....	ix
Conventions: Fonts and symbols .....	x
Conventions: KB, MB, GB and TB .....	xii
Conventions: Mathematical expressions .....	xii
Conventions: Meaning of "Administrators permissions" .....	xii
Conventions: Version numbers .....	xii
Online manual .....	xiii

## **PART 1: Overview**

<b>1. Overview of JP1/Integrated Management</b>	<b>1</b>
1.1 Introducing the JP1/IM series .....	2
1.2 System management issues and integrated management .....	4
1.2.1 System life cycle .....	4
1.2.2 Issues and the role of the JP1/IM series at the design and build phase .....	5
1.2.3 Issues and the role of the JP1/IM series at the operation phase .....	6
1.2.4 Issues and the role of the JP1/IM series at the redesign and rebuild phase .....	8
1.3 Features of JP1/IM - Manager .....	10
1.3.1 Integrated management using JP1 events .....	10
1.3.2 Centralized system monitoring .....	11
1.3.3 Error detection and reporting .....	13
1.3.4 Integrated troubleshooting with JP1/IM - Manager .....	14
1.3.5 Easy-to-build monitoring system .....	15
1.3.6 Flexible system configuration .....	15
1.3.7 Integrated management of the system hierarchy and host settings .....	16
1.4 System operation with JP1/IM - Manager .....	18
1.4.1 System monitoring .....	19
1.4.2 Error detection .....	21
1.4.3 Error investigation .....	21
1.4.4 Error resolution .....	26

1.5 JP1/IM - Manager system configuration .....	28
1.5.1 Component products of a JP1/IM - Manager system .....	28
1.5.2 JP1/IM system hierarchy .....	29
1.5.3 Support for various system configurations .....	31

## **PART 2: Functionality**

### **2. Overview of Functions** 33

2.1 Overview of event management .....	34
2.2 Functionality at each phase of the operating cycle .....	36
2.2.1 Functionality for system monitoring .....	36
2.2.2 Functionality for error detection .....	37
2.2.3 Functionality for error investigation and resolution .....	38
2.2.4 Functionality for building, operating, and rebuilding the system .....	39
2.2.5 Functionality used throughout the operating cycle .....	41
2.3 List of functions .....	43
2.4 Functions provided by the IM database .....	49

### **3. Centralized System Monitoring Using the Central Console** 51

3.1 Centralized monitoring using JP1 events .....	52
3.1.1 Monitoring from the Central Console .....	53
3.1.2 Flow of processing for JP1 event monitoring .....	59
3.1.3 Internal control of JP1 events by JP1/IM - Manager .....	61
3.2 Filtering of JP1 events .....	64
3.2.1 Forwarding filter .....	66
3.2.2 Event acquisition filter .....	67
3.2.3 Event receiver filter .....	69
3.2.4 Severe events filter .....	69
3.2.5 View filter .....	70
3.2.6 Defining filter conditions .....	70
3.3 Issue of correlation events .....	74
3.3.1 Correlation event issue .....	77
3.3.2 Defining correlation event issue .....	94
3.3.3 Status transition and operation settings of the correlation event generation function .....	99
3.3.4 Contents of a correlation event generation history file .....	100
3.3.5 JP1 events subject to correlation processing .....	105
3.3.6 Situations in which a generation condition is satisfied or fails .....	105
3.3.7 Situations in which correlation processing fails .....	106
3.3.8 Issued correlation event .....	107
3.4 Consolidated display of repeated events .....	109
3.4.1 Consolidated display of JP1 events .....	110
3.4.2 Example of consolidation processing of repeated events .....	112



3.5	Searching for events .....	115
3.5.1	Searching for JP1 events .....	115
3.5.2	Event search conditions.....	117
3.5.3	Flow of processing of event searching.....	118
3.6	Event guide function.....	121
3.6.1	Settings for event guide information.....	122
3.6.2	Conditions for displaying event guide information.....	123
3.6.3	Contents displayed as event guide information.....	124
3.7	Setting memo entries .....	126
3.8	Displaying user-defined event attributes .....	127
3.8.1	Displaying the attributes of user-defined events .....	127
3.8.2	Displaying a monitor window from a JP1 event .....	127
3.8.3	Adding items to the Tool Launcher window .....	127
3.8.4	Flow of event information.....	127
3.9	CSV output of information displayed in JP1/IM - View .....	129
3.9.1	Saving event listings (CSV snapshot) .....	129
3.9.2	Saving event information in the integrated monitoring database (CSV report).....	134
3.9.3	Copying JP1 event information and action execution results to the clipboard .....	140
3.10	Specifying the event display start-time .....	145
3.10.1	Specifiable range of event display start-time positions.....	145
3.10.2	Specifying the event display start-time position using the slider.....	149
3.10.3	Specifying the event display start-time position by date and time.....	149
3.10.4	Specifying the event display start-time position using the buttons .....	149
3.10.5	Processing after event display start-time specification .....	150
3.11	Specifying the event display period.....	151
3.11.1	Range of listed JP1 events for a specified display period .....	151
3.12	Performing system operations from JP1/IM.....	154
3.12.1	Launching a linked product by monitor startup .....	154
3.12.2	Tool Launcher.....	157
3.12.3	Executing commands from JP1/IM - View .....	160
<b>4.</b>	<b>Objective-Oriented System Monitoring Using the Central Scope .....</b>	<b>167</b>
4.1	Overview of Central Scope functions.....	168
4.2	Monitoring tree.....	172
4.2.1	Monitoring tree structure.....	172
4.2.2	Statuses of monitoring nodes .....	173
4.2.3	Status change conditions .....	176
4.2.4	Event generation condition.....	183
4.3	Automatically generating a monitoring tree.....	186
4.3.1	Automatically generating a monitoring tree.....	186
4.3.2	Conditions for automatically generating a monitoring tree .....	187
4.3.3	Monitoring tree structures .....	189

4.3.4	Generation types .....	191
4.4	Editing a monitoring tree .....	195
4.4.1	Editing a monitoring tree .....	195
4.4.2	Map display settings .....	197
4.4.3	Setting the monitoring range of a monitoring tree .....	198
4.4.4	Setting the Central Scope monitoring windows .....	203
4.5	Visual monitoring .....	206
4.6	Searching for monitoring nodes or status change events .....	207
4.6.1	Searching for monitoring nodes .....	207
4.6.2	Searching for status change events .....	207
4.7	Guide function .....	214
4.7.1	Settings for guide information .....	215
4.7.2	Utilizing guide information tailored to the system operation .....	219
4.8	Completed-action linkage function .....	222
4.8.1	Behavior of the completed-action linkage function .....	222
4.8.2	Disabling the completed-action linkage function .....	225
4.8.3	Automatically deleting processed status change events .....	226
4.9	Performing system operations from JP1/IM .....	229
4.9.1	Tool Launcher .....	229
4.10	Central Scope .....	230
4.10.1	Overview of the Central Scope .....	230
4.10.2	Host information .....	230
4.10.3	System monitoring using the Central Scope .....	232
4.10.4	Automatic generation of a monitoring tree .....	234
4.10.5	Central Scope databases .....	235
<b>5.</b>	<b>Command Execution by Automated Action .....</b>	<b>237</b>
5.1	Overview of automated actions .....	238
5.2	Managing the status of automated actions .....	240
5.3	Defining an automated action .....	246
5.3.1	Items that can be specified as execution conditions .....	247
5.3.2	Precedence of execution conditions .....	250
5.3.3	Parameter groups and AND condition .....	251
5.3.4	Inherited event information .....	252
5.4	Specifying a command to be executed as an automated action .....	255
5.4.1	Executable commands .....	255
5.4.2	Target host .....	255
5.4.3	User account .....	255
5.4.4	Suppressing identical actions .....	256
5.5	Monitoring the execution of an automated action .....	260
5.5.1	Automated action delay monitoring .....	260
5.5.2	Automated action status monitoring .....	261
5.5.3	Setting up execution monitoring .....	261

5.5.4 Automated action error monitoring using the execution monitoring function .....	262
5.6 Checking the execution status and results of automated actions .....	263
5.7 Canceling automated actions .....	264
5.8 Re-executing an automated action .....	266
5.9 Operation settings for automated actions .....	267
5.10 Flow of automated action execution .....	268
<b>6. System Hierarchy Management Using IM Configuration Management .....</b>	<b>273</b>
6.1 Host management .....	274
6.1.1 Host information managed by IM Configuration Management .....	274
6.1.2 Registering hosts .....	277
6.1.3 Collecting host information .....	280
6.1.4 Displaying host information .....	285
6.1.5 Changing host information .....	285
6.1.6 Deleting hosts .....	288
6.2 System hierarchy management .....	291
6.2.1 Hierarchical configurations managed by IM Configuration Management .....	291
6.2.2 Acquiring the system hierarchy .....	296
6.2.3 Displaying the system hierarchy .....	298
6.2.4 Verifying the system hierarchy .....	299
6.2.5 Editing the system hierarchy .....	302
6.2.6 Applying the system hierarchy .....	306
6.2.7 Synchronizing the system hierarchy .....	308
6.3 Profile management .....	311
6.3.1 Types of profiles that can be managed .....	311
6.3.2 Collecting profile lists .....	314
6.3.3 Collecting profiles .....	317
6.3.4 Displaying profiles .....	324
6.3.5 Editing configuration files .....	326
6.3.6 Obtaining and releasing exclusive editing rights for a configuration file .....	330
6.4 Management of service activity information .....	332
6.4.1 Services whose activity information can be obtained .....	332
6.4.2 Collecting service activity information .....	332
6.4.3 Displaying service activity information .....	335
6.5 Importing and exporting IM Configuration Management information .....	337
6.5.1 Types of information that can be imported or exported .....	337
6.5.2 Exporting IM Configuration Management information .....	339
6.5.3 Importing IM Configuration Management information .....	341
6.6 Virtualization configuration management .....	343
6.6.1 Setting virtual host information .....	343
6.6.2 Displaying a virtualization configuration .....	343
6.6.3 Importing a virtualization configuration to Central Scope .....	344

<b>7. JP1/IM Operation Control</b>	<b>347</b>
7.1 JP1/IM - Manager process management.....	348
7.1.1 Restarting abnormally ended processes.....	349
7.1.2 Issuing JP1 events at detection of process errors .....	350
7.2 JP1/IM - Manager health check function.....	352
7.2.1 Processes monitored by the health check function.....	353
7.2.2 Enabling and disabling the health check function .....	354
7.2.3 How the health check function works .....	354
7.3 Communication performed in the JP1/IM system environment .....	358
7.3.1 Communication between the viewer and manager.....	358
7.3.2 Communication between the manager and authentication server .....	359
7.3.3 Communication between the manager and agent .....	359
7.3.4 Communicating within a local host .....	362
7.3.5 Communicating with JP1/IM - Rule Operation.....	363
7.4 Core functionality provided by JP1/Base .....	364
7.4.1 Managing JP1 users .....	364
7.4.2 Managing JP1 events using JP1/Base.....	368
7.4.3 Managing the system hierarchy .....	375
7.4.4 Managing command execution.....	378
7.4.5 Collecting and distributing definition information.....	390
7.4.6 Managing service startup (Windows only).....	393
7.4.7 Hitachi Network Objectplaza Trace Library (HNTRLib2) .....	394
7.4.8 JP1/Base health check function .....	394
7.4.9 JP1/Base process management .....	397
<b>8. Linking with the JP1/IM Series</b>	<b>399</b>
8.1 Linking with JP1/IM - Rule Operation .....	400
8.1.1 Sending rule startup requests to JP1/IM - Rule Operation .....	400
8.1.2 Checking the status and result of notification to JP1/IM - Rule Operation .....	404
8.1.3 Monitor startup of JP1/IM - Rule Operation .....	406
<b>9. JP1/IM Configuration</b>	<b>407</b>
9.1 JP1/IM configuration example.....	408
9.2 Product structure .....	409
9.2.1 JP1/IM product structure .....	409
9.2.2 Connectivity between JP1/IM products.....	410
9.3 Prerequisite operating systems and programs.....	412
9.3.1 Prerequisite operating systems .....	412
9.3.2 Prerequisite programs .....	413
9.4 Support for various system configurations .....	414
9.4.1 Firewall support.....	414
9.4.2 Support for multiple LANs.....	414
9.4.3 Operation in a cluster system.....	414

9.4.4 Logical host operation in a non-cluster environment.....	415
--	-----

## **PART 3: Design**

<b>10. Overview of Design</b> .....	<b>417</b>
10.1 Flow of JP1/IM deployment.....	418
10.2 Design considerations.....	419
10.3 Overview of design for JP1/IM deployment .....	421
10.3.1 Overview of design .....	421
10.3.2 Designing monitoring.....	421
10.3.3 Designing error detection and reporting.....	424
<b>11. Operation Management Design</b> .....	<b>427</b>
11.1 Considerations for system monitoring using JP1 events .....	428
11.1.1 Considerations for event management using JP1 events.....	428
11.1.2 Considerations for forwarding JP1 events to managers .....	429
11.1.3 Considerations for filtering JP1 events .....	430
11.1.4 Considerations for issuing correlation events.....	436
11.1.5 Considerations for consolidated display of repeated events.....	451
11.1.6 Considerations for changing JP1 event levels .....	456
11.1.7 Considerations for setting event guide information .....	459
11.1.8 Considerations for saving monitoring information (CSV snapshot).....	464
11.1.9 Considerations for saving event information in the integrated monitoring database (output of event report) .....	465
11.2 Considerations for system monitoring from the Central Scope.....	466
11.2.1 Considerations for monitoring trees .....	466
11.2.2 Considerations for visual monitoring .....	468
11.2.3 Considerations for setting guide information.....	469
11.2.4 Considerations for defining a status change condition for a monitoring group .....	470
11.3 Considerations for error investigation in JP1/IM .....	475
11.3.1 Monitor startup .....	475
11.3.2 Tool Launcher.....	475
11.3.3 Considerations for executing commands from JP1/IM - View .....	475
11.4 Considerations for automated actions.....	478
11.5 Considerations for managing the system hierarchy.....	485
<b>12. JP1/IM System Design</b> .....	<b>487</b>
12.1 Operating environment considerations.....	488
12.1.1 Prerequisite operating systems and patches .....	488
12.1.2 Estimating memory and disk space requirements .....	488
12.1.3 Estimating IM database capacity requirements.....	488
12.1.4 Adjusting kernel parameters (in UNIX).....	491

12.1.5	Language environment considerations .....	491
12.1.6	Operation in a multi-language environment.....	491
12.2	Upgrading from a previous version of JP1/IM .....	496
12.2.1	Upgrading from version 8 JP1/IM - Manager products .....	496
12.2.2	Upgrading from JP1/IM - View version 8 .....	501
12.2.3	Upgrading from version 7 JP1/IM - Manager products .....	502
12.2.4	Upgrading from JP1/IM - View version 7 .....	504
12.2.5	Upgrading from JP1/Base version 8 .....	505
12.2.6	Upgrading from JP1/Base version 7 .....	505
12.2.7	Upgrading from JP1/Base version 6 .....	505
12.3	Designing the system configuration .....	506
12.3.1	Basic configuration.....	506
12.3.2	Configuration with JP1/AJS for monitoring job execution.....	508
12.3.3	Configuration with HP NNM for monitoring the network.....	509
12.3.4	Configuration for monitoring JP1 events from a Web browser.....	512
12.3.5	Configuration for monitoring the status of a Cosminexus system environment.....	513
12.3.6	Configuration with JP1/IM - Rule Operation .....	515
12.3.7	Configuration for operation in a cluster system .....	517
12.3.8	Configuration for operation on a logical host in a non-cluster environment.....	518
12.3.9	Configuration for differing product versions.....	519
12.4	Network considerations .....	522
12.4.1	Host names and IP addresses.....	522
12.4.2	Server network configuration .....	523
12.4.3	Operation in a configuration connected to multiple networks .....	524
12.4.4	Operation behind a firewall .....	524
12.4.5	WAN connection.....	525
12.5	Considerations for the system hierarchy.....	526
12.6	Considerations for user authentication .....	528
12.6.1	User authentication blocks.....	528
12.6.2	Access permissions of JP1 users .....	529
12.7	Considerations for the JP1/IM and JP1/Base environments.....	531
12.7.1	Selecting regular expressions .....	531
12.7.2	Troubleshooting in JP1/IM and JP1/Base.....	531
12.7.3	JP1/IM - Manager system environment.....	534
12.7.4	JP1 user environment.....	535
12.7.5	Issuing a JP1 event when a response status changes .....	536
12.7.6	Command execution environment.....	537
12.7.7	System design for using the Central Scope .....	539
12.7.8	Communication timeout period .....	540
12.7.9	JP1/IM - View environment .....	541
12.7.10	Event monitoring from the Web-based JP1/IM - View .....	541
12.7.11	Setting the event acquisition start location .....	542

12.8	Considerations for linking with other integrated management products.....	544
12.8.1	System design for linking with JP1/IM - Rule Operation.....	544
12.9	JP1/IM maintenance considerations.....	546
12.9.1	Backup requirements.....	546
12.9.2	Database maintenance considerations.....	546
12.9.3	Checking disk space.....	546
12.9.4	Use of failure reports.....	547
12.10	Considerations for JP1/IM system-wide maintenance.....	548
12.10.1	Preparatory tasks.....	548
12.10.2	Example of JP1/IM system-wide maintenance.....	550
12.10.3	Example of agent maintenance.....	556
<b>13.</b>	<b>Performance and Estimates</b> .....	<b>559</b>
13.1	JP1/IM processing performance.....	560
13.2	Model for performance evaluation.....	561
13.2.1	User requirements.....	562
13.2.2	Memory, disk capacity, and database capacity required on a monitoring server.....	566
13.2.3	Memory and disk capacity required on a monitor machine.....	567
<b>Appendixes</b>		<b>569</b>
A.	Files and Directories.....	570
A.1	Files and folders of JP1/IM - Manager (for Windows).....	571
A.2	Files and directories of JP1/IM - Manager (for UNIX).....	579
A.3	JP1/IM - View.....	588
B.	List of Processes.....	592
B.1	JP1/IM processes (Windows).....	592
B.2	JP1/IM processes (UNIX).....	595
C.	Port Numbers.....	598
C.1	Port numbers for JP1/IM.....	598
C.2	Direction of communication through a firewall.....	599
C.3	Connection status.....	600
D.	Limits.....	603
E.	Operating Permissions.....	613
E.1	Operating permissions required for system monitoring using the Central Console.....	614
E.2	Operating permissions required for system monitoring using the Central Scope.....	618
E.3	Operating permissions required for IM Configuration Management.....	629
F.	Support for Changing Communication Settings.....	631
G.	Regular Expressions.....	633
G.1	Types of regular expressions.....	633
G.2	Syntax of regular expressions.....	636
G.3	Comparison between types of regular expressions.....	638

G.4 Tips on using regular expressions .....	640
G.5 Examples of using regular expressions .....	641
H. Connectivity with Previous Versions .....	644
H.1 Connectivity with version 8 products .....	644
H.2 Connectivity with version 7 products .....	650
H.3 Connectivity with previous versions of JP1/Base .....	658
I. Performance and Estimation.....	662
I.1 Memory requirements .....	662
I.2 Disk space requirements.....	662
I.3 Network traffic volumes.....	662
J. Kernel Parameters .....	673
K. Version Changes.....	674
K.1 Changes in version 09-00 .....	674
K.2 Changes from version 07-00 to version 08-01 .....	677
K.3 Changes in version 07-11 .....	679
L. Glossary .....	682
<b>Index</b> .....	<b>701</b>

---



## **Chapter**

---

# **1. Overview of JP1/Integrated Management**

---

JP1/Integrated Management (JP1/IM) is a suite of programs for managing an entire corporate information system on an integrated basis. With the growing size and complexity of the systems underpinning an enterprise's business operations, management of the system operation is a vital issue. The JP1/IM series optimizes system operations management by offering integrated management tailored to objectives and integration of operational tasks.

This chapter provides an overview of the JP1/IM series, and describes the features and organization of JP1/IM - Manager, which provides the integrated management functionality central to the JP1/IM series.

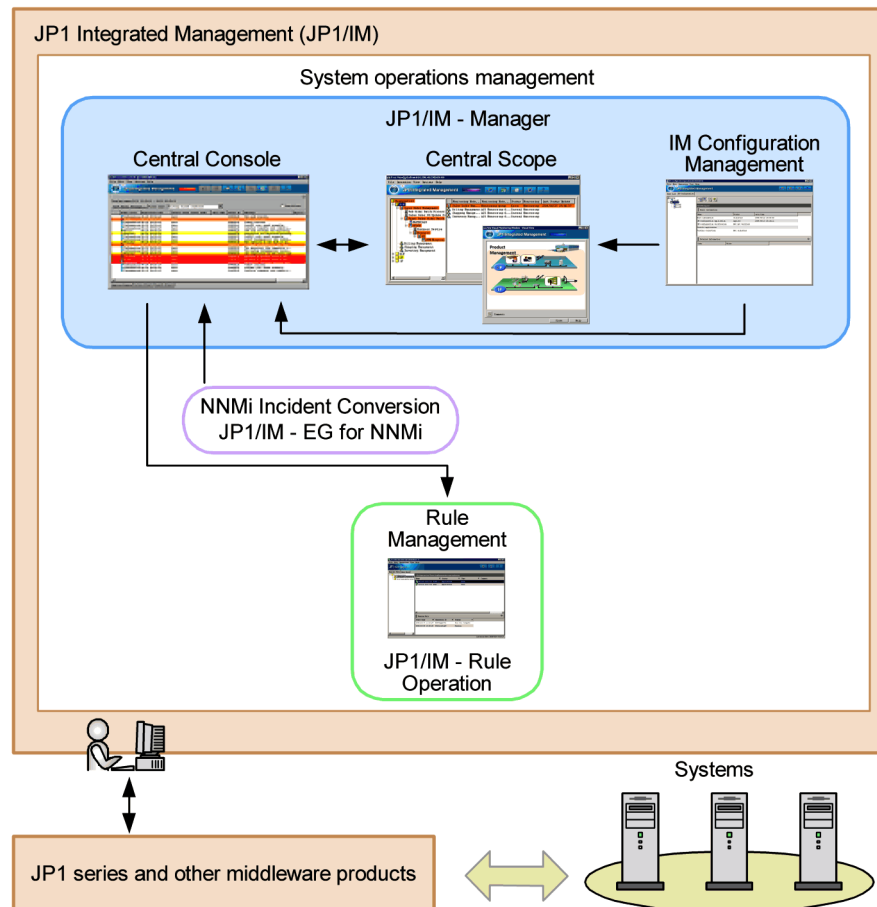
- 1.1 Introducing the JP1/IM series
- 1.2 System management issues and integrated management
- 1.3 Features of JP1/IM - Manager
- 1.4 System operation with JP1/IM - Manager
- 1.5 JP1/IM - Manager system configuration

## 1.1 Introducing the JP1/IM series

The JP1/IM series is a family of core products for realizing integrated management of an IT system. The JP1/IM products centrally manage information about the system's myriad resources, and enable centralized monitoring and operation across the entire IT system.

The JP1/IM series links with a wide range of middleware, including other JP1 products which provide job management and availability management functionality. Using JP1/IM, integrated system management can be realized through configuration and operations management on a system-wide basis.

Figure 1-1: Integrated system management by the JP1/IM series



The JP1/IM series optimizes system management by managing the configuration information created while planning and building the system, and the operational information generated during system operation. By providing a core platform for system management, JP1/IM offers full support for the entire workflow - from designing and building the system, through operation, redesign, and rebuild.

## 1.2 System management issues and integrated management

The need for system management as provided by the JP1/IM series stems from the various challenges that IT systems present as they become more sophisticated.

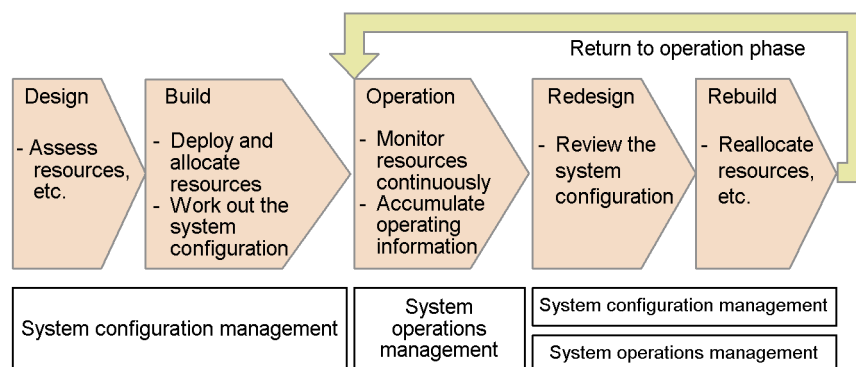
For many enterprises, IT systems are indispensable as the foundation of their business operations. Corporate IT systems are growing in scale and complexity to meet the various demands placed upon them. This in turn makes system management more onerous and costly. Optimizing system operations management is a vital concern.

### 1.2.1 System life cycle

An IT system comprises a diverse range of resources, including servers, networks, and other hardware, and software-based operations such as job execution and security monitoring.

To make proper use of these various resources, administrative tasks must be carried out on an ongoing basis. These include assessing and re-allocating resources, and quickly detecting and resolving any problems that occur in those resources. The workflow and processes involved in ensuring that the system runs reliably are referred to as the *system life cycle*. The system life cycle consists of five phases: system design, build, operation, redesign, and rebuild. The following figure shows the life cycle phases and associated administrative tasks.

Figure 1-2: System life cycle



As this figure shows, the administrative tasks differ at each phase of the system life cycle, as does the information that needs to be managed at each phase. The JP1/IM series optimizes management of system information at each phase of the system life cycle, and provides a framework of support for stable system operation.

The following describes system management issues and the role of the JP1/IM series at each phase of the system life cycle.

## 1.2.2 Issues and the role of the JP1/IM series at the design and build phase

At the design and build phase, you must first consider how to configure the system as a whole. Then you must plan how to deploy and build the resources needed for the processing that the system will perform. To fulfill these tasks, information about the system components needs to be properly managed. This is referred to as *system configuration management*.

The design and build phase is a repeated process of assessing resources, working out the system configuration, deploying resources, pre-operation testing and debugging.

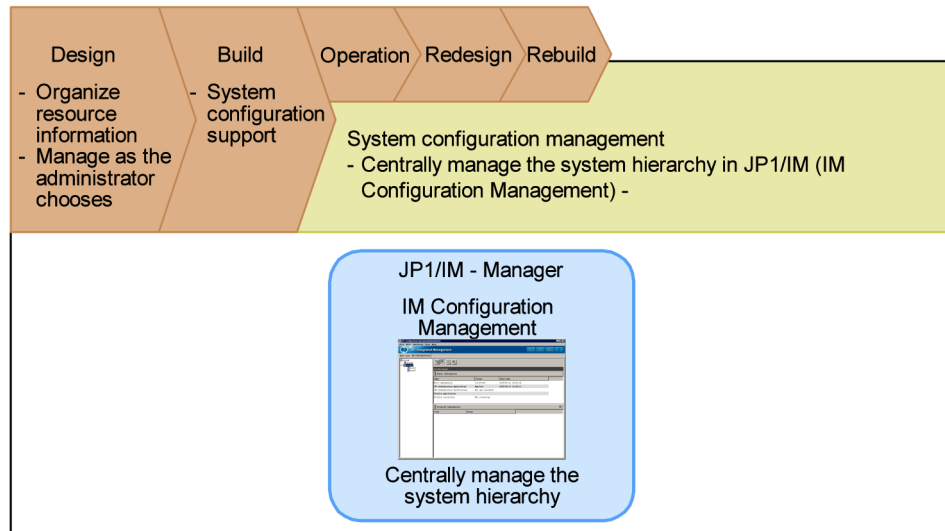
As the resources in a system grow in number, it becomes harder to keep track of them all. Managing the system configuration becomes ever more complex too.

The following table and figure describe the products that the JP1/IM series provides to support system configuration management.

*Table 1-1:* Products for system configuration management

Product	Functionality	Role
JP1/IM - Manager	IM Configuration Management	Provides support for configuring the system. From the manager host, you can centrally manage the hierarchical structure and host settings of the system managed by JP1/IM. To use IM Configuration Management, you must set up the IM Configuration Management database.

Figure 1-3: System configuration management



The JP1/IM series provides functionality for collecting all resource information in one location, where it can be organized and managed as the administrator chooses. The JP1/IM programs support system configuration management by facilitating the organization and classification of resource information in ways that the administrator finds easiest to manage. This functionality optimizes configuration management even in systems with huge volumes of resource information.

### 1.2.3 Issues and the role of the JP1/IM series at the operation phase

To ensure stable system operation during the operation phase, the resources configured in the system need to be monitored round the clock. Monitoring depends on proper management of system operating information and error information. This is referred to as *system operations management*.

In running a system, the processes of monitoring, error detection, investigation, and resolution are handled as a single ongoing cycle.

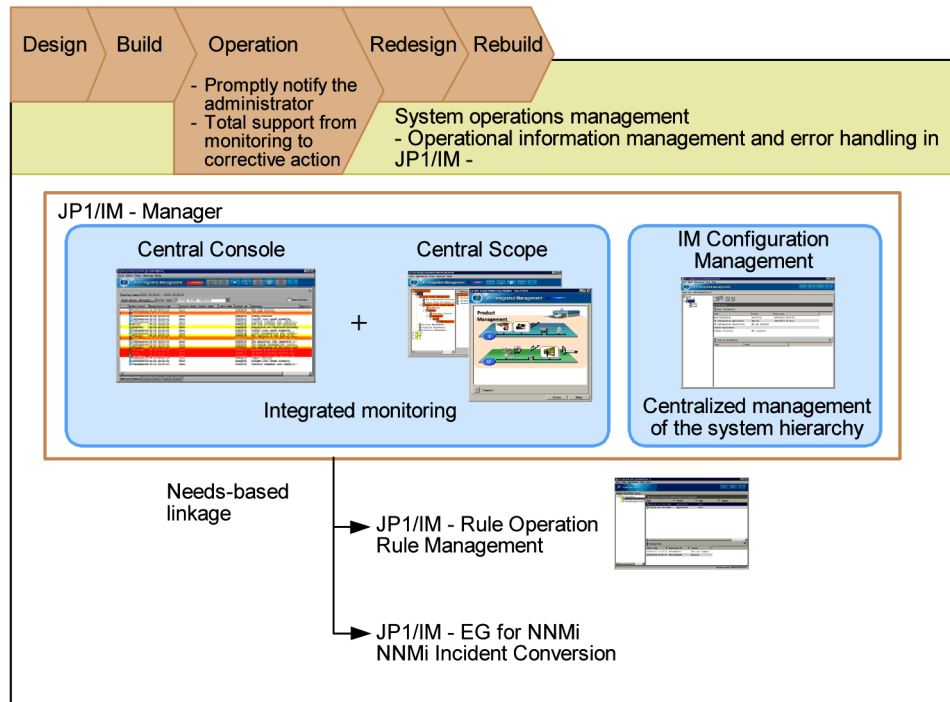
As a system grows in size and complexity, it becomes exponentially more difficult to perform the tasks involved in this operational cycle. The administrator is burdened with a growing workload, and requires a broad range of advanced skills to properly manage the vast array of resources. This puts huge demands on operations management, making the training of system administrators more challenging too.

The following table and figure describe the products that the JP1/IM series provides to support system operations management.

*Table 1-2:* Products for system operations management

<b>Product</b>	<b>Functionality</b>	<b>Role</b>
JP1/IM - Manager	Central Console	Centrally monitors the system as a whole using JP1 events. Integrates all aspects of the operating cycle, from event monitoring to error detection, investigation, and resolution.
	Central Scope	Centrally manages the system based on requirements set by the system administrator, enabling integrated objective-oriented system management.
	IM Configuration Management	Centrally manages, from the manager host, the hierarchical structure and the settings of each host in the system managed by JP1/IM.
JP1/IM - Rule Operation	Rule Management	Defines error-handling procedures and automatically executes actions based on the nature of the error.
JP1/IM - EG for NNMi	NNMi Incident Conversion	Converts NNMi incidents managed by NNMi into JP1 events.

Figure 1-4: System operations management



Note: Central Console can be linked with Rule Management.

The JP1/IM series provides a platform for round-the-clock system monitoring and immediate administrator notification if a problem occurs, as well as operational tasks such as error identification and investigation. The JP1/IM programs provides integrated operating cycle support, from monitoring through to troubleshooting. JP1/IM optimizes operations management even in large-scale, complex systems.

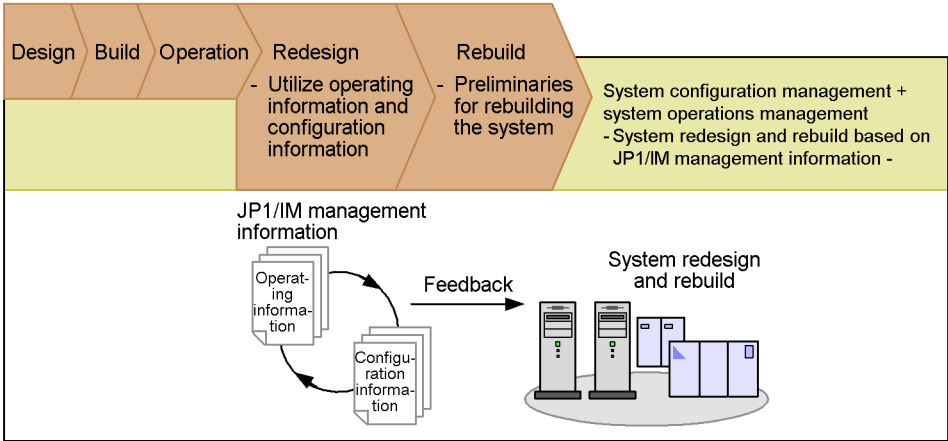
#### 1.2.4 Issues and the role of the JP1/IM series at the redesign and rebuild phase

The redesign and rebuild phase entails evaluating performance based on the system operating information, organizing the system configuration information as needed, and rethinking the system configuration.

You will need to redeploy resources if a particular resource is prone to frequent errors that affect job processing performance. Resource redeployment could have far-reaching effects, beyond the resources in the immediate environment. You will need a good understanding of the system configuration information created at the design and build phase, and you will need to select and deploy appropriate resources based on the operating information accumulated during the operation phase.



Figure 1-5: System rebuild



At the redesign and rebuild phase, the JP1/IM series assists the administrator by optimizing management of the configuration information created at the design and build phase, and the operating information generated at the operation phase, as discussed above. This helps to minimize the administrator's workload when redesigning and rebuilding the system, and maximizes use of the management information accumulated at the design, build, and operation phases.

## 1.3 Features of JP1/IM - Manager

In the previous sections we introduced the JP1/IM series as a whole. This section describes JP1/IM - Manager.

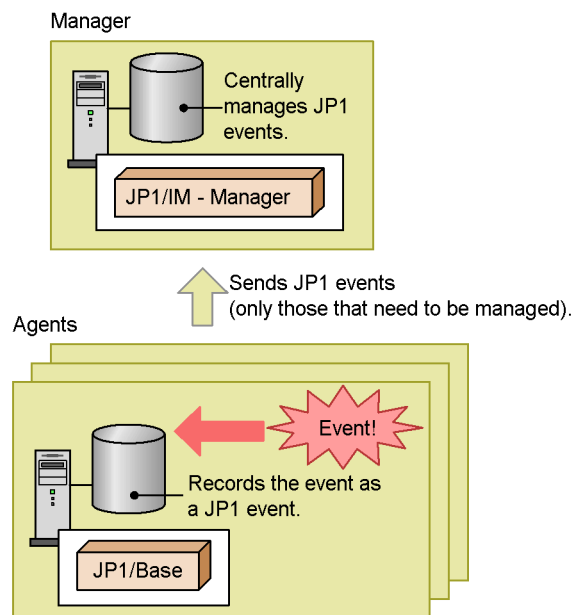
Through the features described below, JP1/IM - Manager integrates monitoring and operation into a unified management process. By simplifying complex tasks, JP1/IM - Manager reduces the workload involved in running a system.

### 1.3.1 Integrated management using JP1 events

JP1/IM - Manager centrally manages the various events that occur in the system as JP1 events. Events generated by JP1/Base, which provides the core functionality for integrated management, are managed by the agent hosts in the system as JP1 events. The agents forward JP1 events to JP1/IM - Manager for centralized management as needed.

Alternatively, JP1 events accumulated at an agent can be acquired by JP1/IM - Manager and managed at the JP1/IM - Manager side.

*Figure 1-6: Integrated management using JP1 events*



Implementing integrated management by simply collecting all JP1 events would result in a deluge of events across the system. Severe events could easily be overlooked, making operations management more difficult. Too many events would also place a

greater load on the monitoring system. Using event filtering, JP1/IM - Manager selects only those events relevant to operations management, allowing JP1 events to be managed appropriately. The filtering feature gives you various choices: You can select which events to send to JP1/IM - Manager, and which to treat as severe events.

In addition, JP1/IM - Manager can manage the following events:

- Various events converted by the JP1/Base event converter. These include messages in log files, entries in the Windows event log, and SNMP traps managed by HP NNM version 7.5 or earlier. JP1/IM - Manager can also manage events issued by a user application calling a command or the API.
- NNMi incidents converted into JP1 events by JP1/IM - EG for NNMi. For details about NNMi incidents, see the manual *Job Management Partner 1/Integrated Management - Event Gateway for Network Node Manager i Description, User's Guide and Reference*.
- Events handled by a wide variety of non-JP1 products and converted into JP1 events.

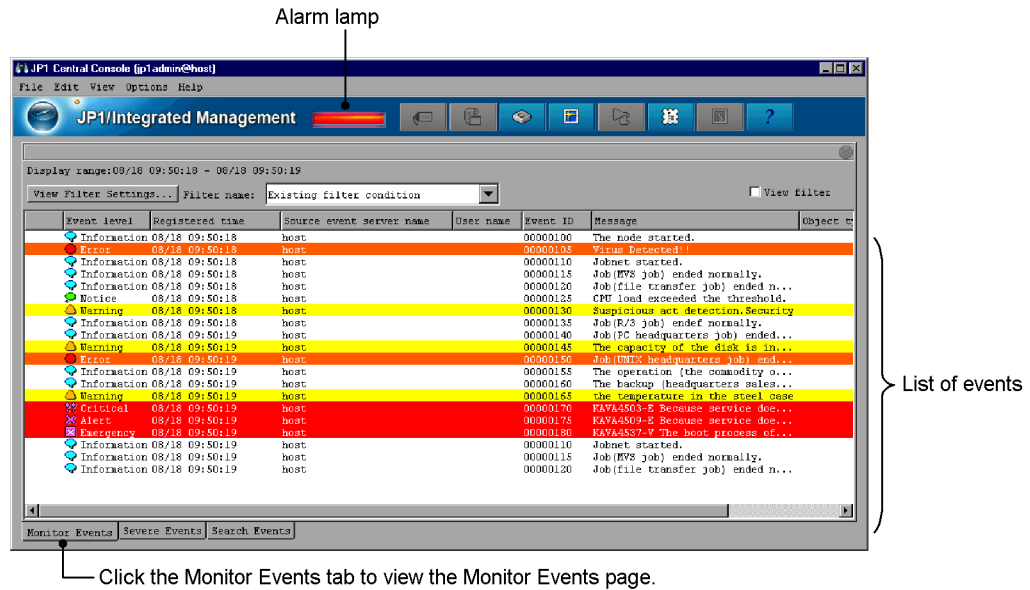
### 1.3.2 Centralized system monitoring

JP1/IM - Manager can centrally monitor the system in its entirety via the Central Console and Central Scope.

The Central Console centrally monitors events in the system by collecting JP1 events as they occur and displaying them in a time series. JP1 events are displayed on the **Monitor Events** page of the Event Console window, so you can monitor everything that is happening across the entire system.

## 1. Overview of JP1/Integrated Management

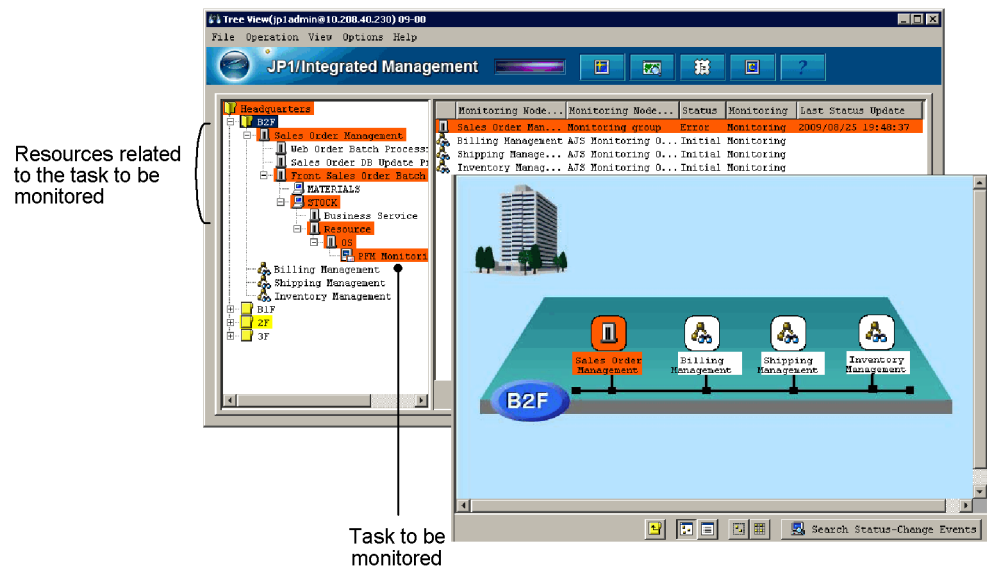
Figure 1-7: Event Console window (Monitor Events page)



Using the Central Scope, the administrator can centrally monitor the system from any chosen viewpoint. The entire system can be displayed in a tree view matched to your purpose, providing a visual understanding of the relationships between the tasks in progress and system resources. Essential monitoring points can also be mapped geographically, enabling centralized monitoring from the required viewpoints, no matter how large the system.

In the Monitoring Tree window, you can group resources and centrally monitor the system in a tree view. In the Visual Monitoring window, you have a map view of objects you selected in a monitoring tree.

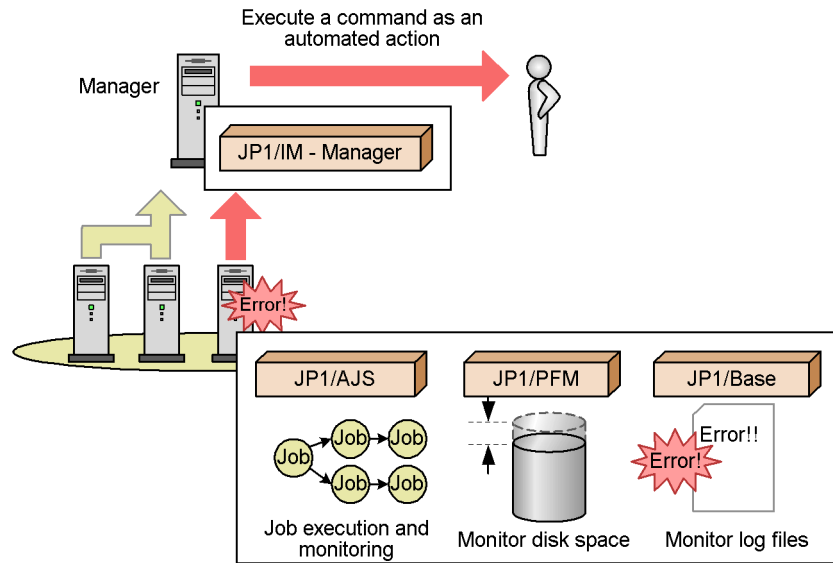
Figure 1-8: Monitoring Tree window



### 1.3.3 Error detection and reporting

JP1/IM - Manager supports automated actions as a means of detecting and reporting problems in the system. An *automated action* is the automatic execution of a command on a host managed by JP1/IM - Manager when a particular JP1 event is received. Commands for sending an email or making a telephone call can be executed as automated actions, notifying the administrator of any problems occurring in the system.

*Figure 1-9: Error reporting using automated actions*

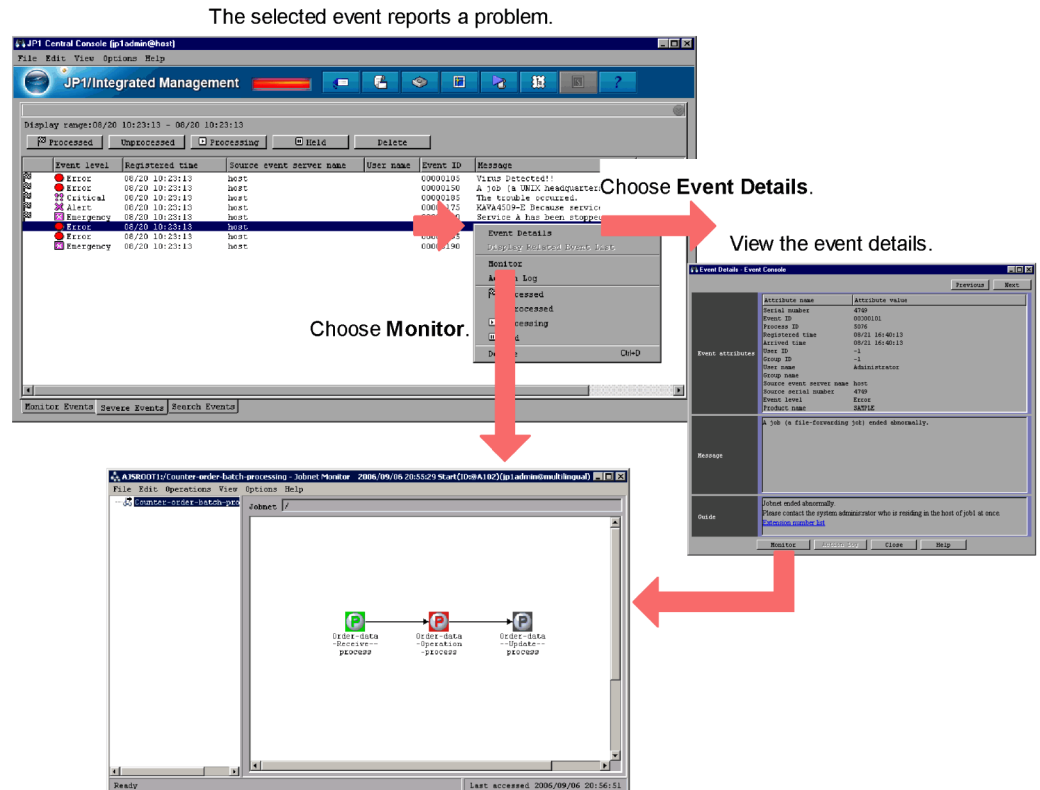


Using the Central Scope, the location of a problem can be represented visually in a tree view or map format, allowing on-the-spot judgment of how the problem in the system might affect business operations.

### 1.3.4 Integrated troubleshooting with JP1/IM - Manager

All operational tasks from monitoring to error investigation can be integrated into a single flow of operations based on JP1/IM - Manager. In the Event Console window of the Central Console, you can select a JP1 event and view the event details. You can also directly launch related applications when needed.

Figure 1-10: Error investigation with JP1/IM - Manager

**Monitor command**

Opens JP1/AJS - View where you can directly view the job in which the error that triggered the JP1 event occurred.

Non-JP1 applications required in managing system operations can also be registered, creating an integrated workflow based on JP1/IM - Manager.

### 1.3.5 Easy-to-build monitoring system

Using the automatic generation function provided by the Central Scope, you can collect information from active systems and create a monitoring window. If the system is modified, difference information can be collected and the monitoring window updated.

JP1/IM - Manager definition information can be distributed as a batch to the monitored hosts, allowing even a large-scale system to be configured with ease.

### 1.3.6 Flexible system configuration

The scalability of JP1/IM's management support means that systems of any size can be

managed, from small office systems to large-scale hierarchical systems. Cross-platform systems that incorporate a mixture of Windows, UNIX or UNIX variants, mainframes or other operating systems are also supported.

JP1/IM - Manager also supports networks with firewalls, cluster systems, and other types of system configurations.

### **1.3.7 Integrated management of the system hierarchy and host settings**

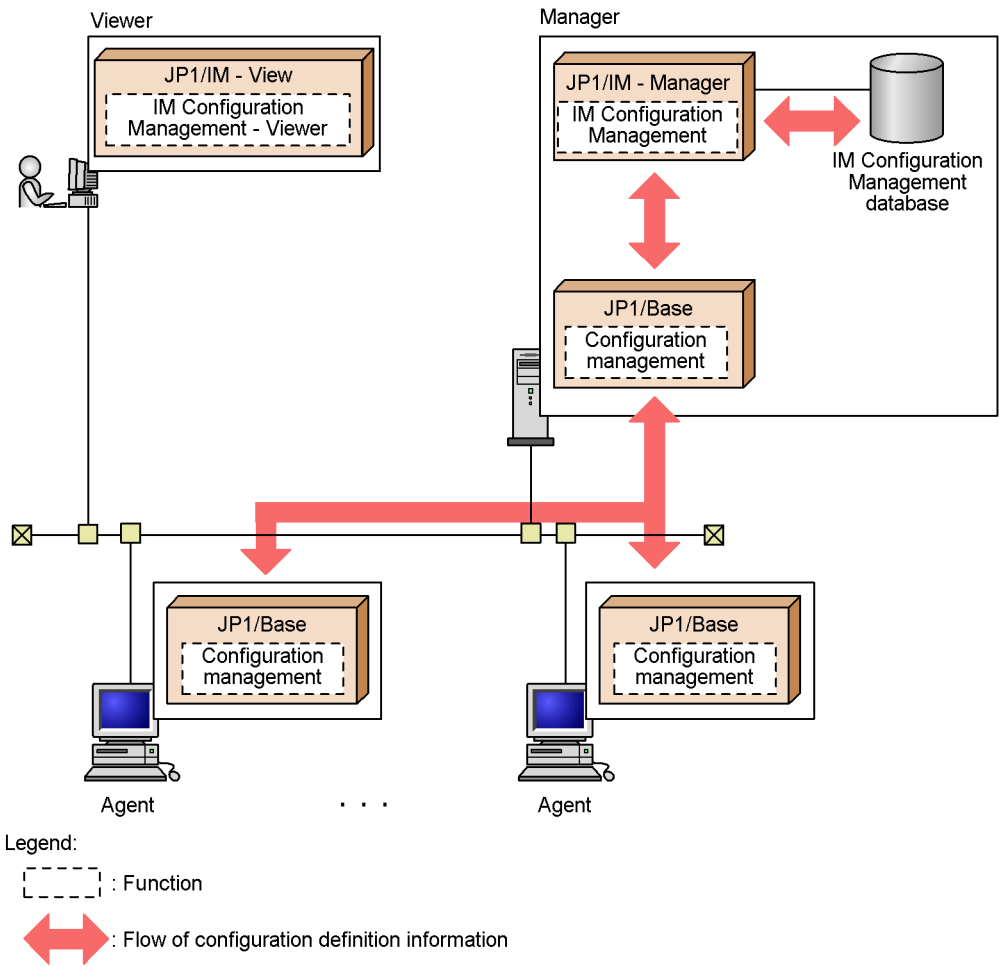
Using the IM configuration management viewer provided by IM Configuration Management, you can centrally manage from the manager host the hierarchical structure and host settings of the systems managed by JP1/IM. To use IM Configuration Management, you must set up the IM Configuration Management database.

IM Configuration Management provides the following functionality:

- **Host management**  
You can register the hosts in the network as management targets with IM Configuration Management. You can also manage host information, such as the host name and IP address of each registered host.
- **Management of the system hierarchy**  
You can define the hierarchical structure of the system managed by JP1/IM, and apply information about the hierarchy (configuration definition information) to the system as a whole.
- **Profile management**  
You can check and edit the user definition information (profiles) set in JP1/Base on the hosts in the system managed by JP1/IM.
- **Management of service activity information**  
You can check whether the services on the managed hosts are active.



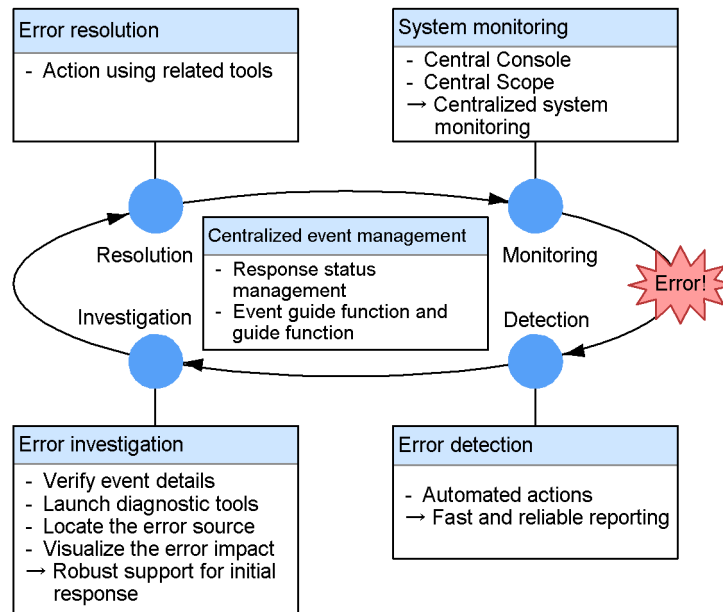
Figure 1-11: Integrated management of the system hierarchy and host settings



## 1.4 System operation with JP1/IM - Manager

JP1/IM - Manager provides full support for a unified flow of operations from system monitoring through to error detection, investigation, and resolution. The following figure shows the functions that support each phase of the system operating cycle.

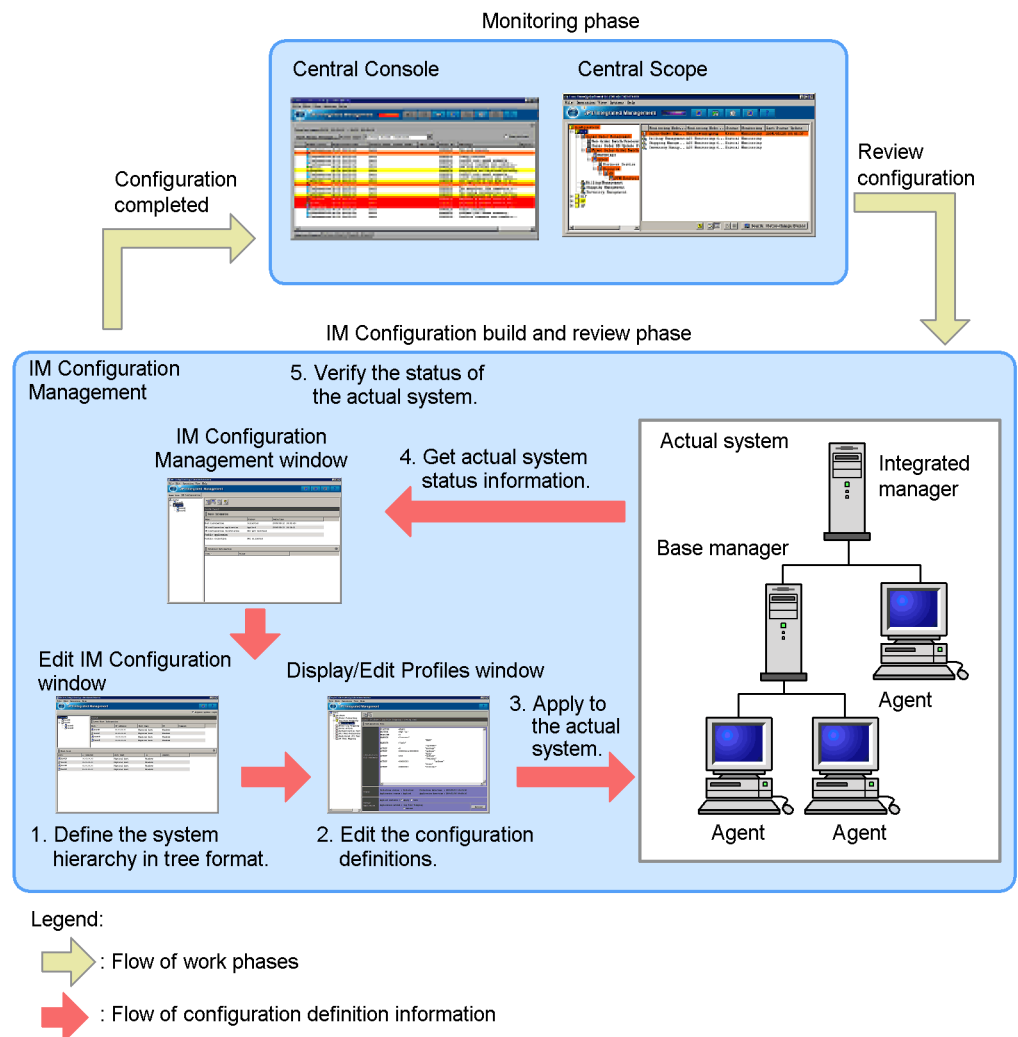
Figure 1-12: System operation with JP1/IM - Manager



No matter how large or complex the system, JP1/IM - Manager enables a diverse range of resources to be managed in an integrated fashion. By providing the capability to accurately grasp the system status, and to rapidly detect and deal with problems as they occur, JP1/IM - Manager ensures that the entire system runs reliably.

When using IM Configuration Management, you can define the system hierarchy in the IM configuration management viewer, and monitor the system from Central Console and Central Scope.

*Figure 1-13: Flow of system configuration and system monitoring with IM Configuration Management (build phase)*



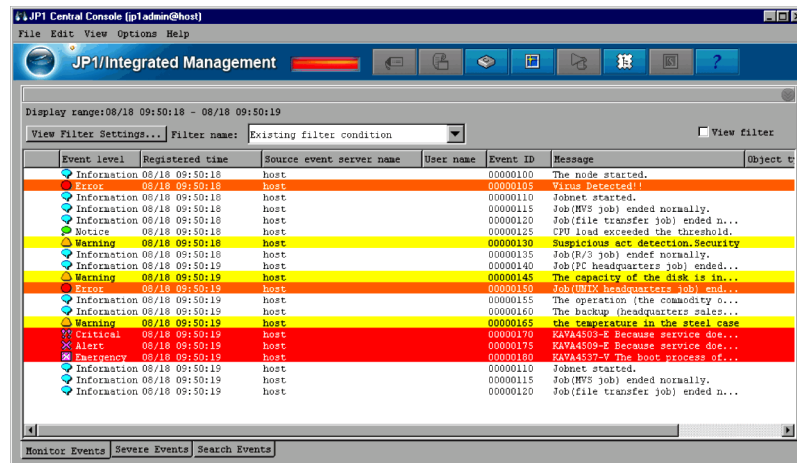
### 1.4.1 System monitoring

#### (1) System monitoring using the Central Console

Using the Central Console, you can monitor the events occurring in the system in the Event Console window. You do not need to constantly monitor the Event Console window if you have set up automated actions to notify the system administrator when an error occurs.

## 1. Overview of JP1/Integrated Management

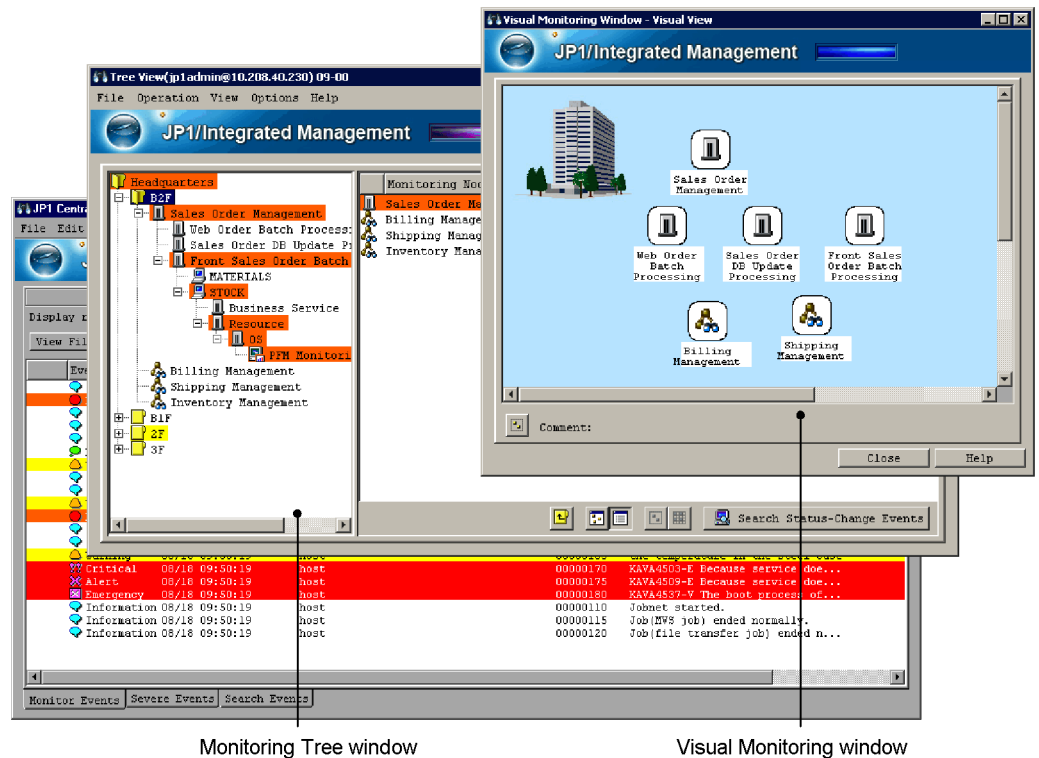
Figure 1-14: System monitoring from the Central Console



## (2) System monitoring using the Central Scope

Using the Central Scope, you can monitor the system in the Monitoring Tree window and Visual Monitoring window. You do not need to constantly monitor these windows if you have set up automated actions to notify the system administrator when an error occurs.

Figure 1-15: System monitoring using the Central Scope



In the Monitoring Tree window, you can configure the monitoring tree according to your objectives. In the Visual Monitoring window, you can place essential monitoring points on a map or organizational chart, and monitor the system in an intuitive manner matched to your purpose.

### 1.4.2 Error detection

The products in the JP1 series issue a JP1 event when an error occurs in the system. Specific error messages can also be converted into JP1 events.

JP1 events that need management follow-up are forwarded to JP1/IM - Manager where they are centrally managed. In the Central Scope, the source of an error can be represented visually in a tree view or map format, allowing on-the-spot judgment of how a problem in the system could affect business operations.

### 1.4.3 Error investigation

JP1/IM - Manager simplifies the investigation of problems occurring in the system by integrating the diagnostic processing into a unified flow of operations based on the Central Console or Central Scope.

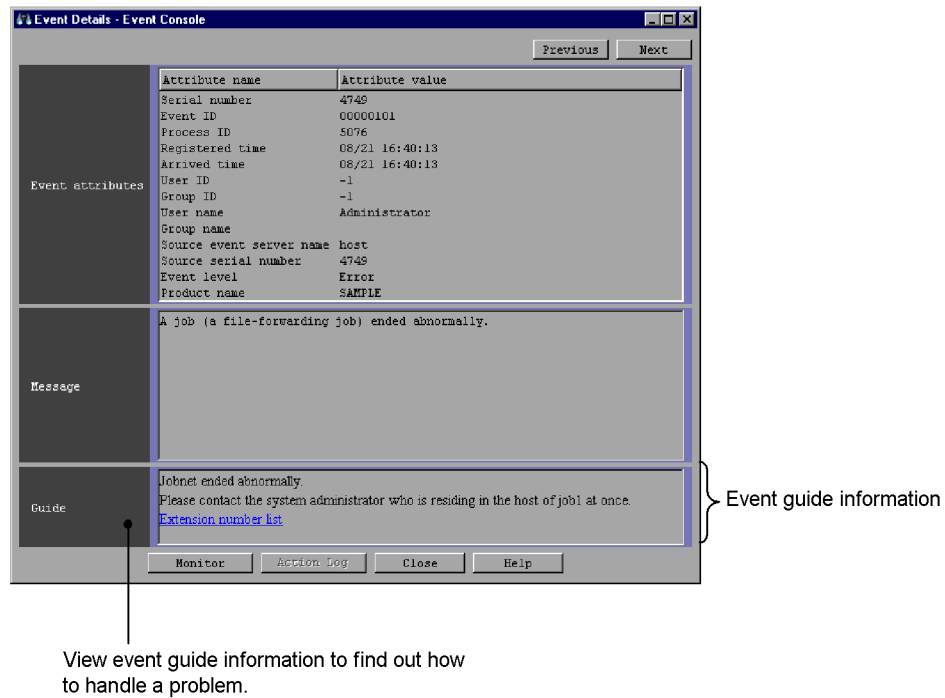
**(1) Error investigation with the Central Console**

The following describes the diagnostic and troubleshooting processing when using the Central Console.

**(a) Event details**

First of all, check the details of the detected error event. If you register action methods and procedures in advance, the initial response will be smoother and faster.

*Figure 1-16:* Troubleshooting advice (event guide information) provided in the Guide area

**(b) Event search**

For some problems, you might want to investigate not only the error-notification event but also related events leading up to the event in question, to see what was happening generally at the time the error occurred. In such cases, you can perform an event search.

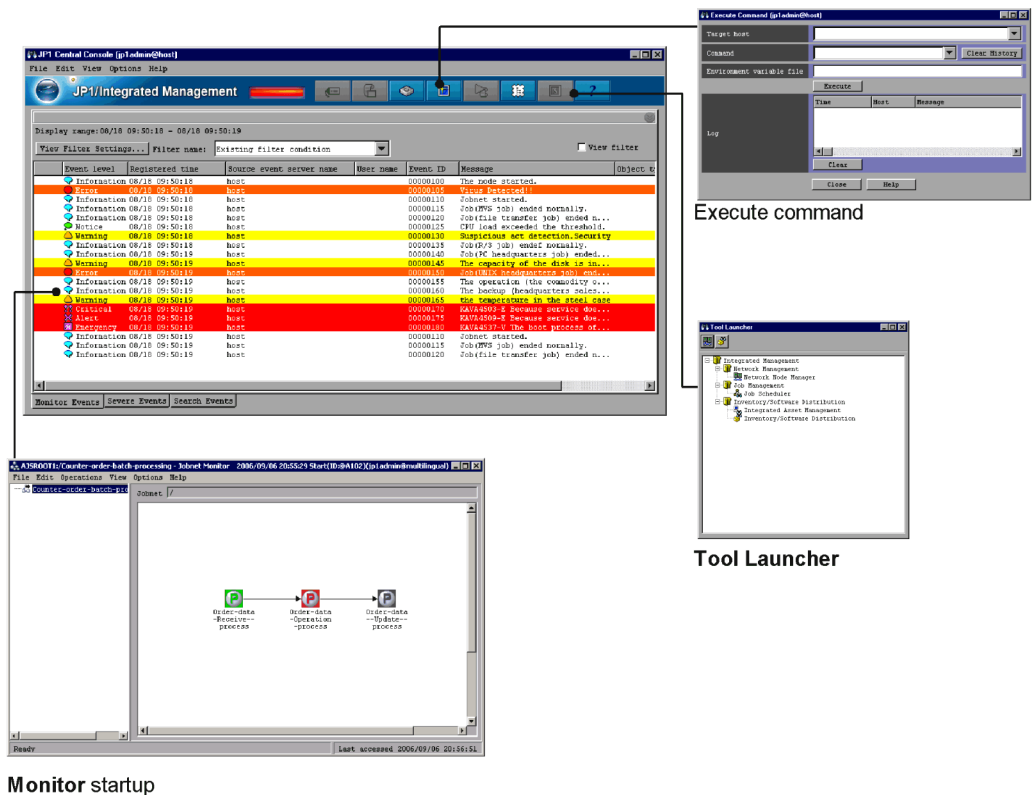
**(c) Event investigation**

After verifying the general circumstances by checking the event details and conducting an event search, investigate each event.

From a displayed JP1 event, you can launch the appropriate management application

and move by intuitive operation from the monitoring window to the investigation window to begin your diagnosis. You can also execute Windows and UNIX commands on an agent host directly from the Central Console. This makes it easy to perform simple checks or tests because you can execute commands without having to connect to the agent host by telnet or other means.

Figure 1-17: Operations performed from JP1/IM - Manager



## (2) Error investigation with the Central Scope

When investigating an error using the Central Scope, first identify the error source, and then link to the Central Console to investigate further.

The following describes the diagnostic and troubleshooting processing when using the Central Scope.

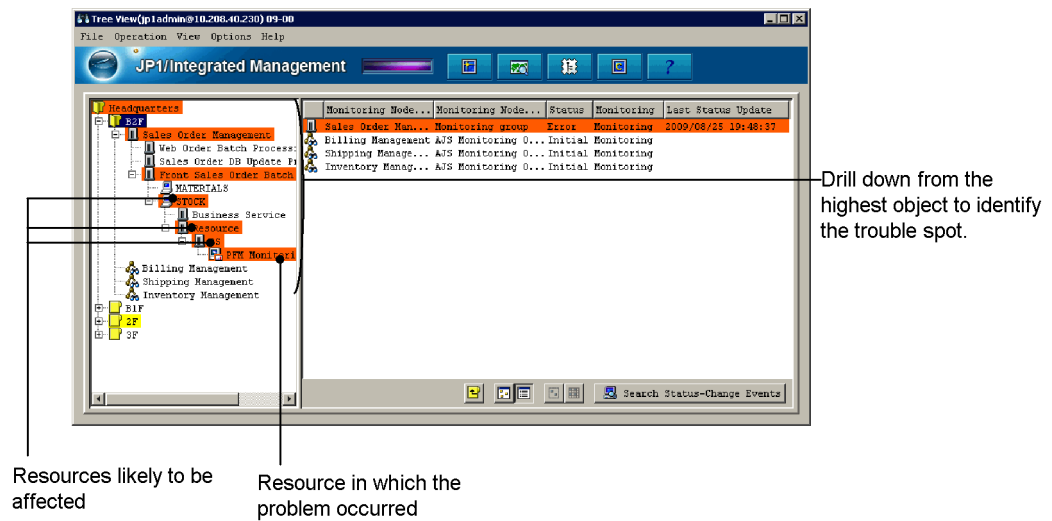
### (a) Identifying the source and extent of an error

When an error occurs in the system, the icons representing the affected nodes change to error status in the Monitoring Tree window and Visual Monitoring window. Starting from the top of the tree, you can check which nodes have error status and identify the

## 1. Overview of JP1/Integrated Management

resource in which the problem occurred.

Figure 1-18: Identifying the error source



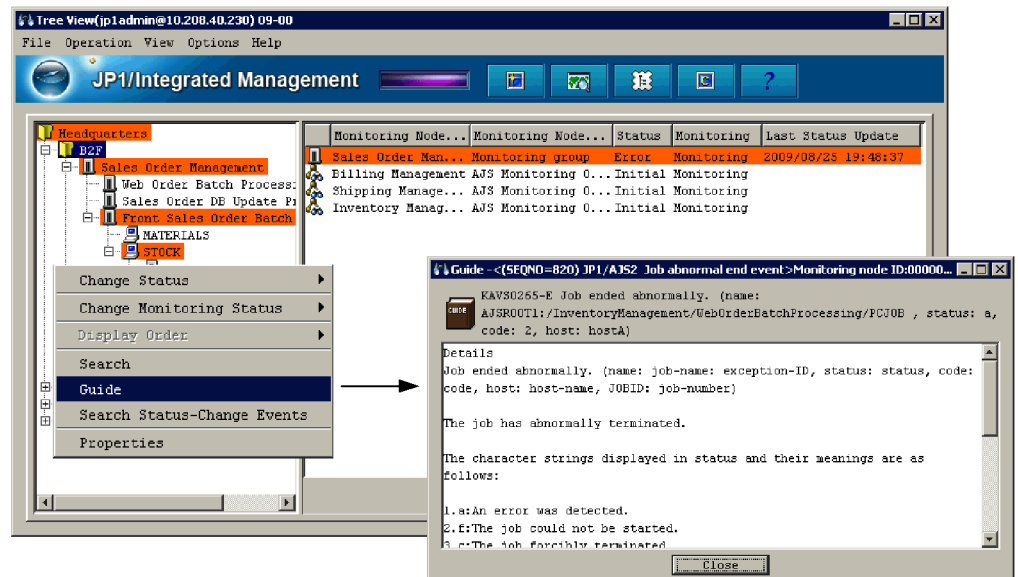
Guide information is a useful means of checking where a problem occurred. The guide function allows you to register operating know-how including troubleshooting procedures for specific problems, and examples of past situations in which certain errors have occurred. Although responding appropriately to whatever problems occur in a diverse range of resources is never easy, the guidance offered by the guide function goes some way toward reducing the system administrator's workload.

### Note:

Guide information must be registered before it can be viewed. For details about guide information, see 4.7 *Guide function* in this manual and 5.6 *Editing guide information* in the *Job Management Partner 1/Integrated Management - Manager Configuration Guide*.



Figure 1-19: Troubleshooting advice provided by the guide function

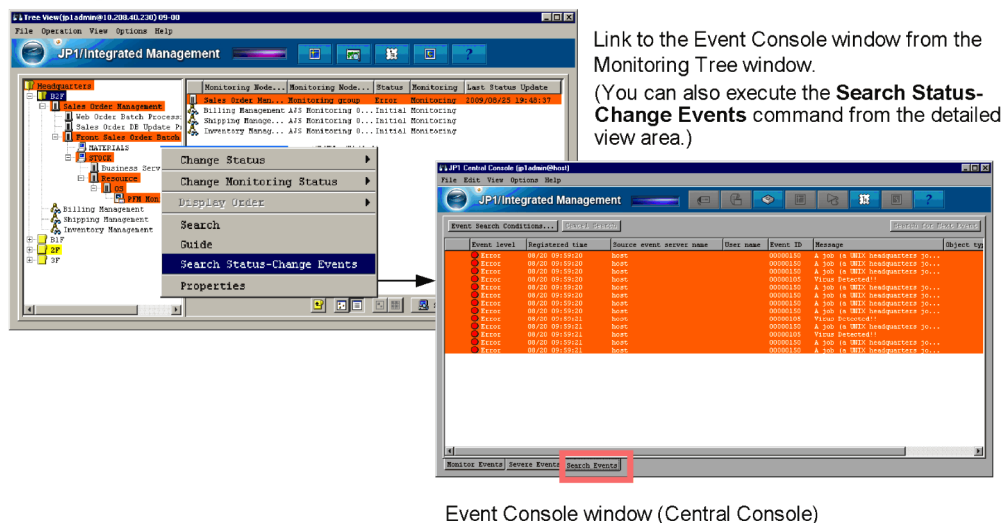
**(b) Identifying events that caused the error**

After you have identified the node that is in error status, you can discover what event caused the problem.

Select the node that is in error status, and then click the **Search Status-Change Events** command. The Event Console window opens with the **Search Events** page displayed. This page lists the JP1 events that caused the node to change to error status.

*Figure 1-20: Identifying events that caused the error*

### Monitoring Tree window (Central Scope)



### (c) Investigating the error

After you have identified the node in which an error occurred, you can discover what event caused the problem. To locate the event, use the Central Console. By linking to the Central Console, you can investigate the nature of the error that triggered the JP1 event.

#### 1.4.4 Error resolution

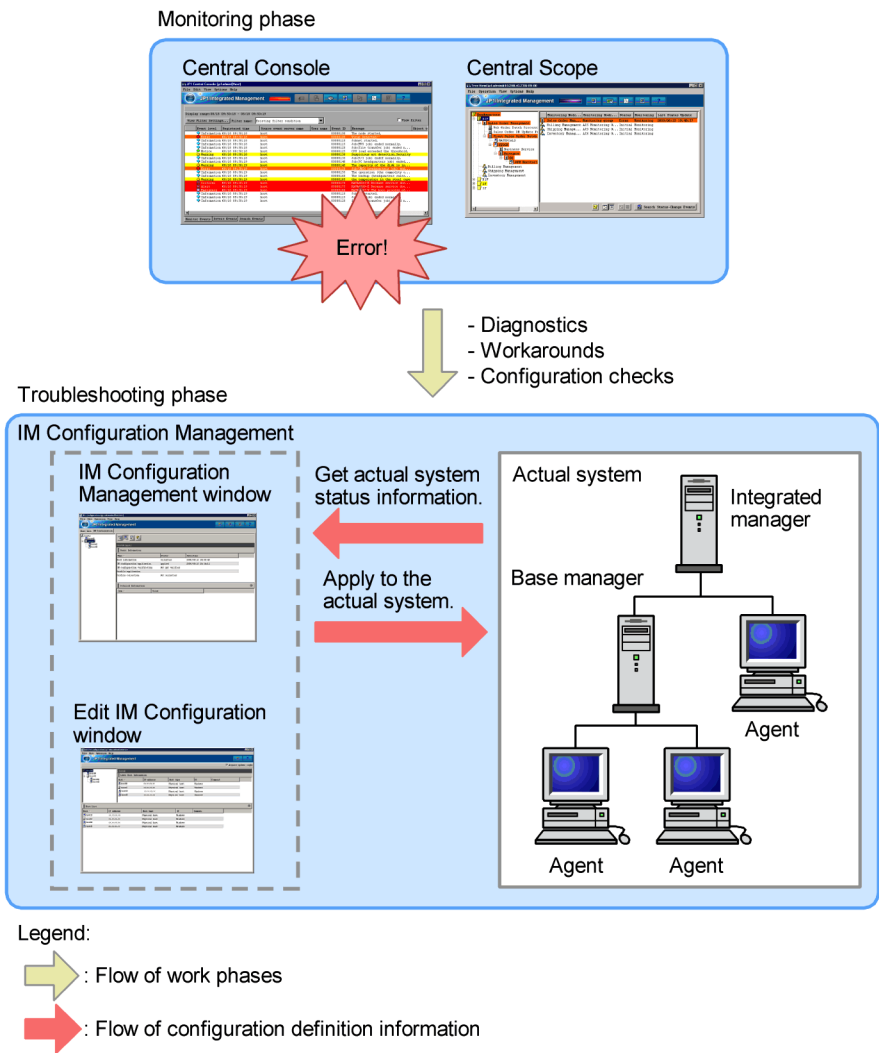
After identifying the location and cause of a problem, take the appropriate action to resolve it.

After resolving the problem, make sure that the system is working normally. Then, in the monitoring tree of the Central Scope, change the status of the objects affected by the error back to **Initial**. You can change the status of monitoring objects individually, or collectively by changing the status of the monitoring group. To restore monitoring objects to **Initial** status individually, select each object and change its status. To restore all the monitoring objects in a monitoring group to **Initial** status in a single operation, select the monitoring group and change its status.

Further errors might be occurring in other resources while you are busy dealing with the original problem. Before you restore the objects' status, take steps to make sure that the entire monitoring group is working normally, including searching for nodes that have error status.

When using IM Configuration Management, you can change the system hierarchy in the IM configuration management viewer as a means of resolving the problem.

Figure 1-21: Flow of system monitoring and system reconfiguration with IM Configuration Management (operation phase)



## 1.5 JP1/IM - Manager system configuration

This section describes the component products and configuration of a JP1/IM - Manager system.

### 1.5.1 Component products of a JP1/IM - Manager system

A JP1/IM - Manager system consists of *managers* that administer the system as a whole, *agents* that run on the monitored servers, and *viewers* that perform monitoring and operations.

A JP1/IM - Manager system requires the following products, depending on the functionality to be used and the host's role in the system:

- Manager host: JP1/IM - Manager and JP1/Base
- Agent host: JP1/Base
- Viewer host: JP1/IM - View

The viewer program can be used on both manager hosts and agent hosts.

A JP1/IM - Manager system consists of the following component products.

*Table 1-3: Component products of a JP1/IM - Manager system*

Product name	Product overview
JP1/IM - Manager	Provides the following manager functionality <ul style="list-style-type: none"> <li>• Central Console</li> <li>• Central Scope</li> <li>• IM Configuration Management</li> </ul>
JP1/IM - View	Broadly classified, JP1/IM - View provides three main windows <sup>#</sup> : <ul style="list-style-type: none"> <li>• Central Console viewer (for Central Console operations)</li> <li>• Central Scope viewer (for Central Scope operations)</li> <li>• IM configuration management viewer (for IM Configuration Management operations)</li> <li>• Rule operation viewer (for rule management operations)</li> </ul> JP1/IM - Manager performs system monitoring and operation using the Central Console viewer and Central Scope viewer.
JP1/Base	Provides the agent functionality. JP1/Base operates as a monitored server and provides the JP1 core functionality, such as JP1 event management and JP1 user management. JP1/Base is a prerequisite product of JP1/IM - Manager.

<sup>#</sup>: This manual describes the Central Console viewer, Central Scope viewer, and IM configuration management viewer only.

### 1.5.2 JP1/IM system hierarchy

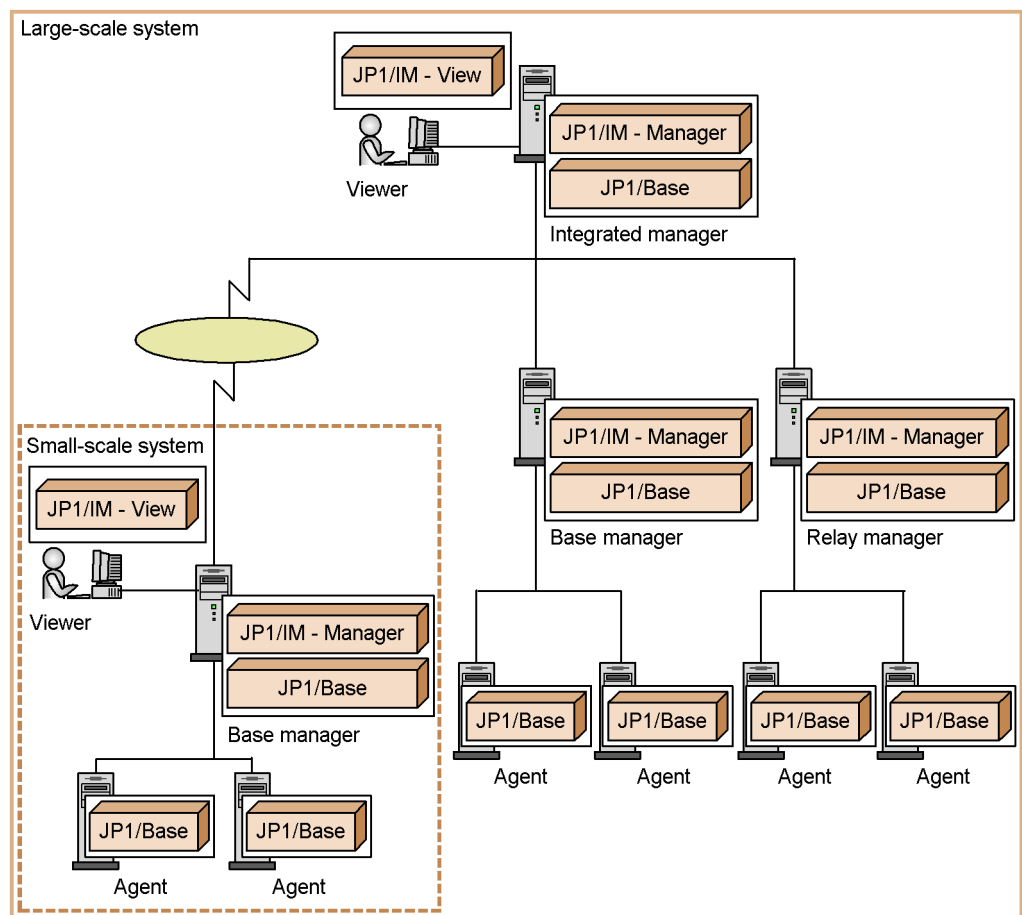
The systems managed by JP1/IM consist of *managers* that administer the system as a whole, *agents* that run on the monitored servers, and *viewers* that perform monitoring and operations.

You can centrally manage the system hierarchy using the IM Configuration Management functionality provided by JP1/IM - Manager. For example, you can define a hierarchical structure, and then distribute the configuration definition information you have created to each host in the system.

Alternatively, you can define the system hierarchy using the configuration definition information in JP1/Base in the usual manner.

In a JP1/IM system, managers can be arranged hierarchically to enable integrated management of systems whatever their size - from a small system serving a regional office to a large-scale system serving the entire enterprise. This allows you to add hosts to those being monitored, and makes it easy to migrate a small system to a large-scale hierarchical system.

Figure 1-22: Scalable system hierarchy



As shown in the above figure, you can build a hierarchical system by arranging base managers and relay manager under an integrated manager. To configure a hierarchical system, JP1/IM - Manager must be installed on the integrated manager host, base manager hosts, and relay manager host.

The types of manager hosts configured in a JP1/IM system are as follows:

Table 1-4: Types of managers in a JP1/IM system

Type of manager host	Description
Integrated manager	Positioned at the top of the system hierarchy. The integrated manager host manages the base managers, relay managers, and agents (other than those under a base manager) in the system hierarchy as a whole.

Type of manager host	Description
Base manager	Positioned at an intermediate level between the integrated manager and agents when agent hosts are managed on a site basis. The base manager host manages lower-level agents, and is itself managed by the integrated manager.
Relay manager	Positioned at an intermediate level between the integrated manager and agents to collect events generated at the agent hosts. The relay manager and lower-level agents are managed by the integrated manager.

### 1.5.3 Support for various system configurations

JP1/IM - Manager supports the following broad range of system configurations, providing flexible integrated management tailored to system requirements.

- Cross-platform support

JP1/IM - Manager provides agents for a variety of platforms, including Windows, UNIX, and mainframe operating systems. Using these agents, JP1/IM - Manager can seamlessly manage various types of heterogeneous systems.

- Support for a variety of network configurations

- Firewall support

JP1/IM supports communication through a port-filtering firewall and Network Address Translation (NAT) in static mode. You can deploy JP1/IM in a network configuration that has a firewall installed between a viewer and manager host, or between a manager and agent host.

- Support for multiple LAN connections

JP1/IM supports network configurations with JP1/IM hosts connected to multiple LANs. You can set up the JP1/IM host to communicate over a specific LAN.

- Support for cluster systems

JP1/IM - Manager supports operation in a cluster system.

In the event of an error, JP1/IM - Manager will fail over and continue working, performing integrated monitoring of the system that runs your business operations.

- Mixed languages and time zones

JP1/IM supports system configurations that encompass more than one language or time zone, which is unavoidable when managing a global system in its entirety. However, several restrictions apply. Consider the system configuration and operation, referring to *12.1.6 Operation in a multi-language environment*.





## **Chapter**

---

# **2. Overview of Functions**

---

This chapter provides an overview of the functions that are fundamental to JP1/IM - Manager.

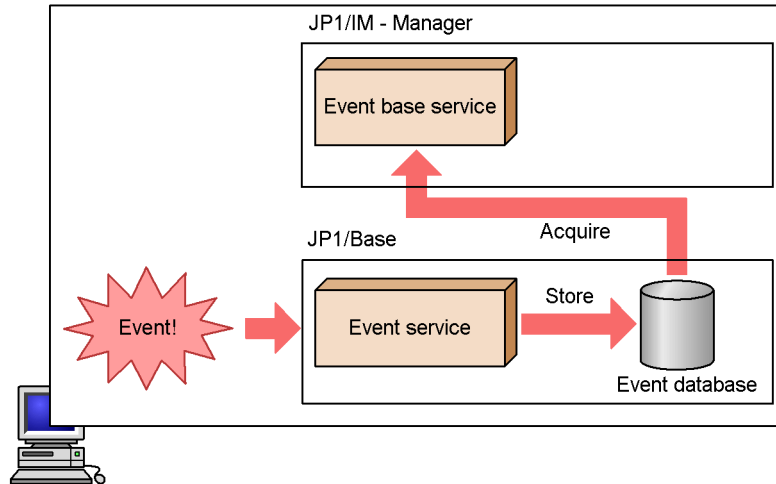
- 2.1 Overview of event management
- 2.2 Functionality at each phase of the operating cycle
- 2.3 List of functions
- 2.4 Functions provided by the IM database

## 2.1 Overview of event management

JP1/IM - Manager centrally manages the various events that occur in the system as *JP1 events*.

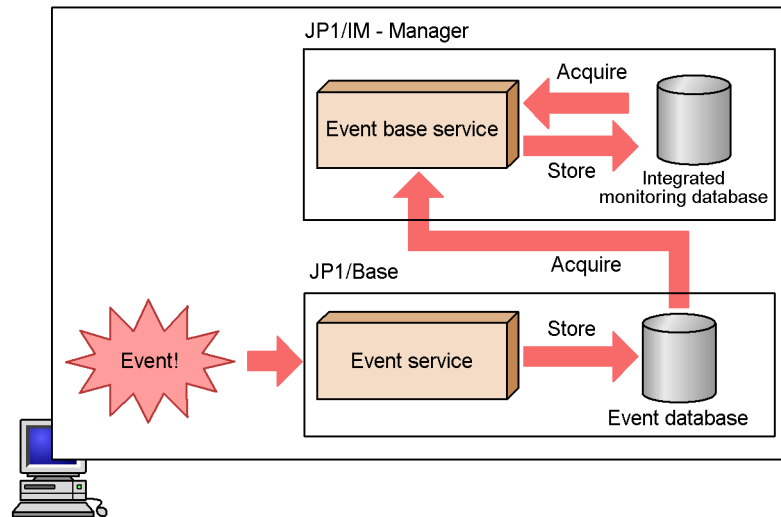
JP1 events are controlled by the JP1/Base event service and are managed by the event database specific to JP1/Base.

Figure 2-1: Overview of JP1 event management



When you use the *integrated monitoring database* provided by JP1/IM - Manager, the event base service of JP1/IM - Manager acquires JP1 events from the JP1/Base event database. JP1/IM - Manager applies JP1/IM - Manager-specific information and stores the acquired JP1 events in the integrated monitoring database. By accessing this JP1 event information in the integrated monitoring database, JP1/IM - Manager can perform processing of various kinds based on the information.

Figure 2-2: Overview of JP1 event management with the integrated monitoring database



---

## 2.2 Functionality at each phase of the operating cycle

---

This section describes the functionality provided at each phase of the operating cycle. JP1/IM - Manager consists of four key components: Central Console, Central Scope, IM Configuration Management, and the core functionality.

### Central Console

The Central Console centrally manages events in the system based on JP1 events, and enables integrated management of the entire system. For details about system monitoring using the Central Console, see 3. *Centralized System Monitoring Using the Central Console* and 5. *Command Execution by Automated Action*.

### Central Scope

The Central Scope enables integrated objective-oriented system management via a visual interface, in accordance with requirements set by the system administrator. For details about the Central Scope, see 4. *Objective-Oriented System Monitoring Using the Central Scope*. To use the Central Scope, you must enable (activate) the central scope service in JP1/IM - Manager. For details about configuring the Central Scope, see 1.18.1 *Settings for using the functions of Central Scope* in the *Job Management Partner 1/Integrated Management - Manager Configuration Guide*.

### IM Configuration Management

Using IM Configuration Management - View, you can centrally manage the hierarchical structure and host settings of the system managed by JP1/IM. To use IM Configuration Management, you must set up the IM Configuration Management database. For details about IM Configuration Management, see 6. *System Hierarchy Management Using IM Configuration Management*.

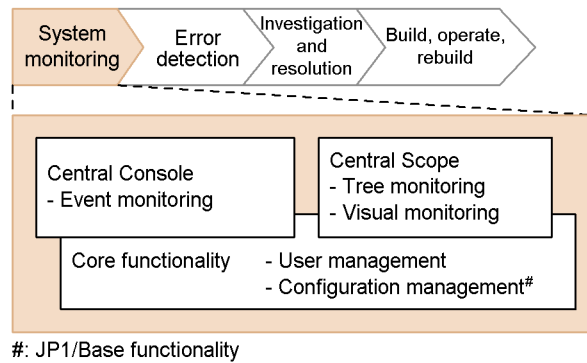
### Core functionality

Much of the core functionality of integrated system management under JP1/IM is provided by JP1/Base, the prerequisite product for JP1/IM - Manager. For details about the core functionality of JP1/IM - Manager and JP1/Base, see 7. *JP1/IM Operation Control*.

### 2.2.1 Functionality for system monitoring

The system needs to be monitored continuously to ensure it is running normally.

Figure 2-3: Functionality for system monitoring



By providing centralized monitoring, the Central Console makes monitoring more efficient, supports early error detection, and reduces management overheads. The Central Console issues correlation events when specific events are received, and centrally monitors the issued events.

When the system being monitored is large and complex, problems might be detected successfully, but their impact on operations is never easy to determine. The Central Scope offers visual representation using monitoring windows in a tree or map view, enabling system monitoring from any viewpoint required by the system administrator. If a problem occurs in a resource, the administrator can visually grasp the extent of its impact on business operations. This enhances management efficiency and enables preventive action to isolate any problems.

User management and configuration management are part of the core functionality for monitoring the system. User management entails mapping of the JP1 user with the OS user when a JP1 user executes a command. IM Configuration Management manages the system hierarchy.

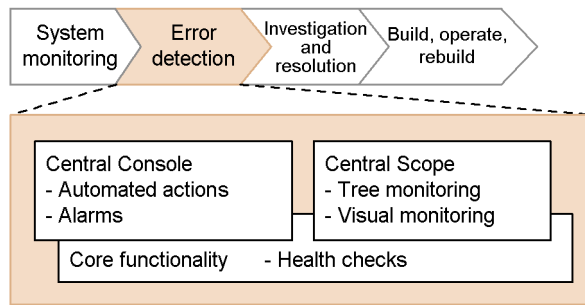
*Note:*

JP1/IM - Manager can only monitor JP1 events that were issued after it began operation. Events that occurred earlier are excluded from monitoring by JP1/IM - Manager.

## 2.2.2 Functionality for error detection

The following figure shows the functionality for detecting errors.

Figure 2-4: Functionality for error detection



The components used for detecting problems in the system are the Central Console, Central Scope, and the core functionality.

In the Central Console, you can set automated actions in advance to detect errors. An *automated action* is the automatic execution of a command which is defined in advance and triggered when a particular event is received. This mechanism can be used for reporting problems to the administrator by email or other means.

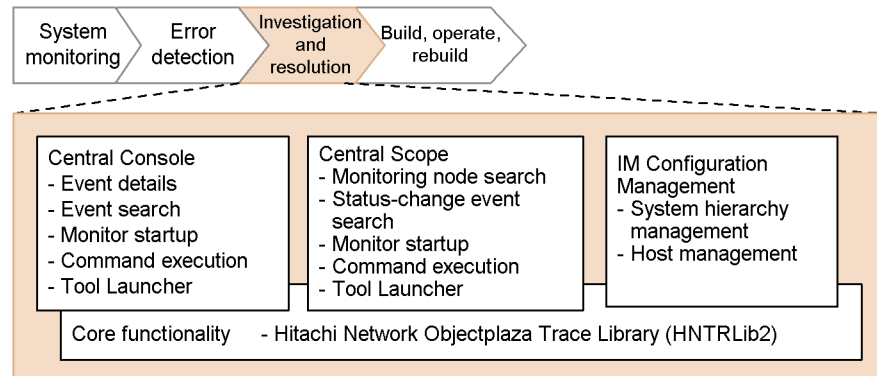
The Central Scope provides tree monitoring and visual monitoring. A JP1 event can be issued from the Central Scope whenever the status of a monitoring node changes, and an automated action can be executed through the Central Console in response to an issued JP1 event. Severe events can be reported by using alarms, and the impact of any errors can be visually represented by changing the icons in the monitoring tree to error status.

The health check provided by the core functionality issues a message or JP1 event whenever an error occurs in a JP1/IM - Manager process. It can also issue a message or JP1 event when an error occurs in a JP1/Base process on the local host or remote host.

### 2.2.3 Functionality for error investigation and resolution

The following figure shows the functionality used in investigating and resolving errors.

Figure 2-5: Functionality for error investigation and resolution



Error investigation and resolution via the Central Console is based on JP1 events. You can display detailed information about a JP1 event, and search for events related to the JP1 event in question. In the course of investigating and resolving a problem, you can launch the application that issued the JP1 event or any other application of your choice, and execute various commands.

Using the Central Scope, you can search for monitoring nodes or events related to the problem. As with the Central Console, you can launch the application that issued the JP1 event, or any other application of your choice, and execute commands to investigate and resolve the problem.

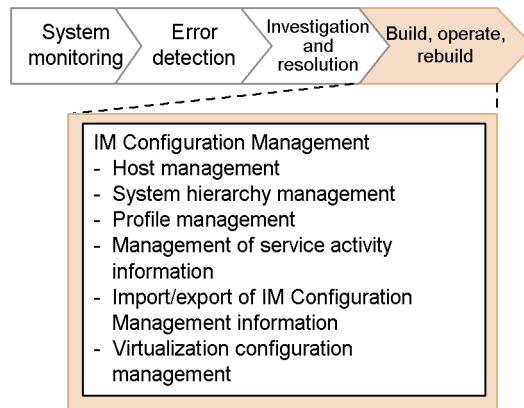
When the range of your investigation extends to the system configuration, use the IM Configuration Management feature. Using IM Configuration Management - View, you can check the status of the host on which the problem occurred, delete that host from the system hierarchy, or apply the hierarchical system information saved in IM Configuration Management to the host. If you do not use IM Configuration Management, you must examine the log information, assess the status of the affected host, and resolve the problem yourself.

Using the Hitachi Network Objectplaza Trace Library (HNTRLib2) with the core functionality, you can output all the trace information generated by the JP1/Base and JP1/IM - Manager processes to a single integrated trace log.

## 2.2.4 Functionality for building, operating, and rebuilding the system

The following figure shows the functionality used at the build, operation, and rebuild phases.

*Figure 2-6: Functionality for building, operating, and rebuilding the system*



It is sometimes necessary to rebuild the system or change its configuration during maintenance mode as a means of investigating and resolving an issue. In such cases, review the system hierarchy using the configuration management functionality provided by IM Configuration Management or by JP1/Base.

We recommend that you use the IM Configuration Management functionality if you want to centrally manage the hierarchical structure of the system from JP1/IM - Manager. Using IM Configuration Management - View, you can define the system hierarchy by registering the hosts you want to manage, and adding, moving, or deleting hosts in the hierarchy.

If you choose not to use IM Configuration Management, you can define the system hierarchy using the JP1/Base configuration management functionality. You also have access to the JP1/Base functionality for collecting and distributing the information defined in JP1/Base on the hosts.

Decide in advance whether you want to use IM Configuration Management or the configuration management and definition collection and distribution functionality provided by JP1/Base. For details about these functions and considerations at the design stage, see the following table.



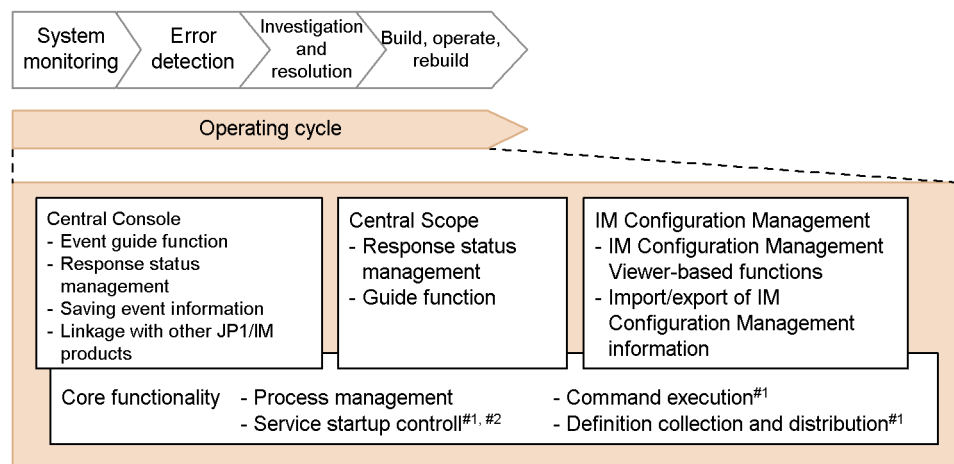
Table 2-1: Details of functions and design considerations

Function	Function details	Design considerations
<ul style="list-style-type: none"> <li>IM Configuration Management</li> </ul>	<ul style="list-style-type: none"> <li>6. System Hierarchy Management Using IM Configuration Management</li> </ul>	<ul style="list-style-type: none"> <li>11.5 Considerations for managing the system hierarchy</li> <li>12.5 Considerations for the system hierarchy</li> </ul>
<ul style="list-style-type: none"> <li>JP1/Base configuration management</li> <li>JP1/Base definition collection and distribution</li> </ul>	<ul style="list-style-type: none"> <li>7.4.3 Managing the system hierarchy</li> <li>7.4.5 Collecting and distributing definition information</li> </ul>	

## 2.2.5 Functionality used throughout the operating cycle

The following figure shows the functions used throughout the operating cycle.

Figure 2-7: Functions used throughout the operating cycle



#1: JP1/Base function

#2: Windows-only function

The functions in the following table are used throughout the operating cycle.

Table 2-2: Functions used throughout the operating cycle

Component	Function	Description
Central Console	Event guide function	<ul style="list-style-type: none"> <li>Displays guidance about methods or procedures for responding to JP1 events.</li> </ul>
	Response status management	<ul style="list-style-type: none"> <li>Manages actions taken in response to severe events.</li> </ul>

Component	Function	Description
	Saving event information	<ul style="list-style-type: none"> <li>Saves JP1 event information displayed in JP1/IM - View (exports the information in CSV form).</li> <li>Saves JP1 event information saved in the integrated monitoring database (outputs event reports).</li> </ul>
	Linkage with other JP1/IM products	<ul style="list-style-type: none"> <li>Sends rule start requests to JP1/IM - Rule Operation.</li> </ul>
Central Scope	Response status management	<ul style="list-style-type: none"> <li>Manages the status of monitoring nodes.</li> </ul>
	Guide function	<ul style="list-style-type: none"> <li>Displays guidance about troubleshooting methods or response procedures.</li> </ul>
IM Configuration Management	IM Configuration Management Viewer-based functions	<ul style="list-style-type: none"> <li>Manages the status of managed hosts.</li> <li>Manages the status of the system hierarchy.</li> <li>Manages the status of the JP1/Base profiles on each host.</li> <li>Checks JP1/Base service activity information on each host.</li> </ul>
	Import/export of IM Configuration Management information	<ul style="list-style-type: none"> <li>Exports management information from IM Configuration Management in case an error occurs, and imports the information at error recovery.</li> </ul>
Core functionality	Process management	<ul style="list-style-type: none"> <li>Controls JP1/IM - Manager startup, termination, and other operations.</li> <li>Checks whether JP1/IM - Manager functions are active.</li> </ul>
	Service startup control <sup>#1, #2</sup>	<ul style="list-style-type: none"> <li>Controls service startup via JP1/Base.</li> </ul>
	Command execution <sup>#1</sup>	<ul style="list-style-type: none"> <li>Executes commands from JP1/IM - View.</li> <li>Executes commands by automated actions.</li> </ul>
	Definition collection and distribution <sup>#1</sup>	<ul style="list-style-type: none"> <li>Collects and distributes definition information among JP1/Base hosts.</li> <li>Collects definition information for creating monitoring trees in Central Console and automatically creates monitoring trees.</li> </ul>

#1: JP1/Base function.

#2: Windows-only function.

You can manage the system configuration information and collect and distribute definition information using either IM Configuration Management or the core functionality. Consider which method to use before you commence operation. For the function details and design considerations, see *Table 2-1*.

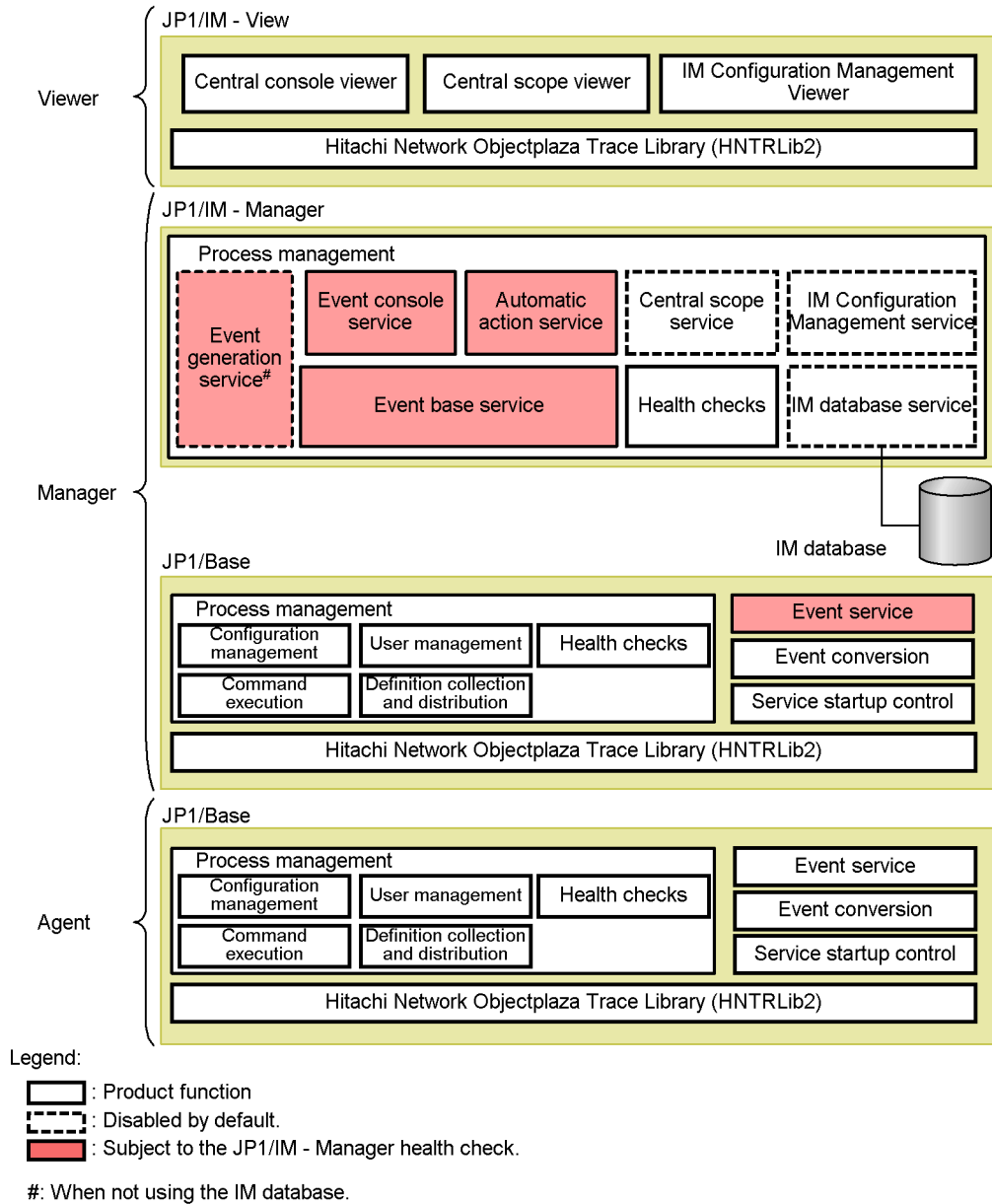
---

## 2.3 List of functions

---

The following figure shows the functions of component programs used for system operation monitoring by JP1/IM - Manager.

Figure 2-8: Functions provided by the component products



JP1/IM - Manager is linked with the prerequisite product JP1/Base, and operates using the core functionality provided by JP1/Base. JP1/Base also runs on the agents in the JP1/IM - Manager system. JP1/IM - Manager thus has an inseparable relationship with

JP1/Base.

The functions in the figure above are summarized below.

*Table 2-3: Summary of product functions*

Function		Description	Service name
Central Console	Centralized monitoring using JP1 events	<ul style="list-style-type: none"> <li>Monitors JP1 events.</li> </ul>	<ul style="list-style-type: none"> <li>Central console viewer</li> </ul>
	JP1 event management	<ul style="list-style-type: none"> <li>Controls the display of JP1 events in the central console viewer.</li> </ul>	<ul style="list-style-type: none"> <li>Event console service</li> </ul>
		<ul style="list-style-type: none"> <li>Manages the integrated monitoring database.</li> </ul>	<ul style="list-style-type: none"> <li>IM database service</li> </ul>
		<ul style="list-style-type: none"> <li>Acquires JP1 event information from the JP1/Base event service.</li> <li>Distributes acquired JP1 event information to the JP1/IM - Manager controls (event console service, automatic action service, and central scope service).</li> </ul>	<ul style="list-style-type: none"> <li>Event base service</li> </ul>
		<ul style="list-style-type: none"> <li>Controls JP1 events.</li> <li>Manages the event database.</li> </ul>	<ul style="list-style-type: none"> <li>JP1/Base</li> </ul>
	JP1 event filtering	<ul style="list-style-type: none"> <li>Filters JP1 events to select those required.</li> </ul>	<ul style="list-style-type: none"> <li>Central console viewer</li> <li>Event console service</li> <li>Event base service</li> <li>Event issue service</li> <li>JP1/Base</li> </ul>
	Automated actions	<ul style="list-style-type: none"> <li>Executes a command automatically, conditional on a specific event being detected by the event base service.</li> </ul>	<ul style="list-style-type: none"> <li>Automatic action service</li> </ul>

Function		Description	Service name
	Issue of correlation events	<ul style="list-style-type: none"> <li>Correlates JP1 events acquired from the JP1/Base event service and registers them as correlation events with JP1/Base.</li> </ul>	<ul style="list-style-type: none"> <li>Event issue service (when not using the integrated monitoring database, or when using JP1/IM - Manager version 8 or earlier)</li> <li>Event base service (when using the integrated monitoring database)</li> </ul>
	Event conversion	<ul style="list-style-type: none"> <li>Extracts information from log files and converts it into JP1 events (log file trapping)</li> <li>Extracts information from the Windows event log and converts it into JP1 events (event log trap conversion)</li> <li>Extracts information from SNMP traps managed by HP NNM version 7.5 or earlier and converts it into JP1 events (SNMP trap conversion).</li> </ul>	<ul style="list-style-type: none"> <li>JP1/Base</li> </ul>
	Display of user-defined event attributes	<ul style="list-style-type: none"> <li>Issues JP1 events from a user application by calling a JP1/Base function.</li> </ul>	
	Event guide function	<ul style="list-style-type: none"> <li>Displays information about pre-registered response methods and procedures.</li> </ul>	<ul style="list-style-type: none"> <li>Central console viewer</li> </ul>
	CSV output of information displayed in JP1/IM - View	<ul style="list-style-type: none"> <li>Outputs JP1 event information displayed in JP1/IM - View in CSV form.</li> </ul>	
	System operation	<ul style="list-style-type: none"> <li>Launches a linked application.</li> <li>Launches an associated application from the Tool Launcher.</li> <li>Executes a command from JP1/IM - View.</li> </ul>	
Central Scope	Tree monitoring	<ul style="list-style-type: none"> <li>Centrally monitors objects in a tree view.</li> <li>Automatically creates a monitoring window.</li> </ul>	<ul style="list-style-type: none"> <li>Central scope viewer</li> <li>Central scope service</li> </ul>

Function		Description	Service name
	Visual monitoring	<ul style="list-style-type: none"> <li>Centrally monitors objects in a map view.</li> </ul>	
	Guide function	<ul style="list-style-type: none"> <li>Displays information about pre-registered response methods and procedures.</li> </ul>	
IM Configuration Management <sup>#1</sup>	Host management	<ul style="list-style-type: none"> <li>Centrally manages the hosts in the JP1/IM system from the manager.</li> </ul>	<ul style="list-style-type: none"> <li>IM Configuration Management - View</li> </ul>
	System hierarchy management	<ul style="list-style-type: none"> <li>Centrally manages the hierarchical structure of the system from the manager.</li> </ul>	<ul style="list-style-type: none"> <li>IM configuration management service</li> </ul>
	Profile management	<ul style="list-style-type: none"> <li>Centrally manages the JP1/Base profiles on each host from the manager.</li> </ul>	<ul style="list-style-type: none"> <li>IM database service</li> </ul>
	Management of service activity information	<ul style="list-style-type: none"> <li>Checks whether JP1/IM - Manager and JP1/Base services are active on each host.</li> </ul>	
	Import/export of IM Configuration Management information	<ul style="list-style-type: none"> <li>Exports and imports IM Configuration Management information.</li> </ul>	
	Management of virtualization configuration information	<ul style="list-style-type: none"> <li>Manages the hierarchical structure of the system, including virtual hosts.</li> </ul>	
Core functionality	Process management	<ul style="list-style-type: none"> <li>Manages JP1/IM - Manager and its functions.</li> </ul>	<ul style="list-style-type: none"> <li>Process management</li> </ul>
	Health check	<ul style="list-style-type: none"> <li>Monitors the status of JP1/IM - Manager processes (other than the central scope service and IM configuration management service on the local host).</li> <li>Monitors the status of JP1/Base processes.</li> </ul>	<ul style="list-style-type: none"> <li>Health check</li> <li>JP1/Base</li> </ul>
	Hitachi Network Objectplaza Trace Library (HNTRLib2)	<ul style="list-style-type: none"> <li>Stores trace information from JP1/Base, JP1/IM - Manager, JP1/IM - View, and other component products.</li> </ul>	<ul style="list-style-type: none"> <li>HNTRLib2</li> </ul>

## 2. Overview of Functions

Function		Description	Service name
	User management	<ul style="list-style-type: none"> <li>Manages JP1 users.</li> <li>Manages command execution permissions.</li> </ul>	<ul style="list-style-type: none"> <li>JP1/Base</li> </ul>
	Configuration management <sup>#2</sup>	<ul style="list-style-type: none"> <li>Manages the configuration of the JP1/IM - Manager system.</li> </ul>	
	Service startup control <sup>#3</sup>	<ul style="list-style-type: none"> <li>Controls the service start/stop sequencing of products (including JP1/Base) registered with the Windows service.</li> </ul>	
	Command execution <sup>#2</sup>	<ul style="list-style-type: none"> <li>Control command execution.</li> <li>Manages command execution log files (manager only).</li> </ul>	
	Definition collection and distribution <sup>#2</sup>	<ul style="list-style-type: none"> <li>Collects and distributes definition information related to the JP1/IM - Manager event service.</li> <li>Collects definition information for creating monitoring trees in JP1/IM - Manager.</li> </ul>	

#1: Available when the IM Configuration Management database has been set up.

#2: JP1/Base function.

#3: Windows-only function.

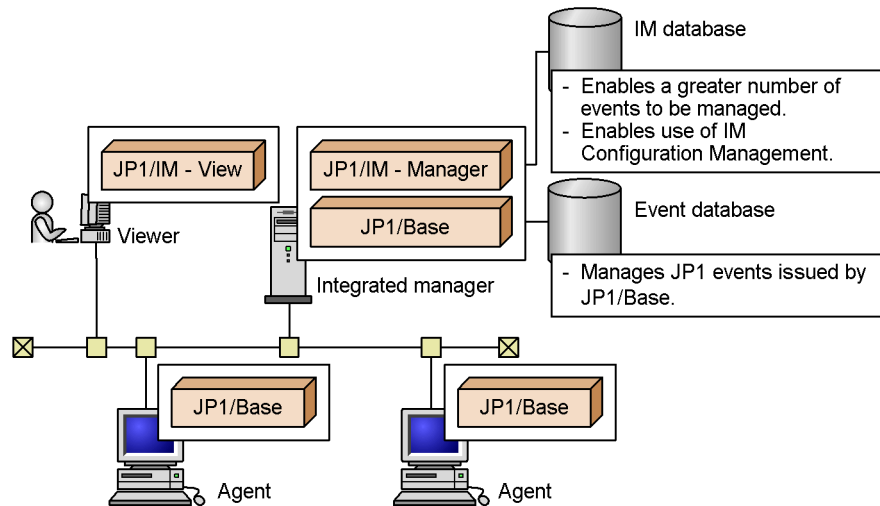


## 2.4 Functions provided by the IM database

JP1/IM - Manager manages JP1 events using its own *IM database* or the event database provided by JP1/Base. You can choose which of these two databases to use.

The following figure shows how the databases are positioned in the system.

Figure 2-9: Positioning of the IM database and JP1/Base event database



*IM database* is a generic term for the following two databases:

- *Integrated monitoring database* used by the Central Console component of JP1/IM - Manager
- *IM Configuration Management database* used by the IM Configuration Management component of JP1/IM - Manager

By setting up the integrated monitoring database and IM Configuration Management database according to the functionality you want to use, you can expand the functionality previously available with the JP1/Base event database.

The following table describes the functionality provided by the integrated monitoring database and IM Configuration Management database.

*Table 2-4:* Functionality provided by the integrated monitoring database and IM Configuration Management database

<b>JP1/IM - Manager component</b>	<b>Database</b>	<b>Available functionality</b>
Central Console	Integrated monitoring database	Add an event display start-time specification area to the Central Console window.
		Change the severity of JP1 events.
		Conduct event searches in the integrated monitoring database.
		Add memos to JP1 events.
		Output event reports to the integrated monitoring database.
IM Configuration Management	IM Configuration Management database	Manage hosts.
		Manage the system hierarchy.
		Manage profiles.
		Manage service activity information.
		Import and export IM Configuration Management information.
		Manage virtualization configurations.

## Chapter

---

# 3. Centralized System Monitoring Using the Central Console

---

This chapter describes how to monitor the system using the Central Console.

- 3.1 Centralized monitoring using JP1 events
- 3.2 Filtering of JP1 events
- 3.3 Issue of correlation events
- 3.4 Consolidated display of repeated events
- 3.5 Searching for events
- 3.6 Event guide function
- 3.7 Setting memo entries
- 3.8 Displaying user-defined event attributes
- 3.9 CSV output of information displayed in JP1/IM - View
- 3.10 Specifying the event display start-time
- 3.11 Specifying the event display period
- 3.12 Performing system operations from JP1/IM

### 3.1 Centralized monitoring using JP1 events

The JP1/IM Central Console centrally monitors major events occurring in the system, such as network problems and server failures, based on JP1 events.

This section describes the following functions used to perform centralized monitoring:

- Monitoring from the Central Console
- Filtering of JP1 events
- Issue of correlation events
- Consolidated display of repeated events
- Searching for events
- Event guide function
- Setting memo entries
- Display of user-defined event attributes
- CSV output of information displayed in JP1/IM - View
- System operations from JP1/IM

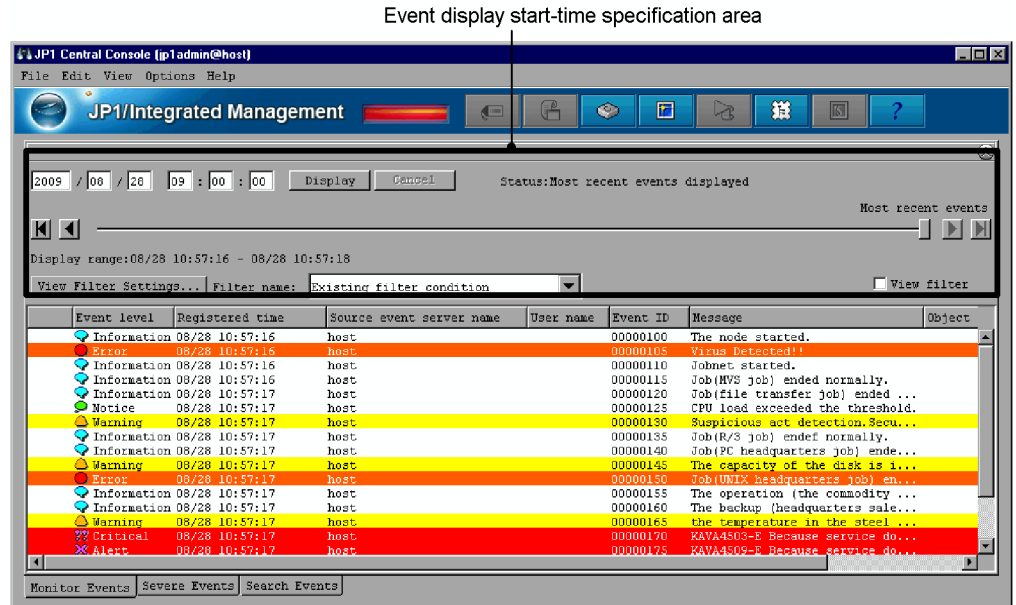
When you use the integrated monitoring database, expanded functionality is available for centralized monitoring, as described in the following table.

*Table 3-1:* Expanded functionality when using the integrated monitoring database

Item	Expanded functionality
Monitoring from the Central Console	You can specify the event display start time and change the event severity level.
JP1 event filtering	You can display more items in the view filter and event receiver filter.
Searching for events	You can specify either the event database or integrated monitoring database as the database to search.
Setting memo entries	You can add memos to JP1 events registered in the integrated monitoring database.
CSV output of information displayed in JP1/IM - View	You can output the JP1 event information saved to the integrated monitoring database in CSV form.

The following figure shows the window for monitoring JP1 events.

Figure 3-1: JP1 event monitoring in the Event Console window



The Event Console window shows a list of JP1 events. JP1 events are managed by JP1/Base, and can be optimally viewed using the various functions provided by JP1/IM.

In the above Event Console window, the area for event display start-time specification is displayed. This area appears only when you use the integrated monitoring database.

Display in the Event Console window

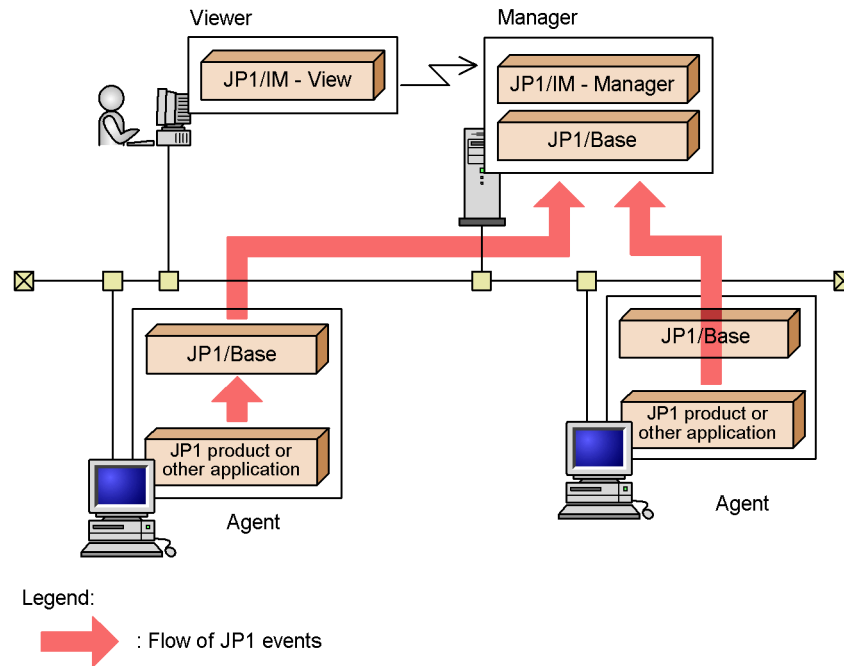
JP1/IM attaches an icon to each event to indicate its level of severity (one of the attributes of JP1 events). This enables visual identification when the user views an event listing.

The event levels of JP1 events are Emergency, Alert, Critical, Error, Warning, Notice, Information, and Debug.

### 3.1.1 Monitoring from the Central Console

The Central Console centrally manages the JP1 events occurring on the agents by extracting the events that need to be dealt with, and then forwarding them to a manager.

Figure 3-2: Overview of JP1 event monitoring from the Central Console



JP1 events are displayed in a time series in the Event Console window. The window has three pages, which you can display as required by clicking the appropriate tab. In some cases, JP1 events might be selected by the filtering function during the pre-processing for display in JP1/IM - View. This is explained below in 3.2 *Filtering of JP1 events*.

JP1 events might also be summarized by the function for consolidating repeated events during the pre-processing for display in JP1/IM - View. This is explained in 3.4 *Consolidated display of repeated events*.

### Monitor Events page

The **Monitor Events** page lists JP1 events in the order in which they occur. Use this page to view events generated in the system in a time series.

The JP1 events listed in the **Monitor Events** page are those passed from the event service to the event base service, and then to the event console service.

The **Monitor Events** page has a view filter, which can be used to filter the displayed events.

When a large number of identical events occur in a short space of time, they can be summarized on the **Monitor Events** page using the function for consolidating repeated events.

## Severe Events page

The **Severe Events** page lists only those JP1 events considered to be severe events.

A *severe event* is a JP1 event that needs to be addressed, such as a failure of some sort. By default, JP1 events whose event level is *Emergency*, *Alert*, *Critical*, or *Error* are defined as severe events.

When a severe event occurs, the alarm lamp in JP1/IM - View flashes to inform the user.

When a large number of identical events occur in a short space of time, they can be summarized on the **Severe Events** page using the function for consolidating repeated events.

## Search Events page

The **Search Events** page displays the results of an event search conducted on a host from JP1/IM - View.

Because only severe events are forwarded to a manager, you must perform an event search if you want to view normal JP1 events. For example, you can use the **Search Events** page to retrieve events immediately before and after a JP1 event indicating a problem when you want to find out what was happening at the time.

You can also use the **Search Events** page to view old events that have disappeared from the JP1/IM - View buffer.

For an overview, see *3.5 Searching for events*.

You can perform the following operations and settings on the JP1 events listed in the three pages of the Event Console window:


- Specify a start time for listing JP1 events

When you use the integrated monitoring database, you can change the JP1 events listed in the Event Console window of JP1/IM - View by specifying a date and time or by moving the slider in the event display start-time specification area. This allows you to see JP1 events when the maximum number of viewable events (JP1/IM - View's scroll buffer size) has been exceeded and there are too many events to fit into the Event Console window all at once.

The event display start-time specification area does not appear in the **Search Events** page.

- View JP1 event details

You can view detailed attribute information about JP1 events. You can also view operating advice, such as troubleshooting procedures, if event guide information has been preset for a selected JP1 event. When you use the integrated monitoring database, you can set and display memos by enabling the function for entering

memos in JP1 events. When a memo has been set, the  icon appears to the left of the listed event.

- Specify a period for listing JP1 events

Using the event display period specification, you can set a base time and a period of days for listing events. For example, suppose the current time is 9:15 am on July 8, and you set the display period as follows:

- **Base time**  
09:00
- **Display period**  
2 days

With this setting, the listing will cover JP1 events that have occurred since 9:00 am on the previous day (July 7).

- Launch linked applications by monitor startup

You can launch the GUI of a linked product associated with a selected JP1 event.

- View the execution results of automated actions

You can view the execution result of an automated action executed in response to a JP1 event.

The execution results of automated actions cannot be displayed in the **Search Events** page.

- Change the display items for JP1 events

The following information can be displayed as JP1 event information in the Event Console window:

Items displayed by default:

**Event level, Registered time, Source host, User name, Event ID, Message, Object type, and Action.**

Items not displayed by default:

**Start time, End time, Product name, Object name, Root object type, Root object name, Arrived time, Occurrence, Serial number, Source process ID, Source user ID, Source group ID, Source user name, Source group name, Source serial number, Type, and Action type.**

When you use the integrated monitoring database, **Original severity level, New severity level, and Memo** are not displayed by default in addition to the above items.

You can change the display items and their order to suit your purpose.



In addition to the above display items, icons representing the event status and the presence of an event memo are displayed in JP1 event listings. These icons appear in front of the event name in the Event Console window. The memo icon does not appear unless you are using the integrated monitoring database.

Event-specific information and other information not covered by the above display items can be displayed in the Event Console window by mapping the event-specific information to one of the above display items.

In this case, # is prefixed to the displayed information.

- Change the severity of JP1 events

When you use the integrated monitoring database, you can change the severity or *event level* of monitored JP1 events. This allows you to manage JP1 events in accordance with your system's operating environment. The event level can be changed to Emergency, Alert, Critical, Error, Warning, Information, Notice, or Debug. You can change the event level for the following functions and monitor the system according to the new setting:

- JP1 event filtering (event receiver filter, severe events filter, and view filter)
- Correlation events
- Event search
- Event guide
- Automated actions
- Output of event report
- Central Scope

For example, the various JP1 events issued by a particular host can be set to the same event level, or a particular JP1 event whose severity is treated differently on different hosts can be set to the same event level on each.

*Figure 3-3:* Changing the event level of all JP1 events issued by host A to "Emergency"

Old levels				New levels		
ID	Severity	Issuing host		ID	Severity	Issuing host
100	Emergency	Host A	→	100	Emergency	Host A
100	Warning	Host B		100	Warning	Host B
100	Alert	Host C		100	Alert	Host C
100	Critical	Host A		100	Emergency	Host A
100	Error	Host A		100	Emergency	Host A
100	Notice	Host B		100	Emergency	Host A
100	Notice	Host B		100	Notice	Host B

To change an event level, use the `jcoimdef` command. For details, see 4.9 *Setting the severity changing function in the Job Management Partner 1/ Integrated Management - Manager Configuration Guide*.

- Set the response status of JP1 events

You can set the response status of JP1 events. Any of the following four statuses can be set, according to how events are processed and the action already taken: **Processed**, **Processing**, **Held**, and **Unprocessed**. You can check the settings in the **Monitor Events** page, **Severe Events** page, or **Search Events** page. The response status is represented by an icon.

The response statuses that can be set and displayed differ for each page, as shown in the following table.

*Table 3-2: Differences in response status settings among pages in the Event Console window*

Page	Specifiable response statuses	Number of events whose response status can be set in one operation	Update of other pages when response status changes <sup>#2</sup>
<b>Monitor Events</b>	Processed, Processing, Held, Unprocessed	Multiple	Automatically updated
<b>Severe Events</b>	Processed, Processing, Held, Unprocessed, Delete <sup>#1</sup>	Multiple	Automatically updated
<b>Search Events</b>	Processed, Processing, Held, Unprocessed	Multiple	After next search

<sup>#1</sup>: When **Delete** is set for a JP1 event on the **Severe Events** page, that JP1 event is no longer listed on the page. However, because events deleted on this page are not erased from the event database or integrated monitoring database, they might still appear on other pages and, if so, their response status can still be set.

<sup>#2</sup>: When a response status is set on another page, the **Monitor Events** page or **Severe Events** page is automatically updated to reflect the changed status (provided the **Apply** check box is selected for **Automatic refresh** in the Preferences window). Otherwise, you can update the response status in the **Monitor Events** page and **Severe Events** page by choosing **View** and then **Refresh**, or by clicking the **Refresh** button. To refresh the **Search Events** page, you must perform another search.

You can also set the response status in the Related Events window, which opens from the Event Console window. You can set and display the same statuses as on the page from which you opened the Related Events window.

You can also generate a JP1 event whenever a response status changes. This allows you to record a history of the actions taken.

- **Highlighting**

You can apply a background color to the JP1 events displayed in the Event Console window (the default is no highlighting). When you enable **Coloring**, highlighting is applied on each page as follows:

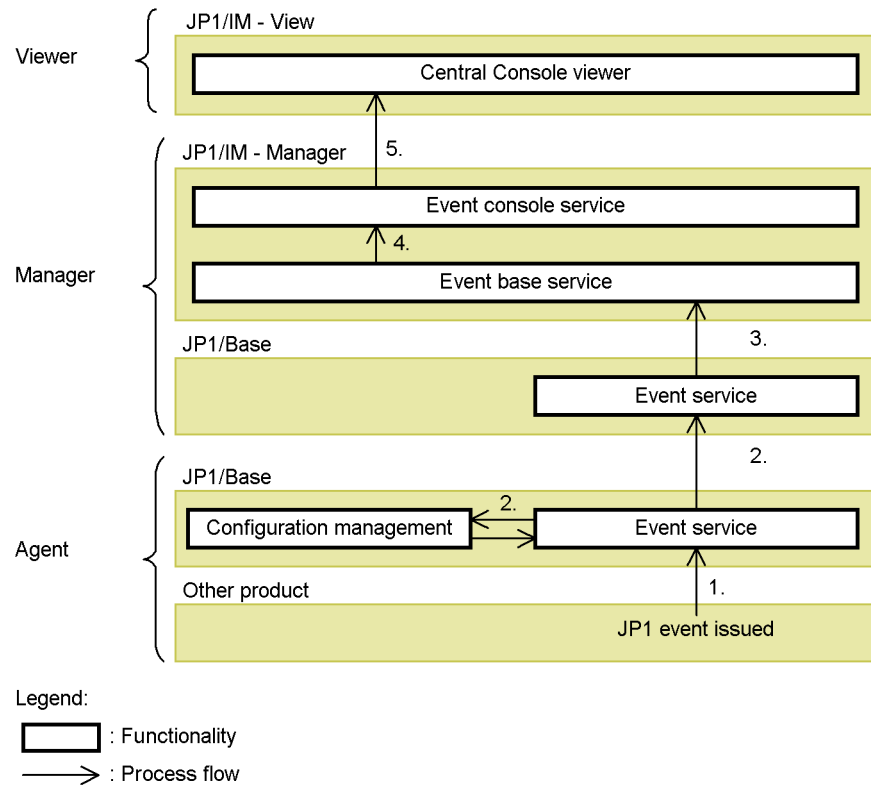
- **Monitor Events** page: Highlight according to the event level.
- **Severe Events** page: No highlighting.
- **Search Events** page: Highlight according to the event level.

When you use the integrated monitoring database, events are highlighted according the user-defined event level.

### 3.1.2 Flow of processing for JP1 event monitoring

The following describes how the JP1/IM and JP1/Base functionality are inter-linked in event monitoring, taking as an example the flow of processing from the time an agent issues a JP1 event until the event appears in the windows of a viewer.

Figure 3-4: Flow of processing for JP1 event monitoring



The flow of processing is described below, following the numbers in the figure:

1. The agent issues a JP1 event, which is registered with its event service.
2. The registered JP1 event is forwarded to a higher-level host in accordance with the definitions in the configuration definition file, and is registered with that host's event service.
3. Information about the registered JP1 event is acquired by the event base service.
4. The event console service acquires the JP1 event information from the event base service.
5. The JP1 event acquired by the event console service is monitored from the viewer.

For details about the event service, see 7.4.2 *Managing JP1 events using JP1/Base*. For details about configuration management, see 7.4.3 *Managing the system hierarchy*. For details about the event base service, see 3.1.3 *Internal control of JP1 events by JP1/IM - Manager*.

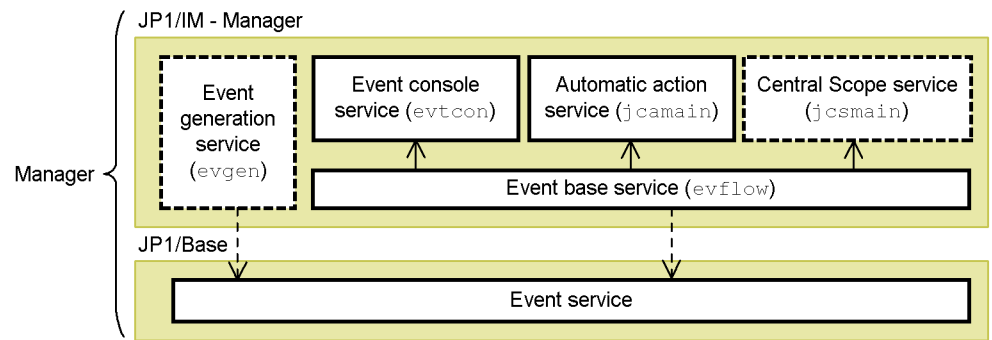
### 3.1.3 Internal control of JP1 events by JP1/IM - Manager

Internal processing in JP1/IM - Manager is based on information about JP1 events collected from the event database in JP1/Base and from the integrated monitoring database in JP1/IM - Manager.

#### (1) JP1 event control when not using the integrated monitoring database

If you do not use the integrated monitoring database, JP1 events are collected from the JP1/Base event database by the JP1/IM - Manager's event base service and event generation service.

Figure 3-5: Internal control of JP1 events by JP1/IM - Manager



Legend:

----> : JP1 event acquisition request to the JP1/Base event service

—> : JP1 event transfer to JP1/IM - Manager internal services

(name) : Process name displayed by executing the `jco_spmc_status` command

----- : Service disabled by default (can be enabled by the `jcoimdef` command)

----- : Service enabled by default

The JP1 events acquired by these two services are processed in various ways after they have been filtered by the event acquisition filter according to set conditions.

#### Processing of acquired JP1 events by the event base service

The event base service forwards JP1 events to the event console service, automatic action service, and Central Scope service. These three services execute processing (for example, event display in JP1/IM - View or an automated action) according to the received JP1 event.

Using the `jcoimdef` command, you can adjust the JP1 event acquisition and transfer processing performed by the event base service (for example, you can change the event acquisition start location, or the transfer timeout period and retry setting). For details, see *jcoimdef* in 1. Commands in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File*

*Reference.*

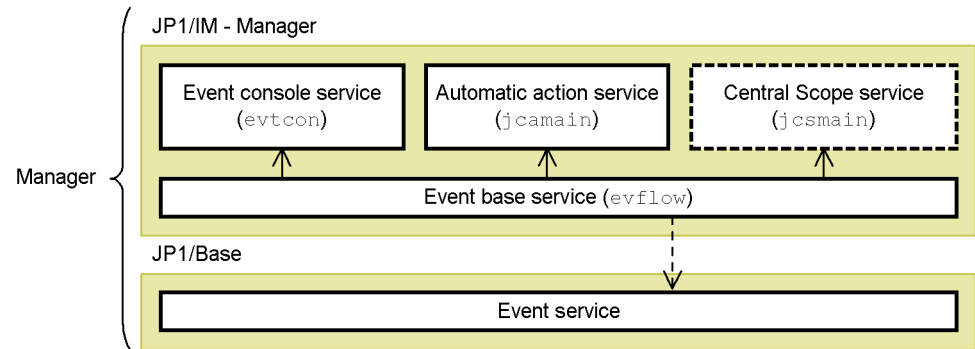
## Processing of acquired JP1 events by the event generation service

This service performs correlation event issue based on issue definitions. For details, see 3.3 *Issue of correlation events*.

**(2) JP1 event control when using the integrated monitoring database**

When you use the integrated monitoring database, JP1 events are collected from the JP1/Base event database by the JP1/IM - Manager's event base service. The acquired JP1 events are stored in the integrated monitoring database.

Figure 3-6: Internal control of JP1 events by JP1/IM - Manager



## Legend:

-----> : JP1 event acquisition request to the JP1/Base event service

————> : JP1 event transfer to JP1/IM - Manager internal services

(name) : Process name displayed by executing the `jco_spmc_status` command

----- : Service disabled by default (can be enabled by the `jcoimdef` command)

———— : Service enabled by default

The JP1 events acquired by the event base service are processed in various ways after they have been filtered by the event acquisition filter according to set conditions.

## Processing of acquired JP1 events by the event base service

The event base service performs correlation event issue based on issue definitions, and then forwards the JP1 events to the event console service, automatic action service, and Central Scope service. These three services execute processing (for example, event display in JP1/IM - View or an automated action) according to the received JP1 event.

Using the `jcoimdef` command, you can adjust the JP1 event acquisition and transfer processing performed by the event base service (for example, you can change the event acquisition start location, or the transfer timeout and retry

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

---

## 3.2 Filtering of JP1 events

---

JP1/IM and JP1/Base use filtering to select and process required JP1 events. For example, you can forward to a manager only those JP1 events that need to be managed, and you can select JP1 events among those displayed on a viewer.

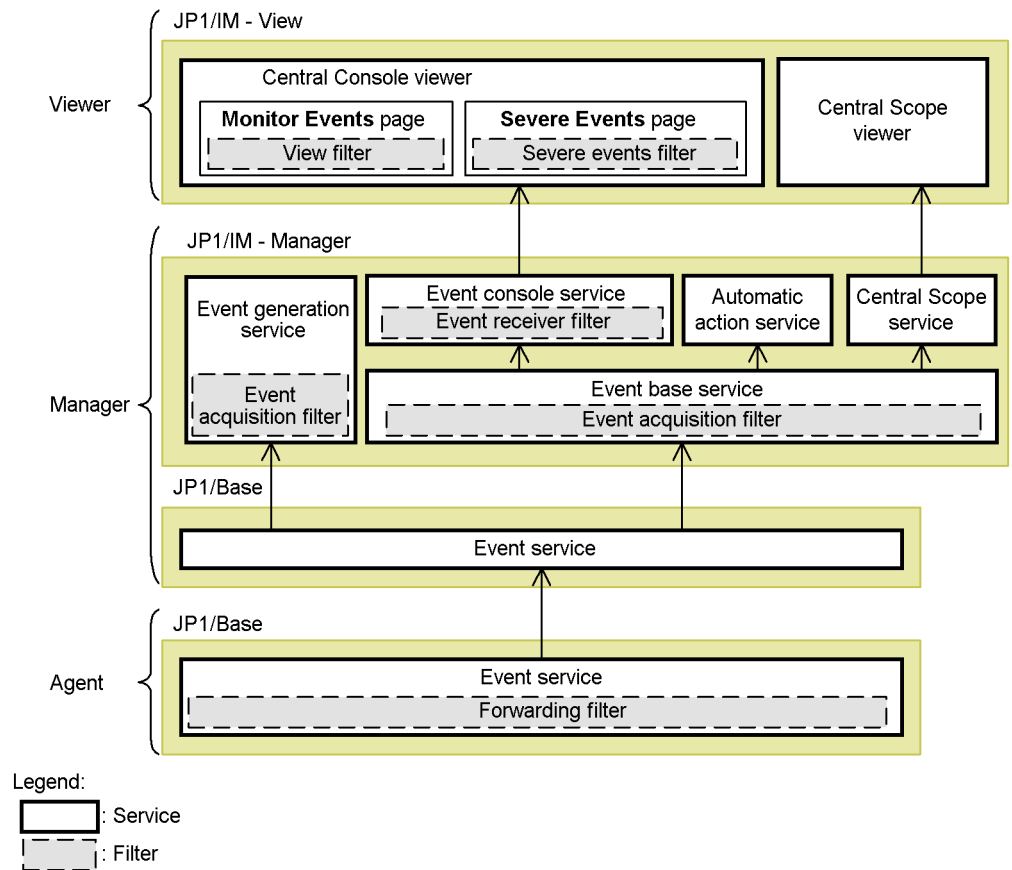
JP1/IM and JP1/Base provide the following five types of filtering:

- Forwarding filter
- Event acquisition filter
- Event receiver filter
- Severe events filter
- View filter

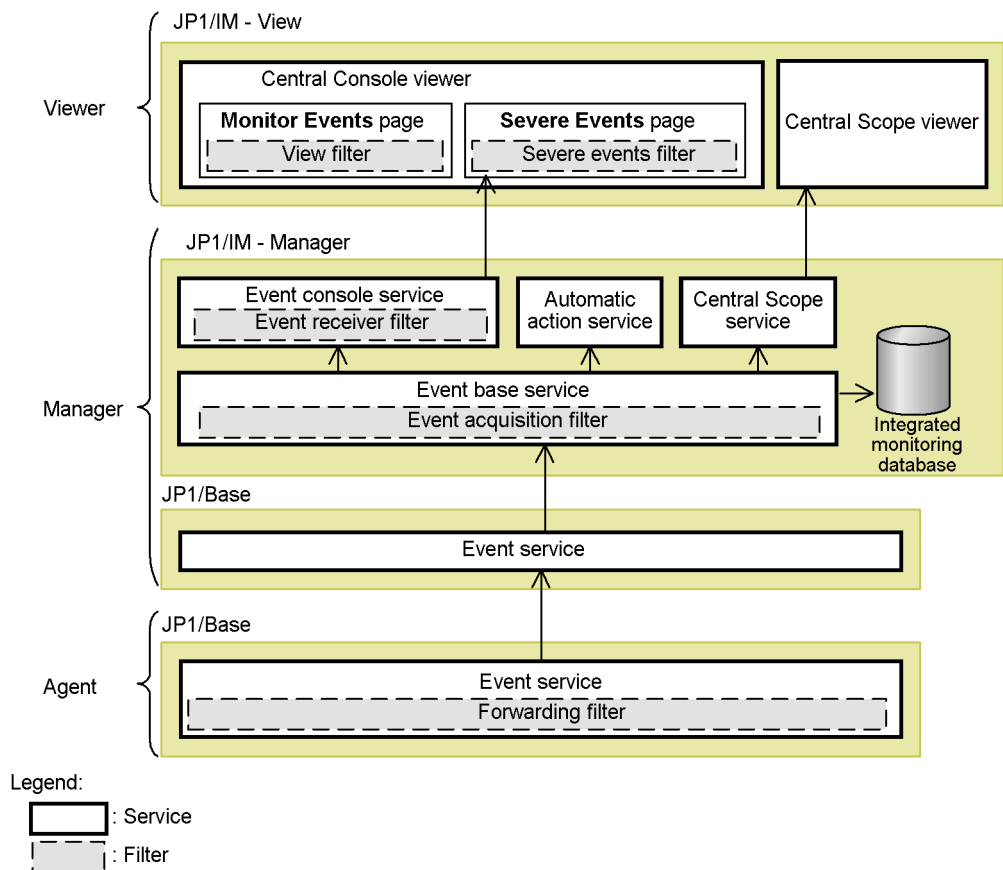
You can combine these filters to select and process the required JP1 events. Of the five different filters, the positioning of the event acquisition filter differs depending on whether you use the integrated monitoring database.



Figure 3-7: Filters provided by JP1/IM and JP1/Base (when not using the integrated monitoring database)



*Figure 3-8: Filters provided by JP1/IM and JP1/Base (when using the integrated monitoring database)*



Depending on whether you use the integrated monitoring database, different services are used to filter JP1 events but the result is the same.

When you use the integrated monitoring database, the JP1 events selected by the event acquisition filter are saved in the integrated monitoring database.

The five filters are described next, in the order in which they are applied, starting from the issuing source.

### 3.2.1 Forwarding filter

A forwarding filter is for selecting JP1 events to be sent to another host. Only one such filter can be set in JP1/Base on each agent.

JP1/IM centrally manages the JP1 events occurring on the agents by forwarding them to a manager. Only those JP1 events that need to be managed by a higher-level

manager are selected and forwarded. You can specify these target JP1 events in a forwarding filter. A forwarding filter can also be used to reduce JP1 event traffic when the load on a manager needs to be restricted or the network has limited capacity.

Forwarding filters are specific to each instance of JP1/Base. A forwarding settings file can be edited on each agent individually, or you can distribute forwarding setting information in a batch from a manager to the agents.

### 3.2.2 Event acquisition filter

An event acquisition filter is for selecting the JP1 events to be acquired from JP1/Base by JP1/IM - Manager (using the event base service). Multiple event acquisition filters can be defined on each manager, but only one of them can be applied.

Using an event acquisition filter, you can select the JP1 events that need to be acquired by JP1/IM - Manager. The following target JP1 events can be specified:

- JP1 events monitored on the **Monitor Events** page or **Severe Events** page of the Event Console window
- JP1 events that trigger automated actions
- JP1 events that change the status of a monitoring object
- JP1 events that issue a correlation event (correlation source events)

For example, in a system where the installed products issue a large number of normal events on a JP1/IM manager (such as events issued by JP1/AJS indicating successful job execution), the JP1 events essential to monitoring the system operation might be overlooked. In this type of situation, an event acquisition filter can be used to filter out normal events so that they will not be acquired.

Event acquisition filters reside in JP1/IM - Manager and can be set from JP1/IM - View. They affect all JP1/IM functions, including JP1 event monitoring, automated actions, and object status monitoring.

When you use the integrated monitoring database, the JP1 events selected by the event acquisition filter are saved in the integrated monitoring database.

*Reference note:*

- To display events in JP1/SES format in JP1/IM - View, you must change the event acquisition filter settings to acquire JP1/SES events. The default settings do not display JP1/SES events.
- If you were using the event acquisition filter (for compatibility) in a previous version of JP1/IM, the filter works in a different position and operates differently from a standard event acquisition filter. Also, even if you are using the integrated monitoring database with the event acquisition filter (for compatibility), events are still selected by the event acquisition filter (for compatibility). For details, see the following:

*12.2.1(1) Upgrading from the Central Console version 8*

*12.2.3(2) Upgrading from JP1/IM - Central Console version 7*

- If you are not using the integrated monitoring database, the event acquisition filter also applies to the event generation service.

The event generation service is inactive by default. When it is started, however, the filter definitions in effect for the event base service are also applied to the event generation service.

If you are using the event acquisition filter (for compatibility), the event generation service operates without any filter conditions.

For details about the event generation service, see *3.3 Issue of correlation events*.

Setting multiple event acquisition filters

You can set multiple event acquisition filters.

For example, if you want to change the type of JP1 events collected or the host from which they are acquired according to the time of day (business hours or night time), you can set different event acquisition filters for the different times of day and switch between them.

Events issued when an event acquisition filter is switched

When you switch to a different event acquisition filter, JP1/IM - Manager issues JP1 events (event IDs 00003F13 and 00003F20) reporting the changed filter conditions. The messages give the name of the filter now in effect and the arrival time and serial number of the last event received by JP1/IM - Manager before the filter was switched.

These JP1 events (event IDs 00003F13 and 00003F20) report that the new event acquisition filter came into effect from the first event received by JP1/IM - Manager after the event corresponding to the arrival time and serial number given in the messages. That is, the filter change and JP1 event issue do not occur at the

same time.

For example, if a large number of other JP1 events were issued at the time the filter was switched, there might be a delay before the JP1 events (event IDs 00003F13 and 00003F20) reporting the changed filter conditions appear in the Event Console window. This could mean that the first JP1 event acquired with the new filter appears before the JP1 events reporting the filter change.

To identify the first JP1 event acquired with the new event acquisition filter, check the messages (event IDs 00003F13 and 00003F20) to find the last JP1 event acquired before the change. (Subsequent JP1 events will have been acquired with the new event acquisition filter.)

For details about the JP1 events (event IDs 00003F13 and 00003F20), see 3. *JP1 Events* in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*. Note that these JP1 events are not issued when the event acquisition filter is operating in compatibility mode.

### 3.2.3 Event receiver filter

An event receiver filter is for selecting (restricting) the JP1 events that can be monitored by individual JP1 users. Multiple event receiver filters can be defined on each manager, but only one can be applied per JP1 user.

To monitor the system operation using JP1/IM, the user must log in to a manager from JP1/IM - View. Depending on the system, the range of resources that can be monitored by each JP1 user might need to be restricted, or you might want multiple JP1 users to monitor different parts of a large system. Using event receiver filters, you can select the JP1 events appearing in the Event Console window according to the JP1 user.

Event receiver filters reside in JP1/IM - Manager and can be set from JP1/IM - View. They affect the **Monitor Events** page, **Severe Events** page, and **Search Events** page of the Event Console window.

### 3.2.4 Severe events filter

A severe events filter is for selecting severe JP1 events that need to be managed.

Only one such filter can be set on each manager. Because the filter settings are managed on the manager, the same severe events filter is applied to all viewers that connect to that manager.

Some JP1 events, such as emergency notices and error reports, require an immediate response from the operator. In JP1/IM, such JP1 events are known as *severe events*.

The **Severe Events** page of the Event Console window is specifically for managing severe events.

When a severe event occurs, the alarm lamp flashes in JP1/IM - View to notify the user. You can manage the response status of severe events on the **Severe Events** page.

Events whose event level is Emergency, Alert, Critical, or Error are defined as severe events in the default severe events filter.

By customizing the default filter, you can select the event levels you want to define as severe events. You can also exclude specific JP1 events that are normally classed as severe events by specifying the event ID or other attribute. Excluded events cannot be handled as severe events, however.

Severe event filters reside in, and can be set from, JP1/IM - View. They affect the **Severe Events** page of the Event Console window.

#### 3.2.5 View filter

A view filter is for temporarily restricting the JP1 events displayed in the **Monitor Events** page of the Event Console window to specific JP1 events only. Multiple view filters can be defined for a specific monitoring user of a viewer, and users can switch view filters by easy operation.

View filters reside in, and can be set from, JP1/IM - View. They affect the **Monitor Events** page of the Event Console window.

#### 3.2.6 Defining filter conditions

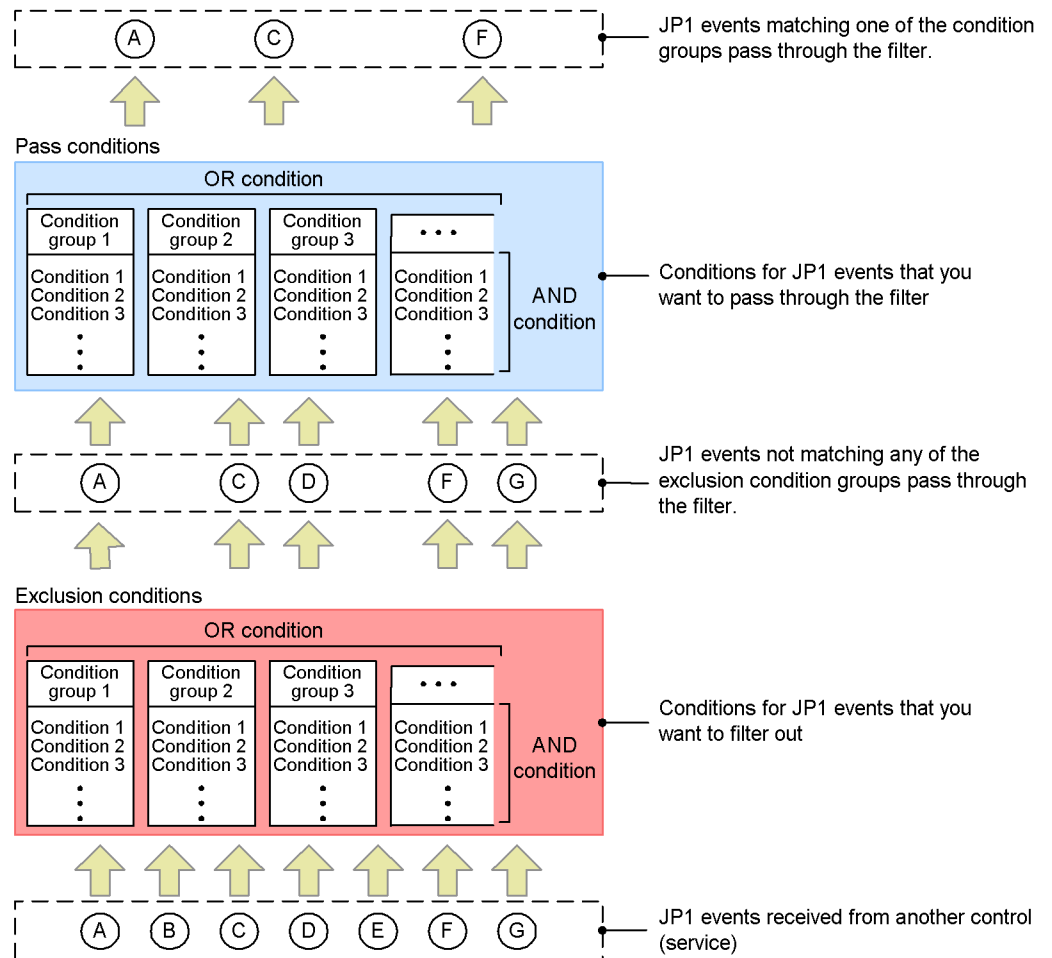
As the conditions in a filter, you can define exclusion conditions and pass conditions. *Exclusion conditions* are a set of conditions for JP1 events that you do not want to display (acquire). *Pass conditions* are a set of conditions for JP1 events that you do want to display (acquire). As a separate class of conditions, there are also *common exclusion conditions*, which allow you to disable or apply a condition group in an event acquisition filter. Filter conditions apply in the following order of precedence: common exclusion conditions, exclusion conditions, and pass conditions.

You can define a combination of common exclusion conditions, exclusion conditions, or pass conditions in a *condition group*. A condition group contains one or more conditions, and is satisfied when all the defined conditions are satisfied. That is, the conditions in a filter are related by an AND condition.

When a filter consists of exclusion conditions and pass conditions, combined into multiple condition groups of either type, those JP1 events matching the conditions in one of the exclusion condition groups are filtered out, and those JP1 events matching the conditions in one of the pass condition groups pass through the filter and are transferred to the higher-level control (see Figure 3-7 *Filters provided by JP1/IM and JP1/Base (when not using the integrated monitoring database)* and Figure 3-8 *Filters provided by JP1/IM and JP1/Base (when using the integrated monitoring database)*). That is, the condition groups of exclusion conditions or pass conditions are related by an OR condition.

The following figure shows how a filter works.

Figure 3-9: Event transfer through a filter to higher-level control



Except for the JP1/Base forwarding filter, you define filter conditions in JP1/IM - View.

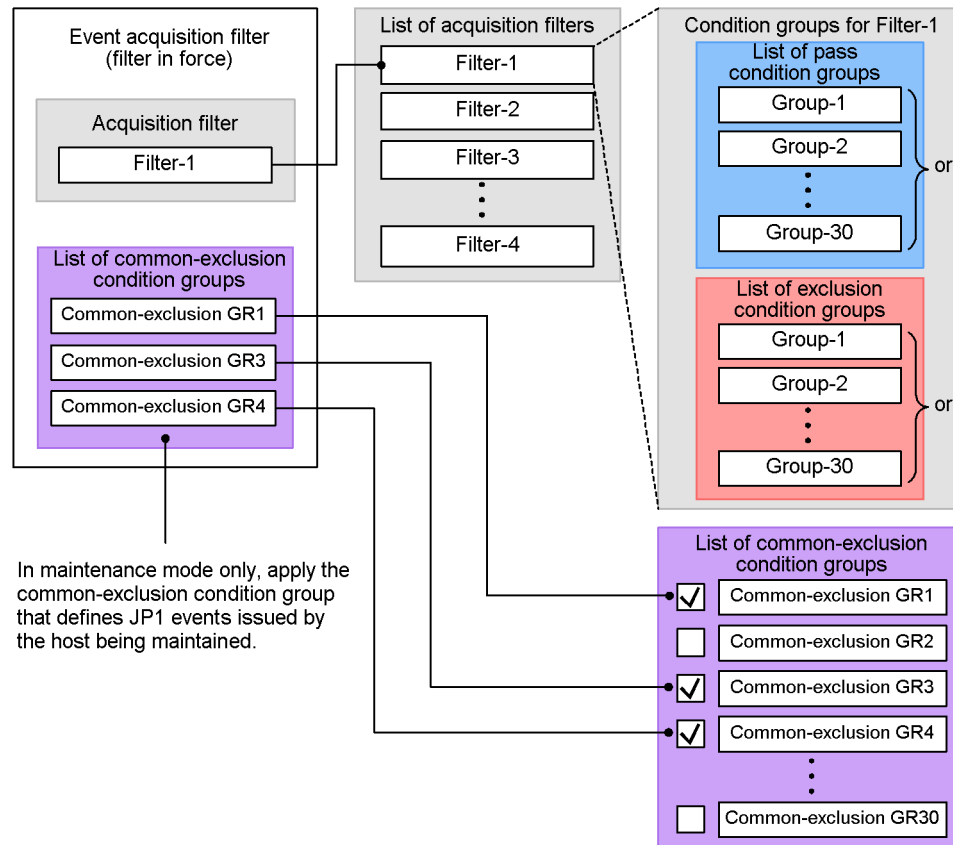
#### (1) Common exclusion conditions (event acquisition filter only)

Common exclusion conditions form part of an event acquisition filter and consist of a group of conditions for filtering out JP1 events. You can apply or disable each group. In maintenance mode, for example, you can set a common-exclusion condition group to temporarily filter out JP1 events issued by the host you are working on, without having to change the pass conditions or exclusion conditions in the event acquisition filter. If you have defined multiple event acquisition filters, and switch among them as required, the common exclusion conditions you set apply to whichever filter is in force.

Of the conditions defined in an event acquisition filter, common exclusion conditions take precedence over exclusion conditions, which take precedence over pass conditions. To define common exclusion conditions, JP1/Base version 09-00 or later is required on the JP1/IM - Manager host.

The following figure shows the relationships among the common exclusion conditions, exclusion conditions, and pass conditions in event acquisition filters.

*Figure 3-10: Relationships among the filter conditions in event acquisition filters*



## (2) Exclusion conditions

Exclusion conditions filter out events. JP1 events that match any one of the defined condition groups do not pass through the filter. Exclusion conditions take precedence over pass conditions. To define exclusion conditions, JP1/Base version 09-00 or later is required on the JP1/IM - Manager host.

You can define exclusion conditions in an event acquisition filter, event receiver filter,



severe events filter, view filter, and in event searches.

**(3) *Pass conditions***

Pass conditions display (acquire) events. JP1 events that match any one of the defined condition groups pass through the filter.

You can define pass conditions in an event acquisition filter, event receiver filter, severe events filter, view filter, and in event searches.

---

### 3.3 Issue of correlation events

---

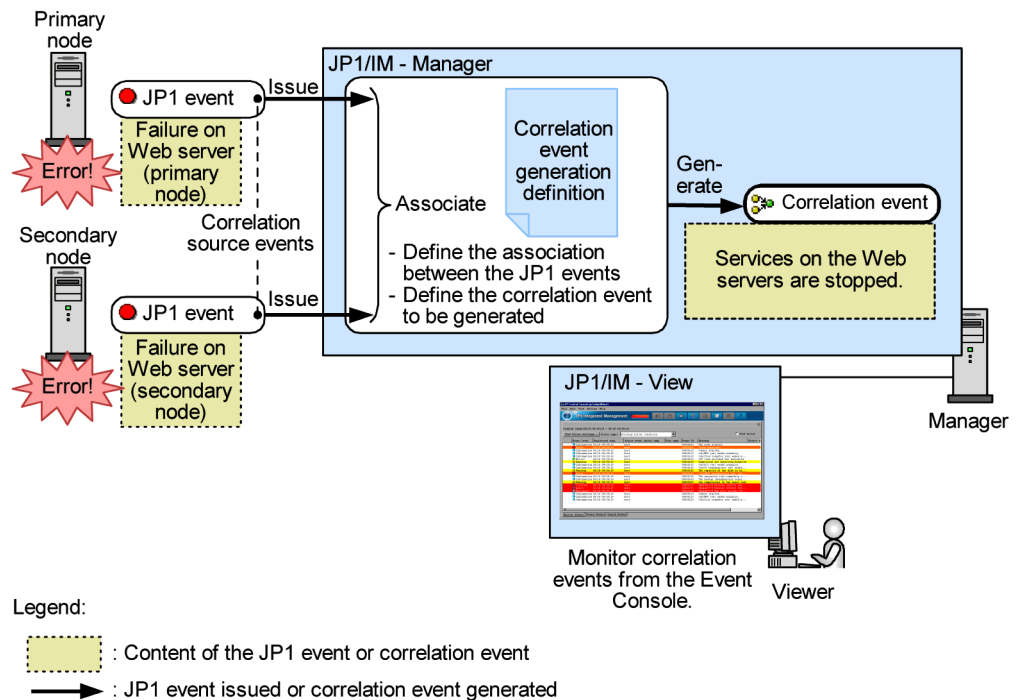
JP1/IM - Manager can issue a new JP1 event whenever two or more related JP1 events are issued. The new event is known as a *correlation event*. The correlation event and the association between the JP1 events can be defined by the user as a *correlation event generation definition*.

The related JP1 event that triggers the correlation event is known as a *correlation source event*. You can define multiple correlation source events, or just one.

For example, suppose JP1/IM - Manager is managing Web servers in a cluster system. If a failure occurs in succession on both the primary node and secondary node, the service provided by the Web servers on these nodes will stop. By associating the JP1 event reporting a failure on the primary node with the JP1 event reporting a failure on the secondary node, and defining a correlation event, you can ensure a speedy response.

The following figure shows the relationships between a correlation event, correlation event generation definition, and correlation source events, based on the above Web server example.

Figure 3-11: Relationships between correlation event, correlation event generation definition, and correlation source events



The JP1 events issued from the Web servers on the primary and secondary nodes are sent to the manager. The two JP1 events are associated and a *correlation event* is issued, according to the *correlation event generation definition*. The JP1 events that triggered the correlation event are known as *correlation source events*.

There are two kinds of correlation events: A *correlation approval event* is issued when a correlation is established; a *correlation failure event* is issued when no correlation is established.

#### Event issued when a correlation is established

You can issue a correlation approval event when the specified events all arrive within a set timeout period, as in these examples:

1. Two Web servers are configured in a cluster system. Errors on the primary node issue event A, and errors on the secondary node issue event B.
2. To detect that services on the Web servers have stopped, write a correlation event generation definition that issues a correlation approval event (event C) when both event A and event B are issued.

#### Event issued when no correlation is established

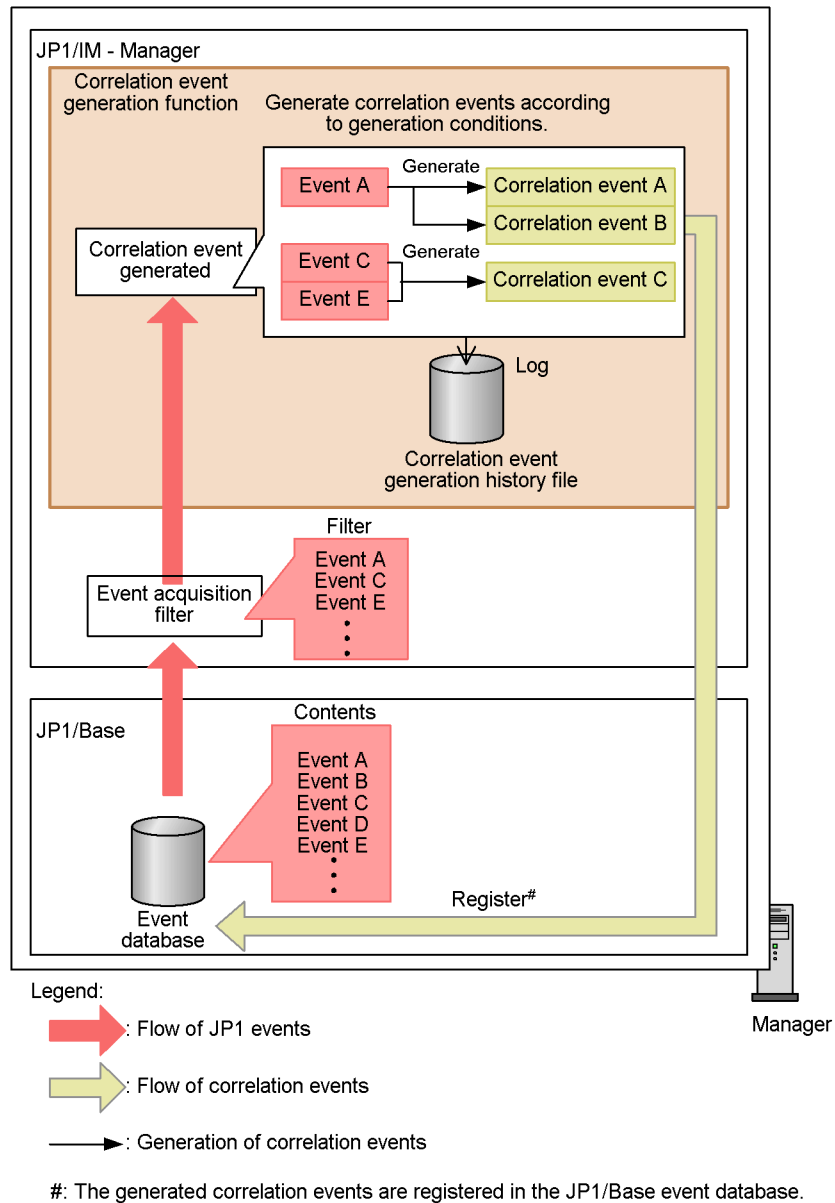
You can issue a correlation failure event when the specified events do not all arrive within the timeout period, as in these examples:

1. Two Web servers are configured in a cluster system. Errors on the primary node issue event A, and errors that occur at failover to the secondary node issue event B.
2. To detect that services on the Web servers have stopped, write a correlation event generation definition that issues a correlation failure event (event C) if event B does not arrive within the set timeout period after event A is issued.

The JP1 events registered with the JP1/Base event database are acquired by JP1/IM - Manager through an event acquisition filter. JP1/IM - Manager then issues correlation events, based on the settings in the correlation event generation definition. These correlation events are also registered with the JP1/Base event database. This processing is known as *correlation event issue*.

The following figure shows an overview of correlation event issue.

Figure 3-12: Overview of correlation event issue



The following describes correlation event issue in further detail.

### 3.3.1 Correlation event issue

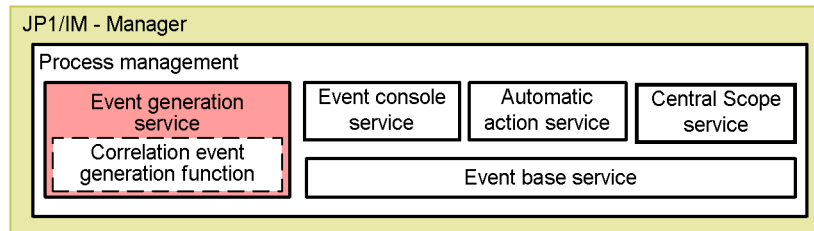
Correlation events are issued by the following JP1/IM - Manager processes:

- When not using the integrated monitoring database: Event issue service
- When using the integrated monitoring database: Event base service

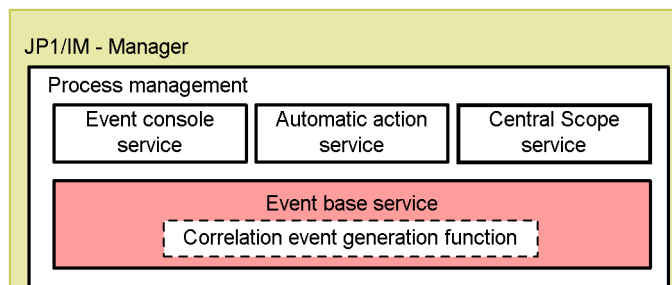
The event generation service and event base service provide the *correlation event generation function*.

This function is positioned internally as shown below.

*Figure 3-13: Position of the correlation event generation function (when not using the integrated monitoring database)*



*Figure 3-14: Position of the correlation event generation function in the event base service (when using the integrated monitoring database)*



When you use the integrated monitoring database, the correlation event generation function is provided by the event base service. This means that event correlation processing can be synchronized with transfer of events to the event console service.

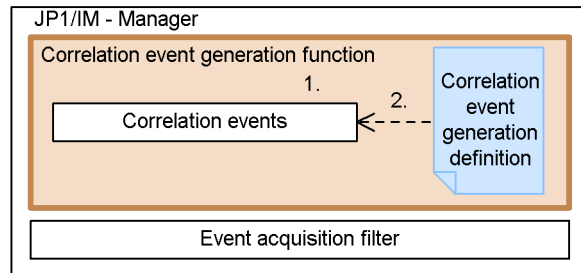
#### **(1) Processing at startup of the correlation event generation function**

When JP1/IM - Manager starts, the correlation event generation function reads the correlation event generation definition in preparation for issuing correlation events.

If you are not using the integrated monitoring database, by default the event generation service does not start when JP1/IM - Manager starts. You must enter a setting using the `jcoimdef` command to start this service at JP1/IM - Manager startup. When you use the integrated monitoring database, the event base service starts automatically but the correlation event generation function is disabled by default. You must use the `jcoimdef` command to enable the function.

The following figure shows the processing at startup of the correlation event generation function.

*Figure 3-15: Processing at startup of the correlation event generation function*



1. Started by the process management (`jco_spm`) in the same way as other services.
2. Read at startup

The flow of processing is described below, following the numbers in the figure:

1. The correlation event generation function is started by the process management functionality.

The correlation event generation function is started and stopped by the process management in the same way as other JP1/IM - Manager services.

If you are not using the integrated monitoring database, by default the event generation service does not start when JP1/IM - Manager starts. You must enter a setting using the `jcoimdef` command to start this service at JP1/IM - Manager startup. When you use the integrated monitoring database, the event base service starts automatically but the correlation event generation function is disabled by default. You must use the `jcoimdef` command to enable the function.

2. The correlation event generation function reads the correlation event generation definition held internally.

The correlation event generation function behaves according to the internally recorded correlation event generation definition. For this reason, if you edit the correlation event generation definition file, you must apply the changes using the `jcoegschange` command; otherwise, the service operation will remain unchanged.

The default definition does not issue correlation events. To issue correlation events, you must edit the correlation event generation definition file and execute the `jcoegschange` command to apply the settings.

*Reference note:*

To change a correlation event generation definition, use the `jcoegschange` command.

You can update an issue definition while the correlation event generation function is active. If the service is stopped, you can update the definition to be used from the next run.

However, you cannot edit a correlation event generation definition while the function is in the process of starting or stopping.

## **(2) JP1 event acquisition after startup of the correlation event generation function**

The processing of JP1 events after the correlation event generation function starts sometimes differs depending on whether you are using the integrated monitoring database. The following describes the flow of processing in each case.

### **(a) Correlation processing when not using the integrated monitoring database**

Once started, the correlation event generation function associates the correlation event generation definitions with events acquired by the event generation service and issues correlation events.

You can select the location in the JP1/Base event database at which the event generation service begins event acquisition after startup. To set the location, select either `cold` or `warm` start mode. These are referred to collectively as *start options*. Using the start options, you can specify whether to resume correlation processing from the previous run. The start options are described in the table below.

*Table 3-3: Start options for correlation event issue*

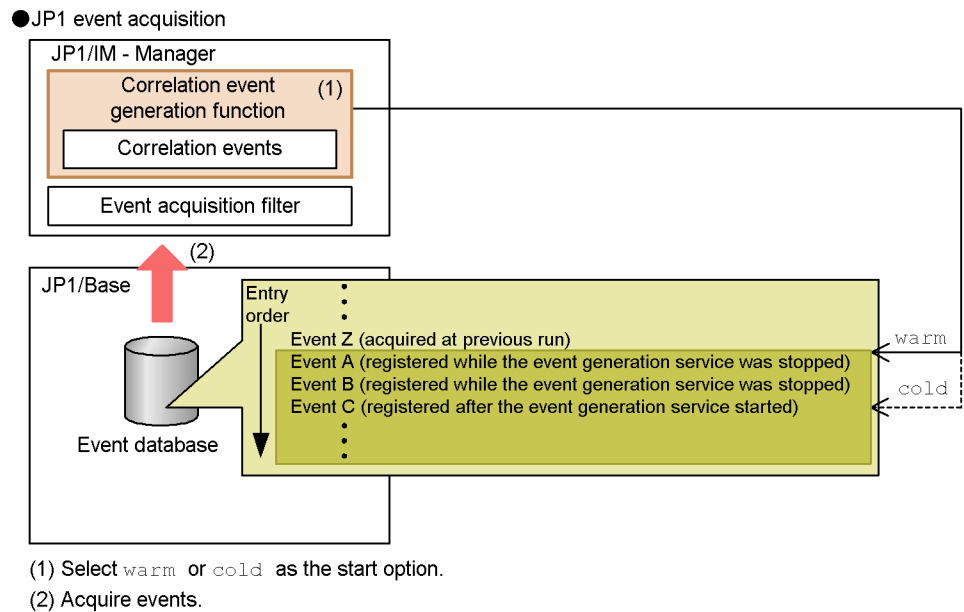
Start option	Description
<code>cold start</code>	Begins acquiring JP1 events that have been registered in the JP1/Base event database since the correlation event generation function started. Stops the correlation processing that was being executed before JP1/IM - Manager stopped. When JP1/IM - Manager is restarted, the function's previous execution status no longer applies.
<code>warm start</code>	Begins acquiring JP1 events registered in the JP1/Base event database, starting from the JP1 event following the last one acquired when the function stopped at the previous run. Records the correlation processing that was being executed before JP1/IM - Manager stopped. When JP1/IM - Manager is restarted, the function's previous execution status takes effect. The default is <code>warm start</code> .

The following figure shows the differences between a `cold start` and `warm start` in



commencing JP1 event acquisition.

Figure 3-16: Differences in starting acquisition of JP1 events



If JP1 events up to event Z have been acquired when the correlation event generation function stops, acquisition will commence from event A (the next event registered after event Z) if the service is restarted in `warm` mode. If the service is restarted in `cold` mode, acquisition will commence from event C (the first event registered after the function restarts).

By default, the correlation event generation function starts in `warm` mode. This is appropriate in most circumstances, but if you do not need to correlate events issued while the function was stopped, switch to `cold` start mode.

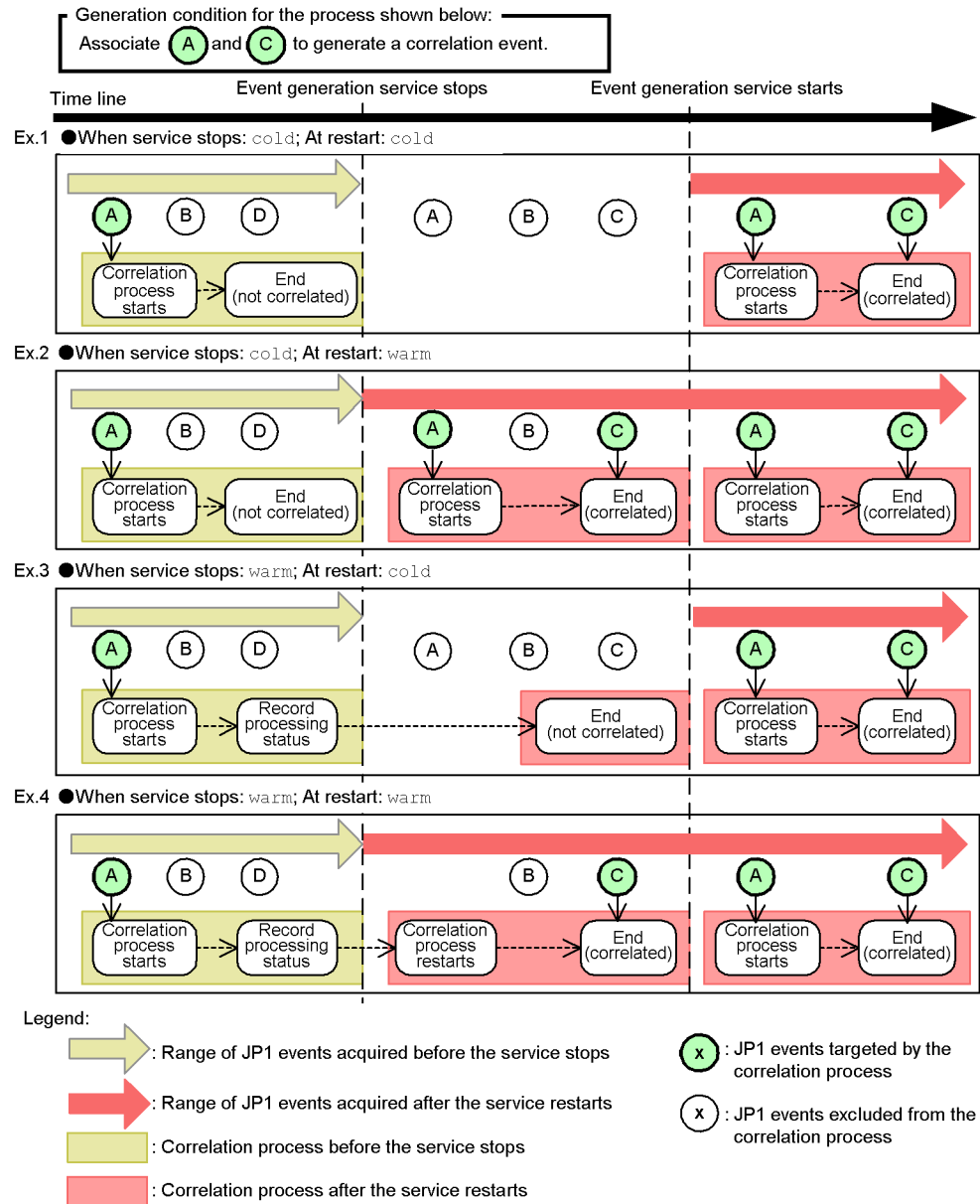
We recommend that you use `warm` starts when running JP1/IM - Manager in a cluster system. If you use `cold` starts, the service will not acquire JP1 events issued while JP1/IM - Manager is being failed over.

Only those JP1 events selected by an event acquisition filter are acquired by the correlation event generation function. For details about event acquisition filters, see *3.2 Filtering of JP1 events*.

#### ■ Correlation processing examples (when not using the integrated monitoring database)

The following figure shows the processing to issue correlation event issue when a `cold` start is specified and when a `warm` start is specified.

**Figure 3-17:** Correlation processing when the event generation service stops and after it restarts (when not using the integrated monitoring database)



The following describes how the correlation process behaves in the examples in *Figure 3-17*.

*Example 1:*

If the `cold` start option applies when the event generation service stops and when it is restarted, the correlation processing behaves as follows:

When the event generation service stops

- Processing ends and information about all target JP1 events is discarded.
- The processing contents are logged to a correlation event generation history file.

After the event generation service restarts:

- Acquisition starts from the JP1 events registered after restart.
- The service reads the correlation event generation definition, and starts processing accordingly.

*Example 2:*

If the `cold` start option applies when the event generation service stops, and `warm` applies when it is restarted, the correlation processing behaves as follows:

When the event generation service stops

- Processing ends and information about all target JP1 events is discarded.
- The processing contents are logged to a correlation event generation history file.

After the event generation service restarts:

- Acquisition starts from the JP1 event following the last one acquired when the service stopped at the previous run.
- The service re-reads the correlation event generation definition, and starts processing accordingly.

*Example 3:*

If the `warm` start option applies when the event generation service stops, and `cold` applies when it is restarted, the correlation processing behaves as follows:

When the event generation service stops

- Information about the JP1 events being correlated, the processing contents, and the information in the correlation event generation definition are output to an internal log to record the processing status.
- The processing contents are logged to a correlation event generation history file.

After the event generation service restarts:

- All information about JP1 events being correlated when the service stopped at the previous run is discarded.
- Acquisition starts from the JP1 events registered after the restart.
- The service reads the correlation event generation definition, and starts processing accordingly.

*Example 4:*

If the `warm` start option applies when the event generation service stops and when it is restarted, the correlation processing behaves as follows:

When the event generation service stops

- Information about the JP1 events being correlated, the processing contents, and the information in the correlation event generation definition are output to an internal log to record the processing status.
- The processing contents are logged to a correlation event generation history file.

After the event generation service restarts:

- Acquisition starts from the JP1 event following the last one acquired when the service stopped at the previous run.
- The service re-reads the correlation event generation definition, and starts processing accordingly.
- The service references the internal log and resumes processing from the JP1 events being correlated, if any, when the previous run stopped.

However, if you change the correlation event generation definition after the service stops and before it restarts, all information about JP1 events being correlated at the end of the previous run is discarded (same behavior as for a `cold` start).

*Note:*

If the event generation service ends abnormally, information about the JP1 events being correlated cannot be recorded. Therefore, at the next run, the service will behave as for a `cold` start: Information about the JP1 events being correlated at the end of the previous run is discarded, and acquisition starts from the JP1 events registered after the service restarts.

The event generation service terminates abnormally when:

- The service process is forcibly terminated (killed).
- The system is forcibly powered off.

### (b) Correlation processing when using the integrated monitoring database

Once started, the correlation event generation function associates the correlation event generation definitions with events acquired by the event base service and issues correlation events.

You can select the location in the JP1/Base event database at which the event base service begins event acquisition after startup. Set the location by executing the `jcoimdef` command with the `-b` option specified.

The correlation processing behaves differently depending on the combination of acquisition start location and start option, as follows:

*Table 3-4: Correlation processing behavior*

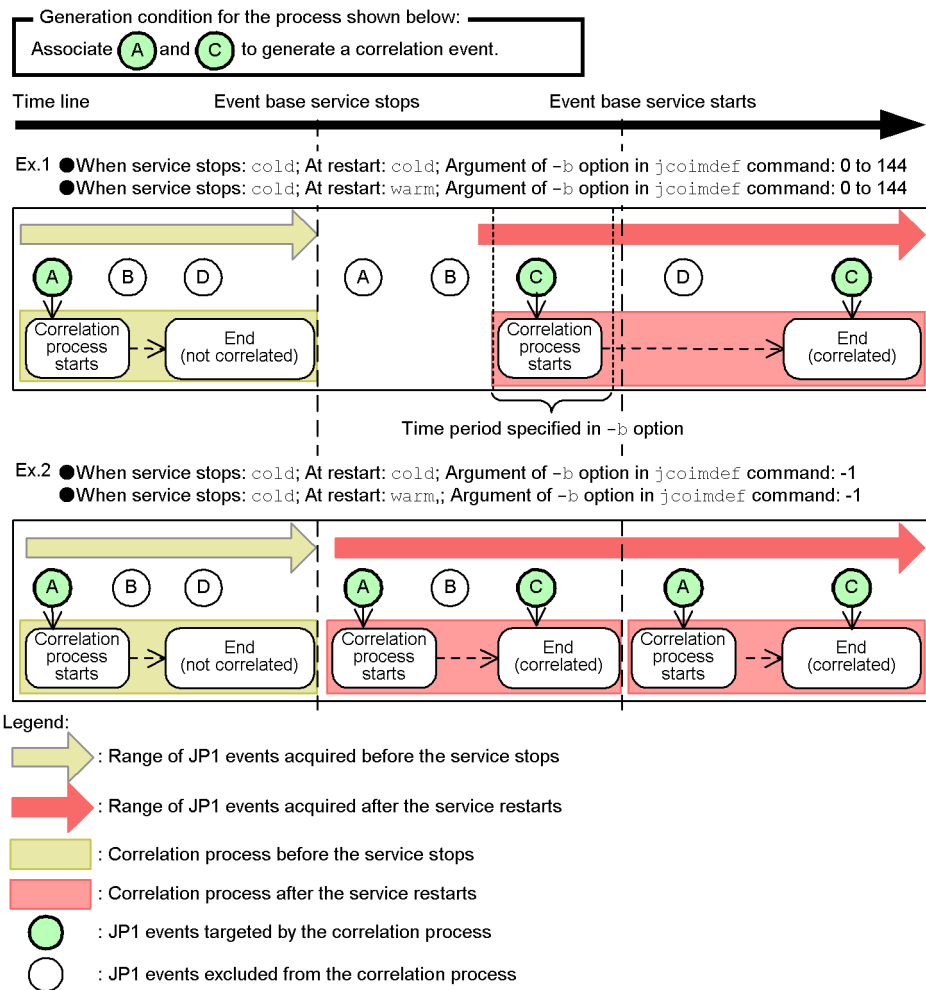
Start option	Value of the -b option	Correlation processing
warm	-1 (default)	The status of the JP1 events being correlated is inherited. Acquisition starts from the JP1 event following the last one acquired when the service stopped at the previous run. If no JP1 events had been acquired at the end of the previous run, acquisition starts from the oldest JP1 event registered in the event database.
	0 to 144	Message <code>KAVB2316-W</code> is output and the status of JP1 events being correlated is not inherited.
cold	-1 to 144	All correlation processing stops and ends. The status of JP1 events being correlated is not inherited.

JP1 events already processed by the correlation event generation function are not subject to correlation processing a second time.

### ■ Correlation processing examples (when using the integrated monitoring database)

The following figure shows the processing to issue correlation event when a `cold` start is specified and when a `warm` start is specified.

**Figure 3-18:** Correlation processing when the event base service stops (in cold start mode) and when it restarts



The following describes how the correlation processing behaves in the examples in *Figure 3-18*.

**Example 1:**

If the cold or warm start option applies when the event base service starts, and a value in the range 0 to 144 is specified in the -b option of the jcoimdef command, the correlation processing behaves as follows:

When the event base service stops

- Processing ends and information about all target JP1 events is

discarded.

- The processing contents are logged to a correlation event generation history file.

After the event base service restarts:

- Acquisition starts at the number of hours specified in the `jcoimdef` command's `-b` option prior to the restart time.
- The service reads the correlation event generation definition, and starts processing accordingly.

*Example 2:*

If the `cold` or `warm` start option applies when the event base service starts, and `-l` is specified in the `-b` option of the `jcoimdef` command, the correlation processing behaves as follows:

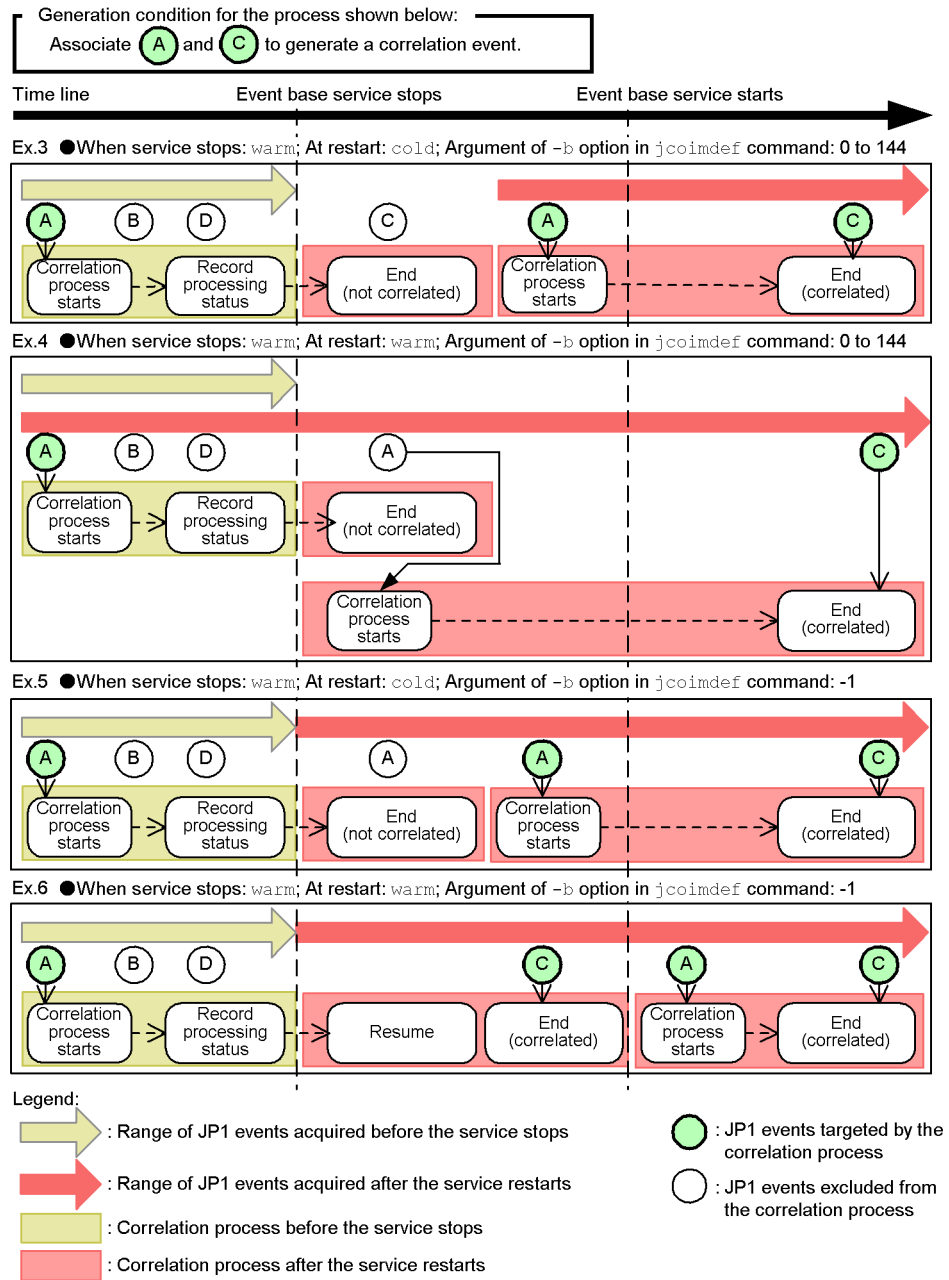
When the event base service stops

- Processing ends and information about all target JP1 events is discarded.
- The processing contents are logged to a correlation event generation history file.

After the event base service restarts:

- Acquisition starts from the JP1 event following the last one acquired when the service stopped at the previous run.
- The service re-reads the correlation event generation definition, and starts processing accordingly.

**Figure 3-19: Correlation processing when the event base service stops (in warm start mode) and when it restarts**



The following describes how the correlation processing behaves in the examples in



*Figure 3-19.**Example 3:*

If the `cold` start option applies when the event base service starts, and a value in the range 0 to 144 is specified in the `-b` option of the `jcoimdef` command, the correlation processing behaves as follows:

When the event base service stops

- Information about the JP1 events being correlated, the processing contents, and the information in the correlation event generation definition are output to an internal log to record the processing status.
- The processing contents are logged to a correlation event generation history file.

After the event base service restarts:

- All information about JP1 events being correlated when the service stopped at the previous run is discarded.
- Acquisition starts at the number of hours specified in the `jcoimdef` command's `-b` option prior to the restart time.
- The service reads the correlation event generation definition, and starts processing accordingly.

*Example 4:*

If the `warm` start option applies when the event base service starts, and a value in the range 0 to 144 is specified in the `-b` option of the `jcoimdef` command, the correlation processing behaves as follows:

When the event base service stops

- Information about the JP1 events being correlated, the processing contents, and the information in the correlation event generation definition are output to an internal log to record the processing status.
- The processing contents are logged to a correlation event generation history file.

After the event base service restarts:

- Acquisition starts at the number of hours specified in the `jcoimdef` command's `-b` option prior to the restart time.
- The service re-reads the correlation event generation definition, and starts processing accordingly.
- The service references the internal log and starts processing from the JP1 events that have not yet been correlated.

*Example 5:*

If the `cold` start option applies when the event base service starts, and `-1` is specified in the `-b` option of the `jcoimdef` command, the correlation processing behaves as follows:

When the event base service stops

- Information about the JP1 events being correlated, the processing contents, and the information in the correlation event generation definition are output to an internal log to record the processing status.
- The processing contents are logged to a correlation event generation history file.

After the event base service restarts:

- Acquisition starts from the JP1 event following the last one acquired when the service stopped at the previous run.
- The service re-reads the correlation event generation definition, and starts processing accordingly.

*Example 6:*

If the `warm` start option applies when the event base service starts, and `-1` is specified in the `-b` option of the `jcoimdef` command, the correlation processing behaves as follows:

When the event base service stops

- Information about the JP1 events being correlated, the processing contents, and the information in the correlation event generation definition are output to an internal log to record the processing status.
- The processing contents are logged to a correlation event generation history file.

After the event base service restarts:

- Acquisition starts from the JP1 event following the last one acquired when the service stopped at the previous run.
- The service re-reads the correlation event generation definition, and starts processing accordingly.
- The service references the internal log and resumes processing from the JP1 events being correlated, if any, when the previous run stopped.

*Note:*

If the event base service ends abnormally, information about the JP1 events being correlated cannot be recorded. Therefore, at the next run, the service will behave as for a `cold` start: Information about the JP1 events being correlated at the end of the previous run is discarded, and acquisition starts from the JP1 events registered after the service restarts.

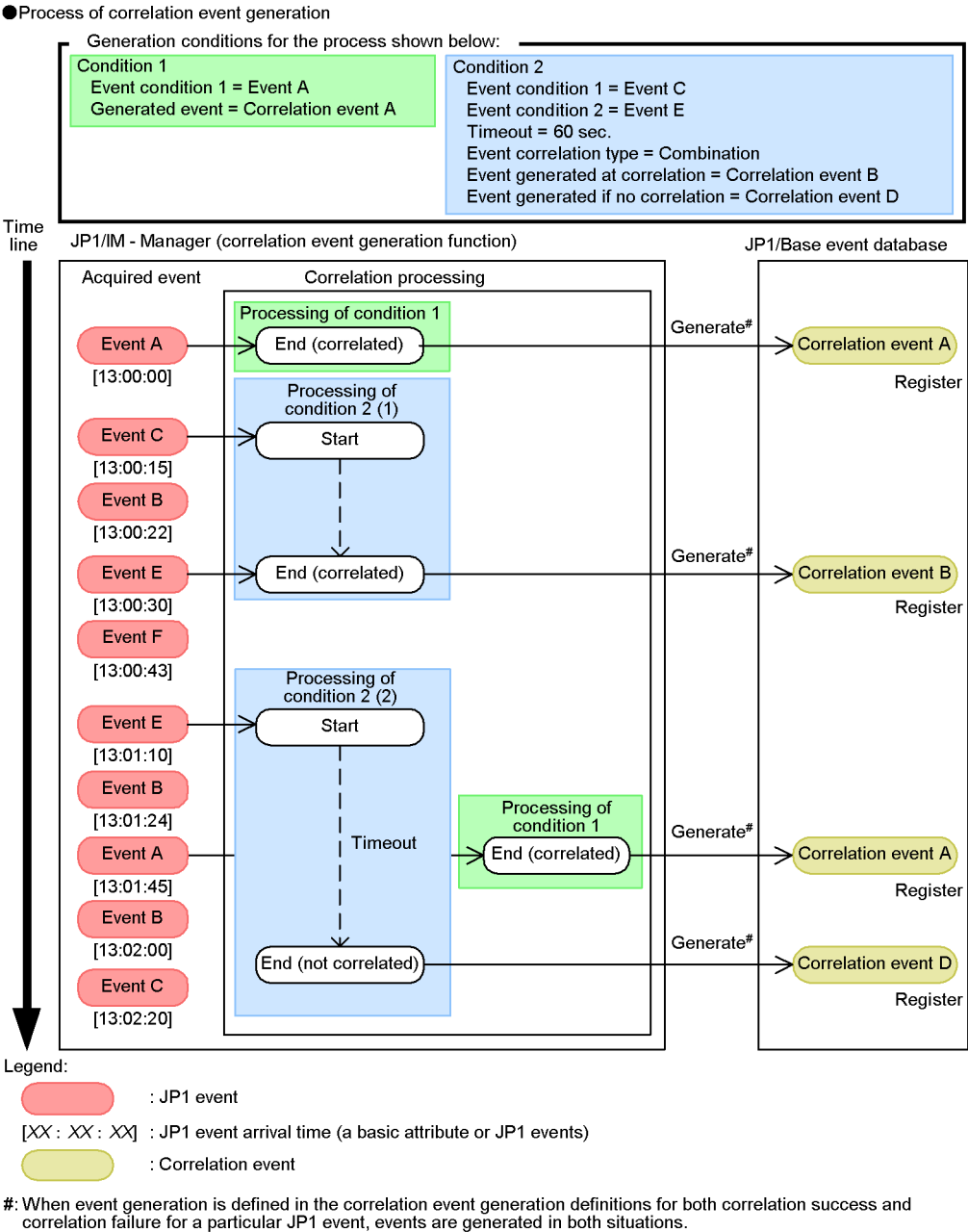
The event base service terminates abnormally when:

- The service process is forcibly terminated (killed)
- The service process is forcibly terminated by the `jcogencore` command.
- The system is forcibly powered off.

**(3) Correlation event issue after JP1 event acquisition**

The following figure shows the processing to issue correlation event after JP1 events have been acquired.

Figure 3-20: Correlation event issue after JP1 event acquisition



When only one event condition is defined in a correlation event generation condition,

the correlation processing is successful and terminates when a JP1 event matching that event condition is issued.

When multiple event conditions are defined in a correlation event generation condition, the correlation processing is successful and terminates when a JP1 event matching one of the event conditions is issued, and a JP1 event matching another event condition is issued subsequently. If the subsequent match does not occur within the timeout period,<sup>#</sup> the correlation processing fails and terminates. If you have defined correlation event generation definitions that issue correlation approval events and correlation failure events, both types of correlation events will be issued.

<sup>#</sup>: A basic attribute of JP1 events. Based on the arrival time.

*Reference note:*

When you define multiple event conditions, you can select one of three event correlation types: *sequence*, *combination*, or *threshold*.

- *sequence* starts correlation processing based on the order in which the JP1 events are issued. If *sequence* had been set as the event correlation type in generation condition 2 in the above figure, processing of event condition 2 would not start until event condition 1 had been satisfied.
- *combination* is the event correlation type specified in generation condition 2 in the above figure. *combination* starts correlation processing regardless of the order in which event conditions 1 and 2 are satisfied.
- *threshold* issues a correlation event when the number of issued JP1 events matching the defined event condition reaches a threshold.

The processing performed in correlation event issue is output and saved to a correlation event generation history file, and can be referenced as required. For details about this file, see *3.3.4 Contents of a correlation event generation history file*.

#### **(4) Correlation processing when activating or deactivating the integrated monitoring database**

The following table describes the event acquisition start location when correlation processing resumes after the integrated monitoring database is activated or deactivated.

*Table 3-5: JP1 event acquisition location of the correlation processing when activating or deactivating the integrated monitoring database*

Direction of change	Start option at restart	JP1 event acquisition location when correlation processing resumes
Stop using the integrated monitoring database	cold	The point at which the event base service starts
	warm	The point at which the event base service stopped at the previous run
Start using the integrated monitoring database	cold	According to the value set in the -b option of the jcoimdef command
	warm	

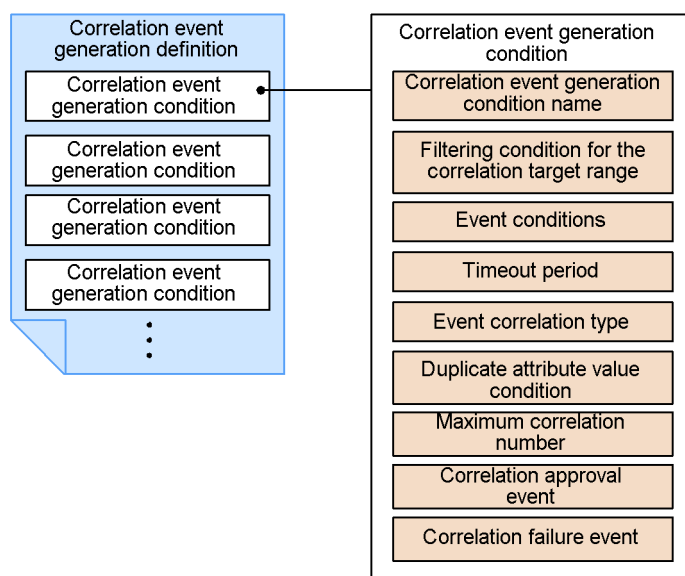
### 3.3.2 Defining correlation event issue

To issue correlation events, you must prepare a correlation event generation definition.

A correlation event generation definition consists of multiple generation conditions, each of which contains several items.

The following figure shows the structure of a correlation event generation definition.

*Figure 3-21: Structure of a correlation event generation definition*



Define the above items in a correlation event generation definition file. The items and their meaning are explained next. For details about how to specify each item, and the input rules and restrictions, see *Correlation event generation definition file* in 2.

*Definition Files* in the manual *Job Management Partner 1/Integrated Management -*

*Manager Command and Definition File Reference.***(1) Correlation event generation condition name**

A name identifying the correlation event generation condition.

**(2) Filtering condition for the correlation target range**

A condition for filtering the range of JP1 events processed according to the correlation event generation condition.

As the filtering condition, specify an attribute value of the target JP1 events. For example, by specifying the name of the event server that issued the event (B.SOURCESERVER), you can restrict the processing to issue correlation event to JP1 events issued from a specific agent host.

**(3) Event condition**

A condition for determining a JP1 event (correlation source event) that triggers a correlation event.

Specify an attribute value of the JP1 events targeted or excluded from the processing to issue correlation event. You can specify multiple event conditions in a generation condition.

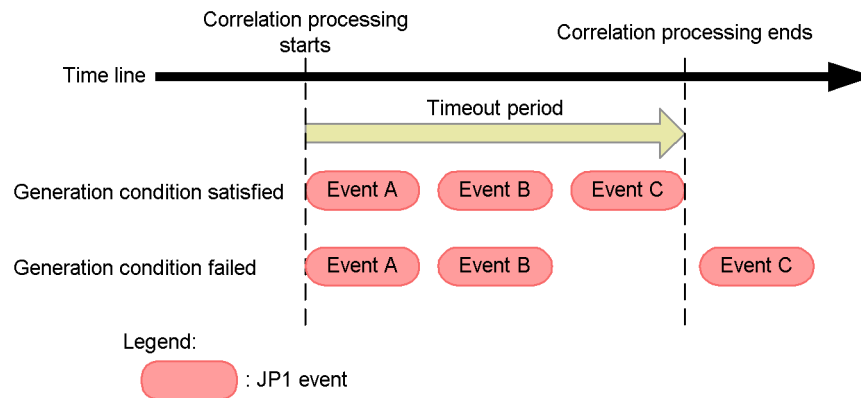
When you specify multiple event conditions, those that exclude specific JP1 events (NOT specification) are applied first.

**(4) Timeout period**

The maximum wait time for a JP1 event matching an event condition.

The timeout period is counted from the arrival time (a basic attribute of JP1 events) of the first JP1 event matching an event condition. If the specified timeout period elapses without the generation condition being met, no correlation event is issued and the correlation processing terminates.

The following example shows when the generation condition is satisfied and when it fails for a succession of events A, B, and C.

*Figure 3-22: Timeout period***(5) Event correlation type**

The method by which JP1 events matching an event condition are correlated.

There are three event correlation types:

- Correlation based on event sequence

The correlation event generation condition is satisfied or fails according to whether JP1 events matching the defined event conditions are issued in a set sequence.

- Correlation based on event combination

The correlation event generation condition is satisfied or fails according to whether JP1 events matching the defined combination of event conditions are issued, regardless of the order in which they occur.

- Correlation based on thresholds

The correlation event generation condition is satisfied or fails according to whether the number of issued JP1 events matching a defined event condition reaches a set threshold.

**(6) Duplicate attribute value condition**

A condition that groups JP1 events matching an event condition on the basis of their attribute value, and issues a correlation event on a group basis. Multiple duplicate attribute value conditions can be specified in a generation condition.

In a duplicate attribute value condition, you can specify a JP1 event attribute name or part of an attribute value. For example, suppose JP1 events indicating an authentication error are associated and issue a correlation event. By specifying the name of the server that issued the event (B . SOURCE SERVER), you can issue correlation events on an authentication server basis.



**(7) Maximum correlation number**

The maximum number of sets of JP1 events that can be processed concurrently by one correlation event generation condition.

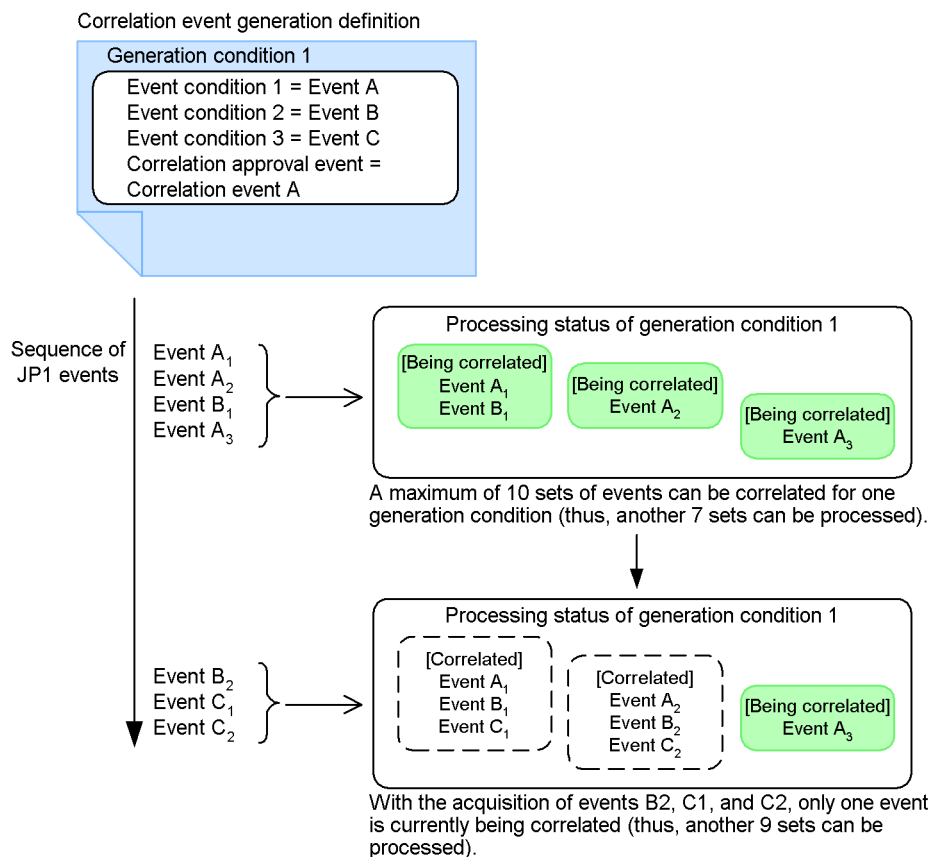
The default when this item is unspecified is 10. When 10 sets of target JP1 events have been acquired for one generation condition, any further target JP1 events that are acquired during correlation processing of that condition will not be processed.

In this case, the following warning message is output to the integrated trace log:  
KAJV2301-W A JP1 event (event ID = *event-ID*, serial number in the event database = *serial-number*) could not be correlated because the correlation event generation condition (*condition-name*) has already correlated *maximum-number* pairs of JP1 events.

For example, suppose a duplicate attribute value condition is specified, and correlation events are issued by each of the 50 servers in the system. If each server issues a JP1 event at the same time, the first 10 sets of JP1 events can be processed, but the remaining 40 sets cannot. In this type of situation, you would specify 50 sets as the maximum correlation number.

The following figure shows how the correlation processing works when the maximum correlation number is the default (10 sets).

**Figure 3-23:** Correlation processing based on the default maximum correlation number (10 sets)



*Note:*

A maximum of 20,000 sets of JP1 events can be correlated concurrently by all the correlation event generation conditions. Avoid specifying a large maximum correlation number in a large number of generation conditions.

### **(8) Correlation approval event**

A JP1 event (*correlation event*) that is issued when a correlation event generation condition is satisfied. You can specify any attribute name and any attribute value for the correlation event. By using a variable to specify an attribute of the correlation source event, you can pass the attribute value to the correlation event.

For details about issued correlation events, see 3.3.8 *Issued correlation event*.

**(9) Correlation failure event**

A JP1 event (*correlation event*) that is issued when a correlation event generation condition is not satisfied. You can specify any attribute name and any attribute value for the correlation event. By using a variable to specify an attribute of the correlation source event, you can pass the attribute value to the correlation event.

For details about issued correlation events, see 3.3.8 *Issued correlation event*.

**3.3.3 Status transition and operation settings of the correlation event generation function**

The correlation event generation function can have any of the statuses shown in the table below.

*Table 3-6: Statuses of the correlation event generation function*

No.	Status	Description
1	Starting	The correlation event generation function is starting.
2	Running	The correlation event generation function has started and is active.
3	Standby	The correlation event generation function has started but is inactive.
4	Stopping	The correlation event generation function is stopping.
5	Stop	The correlation event generation function has stopped.

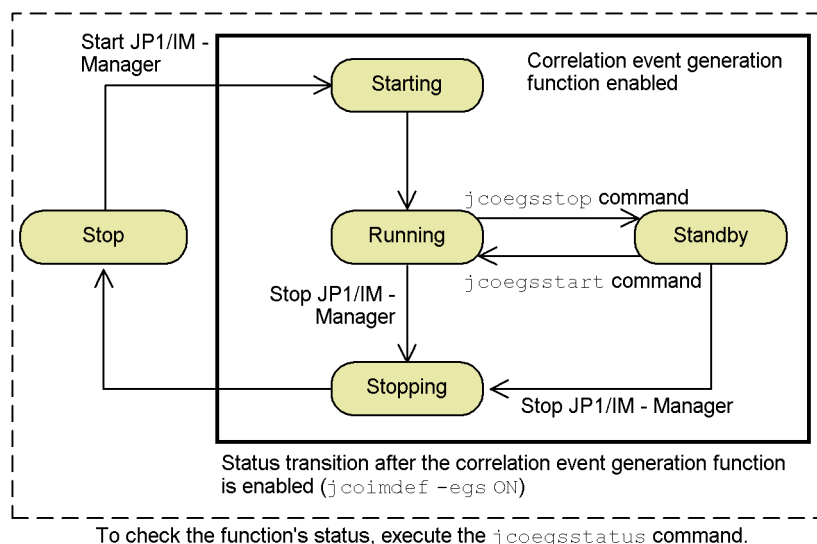
You can check the status of the correlation event generation function using the `jcoegsstatus` command.

To enable the correlation event generation function, after installing JP1/IM - Manager, execute `jcoimdef - egs ON`. After you have performed this setup, the function will start automatically the next time you start JP1/IM - Manager.

When the correlation event generation function has started, you can make it inactive by using the `jcoegsstop` command, and activate it again using the `jcoegsstart` command.

The following figure shows the status transition of the function.

Figure 3-24: Status transition of the correlation event generation function



Legend:

: Status of the correlation event generation function

When a large number of unwanted JP1 events have been issued through system maintenance, for example, you can temporarily suspend correlation processing by switching the correlation event generation function to inactive status. The function supports this kind of issued operation.

### 3.3.4 Contents of a correlation event generation history file

Information about the operating status and correlation processing of the correlation event generation function is logged to a correlation event generation history file. By referencing this file, you can check whether correlation events are being issued according to the defined correlation event generation conditions. For example, if a large number issue failures are being logged for a specific generation condition, it could be that the target JP1 events are an inappropriate combination, or the timeout period might be too short. When periodically reviewing the conditions, look at the correlation event generation history file as a reference. The file can be found in the following location:

In Windows:

`console-path\operation\evgen\egs_discrim{1|2|3}.log`

In UNIX:

`/var/opt/jplcons/operation/evgen/egs_discrim{1|2|3}.log`

You can change the maximum size and number of correlation event generation history files. For details, see *Correlation event generation environment definition file* in 2. *Definition Files* in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.

### (1) Format of a correlation event generation history file

The format of a correlation event generation history file is as follows:

```
{+ | -}serial-number time processing-contents
```

The serial number is that of the correlation event issue log. The numbers run from 00000001 to 99999999, and then start again from 00000001. When the correlation event generation function is restarted, the serial numbers also start again from 00000001. The time is output in *YYYY/MM/DD hh:mm:ss.SSS* format (*YYYY*: year, *MM*: month, *DD*: day, *hh*: hour, *mm*: minute, *ss*: second, *SSS*: second).

Basically, a one-line log entry beginning with a plus sign (+) is output per processing. Where the entry spans multiple lines, the first line begins with a plus sign (+) and the continuation lines begin with a hyphen (-). The contents logged to the file are described next.

### (2) Processing results logged to a correlation event generation history file

The following table describes the processing results logged to a correlation event generation history file.

*Table 3-7: Processing results logged to a correlation event generation history file*

No.	Processing result	Format	Remarks
1	The correlation event generation function is active.	+Correlation event generation function : RUNNING -VERSION= <i>version-of-correlation event-generation-definition-file</i> -[ <i>generation-condition-name</i> ] -TARGET= <i>filtering-condition-for-correlation-target-range</i> -CON= <i>event-condition</i> -TIMEOUT= <i>timeout-period</i> -TYPE= <i>event-correlation-type</i> -SAME_ATTRIBUTE= <i>duplicate-attribute-value-condition</i> -CORRELATION_NUM= <i>maximum-correlation-number</i> -SUCCESS_EVENT= <i>correlation-approval-event</i> :	The output items are the contents of the correlation event generation definition file being used.

### 3. Centralized System Monitoring Using the Central Console

No.	Processing result	Format	Remarks
2	The correlation event generation function is inactive.	+Correlation event generation function : STANDBY	--
3	A JP1 event matching the event condition has been issued and correlation processing has started.	+Generation start <i>condition-name</i> ( <i>correlation-number</i> ) <i>JP1-event-information</i> -SAME_ATTRIBUTE= <i>same-attribute-name</i> : <i>same-attribute-value</i> : -SAME_ATTRIBUTE= <i>same-attribute-name</i> : <i>same-attribute-value</i>	<i>correlation-number</i> is for identifying the start of processing and the processing result (satisfied or unsatisfied) for each set of JP1 events when multiple sets are being correlated with one generation condition.
4	The generation condition was satisfied.	+Generation success <i>condition-name</i> ( <i>correlation-number</i> ) - <i>JP1-event-information-1</i> - <i>JP1-event-information-2</i> : - <i>JP1-event-information-n</i> -SAME_ATTRIBUTE= <i>same-attribute-name</i> : <i>same-attribute-value</i> : -SAME_ATTRIBUTE= <i>same-attribute-name</i> : <i>same-attribute-value</i>	--
5	A correlation event has been issued.	+Correlation event generation succeeded. <i>condition-name</i> ( <i>correlation-number</i> ) <i>serial-number-in-event-database</i>	--

No.	Processing result	Format	Remarks
6	The generation condition was not satisfied. (Correlation processing has stopped.)	+Generation fail <i>condition-name</i> ( <i>correlation-number</i> ) <i>reason-for-failure</i> -JP1-event-information-1 -JP1-event-information-2 : -JP1-event-information-n -SAME_ATTRIBUTE= <i>same-attribute-name</i> : <i>same-attribute-value</i> : -SAME_ATTRIBUTE= <i>same-attribute-name</i> : <i>same-attribute-value</i>	The reason why the generation condition was not satisfied is output as one of the following: <ul style="list-style-type: none"> <li>The correlation event generation definition has been updated: definition_update</li> <li>The correlation event generation function was restarted in cold start mode: cold_start</li> <li>The correlation event generation function is inactive. standby</li> <li>Internal error unknown</li> </ul>
7	The correlation event generation definition has been updated.	+Correlation event generation definition update -VERSION= <i>version-of-correlation event-generation-definition-file</i> -[ <i>generation-condition-name</i> ] -TARGET= <i>filtering-condition-for-correlation-target-range</i> -CON= <i>event-condition</i> -TIMEOUT= <i>timeout-period</i> -TYPE= <i>event-correlation-type</i> -SAME_ATTRIBUTE= <i>duplicate-attribute-value-condition</i> -CORRELATION_NUM= <i>maximum-correlation-number</i> -SUCCESS_EVENT= <i>correlation-approval-event</i> :	The output items are the contents of the correlation event generation definition file being used.

### 3. Centralized System Monitoring Using the Central Console

No.	Processing result	Format	Remarks
8	Output to the header at the following times: <ul style="list-style-type: none"> <li>When the correlation event generation function starts</li> <li>When the correlation event generation history file is switched</li> </ul>	JP1/IM - Central Console/Correlation Event Generation Service	--
9	A JP1 event matching the event condition has been issued and correlation processing has started, but the JP1 event does not contain the attribute defined in the duplicate attribute value condition.	+A JP1 event that matches the correlation event generation condition occurred, and the correlation event generation processing started, but the event attribute defined in that attribute value condition does not exist in the JP1 event . ( <i>condition-name</i> ( <i>correlation-number</i> ) <i>serial-number-in-event-database</i> <i>attribute-name</i> )	The attribute not present in the JP1 event being correlated is output to <i>attribute-name</i> at the left.
10	A JP1 event was received after the number of JP1 event sets being correlated had reached the limit of 20,000 sets.	+Generation fail <i>condition-name</i> ( <i>correlation-number</i> ) exceeded the threshold (20000) - <i>JP1-event-information</i>	--

Legend:

--: None

The item *JP1-event-information* in the table is output in the following format:  
*serial-number-in-event-database* , *event-ID* , *source-event-server-name* , *arrival-time* , *event-level*

When the correlation event generation function starts or the correlation event generation history file is switched, the header information is output in the following format:

-----  
JP1/IM - Central Console/Correlation Event Generation Service



**(3) Example output to a correlation event generation history file**

An example of output to a correlation event generation history file is shown below.

*Figure 3-25: Example of output to a correlation event generation history file*

```
+00000001 2004/12/18 00:00:00.000 -----
+00000002 2004/12/18 00:00:00.000 JP1/IM - Central Console/Correlation Event Generation Service
+00000003 2004/12/18 00:00:00.000 Correlation event generation function : RUNNING    ...Function is active.
-[over_error]                                     ...Output generation
                                                condition

-CON=CID:1, B.ID==4704:0, E.SEVERITY=="Error"
-CON=CID:2, B.ID==4705:0, E.SEVERITY=="Error"
-SUCCESS_EVENT=B.MESSAGE:$EV1_B.MESSAGE, E.SEVERITY:Error
+00000004 2004/12/18 12:35:05.100 Generation start over_error(0) 10001, 4704, hostA, 2004/12/18 12:35:04,
Error                                     ...Start correlation
+00000005 2004/12/18 12:35:11.123 Generation start over_error(1) 10004, 4704, hostA, 2004/12/18 12:35:11,
Error                                     ...Start correlation
+00000006 2004/12/18 12:36:01.060 Generation success over_error(0) 123             ...Condition satisfied
-10001, 4704, hostA, 2004/12/18_12:35:04, Error
-10008, 4705, hostB, 2004/12/18_12:36:01, Error
+00000007 2004/12/18 12:36:11.193 Generation fail over_error(1) timeout           ...Condition failed (timeout)
-10004, 4704, hostA, 2004/12/18_12:35:11, Error
```

**3.3.5 JP1 events subject to correlation processing**

The processing performed by the correlation event generation function applies to the following JP1 events.

Target JP1 events

- JP1 events issued by an application program (system events)
- JP1 events issued by a user (user events)

Correlation processing does not apply to the following JP1 events.

Excluded JP1 events

- JP1 events not registered in the JP1/Base event database (events used in JP1/IM - Manager's internal processing and displayed only in JP1/IM - View)
- Correlation events

**3.3.6 Situations in which a generation condition is satisfied or fails**

The situations in which a generation condition is satisfied or fails are described below. When a JP1 event matches multiple correlation event generation conditions, it is processed by each condition.

**(1) generation condition satisfied**

- Only one event condition defined in the generation condition:  
The condition is satisfied when a matching JP1 event is acquired.
- Multiple event conditions defined in the generation condition (combination

specified):

The condition is satisfied when all the matching JP1 events are acquired within the specified time.

- Multiple event conditions defined in the generation condition (sequence specified):

The condition is satisfied when matching JP1 events are acquired within the specified time and in the specified sequence.

- Threshold defined in the generation condition:

The condition is satisfied when the number of matching JP1 events acquired within the specified time reaches the defined threshold.

## **(2) generation condition fails**

- Multiple event conditions defined in the generation condition (combination specified):

The condition fails if all the matching JP1 events are not acquired within the specified time.

- Multiple event conditions defined in the generation condition (sequence specified):

The condition fails if the matching JP1 events are not acquired within the specified time and in the specified sequence.

- Threshold defined in the generation condition:

The condition fails if the number of acquired matching JP1 events does not reach the defined threshold within the specified time.

### **3.3.7 Situations in which correlation processing fails**

Correlation event generation conditions are not satisfied if processing stops.

Correlation processing stops in the following cases:

- The correlation event generation function was restarted in `cold` mode while a JP1 event was being processed.

Correlation fails because information about the JP1 event being processed is discarded as part of the restart processing.

- A JP1 event was being processed when the correlation event generation definition was changed (by the `jcoegschange` command).

Correlation fails because information about the JP1 event being processed at the time the changed definition was being applied is discarded.

- The correlation event generation function was stopped by the `jcoegsstop`

command.

- The event generation service ended abnormally (when not using the integrated monitoring database).
- The event base service ended abnormally (when using the integrated monitoring database).

### 3.3.8 Issued correlation event

A correlation event is issued when a correlation event generation condition is satisfied or fails. The issued correlation event is registered in the JP1/Base event database.

You can specify any attribute name and any attribute value for the issued event. By using a variable to specify an attribute of the correlation source event, you can pass the attribute value to the correlation event.



The following table describes the contents of an issued correlation event. The table does not cover attributes that can be optionally specified by the user, such as a message (B.MESSAGE).

*Table 3-8: Contents of correlation events issued by the correlation event generation function*

Attribute type		Item	Attribute name	Contents
Basic attribute		Event ID	ID	User-defined event ID A value in the range from 0 to 1FFF and from 7FFF8000 to 7FFFFFFF is displayed.
		Message	MESSAGE	User-defined message
Extended attribute	Common information	Product name	PRODUCT_NAME	/HITACHI/JP1/IM/ GENERATE_EVENT <sup>#</sup>
		Object type	OBJECT_TYPE	SERVICE <sup>#</sup>
		Object name	OBJECT_NAME	EGS <sup>#</sup>
		Occurrence	OCCURRENCE	Correlation event type. Either of the following is set: <ul style="list-style-type: none"> <li>• Generation condition satisfied: SUCCESS</li> <li>• Generation condition failed: FAIL</li> </ul>

Attribute type		Item	Attribute name	Contents
	Program-specific information	Relation event database sequence number	JP1_GENERATE_SOURCE_SEQNO	<i>serial-number-in-event-database</i> $\Delta$ <i>serial-number-in-event-database</i> $\Delta$ <i>serial-number-in-event-database</i> . . . # (serial number of each correlation source event in the event database, separated by spaces)
		Correlation event generation condition name	JP1_GENERATE_NAME	Name of the satisfied correlation event generation condition

#: Fixed value, not definable by the user.

To check issued correlation events, you must display **Type** in the Event Console window. Add **Type** to the **Display items & order** box in the Preferences window. With this setting, an icon is displayed in the **Type** field. The  icon indicates the generation condition was satisfied; the  icon indicates the generation condition failed.

You can perform the same operations and settings on correlation events as on JP1 events. For example, correlation events can trigger an automated action, and can be filtered by an event acquisition filter or event receiver filter. You can also view the correlation source events that resulted in a correlation event in the Related Events (Correlation) window or Related Events (Correlation fails) window.

Note, however, that you cannot make an issued correlation event subject to any further correlation processing.

For details about the Preferences window, see *2.16 Preferences window* in the manual *Job Management Partner 1/Integrated Management - Manager GUI Reference*.

For details about the Related Events (Correlation) and Related Events (Correlation fails) windows, see *2.9 Related Events (Correlation) window* in the manual *Job Management Partner 1/Integrated Management - Manager GUI Reference*.

### 3.4 Consolidated display of repeated events

In JP1/IM - View, JP1 events that are issued repeatedly can be displayed in summarized form. This function is called *consolidated display of repeated events*.

Using this function, you can prevent other important JP1 events from being overlooked when a large number of events with the same contents are issued in a short space of time.

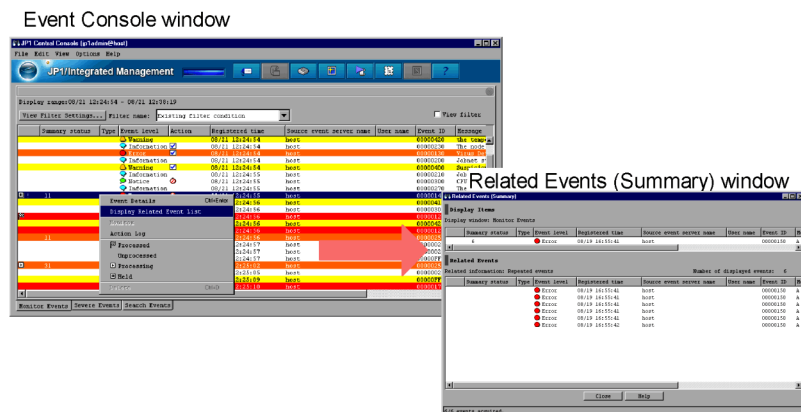
The consolidated display function summarizes identical JP1 events received in succession by JP1/IM - View for display on the **Monitor Events** page or **Severe Events** page of the Event Console window. The function can be set separately by each user.

An event that summarizes identical JP1 events is known as a *consolidation event*. There are two types of consolidation events: an event in which repeated events are still being consolidated (*event being consolidated*) and an event in which the consolidation processing has been completed (*consolidation completion event*).

The first of identical JP1 events received by JP1/IM - View is known as a *consolidation start event*. The subsequently received identical JP1 events are called *repeated events*, and events that are not repeated, and therefore not consolidated, are known as *non-consolidation events*.

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

Figure 3-26: Example of viewing repeated events



*Reference note:*

The Related Events window has two forms:

- Related Events (Summary) window for viewing consolidation events
- Related Events (Correlation) window for viewing correlation source events

Both windows can be displayed by selecting the required event in the Event Console window, and then choosing **Display Related Event List** from the **View** menu or from the pop-up menu. However, if you select a consolidated correlation event, the window that opens from the Event Console window will be the Related Events (Summary) window.

To view the correlation source events, you must then open the Related Events (Correlation) window from the Related Events (Summary) window.

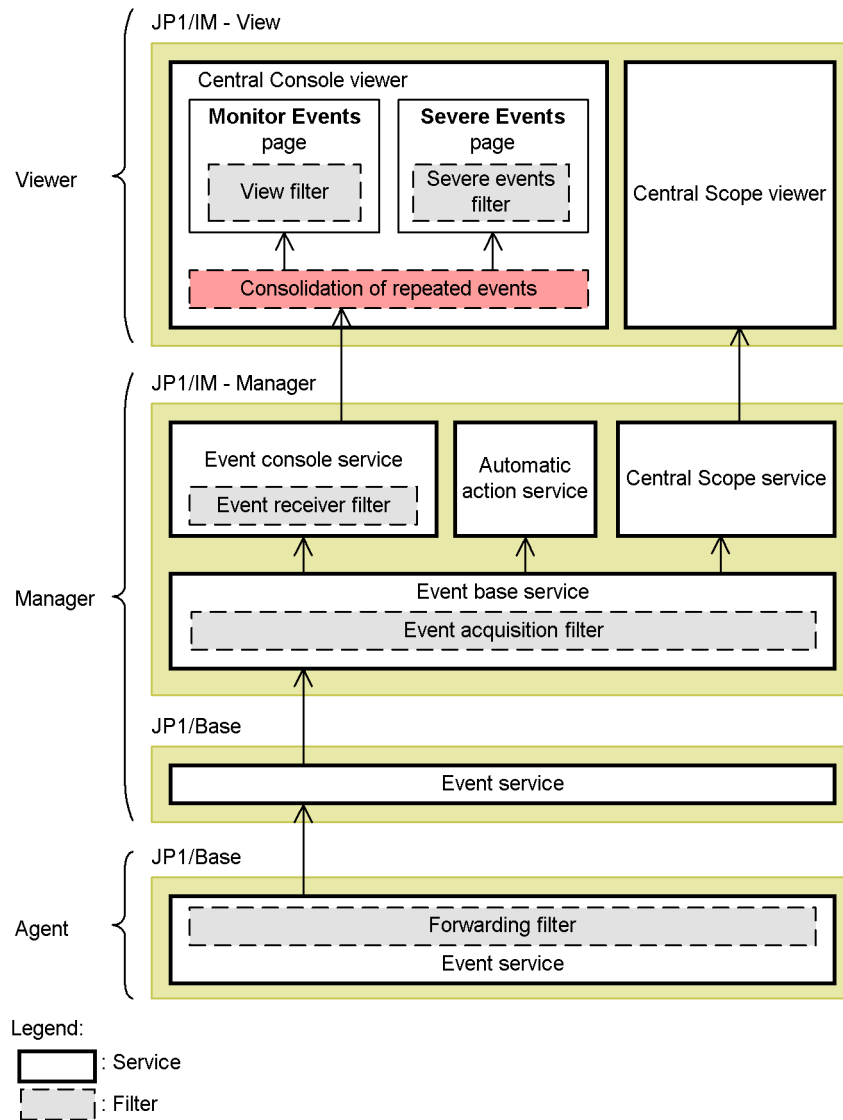
### 3.4.1 Consolidated display of JP1 events

Event consolidation is implemented through JP1/IM - View. Each JP1 event received from JP1/IM - Manager is compared with the consolidation start event. When the contents of a JP1 event match those of the consolidation start event, the JP1 event is judged to be a repeated event and is aggregated into the consolidation event.

The consolidation event resulting from the repeated events passes through the view filter or severe events filter in JP1/IM - View and appears on the **Monitor Events** page or **Severe Events** page of the Event Console window.

The following figure shows the relationships between consolidated display of repeated events and each of the JP1 event filters.

Figure 3-27: Relationships between consolidated display of repeated events and JP1 event filters



#### (1) Event comparison attribute

On receipt of a new JP1 event, JP1/IM - View compares its contents with the consolidation start event, based on the attribute values of the JP1 event. If all attribute values match, the new JP1 event is judged to have the same contents as the consolidation start event.

JP1 event attributes consist of the following detailed information: Source host, event level, object type, object name, root object type, root object name, occurrence, user name, message, product name, action, type, and event ID. You cannot compare event contents based on specific JP1 event attributes only. If you changed the event level of a JP1 event using the function for changing the severity level, the new event level applies when the JP1 event contents are compared.

#### **(2) Conditions for completion of event consolidation**

Event consolidation ends when any one of the following conditions is satisfied:

- The contents of the received JP1 event do not match the consolidation start event.
- The difference between the arrival times of the consolidation start event and received JP1 event exceeds the set timeout value.
- The number of repeated events exceeds the maximum repeat count (100).
- The user clicks the **OK** button in the Preferences window.
- The event being consolidated was not defined as a severe event, but becomes so due to a change in the severe event definition.
- The event being consolidated was defined as a severe event, but is no longer so due to a change in the severe event definition.

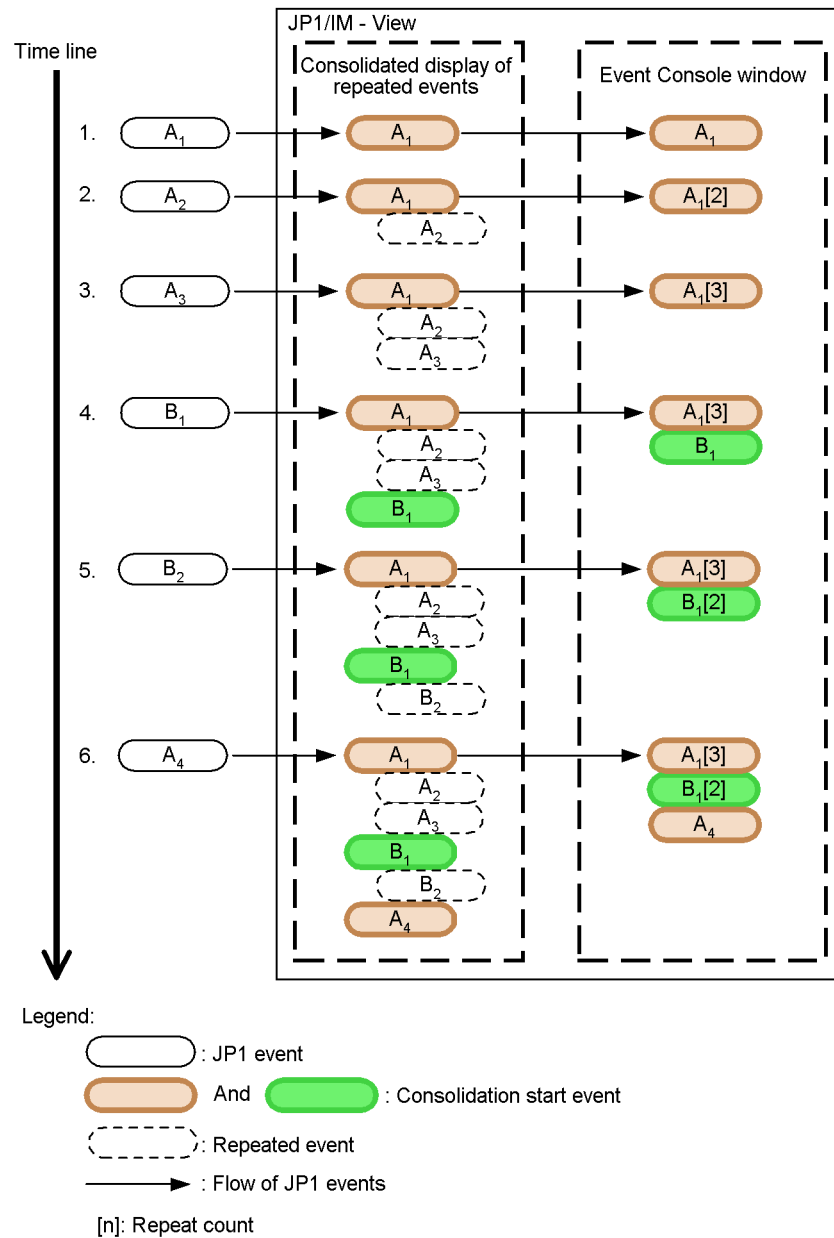
For details about the conditions for completing event consolidation, see *11.1.5 Considerations for consolidated display of repeated events*.

#### **3.4.2 Example of consolidation processing of repeated events**

The following figure shows an example of consolidation processing of repeated events.



Figure 3-28: Consolidation processing of repeated events



The flow of processing described below, following the numbers in the figure:

1. JP1/IM - View receives JP1 event A<sub>1</sub> and begins consolidation. JP1 event A<sub>1</sub>

becomes a consolidation start event.

Information about consolidation start event  $A_1$  appears in the Event Console window.

2. JP1/IM - View receives JP1 event  $A_2$  and compares its contents with the consolidation start event  $A_1$ . Because  $A_2$  and  $A_1$  have identical contents, JP1 event  $A_2$  is judged to be a repeated event and is aggregated into  $A_1$ .

Information about consolidation start event  $A_1$  and the repeat count (2) appears as  $A_1 [2]$  in the Event Console window.

3. JP1/IM - View receives JP1 event  $A_3$  and compares its contents with the consolidation start event  $A_1$ . Because  $A_3$  and  $A_1$  have identical contents, JP1 event  $A_3$  is judged to be a repeated event and is aggregated into  $A_1$ .

Information about consolidation start event  $A_1$  and the repeat count (3) appears as  $A_1 [3]$  in the Event Console window.

4. JP1/IM - View receives JP1 event  $B_1$  and compares its contents with the consolidation start event  $A_1$ . Because  $B_1$  and  $A_1$  do not have identical contents, aggregation into consolidation start event  $A_1$  ends and aggregation into JP1 event  $B_1$  begins. Thus,  $B_1$  becomes the current consolidation start event.

Information about  $B_1$  and the previous consolidation event  $A_1$  appears in the Event Console window.

5. JP1/IM - View receives JP1 event  $B_2$  and compares its contents with the consolidation start event  $B_1$ . Because  $B_2$  and  $B_1$  have identical contents, JP1 event  $B_2$  is judged to be a repeated event and is aggregated into  $B_1$ .

Information about  $B_1$  and its repeat count (2), and about the previous consolidation event  $A_1$ , appears in the Event Console window. (The former appears as  $B_1 [2]$ .)

6. JP1/IM - View receives JP1 event  $A_4$  and compares its contents with the consolidation start event  $B_1$ . Because  $A_4$  and  $B_1$  do not have identical contents, aggregation into consolidation start event  $B_1$  ends and aggregation into JP1 event  $A_4$  begins. Aggregation into the earlier consolidation start event  $A_1$  has already ended; therefore JP1 event  $A_4$  cannot be aggregated into  $A_1$ . Thus,  $A_4$  becomes the new consolidation start event.

Information about the earlier event  $A_1$ , previous event  $B_1$ , and current consolidation event  $A_4$  appears in the Event Console window.

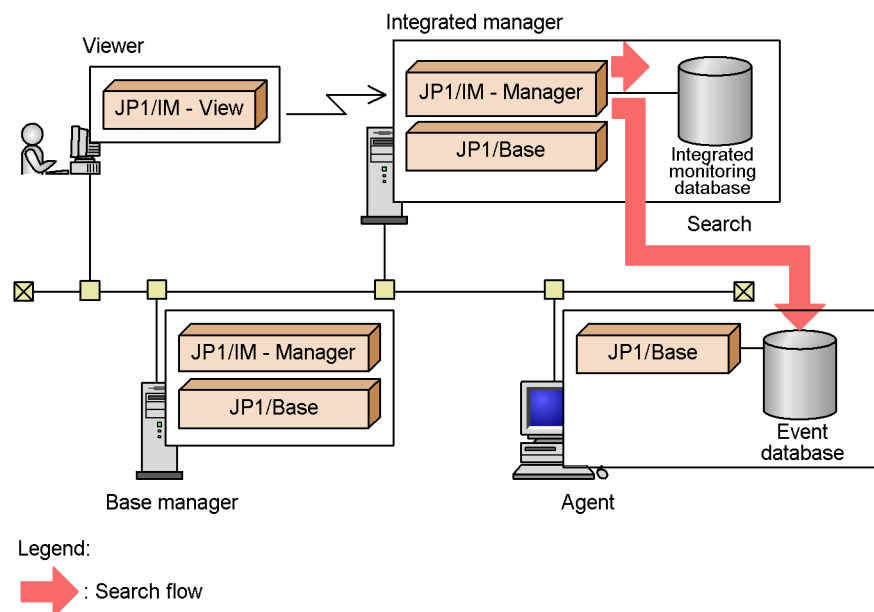
## 3.5 Searching for events

In JP1/IM, you can search for JP1 events registered with JP1/Base using various search conditions, and display them on the **Search Events** page of the Event Console window. When you use the integrated monitoring database, you can display JP1 events registered with the integrated monitoring database on the **Search Events** page of the Event Console window. As well as JP1 event attributes, the search conditions might include the response status of severe events and whether or not an automated action has been executed. You can also use regular expressions for some types of searches.

As the host on which to search, you can specify not only the manager that you are logged in to, but also a remote host on which JP1/Base is installed.

When you use the integrated monitoring database, you can specify which database to search. You can specify either the integrated monitoring database or the JP1/Base event database.

Figure 3-29: Overview of event searching



The following describes JP1 event searches and search conditions, followed by a description of the flow of processing when searching for events.

### 3.5.1 Searching for JP1 events

JP1 events that need to be managed appear on the **Monitor Events** page of the Event

Console window, but you can also use the event search function to display the following JP1 events:

- Past JP1 events that have disappeared from the **Monitor Events** page because the number of JP1 events has exceeded the maximum number of viewable events (JP1/IM - View's scroll buffer size)
- JP1 events erased from the **Severe Events** page by the **Delete** button
- JP1 events without the event level extended attribute (only JP1 events for which an event level is specified are displayed in JP1/IM - View)
- JP1 events filtered out by the forwarding filter and not sent to a JP1/IM manager (normal events, for example)
- JP1 events filtered out by the event acquisition filter and not acquired by JP1/IM (normal events, for example)
- JP1 events stored in the integrated monitoring database, if being used

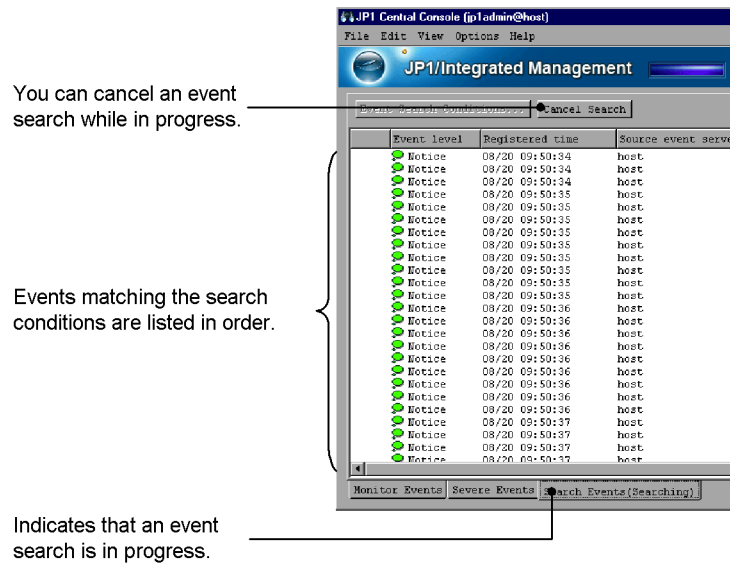
You can check the contents of the events displayed as the search result on the **Search Events** page using the **Event Details** button and **Monitor** button in the same way as on the **Monitor Events** page.

#### Progress display

While an event search is in progress, **(Searching)** appears on the tab of the **Search Events** page. When the search is completed, a dialog box reports that the search has ended and **(Searching)** disappears. This is a way of telling whether a search is still in progress when there are a large number of events to be searched or the search is taking a long time.

Events found to match the search conditions are listed in order on the **Search Events** page. The following figure shows the **Search Events** page while a search is in progress.

Figure 3-30: Search Events page during an event search



### Canceling a search

You can cancel an event search already in progress if you have set the wrong search conditions, for example, or if you have just found the events you were looking for.

To cancel an event search, click the **Cancel Search** button on the **Search Events** page, or choose **View** and then **Cancel Search**.

When you cancel an event search, the JP1 events found up to that point are listed in the window.

#### Reference note:

You can perform other tasks during an event search. For example, you can perform event monitoring in parallel with an event search. The menu commands for other tasks that you can perform remain selectable.

Some selectable menu commands cannot be used while a search is in progress. If you attempt to use them, an error message appears.

### 3.5.2 Event search conditions

The following conditions apply to event searches:

- JP1/Base must be installed and the event service must be active on the host to be

searched. (But the host does not need to be managed within a hierarchical system configuration.)

- The host to be searched must be directly reachable from the JP1/IM manager.

To conduct an event search, the JP1/IM - Manager (JP1/IM - Central Console) to which you are logged in from JP1/IM - View connects directly to the host to be searched. The host must have a resolvable host name and be able to communicate. In particular, take care when searching for events in a firewall environment or when the host is connected to multiple LANs.

Sometimes a JP1 event might arrive from a host that cannot be searched (because it is not directly reachable). This occurs because events are not transferred directly from agent to manager, but are forwarded in stages from agent to base manager, and from base manager to integrated manager. Event transfer and event searches use different communication paths. An event search can only be conducted on a host that the manager can communicate with directly.

- The JP1 events to be searched must still reside in the event database or integrated monitoring database.

If you specify the event database in the search conditions, JP1 events in the event database are searched. If you specify the integrated monitoring database in the search conditions, JP1 events in the integrated monitoring database are searched.

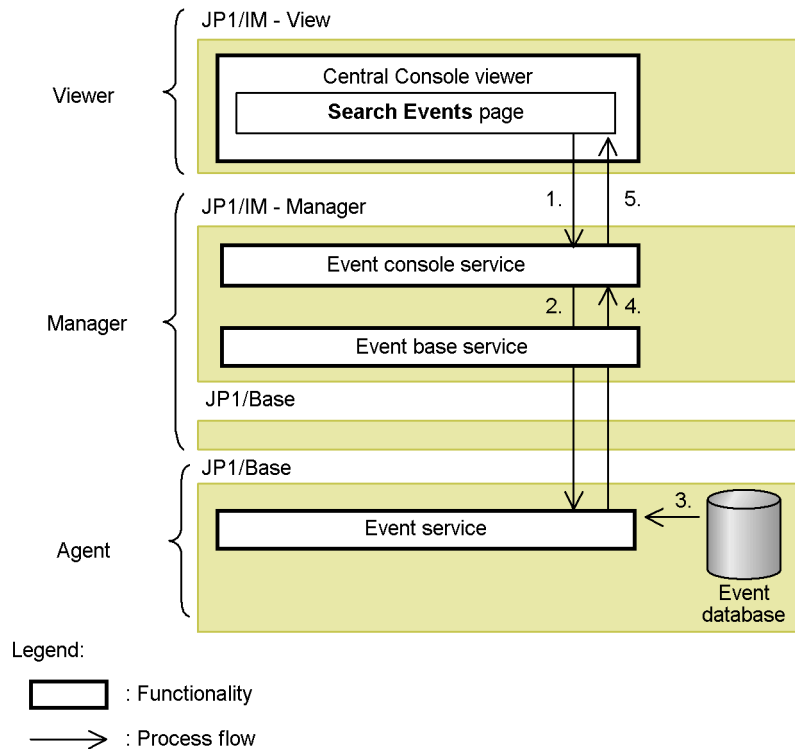
Each instance of JP1/Base has two event databases. When the maximum capacity (default 10 MB) of one event database is reached, the other event database is swapped in. At this point, the contents of the swapped-in event database are erased, and the erased JP1 events cannot be searched.

The information in the event database and integrated monitoring database takes the form of files that are overwritten in a wrap-around cycle. Old JP1 events that have been overwritten cannot be retrieved.

### 3.5.3 Flow of processing of event searching

The flow of processing when searching for events differs according to the database you specify.

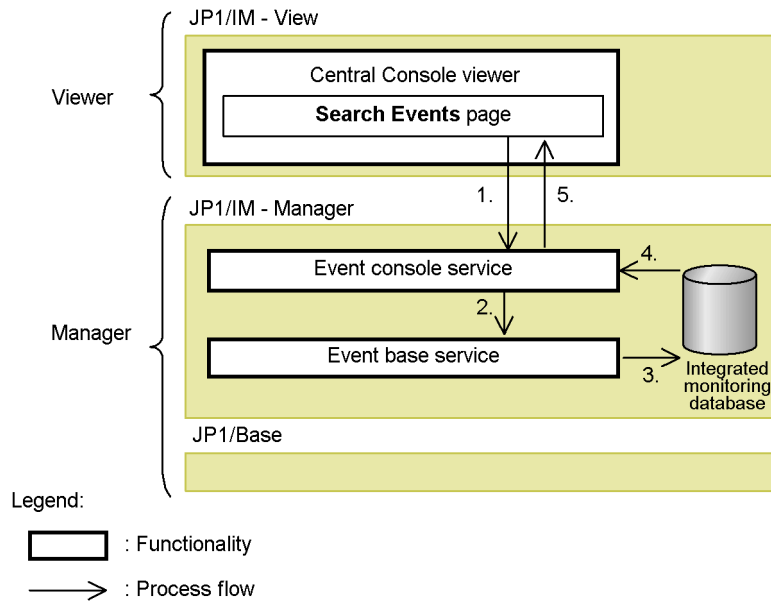
The following describes the flow of processing when searching the event database and when searching the integrated monitoring database.

*Figure 3-31: Flow of processing of event searching (event database specified)*

The flow of processing when searching the event database is described below, following the numbers in the figure:

1. On the **Search Events** page of the Event Console window, specify conditions about the host to search and the JP1 events to retrieve, and then execute the search.
2. On receiving the search request from JP1/IM - View, the event console service of JP1/IM - Manager issues a search request to the event service of JP1/Base on the target host.
3. The event service of JP1/Base acquires JP1 events matching the search conditions from the event database.
4. The event service of JP1/Base sends back information about the JP1 events matching the search conditions to the event console service of JP1/IM - Manager.
5. The event console service of JP1/IM - Manager sends the received information back to JP1/IM - View, and the information is displayed on the **Search Events** page of the Event Console window.

*Figure 3-32: Flow of processing event searching (integrated monitoring database specified)*



The flow of processing when searching the integrated monitoring database is described below, following the numbers in the figure:

1. On the **Search Events** page of the Event Console window, specify conditions about the host to search and the JP1 events to retrieve, and then execute the search.
2. On receiving the search request from JP1/IM - View, the event console service of JP1/IM - Manager issues a search request to the event base service of JP1/IM - Manager on the target host.
3. The event base service of JP1/IM - Manager acquires JP1 events in memory and saves them to the integrated monitoring database.
4. The event console service of JP1/IM - Manager acquires JP1 events matching the search conditions from the integrated monitoring database.
5. The event console service of JP1/IM - Manager sends the received information back to JP1/IM - View, and the information is displayed on the **Search Events** page of the Event Console window.



## 3.6 Event guide function

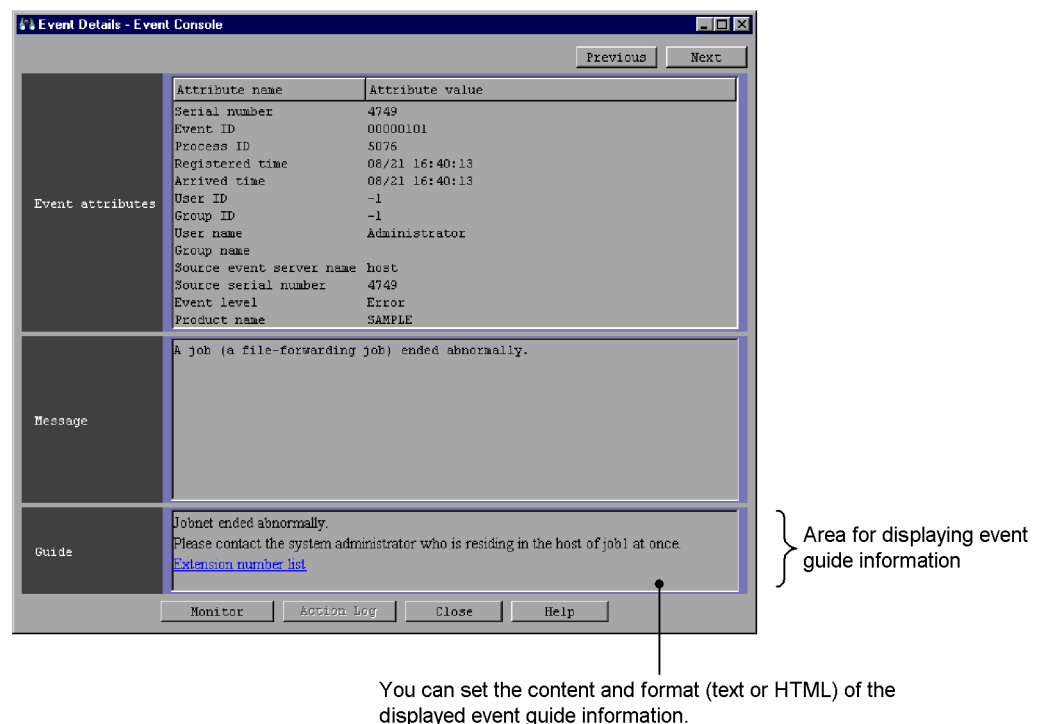
The event guide function displays guidance on handling JP1 events displayed in the Event Console window.

The system administrator carries out error investigation and resolution based on JP1 events, but it is difficult to learn all the tracking and troubleshooting procedures for the numerous JP1 events that might be issued from a linked JP1 product or user application.

The event guide function allows you to record your experience and success in resolving problems, and to reference and accumulate diagnostic case studies, troubleshooting examples, and so on.

The information displayed by the event guide function is known as *event guide information*. You can specify the contents and format (text or HTML) of this information. Event guide information appears in the Event Details window as part of the JP1 event details. The following figure shows a display example.

*Figure 3-33:* Example of event guide information displayed in the Event Details window



You can set the content and format (text or HTML) of the displayed event guide information.

By default, the **Guide** area does not appear in the Event Details window.

The event guide information file is referenced when you log in to JP1/IM - View. If one or more applicable conditions are found, the **Guide** area is displayed. The file and its settings are described next.

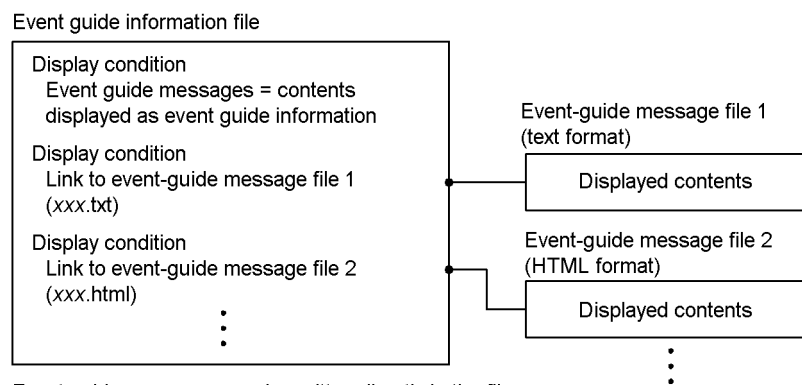
### 3.6.1 Settings for event guide information

Event guide information is set in an event guide information file managed by JP1/IM - Manager.

In this file, you can enter settings about the contents to be displayed as event guide information, conditions about the target JP1 events, and other definitions.

The contents displayed as event guide information are called *event guide messages*. Messages can be stored and managed in individual files known as *event-guide message files*. The relationship between the two types of files is shown below.

Figure 3-34: Relationship between the event guide information file and event-guide message files



Event guide messages can be written directly in the file or stored in another file.

The update timing after you edit an event guide message differs for the event guide information file and event-guide message files, as follows:

- Event guide information file

To apply the changes (edited message or condition definition) in the event guide information file, you must restart JP1/IM - Manager or execute the `jco_spmc_reload` command.

After the changes have been applied, the **Guide** area, if not currently displayed, appears in the Event Details window the next time a user logs in to JP1/IM - View.

- Event-guide message file

After you edit an event-guide message file, the changes appear when you simply refresh the Event Details window.

We recommend that you use an event-guide message file if you periodically edit messages.

### 3.6.2 Conditions for displaying event guide information

Using a condition (`EV_COMP`), you can specify which of the issued JP1 events to target in displaying event guide information. When you specify multiple conditions, an AND condition is assumed and the guide information is displayed when all the conditions are satisfied.

`EV_COMP` is a JP1 event comparison condition in the format *attribute-name:attribute-value*. You can set a maximum of 100 such conditions.

- *attribute-name*

Specify the name of a JP1 event attribute (basic or extended attribute).

For example, you can specify the event ID (`B.ID`), event level (`E.SEVERITY`), or other attribute name. If you changed the event level of a JP1 event using the function for changing the severity level, the new event level applies when the JP1 event contents are compared.

You can also specify program-specific information (provided as an extended attribute of JP1 events) for a particular JP1 product.

For example, you can specify the host that executes JP1/AJS jobs (`E.CO`).

- *attribute-value*

Specify the attribute value corresponding to the attribute name.

For example, to specify JP1 events whose event level (`E.SEVERITY`) is `Error`, specify `E.SEVERITY:Error`. To specify an event whose event ID (`B.ID`) is `00000111`, specify `B.ID:00000111:00000000`.

When event guide information is displayed in JP1/IM - View, the contents of the event guide information file are referenced from the top. When an item matching the conditions is found, referencing stops and the applicable information appears in the Event Details window.

Because the Event Details window displays only the first of possibly multiple items in the event guide information file that match the conditions, bear the following in mind when setting display conditions:

- Make sure that the comparison condition does not duplicate a comparison condition set for a different event guide item.

For example, by setting multiple conditions in a comparison condition, such as an event level or message in addition to the event ID, you can differentiate the comparison condition from that set for another event guide item.

A regular expression can be written as an attribute value, but it must require a complete match.

- Set no more than one event guide item for one JP1 event.

To set multiple items for one JP1 event, consider writing multiple action procedures in HTML format in an event-guide message file.

### 3.6.3 Contents displayed as event guide information

To write event guide messages directly in an event guide information file, specify `EV_GUIDE`. To use event-guide message files, specify `EV_FILE` instead of `EV_GUIDE` and write the file locations.

Messages can be written in text format or HTML format. The attribute values of JP1 events can also be used as variables in messages (by prefixing the attribute value with `$`). For example, if you write `$B.MESSAGE Δ` (where `Δ` represents a space), JP1 event messages (`B.MESSAGE`) will be handled as variables, and the attribute value of the JP1 event will be displayed in the event guide message.

Event-guide message file as a useful tool when editing

When event guide messages are written directly in an event guide information file (`EV_GUIDE` specified), each message is a single line. You cannot format the message layout by inserting linefeed codes. However, you can do so in an event-guide message file (`EV_FILE` specified). This is illustrated in the figure below.

Figure 3-35: Examples of writing event guide information

Coding in an event guide information file (extract)

```

:
EV_GUIDE=Detailed information\nJobnet ended abnormally.
(name: jobnet-name: execution-ID)\n\nThe jobnet terminated abnormally/\n\n
(S) \nContinues processing. The execution ID is output when yes is
specified in the LOGINFOALL parameter in the configuration definition file
or when ALL is specified for information output to the scheduler log and
event log in the Scheduler Log Settings page of the Manager Environment
Settings dialog box.\n\n
(O) \nCheck what caused the jobnet to end abnormally and take appropriate
action.
:

```

Linefeed codes cannot be inserted to format the message.

Linefeed codes cannot be inserted to format the message.

```

Detailed information
Jobnet ended abnormally. (name: jobnet-name: execution-ID)

The jobnet ended abnormally.

(S)
Continues processing. The execution ID is output when yes is specified
in the LOGINFOALL parameter in the configuration definition file or
when ALL is specified for information output to the scheduler log and
event log in the Scheduler Log Settings page of the Manager
Environment Settings dialog box.

(O)
Check what caused the jobnet to end abnormally and take appropriate
action.

```

Linefeed codes can be inserted to format the message.

Because you can apply formatting in this way, an event-guide message file is useful when you are preparing messages in HTML format, and there is a large amount of information or you need to periodically review the message contents.

About event guide information files:

See *Event guide information file (jco\_guide.txt)* in 2. *Definition Files* in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.

---

## 3.7 Setting memo entries

---

You can set additional information about a JP1 event displayed in the Event Console window. This functionality is available for JP1 events registered in the integrated monitoring database when you use the integrated monitoring database.

When an issue is encountered during investigation of a JP1 event, the system administrator will need to record what steps were taken or report the issue to other users. By entering a memo to accompany the particular JP1 event, the system administrator can summarize what steps were taken and write notes to other users. Users can then find out the state of investigation and what precautions to take, simply by referencing the JP1 event in the Event Console window.

Memo entries are subject to content comparisons in the following:

- View filter conditions
- Event search conditions

The contents of a memo entry can be included in an event report output by the `jcoevtreport` command.

To use the memo functionality, enable memo entry in the `jcoimdef` command.

---

## 3.8 Displaying user-defined event attributes

---

By customizing the JP1/IM definition files, you can extend the functionality available when another application is linked with JP1/IM. With the extended functions, you can perform the following operations.

### 3.8.1 Displaying the attributes of user-defined events

User applications can issue JP1 events by calling a JP1/Base function. You can add user-defined event attributes (extended attributes specific to the issuing program) to the issued JP1 event. A JP1 event that has a user-defined event attribute is known as a *user-defined event*.

Event attributes (program-specific extended attributes) are not normally displayed in the Event Details window in JP1/IM - View, but you can display them if you create a definition file that defines the event attributes. For details about how to display user-defined events using a definition file, see *4.8 How to display user-specific event attributes* in the *Job Management Partner 1/Integrated Management - Manager Configuration Guide*.

### 3.8.2 Displaying a monitor window from a JP1 event

By creating a definition file of user-defined events, from the JP1 event listing in JP1/IM - View you can launch and operate the GUI of the application that issued a particular JP1 event. For details about how to launch a monitor window from a JP1 event based on a definition file, see *4.12.1 How to open monitor windows* in the *Job Management Partner 1/Integrated Management - Manager Configuration Guide*.

### 3.8.3 Adding items to the Tool Launcher window

You can add items to the function tree displayed in the Tool Launcher window of JP1/IM - View. This allows you to launch the GUI of a system management program or application management program.

To add an item to the Tool Launcher window, use a definition file.

For details about how to add items to the Tool Launcher window using a definition file, see *4.13.2 How to add new menus* in the *Job Management Partner 1/Integrated Management - Manager Configuration Guide*.

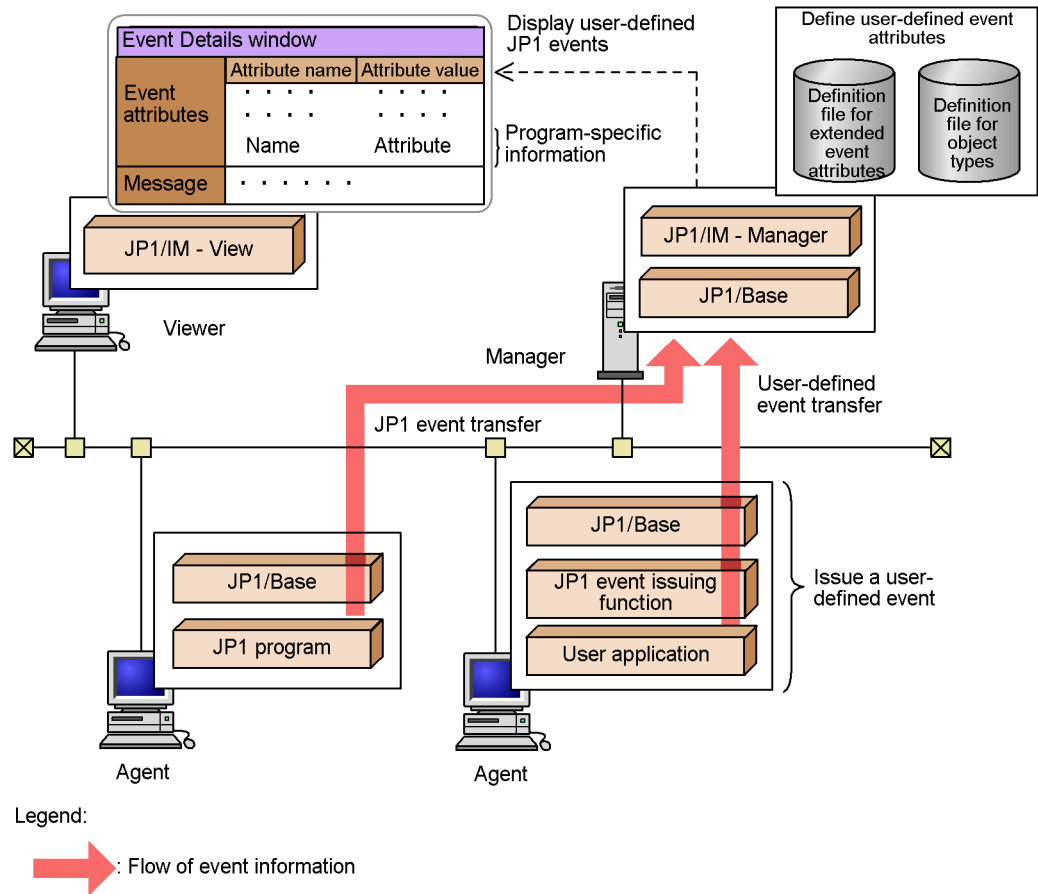
### 3.8.4 Flow of event information

Using the JP1 event issuing function provided by JP1/Base, you can execute user-defined events that have user-defined event attributes (program-specific extended attributes) directly from a user application.

In JP1/IM, you can create a definition file and display these user-defined event attributes in the Event Details window.

The following figure provides an overview of the flow of processing from issuing a user-defined event to displaying its user-defined event attributes.

*Figure 3-36:* Flow of processing from issuing a user-defined event to displaying its attributes





---

## 3.9 CSV output of information displayed in JP1/IM - View

---

In JP1/IM, you can output the information displayed in JP1/IM - View in CSV format. The following functions support CSV output:

- Saving event listings to a file
- Saving event information in the integrated monitoring database to a file
- Copying JP1 event information and action execution results to the clipboard

These functions are described next.

### 3.9.1 Saving event listings (CSV snapshot)

In JP1/IM, you can take a CSV snapshot<sup>#</sup> of the event information displayed in JP1/IM - View. Based on this information, you can keep a history of day-to-day monitoring and actions. You can also use your CSV snapshots when reviewing the system during maintenance, for example.

The following describes the types of information you can export as a CSV snapshot, and the output format, items, and timing.

#: *Snapshot* refers to extracting information at a particular point in time.

#### (1) Information that can be exported as a snapshot

You can take a CSV snapshot of the event lists in following pages:

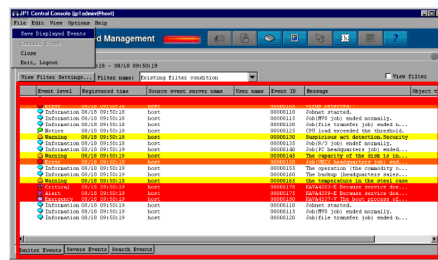
- **Monitor Events** page of the Event Console window
- **Severe Events** page of the Event Console window
- **Search Events** page of the Event Console window

#### (2) Snapshot image and format

The following figure shows a CSV snapshot.

Figure 3-37: CSV snapshot image

Event Console window



CSV snapshot

Output time, Login user name, Host connection, Window name	Line 1
display item, display item, display item	Line 2
Event information (topmost in the window)	Line 3
Event information#	Line 4
.	.
.	.
.	.

#: Output on each line in the same order as displayed in the window.

Line 1 is the CSV header information, separated by commas.

Line 2 is the display items set in JP1/IM - View, separated by commas.

Line 3 is the event information listed first in the window, separated by commas in the same way as the display items (line 2).

Line 4 and subsequent lines are event information output in the same format as line 3, following the window display items.

The CSV output format is as follows:

- Items are separated by commas ( , ).  
*item1 , item2 , item3 , item4 , item5 , . . .*
- Any item containing a comma ( , ) is enclosed with double quotation marks ( " ).  
*item1 , "item,2" , item3 , item4 , item5 , . . .*
- Any item containing a control character (0x00 to 0x1F, and 0x7F to 0x9F) is enclosed with double quotation marks ( " ).  
*item1 , "item(0x00)2" , item3 , item4 , item5 , . . .*
- When an item contains a double quotation mark ( " ), another double quotation mark is inserted before it, and the whole is enclosed with double quotation marks ( " ).  
*item1 , "item" "2" , item3 , item4 , item5 , . . .*
- Empty items are shown as blank (nothing is entered).  
*item1 , , item3 , item4 , item5 , . . .*

### (3) Snapshot output items

The following table describes the header information output to line 1 of a CSV snapshot.




Table 3-9: Output header information

Header item	Output contents
Output time	The time at which the snapshot was taken is output in the following format (year/month/day hour:minute:second): <i>YYYY/MM/DD hh:mm:ss</i>
Login user name	The name of the JP1 user who took the CSV snapshot
Host connection	The name of the manager host to which the JP1 user was logged in when the snapshot was taken
Window name	The name of the page ( <b>Monitor Events</b> , <b>Severe Events</b> , or <b>Search Events</b> ) displayed in the Event Console window when the snapshot was taken


The contents (display items) output to line 2 of the snapshot differs according to the settings in the JP1/IM - View Preferences window. The contents (event information) output to line 3 and subsequent lines also differs according to the contents in line 2.










The following table describes the contents output to line 2 and subsequent lines.

Table 3-10: Contents output to the body of a snapshot

Display item (contents in line 2)	Event information (contents in line 3 onward)	Output conditions
Response status	<p>The icons in the window are converted into character strings and output as follows:</p> <p> -&gt; Processed</p> <p> -&gt; Processing</p> <p> -&gt; Held</p> <p>(no icon) -&gt; Unprocessed</p> <p>When the response status differs among the JP1 events in a consolidation event, the icon is followed by an exclamation mark (!). In the snapshot, the exclamation mark appears to the right of the string.</p> <p>When a JP1 event has a memo entry, the icon and exclamation mark are followed by a comma and then Memo.</p>	--
Summary status	The character strings displayed in the window are output as is.	Output when <b>Enable</b> is selected for <b>Display most significant status</b> .

### 3. Centralized System Monitoring Using the Central Console

Display item (contents in line 2)	Event information (contents in line 3 onward)	Output conditions
Event level	The character strings displayed in the window are output as is. The severity color coding and icons are not output.	Output when this item is set in the <b>Display items &amp; order</b> list box in the Preferences window.
Original severity level		
New severity level	The icon in the window is converted into a character string and output as follows:  New severity level flag -> Changed (no icon) -> (blank)	
Start time	Output in the following format: YYYY/MM/DD hh:mm:ss	
End time		
Arrived time		
Registered time		
Source host	The character strings displayed in the window are output.	
User name		
Message		
Event ID		
Product name		
Object type		
Object name		
Root object type		
Root object name		
Occurrence		
Serial number		
Source process ID		
Source user ID		
Source group ID		
Source user name		
Source group name		

Display item (contents in line 2)	Event information (contents in line 3 onward)	Output conditions
Source serial number		
Action	<p>The icons in the window are converted into character strings and output as follows:</p> <p> -&gt; Execute</p> <p> -&gt; Partially suppress</p> <p> -&gt; Suppress</p> <p>(no icon) -&gt; (blank)</p> <p>When the action status differs among the JP1 events in a consolidation event, the icon is followed by an exclamation mark (!). In the snapshot, the exclamation mark appears to the right of the string.</p>	
Type	<p>The icons in the window are converted into character strings and output as follows:</p> <p> -&gt; Complete-correlations event</p> <p> -&gt; Incomplete-correlations event</p> <p>(no icon) -&gt; (blank)</p>	
Action type	<p>The icons in the window are converted into character strings and output as follows:</p> <p> -&gt; Command</p> <p> -&gt; Rule</p> <p>  -&gt; Command, Rule</p> <p>(no icon) -&gt; (blank)</p>	

Legend:

--: None.

When a program-specific extended attribute is mapped to a display item in the event-information mapping definitions, the attribute value is output to the snapshot in the same format as displayed in the Event Console window (value prefixed with # followed by a space).

If there are no events displayed in the window, only the header information (line 1) and the display items (line 2) will appear in the snapshot. If there is no information for a particular display item, that field is blank.

If the character string is a control character, it is converted into a space when displayed in the window, but appears as is when output to a CSV snapshot.

#### (4) **Snapshot timing**

To take a CSV snapshot, choose **File** and then **Save Displayed Events** in the Event Console window. The currently displayed event information is captured in the snapshot.

*Note:*

- By default, the event information displayed in the **Monitor Events** page and **Severe Events** page of the Event Console window is automatically refreshed at 5-second intervals.

To stop the event information from being refreshed automatically when taking a snapshot, in the Preferences window change **Automatic refresh** from **Apply** to **Do not apply**.

- You cannot export CSV snapshot files to a removable medium.

### 3.9.2 Saving event information in the integrated monitoring database (CSV report)

The functionality for outputting event information from the integrated monitoring database is referred to as *output of an event report*.

Using this feature in JP1/IM, you can save information about the JP1 events registered in the integrated monitoring database as a CSV-formatted report. To output an event report, execute the `jcoevtreport` command. As a command option, you can specify what event information to output.

For the command syntax, see `jcoevtreport` in *1. Commands* in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.

The following describes the range of information you can output in an event report, and the output format, items, and command options.

#### (1) **Information that can be output to an event report**

You can output the following event information to an event report:

- Time-specified event information

You can specify the arrival time of the JP1 events to be output.

- Program-specific event information

You can specify particular items of program-specific information. If you do not specify any items, all items are output.

- Information about events that match a filter condition

You can limit the JP1 events to be output using pass conditions or exclusion

conditions in a filter. For the items you can specify in a filter condition, see Table 3-11 *Contents output to an event report*.

You can specify a maximum of 50 filter conditions in one pass condition group or one exclusion condition group. In a filter for extended attributes (program-specific information), however, you can specify a maximum of five filter conditions in one pass condition group or one exclusion condition group.

## (2) Image and format of an event report

When you specify the header option, header information is output to line 1, separated by commas.

In line 2 and subsequent lines, event information is output in the following order, separated by commas:

*basic attribute, extended attributes (common information), IM attributes, extended attribute (program-specific information)*

In the extended attribute (program-specific information), event information is output as follows, after the IM attributes:

*number of program-specific extended attributes, attribute name, attribute value*

If you do not specify output of extended attributes, the number of program-specific extended attributes appears as 0, and the attribute name and value are blank (nothing is entered).









## (3) Items output to an event report

When you specify the header option, header information for the attribute name or item name is output to line 1 of the CSV file. By default, no headers are output.










Table 3-11: Contents output to an event report













Attribute type	Item	Header information
Basic attribute	Serial number	The character string displayed in the window is output.
	Event ID	The character string displayed in the window is output.
	Source process ID	The character string displayed in the window is output.
	Registered time	Output in either of the following formats: <ul style="list-style-type: none"> <li>YYYYMMDDhhmmss</li> <li>Cumulative seconds from 1970/01/01 00:00:00 (GMT)</li> </ul>
	Arrived time	
	Registered reason	Output in decimal format.
	Source user ID	
	Source group ID	

### 3. Centralized System Monitoring Using the Central Console

Attribute type	Item	Header information
	Source user name	Output as a character string.
	Source group name	
	Source host	
	Destination event server name	
	Source IP address	The IP address is output as a character string.
	Destination IP address	
	Source serial number	The character string displayed in the window is output.
	Code set	Output as a character string.
	Message	The character strings displayed in the window are output.
Extended attribute (common information)	Event level	<p>The character string is converted and output as follows:</p> <ul style="list-style-type: none"> <li> Emergency -&gt; Emergency</li> <li> Alert -&gt; Alert</li> <li> Critical -&gt; Critical</li> <li> Error -&gt; Error</li> <li> Warning -&gt; Warning</li> <li> Normal -&gt; Normal</li> <li> Information -&gt; Information</li> <li> Debug -&gt; Debug</li> </ul> <p>For all other event levels, the character string displayed in the window is output as is.</p> <p>The severity color coding and icons are not output.</p>
	User name	The character string displayed in the window is output.
	Product name	
	Object type	
	Object name	
	Root object type	
	Root object name	
	Object ID	Output as a character string.
	Occurrence	The character string displayed in the window is output.



Attribute type	Item	Header information
	Start time	Output in either of the following formats: <ul style="list-style-type: none"> <li>YYYYMMDDhhmmss</li> <li>Cumulative seconds from 1970/01/01 00:00:00 (GMT)</li> </ul>
	End time	
	Return code	Output as a character string.
Extended attribute (program-specific information)	E .xxxxx	Output as a character string.
IM attributes	Action type	The icons in the window are converted into character strings and output as follows:  -> Command  -> Rule   -> Command, Rule (no icon) -> (blank)
	Action suppression	The icons in the window are converted into character strings and output as follows:  -> Execute  -> Partially suppress  -> Suppress (no icon) -> (blank)
	Severe event	Either of the following is output: If the JP1 event is not severe: Blank If the JP1 event is severe: Severe Event
	Correlation event	The icons in the window are converted into character strings and output as follows:  -> Complete-correlations event  -> Incomplete-correlations event (no icon) -> (blank)

Attribute type	Item	Header information
	Original severity level	<p>The icon is converted and output as follows:</p> <p> Emergency -&gt; Emergency</p> <p> Alert -&gt; Alert</p> <p> Critical -&gt; Critical</p> <p> Error -&gt; Error</p> <p> Warning -&gt; Warning</p> <p> Normal -&gt; Normal</p> <p> Information -&gt; Information</p> <p> Debug -&gt; Debug</p> <p>For all other event levels, the character string displayed in the window is output as is.</p> <p>The severity color coding and icons are not output.</p>
	New severity level	<p>The icon in the window is converted and output as follows:</p> <p> -&gt; Changed</p> <p>(no icon) -&gt; (blank)</p>
	Response status	<p>The icons in the window are converted into character strings and output as follows:</p> <p> -&gt; Processed</p> <p> -&gt; Processing</p> <p> -&gt; Held</p> <p>(no icon) -&gt; Unprocessed</p>
	Severe event release	<p>The following character string is output:</p> <p>If the severe event has not been released: Blank</p> <p>If the severe event has been released: Released</p>
	Severe event deletion	<p>The following character string is output:</p> <p>If the severe event has not been deleted: Blank</p> <p>If the severe event has been deleted: Delete</p>
	Memo	The character strings displayed in the window are output.

#### (4) Command options

You can specify the following options in the `jcoevtreport` command to output maintenance information and to save the event report:

- Export maintenance information

`jcoevtreport -sys -s 20090101000000 -e 20090103000000` (This example outputs JP1 events that were registered in the integrated monitoring

database between 2009/01/01 00:00:00 and 2009/01/03 00:00:00.)

- Save events before deletion

```
jcoevtreport -save
```

These two options are explained next.

#### (a) Export maintenance information

When an error occurs in the integrated monitoring database, this option outputs information about all JP1 events registered between the output start time and end time to the event report.

The attribute name appears in the header part.

Because the purpose is to collect data for investigating a database error, you cannot specify what items to output or any filtering conditions.

#### (b) Save events before deletion

This option outputs an event report about JP1 events due for deletion to free up space in the integrated monitoring database.

With this option specified, the command outputs in CSV format all the JP1 events registered in the integrated monitoring database that have not previously been saved to an event report.

#### ■ Warning before deletion of unsaved JP1 events

You can issue a deletion warning event (event ID: 3F52) when the ratio of JP1 events in the integrated monitoring database that have not been output to an event report (relative to the maximum size of the database) exceeds a set threshold for issuing a deletion warning event (by default, when the unsaved data exceeds 80% of the database capacity).

Specify the ratio of unsaved JP1 events in the `-dbntcpos` option of the `jcoimdef` command.

Specify the threshold for issuing a deletion warning event in the `-dbntc` option of the `jcoimdef` command.

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

#### ■ Display information about saving events before deletion in the standard output

You can specify an option to display information about saving events due for deletion. Set the `-showsv` option of the `jcoevtreport` command to display this information in the standard output.

This option lets you see how much free space will be required to save the events, and

helps you adjust the timing for outputting an event report before the target events are deleted.

With this option specified, the following items can be displayed in the standard output:

- Ratio of JP1 events that have not been output to an event report (relative to the maximum size of the integrated monitoring database)

The ratio of JP1 events in the integrated monitoring database that have not been output to an event report is shown as a percentage.

- Data size of the JP1 events that have not been output to an event report

The data size of the JP1 events in the integrated monitoring database that have not been output to an event report is shown in megabytes.

- Threshold for issuing a deletion warning event

If issue of a deletion warning event is specified, the threshold is shown as a percentage. If you specify OFF in the `jcoimdef` command's `-dbntc` option, a hyphen (-) is shown.

### 3.9.3 Copying JP1 event information and action execution results to the clipboard

In JP1/IM, you can copy selected JP1 event information and action execution results to the clipboard in CSV format. You can then make temporary use of the information. For example, you can copy information about a JP1 event triggered by a major error into a text editor or the body of an email.

The clipboard feature is enabled by default. For the procedure to enable or disable copying to the clipboard, see *4.11 Customizing the JP1/IM - View operation* in the *Job Management Partner 1/Integrated Management - Manager Configuration Guide*.

The following describes the windows and types of information that you can copy to the clipboard, and the output format and output items.

#### (1) Target windows and types of information

You can copy the following types of information to the clipboard:

- JP1 event information
- Action log
- Command log

The clipboard feature can be used in all windows in which these types of information are displayed. The following table lists the applicable windows and display items.

*Table 3-12:* Applicable windows and display items when copying to the clipboard

Window name	Display item	Information
Event Console window <ul style="list-style-type: none"> <li>• <b>Monitor Events</b> page</li> <li>• <b>Severe Events</b> page</li> <li>• <b>Search Events</b> page</li> </ul>	List of events	JP1 event information
Event Details window	<b>Event attributes</b>	JP1 event information (detailed information)
Related Events (Summary) window	<ul style="list-style-type: none"> <li>• <b>Display Items</b></li> <li>• <b>Related Events</b></li> </ul>	JP1 event information
Related Events (Correlation) window	<ul style="list-style-type: none"> <li>• <b>Display Items</b></li> <li>• <b>Related Events</b></li> </ul>	JP1 event information
Action Log window	<b>Log</b>	Action log
Action Log Details window	<b>Log</b>	Action log (detailed information)
List of Action Results window	<b>Log</b>	Action log
Execute Command window	<b>Log</b>	Command log

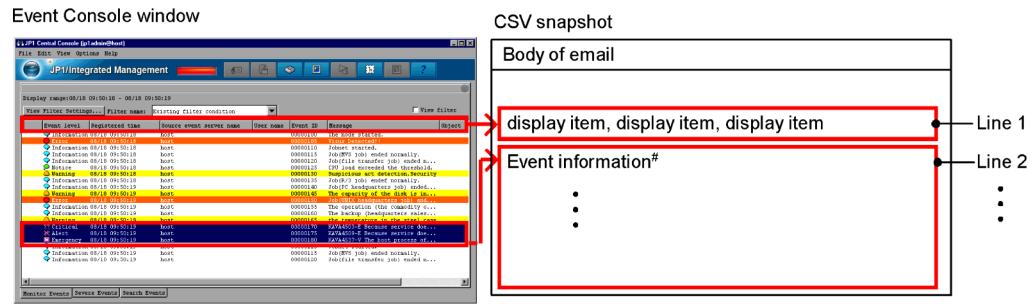
In the Event Console window, you can copy information to the clipboard by choosing **Edit** and then **Copy**, or by pressing the **Ctrl+C** keys. In all other windows, press the **Ctrl+C** keys to copy selected information to the clipboard.

## (2) CSV image and format

Information copied to the clipboard can be output in CSV format, in the same order as displayed in JP1/IM - View. The display item names are added as header information to identify the items.

The following figure shows the CSV output.

Figure 3-38: CSV clipboard image



#: Only the selected event information is output in the same order as displayed in the window.

Line 1 is the display item names corresponding to the information selected in JP1/IM - View, separated by commas.

Line 2 and subsequent lines are the selected information, separated by commas and following the order of the display item names in line 1.

The CSV output format is as follows:

- Items are separated by commas ( , ).  
*item1 , item2 , item3 , item4 , item5 , . . .*
- Lines are separated by linefeed codes (CRLF).  
*item1 , item2 , item3 , item4 , item5 , . . . (CRLF)*  
*item1 , item2 , item3 , item4 , item5 , . . . (CRLF)*
- Any item containing a comma ( , ) is enclosed with double quotation marks ( " ).  
*item1 , "item,2" , item3 , item4 , item5 , . . .*
- Any item containing a control character (0x00 to 0x1F, and 0x7F to 0x9F) is enclosed with double quotation marks ( " ).  
*item1 , "item(0x00)2" , item3 , item4 , item5 , . . .*
- When an item contains a double quotation mark ( " ), another double quotation mark is inserted before it, and the whole is enclosed with double quotation marks ( " ).  
*item1 , "item" " 2" , item3 , item4 , item5 , . . .*
- Empty items are shown as blank (nothing is entered).  
*item1 , , item3 , item4 , item5 , . . .*

### (3) CSV output items

The following describes the items and contents that are copied to the clipboard.



## JP1 event information

The contents output when copying JP1 event information to the clipboard are the same as the contents output to line 2 and subsequent lines when saving an event listing as a CSV snapshot. For details, see Table 3-10 *Contents output to the body of a snapshot*. As there is no header information, the display item names are output to line 1, and the event information is output to line 2 onward.

## Action log

The following table describes the contents output as an action log.

Table 3-13: Contents output as an action log

Display item name	Output contents
Type <sup>#</sup>	The icons in the window are converted into character strings and output as follows:  -> Command  -> Rule
Action serial number	The character string displayed in the window is output.
Action	The character string displayed in the window is output.
Host	The character string displayed in the window is output.
Status	The character string displayed in the window is output.
Delay	The character string displayed in the window is output.
Registered time	Output in the following format: YYYY/MM/DD hh:mm:ss
Event arrival time	Output in the following format: YYYY/MM/DD hh:mm:ss
End time	Output in the following format: YYYY/MM/DD hh:mm:ss
Return code	The character string displayed in the window is output.

<sup>#</sup>: Output only when linked with JP1/IM - Rule Operation.

## Command log

The following table describes the contents output as a command log.

*Table 3-14: Contents output as a command log*

Display item name	Output contents
Time	Output in the following format: <i>YYYY/MM/DD hh:mm:ss</i>
Host	The character string displayed in the window is output.
Message	The character strings displayed in the window are output.

## JP1 event information (details) or action log (details)

The following table describes the contents output as detailed information about a JP1 event or an action log entry.

*Table 3-15: Contents output as detailed information*

Display item name	Output contents
Attribute name	The character string displayed in the window is output.
Attribute value	The character string displayed in the window is output. If the time is displayed as the attribute value, it is output in the following format: <i>YYYY/MM/DD hh:mm:ss</i>

**(4) Notes**

Note the following when copying displayed information to the clipboard:

- The functionality is not supported in the Web-based JP1/IM - View.
- If you want to copy information to the clipboard by pressing the **Ctrl+C** keys, make sure that the functionality is enabled. It is enabled by default.
- The information copied to the clipboard is the item selected in the window that has the focus when you perform a copy operation by choosing a command or by pressing the shortcut keys. The selected information is not copied if it was changed to an unselected state as the result of an auto-refresh action that scrolled the item out of view before it was copied.
- When the amount of information to be copied to the clipboard exceeds the maximum memory usage, the copy processing is canceled and the information is not copied.



## 3.10 Specifying the event display start-time

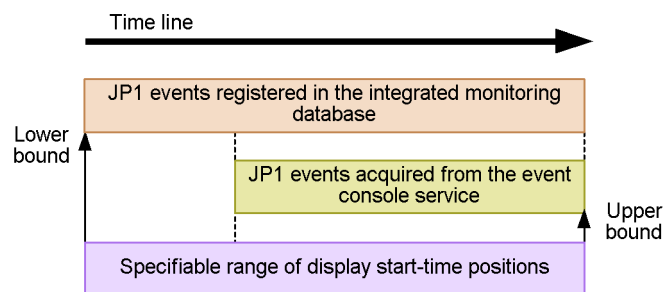
In the event display start-time specification area of the Event Console window, you can specify the start-time position for listing JP1 events.

To specify the display start-time position, you must first activate the integrated monitoring database. This enables JP1/IM to reference information about the JP1 events that have been acquired from JP1/Base and registered in the integrated monitoring database.

### 3.10.1 Specifiable range of event display start-time positions

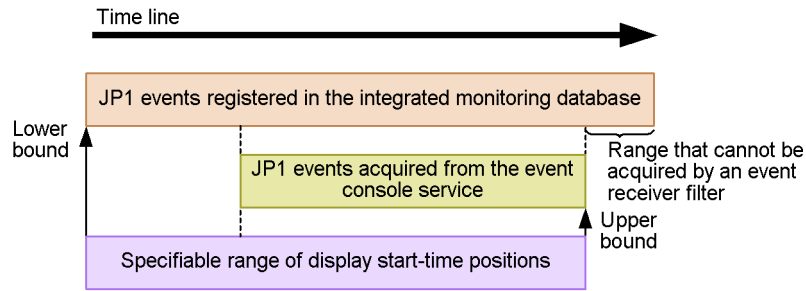
The range of start-time positions that you can specify is from the arrival time of the oldest JP1 event registered in the integrated monitoring database (lower bound) to the arrival time of the JP1 event most recently acquired from the event console service (upper bound).

*Figure 3-39: Specifiable range of display start-time positions when the integrated monitoring database contains JP1 events acquired from the event console service*



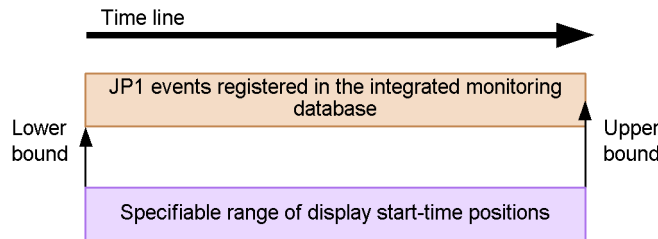
JP1 events that cannot be acquired from the event console service (by using an event receiver filter) cannot be displayed.

*Figure 3-40:* Specifiable range of display start-time positions when the integrated monitoring database contains some JP1 events that cannot be acquired from the event console service



When the integrated monitoring database contains only JP1 events that are not acquired from the event console service, the lower bound of the specifiable range is the arrival time of the oldest JP1 event, and the upper bound is the arrival time of the most recent JP1 event.

*Figure 3-41:* Specifiable range of display start-time positions when the integrated monitoring database contains only JP1 events not acquired from the event console service

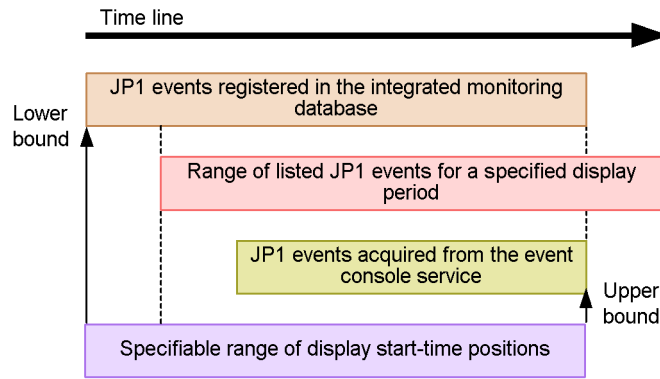


When JP1 events are listed by display period specification, the lower bound of the specifiable start-time positions is the arrival time of the oldest JP1 event in the specified period or the arrival time of the oldest JP1 event registered in the integrated monitoring database, whichever is later. The upper bound is the arrival time of the most recent JP1 event in the specified display period or the arrival time of the most recent JP1 event acquired from the event console service, whichever is earlier.

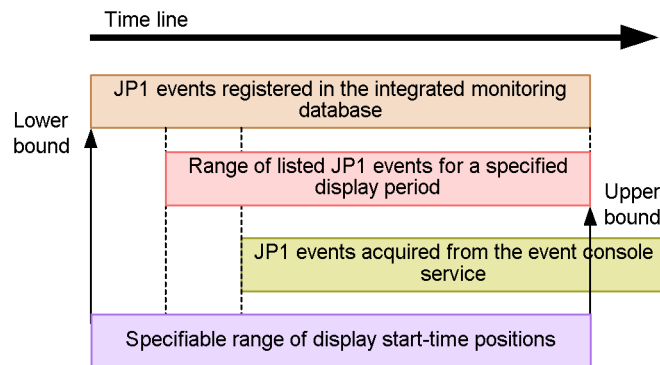
The figures below show the specifiable range of display start-time positions where the upper bound differs in each case.

- In the following figure, the oldest JP1 event registered in the integrated monitoring database has an earlier arrival time than the oldest JP1 event in the specified display period, and the most recent JP1 event in the specified display period has a later arrival time than the most recent JP1 event acquired from the

event console service.

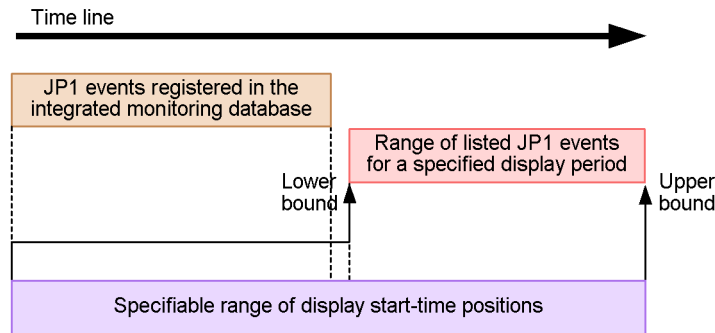


- In the following figure, the oldest JP1 event registered in the integrated monitoring database has an earlier arrival time than the oldest JP1 event in the specified display period, and the most recent JP1 event in the specified display period has an earlier arrival time than the most recent JP1 event acquired from the event console service.

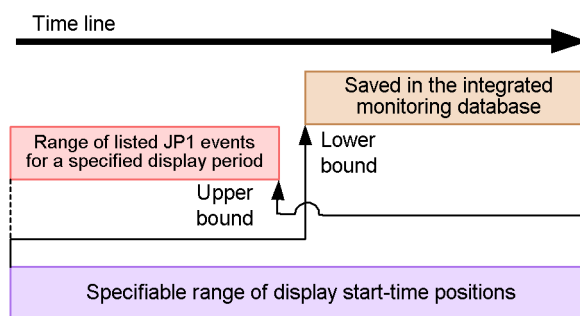


Note that the event display start-time specification area is unavailable when:

- No JP1 events have been registered in the integrated monitoring database.
- JP1 events are listed by display period specification, and no JP1 events were registered in the integrated monitoring database during the specified period, as illustrated below:



- JP1 events are listed by display period specification, and a time discrepancy between JP1/IM - Manager and JP1/IM - View means that the most recent JP1 event than can be displayed in the specified period is registered after the oldest event registered in the integrated monitoring database (that is, the lower and upper bounds of the specifiable range of display start-time positions are reversed):



When JP1 events are listed by display period specification, the time at which the JP1 event arrived at JP1/IM - Manager is compared with the current time of the JP1/IM - View host. Any discrepancy between the times of JP1/IM - Manager and JP1/IM - View could result in a JP1 event outside the specified display period being included in the listing. We recommend that you synchronize the time settings of JP1/IM - Manager and JP1/IM - View.

The event display start-time specification area appears in the window only if you are using the integrated monitoring database.

For details about specifying a display period, see *3.11 Specifying the event display period*.

### 3.10.2 Specifying the event display start-time position using the slider

You can easily specify the start-time position for listing JP1 events using the slider in the event display start-time specification area.

The slider is at the far right when the most recent events are displayed. As you move the slider to the left, events saved in the integrated monitoring database are listed from the start-time position indicated by the slider, up to the maximum number of viewable events (scroll buffer size). The listed events are those that have passed through an event receiver filter or view filter.

When you move the slider to the far left, the oldest event is displayed.

### 3.10.3 Specifying the event display start-time position by date and time

You can specify a precise start-time position by specifying the arrival time of the events you want to view. Set the desired arrival time in the event display start-time text boxes in the event display start-time specification area.

When you enter an arrival time, events saved in the integrated monitoring database are listed from the specified time up to the maximum number of viewable events (scroll buffer size). The slider in the event display start-time specification area moves to the time position that you entered in the start-time text boxes.

The defaults for the start-time text boxes depends on the time at which you were logged in to JP1/IM - Manager.

If you log in to JP1/IM - Manager later than the base time on a particular day, the base time of that day is displayed in the text boxes by default.

*Example:* The base time is 09:00, and you log in at 2008/07/08 10:00.

The default date and time shown in the event display start-time text boxes is 2008/07/08 09:00.

If you log in to JP1/IM - Manager earlier than the base time on a particular day, the base time of the previous day is displayed in the text boxes by default.

*Example:* The base time is 09:00, and you log in at 2008/07/08 08:00.

The default date and time shown in the event display start-time text boxes is 2008/07/07 09:00.

### 3.10.4 Specifying the event display start-time position using the buttons

The event display start-time specification area has the following buttons: **Oldest Event**, **Previous Event**, **Next Event**, and **Most Recent Event**.

Click the **Oldest Event** button to list the maximum number of viewable events (scroll buffer size) stored in the integrated monitoring database, starting from the oldest event.

Click the **Previous Event** button or **Next Event** button to move the viewable events up or down one event.

Click the **Most Recent Event** button to return the event listing to the state before you set the start-time position.

### 3.10.5 Processing after event display start-time specification

When you specify an event display start-time position, JP1/IM retrieves the maximum number of viewable events (scroll buffer size) stored in the integrated monitoring database that match the specified search condition.

At completion of the search, the retrieved events are listed in the Event Console window.

The **Status** display, and whether the **Cancel** button is available, change according to the search progress and result.

For details, see *2.2 Monitor Events* page in the manual *Job Management Partner 1/ Integrated Management - Manager GUI Reference*.

---

## 3.11 Specifying the event display period

---

You can change the JP1 events listed in the Event Console window, restricting the listing to a specified period.

To restrict the listing, set a base time and a duration.

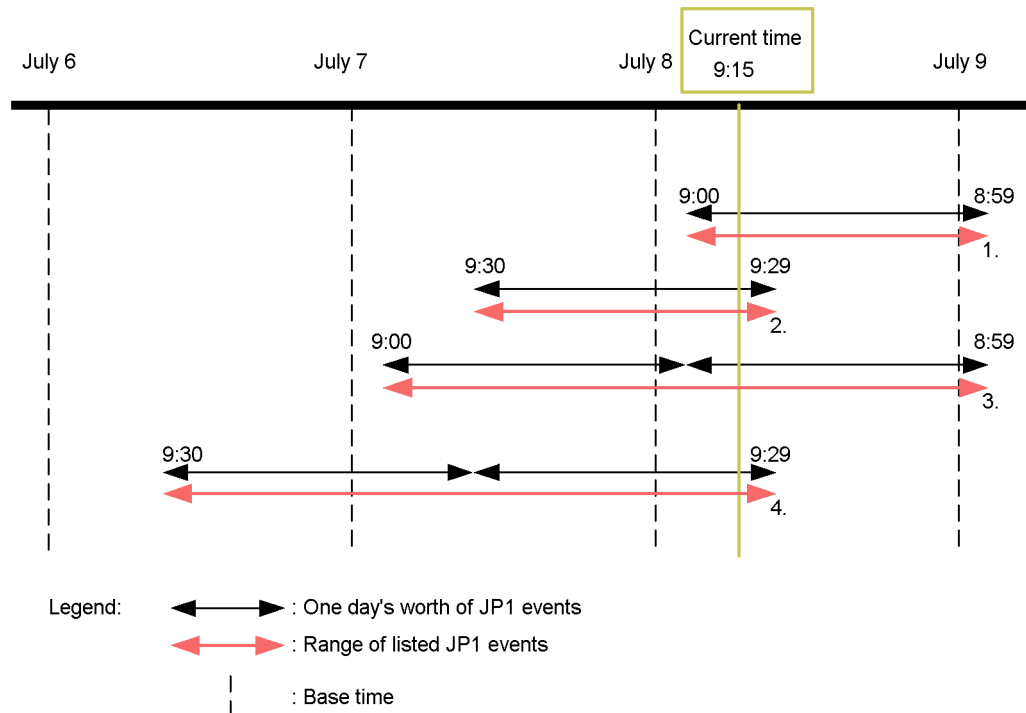
### 3.11.1 Range of listed JP1 events for a specified display period

The display period specification applies to JP1 events that have passed through an event acquisition filter, event receiver filter, severe events filter, or view filter.

To determine whether a specific JP1 event occurred during the specified display period, its arrival time at JP1/IM - Manager is compared with the current time of the JP1/IM - View host. Any discrepancy between the times of JP1/IM - Manager and JP1/IM - View could result in a JP1 event outside the specified display period being included in the listing. We recommend that you synchronize the time settings of JP1/IM - Manager and JP1/IM - View.

The following figures illustrate the range of JP1 events that are listed when you specify a display period.

Figure 3-42: Range of listed events when the current time is 9:15 am on July 8



The numbers below correspond to the numbers in the figure.

1. Range of listed JP1 events when the display period is one day and the base time is 9:00.
2. Range of listed JP1 events when the display period is one day and the base time is 9:30.
3. Range of listed JP1 events when the display period is two days and the base time is 9:00.
4. Range of listed JP1 events when the display period is two days and the base time is 9:30.

When you use the integrated monitoring database, the listing specification applies to JP1 events saved in the database.

If you specify a start-time position for listing JP1 events with the integrated monitoring database, the range of JP1 events that are listed changes as follows:



Figure 3-43: Range of listed events when the display period is two days and the current time is earlier than the base time

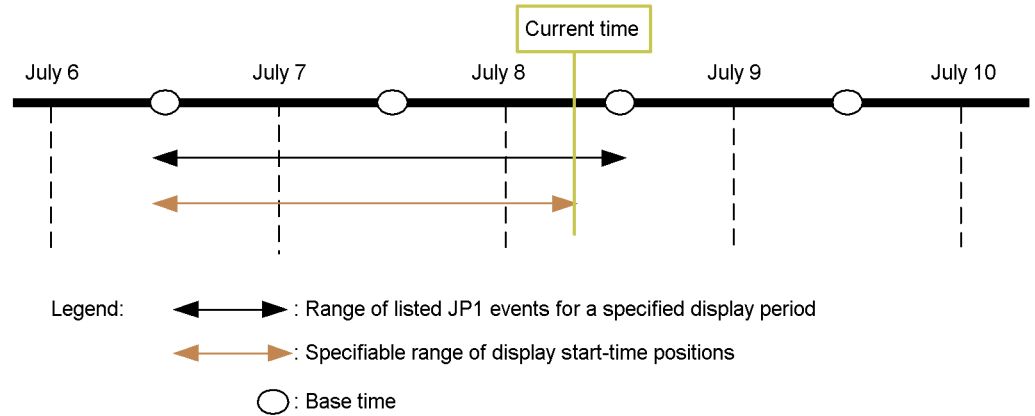
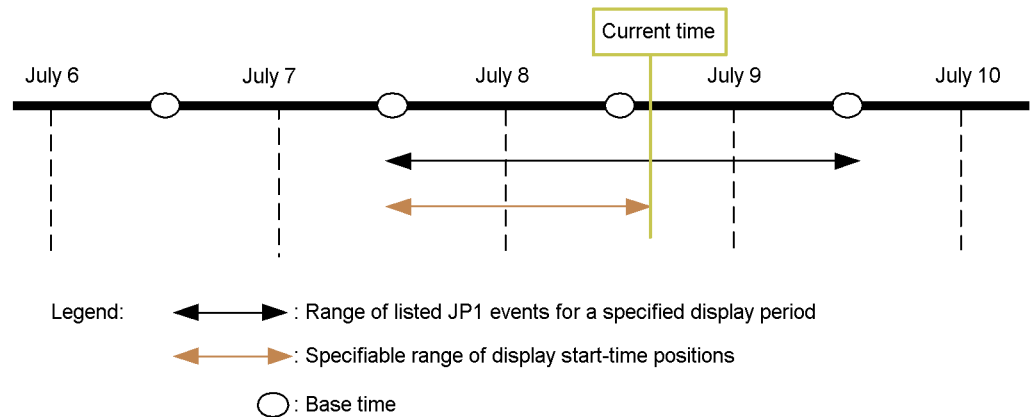


Figure 3-44: Display range when the display period is two days and the current time is later than the base time



For details about the event display period specification, see 5.1.8 *Displaying events by specifying a time period* in the *Job Management Partner 1/Integrated Management - Manager Administration Guide*.

For details about the event display start-time specification, see 3.10 *Specifying the event display start-time*.

---

## 3.12 Performing system operations from JP1/IM

---

When a problem is detected during system monitoring, you can investigate using the following JP1/IM operations:

- Launch linked applications by monitor startup
- Tool Launcher
- Command execution from JP1/IM - View

This section describes these JP1/IM operations.

To launch a linked application by monitor startup or from the Tool Launcher, the OS user who started JP1/IM - View must have execution rights for that application.

### 3.12.1 Launching a linked product by monitor startup

In JP1/IM, you can select a JP1 event in the Event Console window and launch the GUI of the relevant application. This is known as *monitor startup*.

Depending on the application, by invoking the monitor startup you can directly launch a window related to the selected JP1 event. For example, if you select a job execution event issued by JP1/AJS and invoke the monitor startup, you will be taken directly to the window for managing the execution status of that job without having to navigate from a higher-level jobnet window.

Because you can launch an application window directly from a JP1 event that you want to investigate, you can quickly get on with the task by intuitive operation.

To use this functionality, the application that issued the JP1 event must support linkage with the monitor startup. For details about monitor startup support in a particular product, see the relevant manual. For example, the JP1/AJS and JP1/PFM documentation describes the setup required to invoke the monitor startup from the Event Console window.

- JP1/AJS: See the description of JP1/IM-based monitoring in the *Job Management Partner 1/Automatic Job Management System 3 Linkage Guide* or *Job Management Partner 1/Automatic Job Management System 2 Linkage Guide*.
- JP1/PFM: See the description of JP1/IM linkage in the *Job Management Partner 1/Performance Management Planning and Configuration Guide*.

You can add and change the applications that can be launched using the monitor startup by customizing a JP1/IM definition file. For an overview and description of how to customize the settings, see *4.12 Setting monitor startup for linked products* in the *Job Management Partner 1/Integrated Management - Manager Configuration Guide*.

*Note:*

The authentication information in JP1/IM - View is accessed when a user opens a window of any of the following linked products using the monitor startup functionality:

- JP1/IM - Rule Operation
- JP1/AJS - View
- JP1/AJS2 - Scenario Operation View
- JP1/AJS2 - View for Mainframe

Note that JP1/IM - View authentication information is invalidated in the following cases:

- The authentication server that the user is logged in to is restarted.
- The information is reloaded by the `jbs_spmc_reload` command on the authentication server that the user is logged in to.
- The primary authentication server that the user is logged in to is switched to the secondary authentication server.

When the authentication information in JP1/IM - View is invalid, the operations that can be performed depend on the product versions, as follows:

- When JP1/IM - Manager and JP1/IM - View are both version 09-00 or later, the JP1/IM - View user is automatically re-authenticated and authentication information is re-acquired.
- When either JP1/IM - Manager or JP1/IM - View is earlier than version 09-00, authentication fails on the linked product side.

### **(1) Overview of opening user-specified monitor windows**

The functionality provided by JP1/IM - View lets you open a monitor window for a listed JP1 event. In the monitor window, you can view details about the job or application that issued the event, and directly operate on that job or application. Note that this functionality is not available with the Web-based JP1/IM - View.

By customizing a JP1/IM definition file, in addition to the windows you can open by default<sup>#</sup>, you can open the user-specified windows listed below (only one application can be launched for a JP1 event):

- User-specified application window  
Specify the executable file of the application.
- Web page  
Specify the URL of the Web page you want to open.

You can also pass information about the particular JP1 event to the launched application.

#

By default, you can open any of the following:

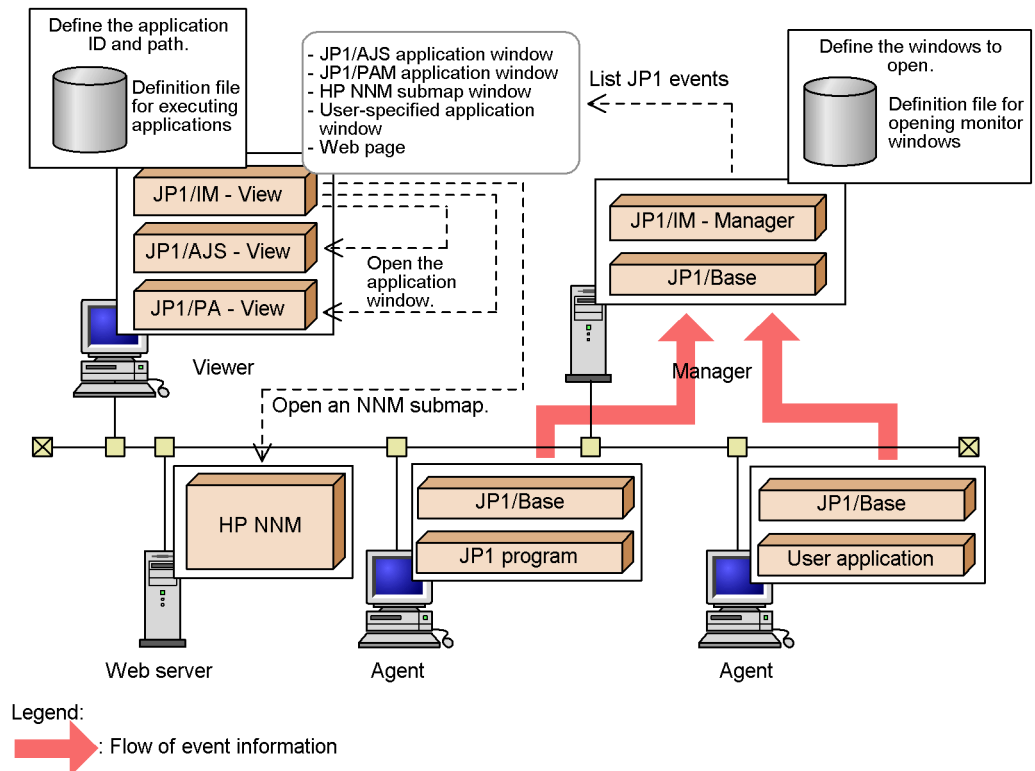
- JP1/AJS (application window)
- JP1/PAM (application window)
- A submap window (Web page) of HP NNM version 7.5 or earlier

Some settings might have been added to the above products to enhance linkage with JP1/IM. Refer to the documentation of the application you want to use with JP1/IM.

For details about launching a monitor window for HP NNMi, see the manual *Job Management Partner 1/Integrated Management - Event Gateway for Network Node Manager i Description, User's Guide and Reference*.

The following figure provides an overview of opening monitor windows.

Figure 3-45: Opening monitor windows from JP1 events listed in JP1/IM - View



## (2) Prerequisites

- To open an application program window, the executable file for that window must be placed on the machine on which JP1/IM - View is installed. The user who starts JP1/IM - View must also have permission to execute the application program to be launched.
- To open a Web page, a Web server is required for the supported Web browser to connect to.

### 3.12.2 Tool Launcher

From the Tool Launcher window in JP1/IM - View, you can launch windows of products in the JP1 series and many other applications. The Tool Launcher window lists the application functions that are linked with JP1/IM, allowing the windows of the appropriate application to be launched directly from the listing.

You can launch the following two types of windows from JP1/IM - View:

Windows of applications on the viewer

You can launch and view the windows of any linked application installed on the same machine as JP1/IM - View.

#### Web pages

You can view the Web pages provided by any linked application in the system. Your Web browser starts with the required Web page. To view a Web page from the Tool Launcher, you must set the Web page's Uniform Resource Locator (URL) in advance.

A number of applications linked with JP1/IM are pre-registered in the Tool Launcher. For details, see *7.3.2 Functions that can be operated from the Tool Launcher window* in the *Job Management Partner 1/Integrated Management - Manager Administration Guide*.

If the application you want to register in the Tool Launcher is not mentioned in the above manual, see the documentation for that product. For example, the JP1/PPM manual explains how to register JP1/PPM functionality in the Tool Launcher.

- JP1/PPM: See the description of JP1/IM linkage in the *Job Management Partner 1/Performance Management Planning and Configuration Guide*.

You can add and change the applications that can be displayed in the Tool Launcher window by customizing a JP1/IM definition file. For an overview and detailed description of how to customize the settings, see *4.13 Setting the Tool Launcher window* in the *Job Management Partner 1/Integrated Management - Manager Configuration Guide*.

*Note:*

The authentication information in JP1/IM - View is accessed when a user opens a window of any of the following linked products from the Tool Launcher:

- JP1/IM - Rule Operation
- JP1/AJS - View
- JP1/AJS2 - Scenario Operation View
- JP1/AJS2 - View for Mainframe

Note that JP1/IM - View authentication information is invalidated in the following cases:

- The authentication server that the user is logged in to is restarted.
- The information is reloaded by the `jbs_spmc_reload` command on the authentication server that the user is logged in to.
- The primary authentication server that the user is logged in to is switched to the secondary authentication server.

When the authentication information in JP1/IM - View is invalid, the operations that can be performed depend on the product versions, as follows:

- When JP1/IM - Manager and JP1/IM - View are both version 09-00 or later, the JP1/IM - View user is automatically re-authenticated and authentication information is re-acquired.
- When either JP1/IM - Manager or JP1/IM - View is earlier than version 08-01, authentication fails on the linked product side.

### **(1) Overview of adding items to the Tool Launcher window**

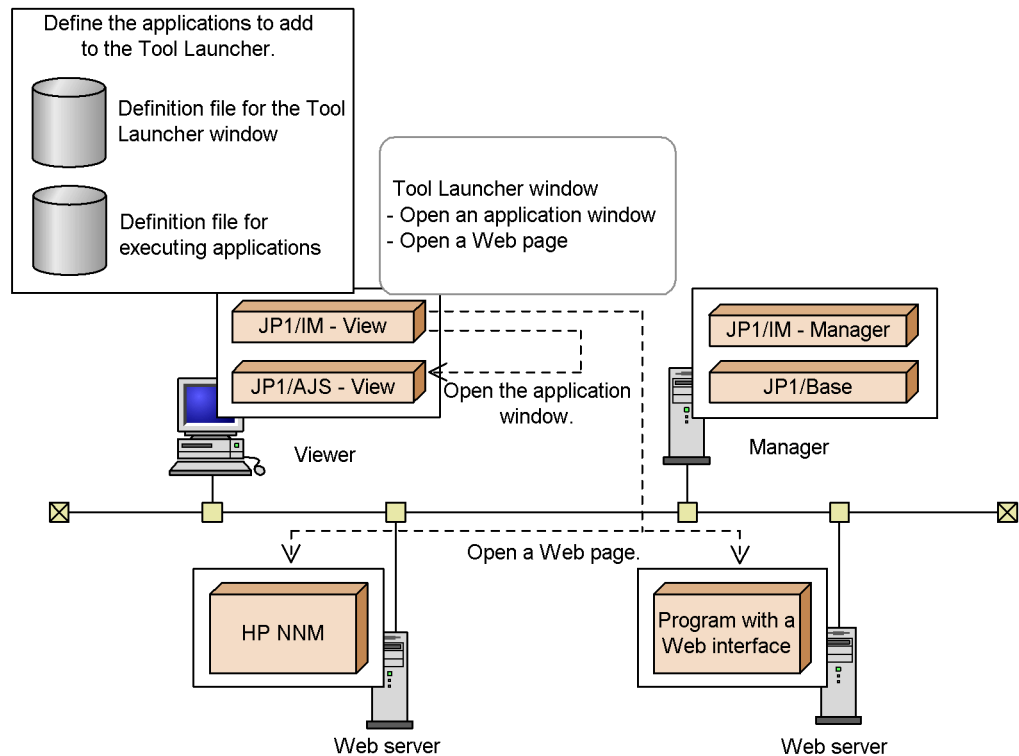
The Tool Launcher window of JP1/IM - View lists the programs linked with JP1/IM. From the Tool Launcher, you can launch another management application program or open a Web page.

By customizing a JP1/IM - View definition file, you can add a new item to the Tool Launcher window. As the window to open from the new item, you can specify the following:

- User-specified application window  
Specify the executable file of the application.
- Web page  
Specify the URL of the Web page you want to open.

The following figure provides an overview of adding items to the Tool Launcher window.

Figure 3-46: Adding items to the Tool Launcher window



## (2) Prerequisites

To open an application program window, the executable file for that window must be placed on the machine on which JP1/IM - View is installed. The user who starts JP1/IM - View must also have permission to execute the application program to be launched.

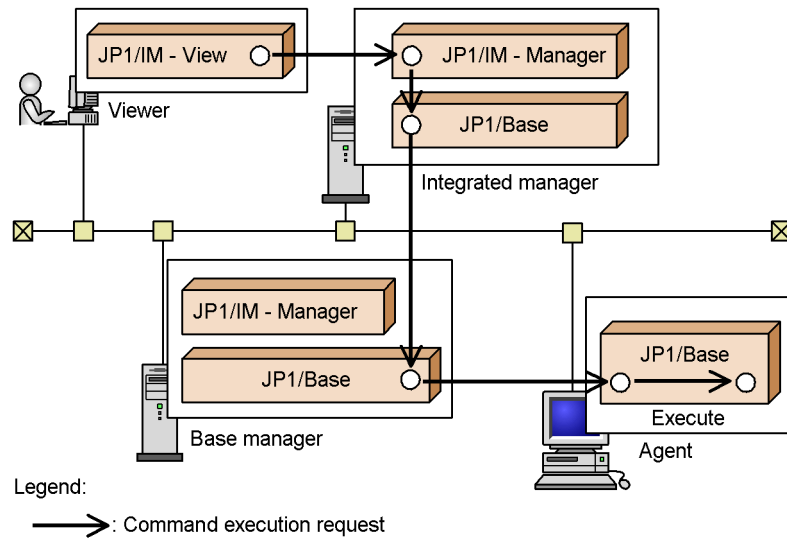
To open a Web page, a Web server is required on the host specified in the URL (the host on which the product that provides the Web page is installed).

### 3.12.3 Executing commands from JP1/IM - View

In JP1/IM, requests can be issued from the Event Console window to execute a command on a managed host. You perform this request in JP1/IM - View's Execute Command window. The entered execution request is forwarded to the specified host from the manager that you are logged in to, according to the system configuration defined in the JP1/Base configuration management. The command is then executed on the target host.



Figure 3-47: Overview of command execution from JP1/IM - View



The following describes the conditions required for command execution and the types of commands you can execute. This is followed by a description of the flow of processing for the execution.

### (1) Executable commands

The following types of commands can be executed from JP1/IM - View:

On a Windows host:

- Executable file (.com or .exe)
- Batch file (.bat)
- Script file of JP1/Script (.spt) (provided the .spt file extension is associated with JP1/Script so that it can be executed)

On a UNIX host:

- UNIX command
- Shell script

However, the following types of commands cannot be executed:

- Commands that require interactive operation
- Commands that display windows
- Commands that use an escape sequence or control code
- Non-terminating commands such as daemons

- Commands (Windows only) that require interaction with the desktop, such as the Windows message structure or DDE
- Commands that shut down the OS, such as `shutdown` and `halt`

## **(2) Conditions for command execution**

The following conditions apply to command execution from JP1/IM - View:

- The JP1 user who requests command execution from JP1/IM - View must be registered in the authentication server and have the required permission for executing commands remotely.
- The system configuration must be defined using the JP1/Base configuration management.
- To execute a command on multiple hosts concurrently, the hosts must be grouped according to the host group definitions of the JP1/Base command execution function.
- The JP1 user issuing the request must be mapped to an OS user on the target host.
- To specify the command execution environment, you must first prepare an environment variable definition file on the target host.

## **(3) Checking the command execution status and result**

In the Execute Command window of JP1/IM - View, you can check the status and result of an executed command. To view the command execution log, execute the `jcocmdlog` command on the manager.

A JP1 event can be issued to report the execution status of a command. Because JP1 events are not issued by default, you must change the settings for issuing JP1 events by specifying the `-cmdevent` option of the `jcocmddef` command.

*Note:*

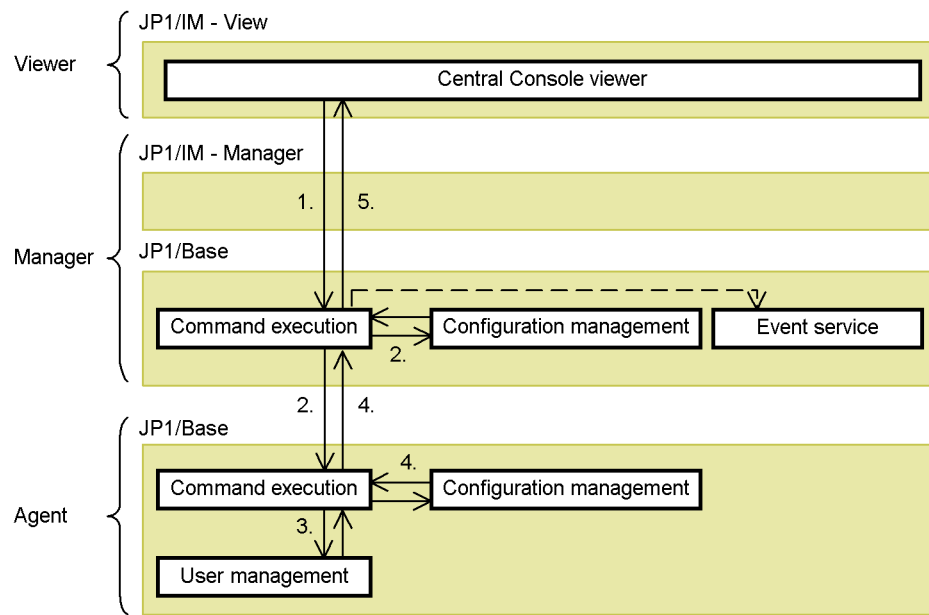
- When multiple commands are executed, the results might be output in a different order from the execution order. The result output timing is affected by such things as the time required to execute each command, performance and workload differences among the hosts on which the commands are executed, and retry after a communication error.
- The Execute Command window in JP1/IM - View shows the command execution results at the time they were received by the manager. Therefore, when you open this window, the displayed result might be for a previously executed command.
- If you mistakenly execute a command that cannot be executed from JP1/IM - View (see (1) *Executable commands*), the command fails to terminate (message KAVB2013-I is not displayed in the **Log** area in the Execute Command window). In this situation, you can recover by using the status check and deletion commands provided by JP1/Base. For details, see 7.4.4(6) *Commands for troubleshooting*.

**(4) Flow of processing for command execution**

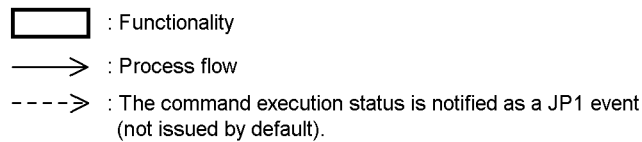
The following describes how the JP1/IM and JP1/Base functionality are inter-linked in command execution, taking as an example the flow of processing when a command is executed on an agent from a viewer.

The description below assumes that a JP1 user who has permission to execute commands is logged in to the manager. (For details about login requirements and the permissions required to execute commands, see 7.4.1 *Managing JP1 users*.)

Figure 3-48: Flow of processing for command execution (command executed remotely on an agent)



Legend:



The flow of processing is described below, following the numbers in the figure:

1. Open the Execute Command window in JP1/IM - View, and execute a command.  
You can specify the target host, command name, and command execution environment in this window. (The command execution environment must be defined in advance by setting up an environment variable definition file on the target host.)
2. On receiving the command execution request, JP1/Base on the manager host references the configuration definitions and passes the request to the target host.
3. JP1/Base on the agent host where the request was received first references the user mapping definitions and then executes the command using the permissions of the mapped OS user.<sup>#</sup>

#: User mapping (JP1/Base user management) is processed on the target host

where the command is to be executed. Thus, user mapping must be set up in advance on the agent to execute a command from JP1/IM - View on an agent, or on the manager to execute a command from JP1/IM - View on a manager.

4. After the command has been executed, JP1/Base on the agent reports the result to the higher-level host defined in the configuration definitions.
5. On receiving the command execution result, JP1/Base on the manager records the result in a command execution log (ISAM) file, and then reports the result to JP1/IM - View.

Command execution from JP1/IM - View is realized by the JP1/Base command execution function. See also *7.4.4 Managing command execution*.



## Chapter

---

# 4. Objective-Oriented System Monitoring Using the Central Scope

---

The Central Scope provides functionality for monitoring a system according to objectives set by the system administrator.

This chapter describes the functions of the Central Scope.

- 4.1 Overview of Central Scope functions
- 4.2 Monitoring tree
- 4.3 Automatically generating a monitoring tree
- 4.4 Editing a monitoring tree
- 4.5 Visual monitoring
- 4.6 Searching for monitoring nodes or status change events
- 4.7 Guide function
- 4.8 Completed-action linkage function
- 4.9 Performing system operations from JP1/IM
- 4.10 Central Scope

---

## 4.1 Overview of Central Scope functions

---

The Central Scope supports objective-oriented system monitoring based on tree views, map views, and action guidance. You can easily build a Central Scope environment using the auto-generation and editing functions of the Monitoring Tree window.

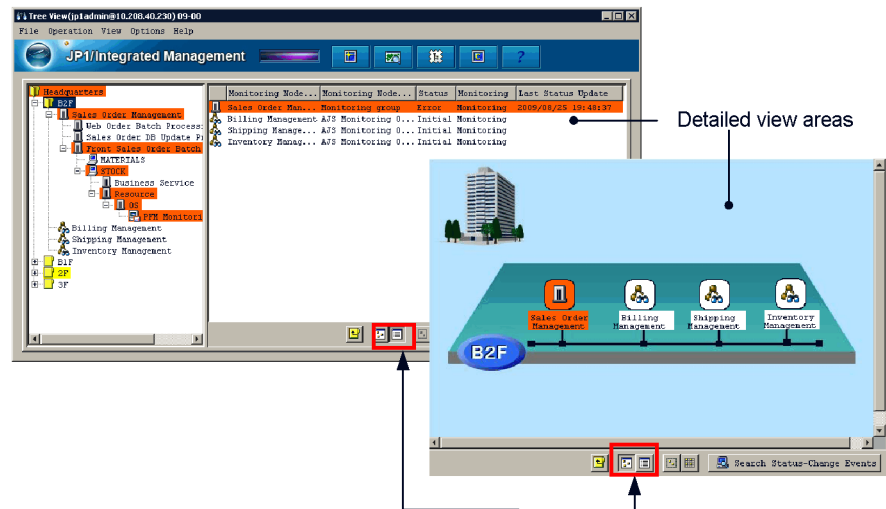
*Note:*

The Central Scope is disabled (does not start) by default. To use this functionality, you must enable the Central Scope in the `jcoimdef` command options.



Figure 4-1: Display examples of the Monitoring Tree window and Visual Monitoring window

Monitoring Tree window



Click these buttons to see detailed information or a map view.

Visual Monitoring window



The functions of the Central Scope are summarized as follows.

- Monitoring Tree window

Displays the resources managed by JP1/IM according to the monitoring objectives.

The monitoring tree shows the *monitoring objects* monitored by the Central

Scope, indicated by icons and arranged in *monitoring groups* in a tree structure.

The icons are designed so that you can see, from the inter-relationship of jobs and servers in the tree, which jobs will be affected by a server failure, for example. In the detailed view area, you can view information in map format, like the Visual Monitoring window.

By using JP1 resource groups, you can control the monitoring range permitted to individual JP1 users, and exercise precise control over access to the nodes in a monitoring tree.

##### ■ Auto-generation and editing of a monitoring tree

A monitoring tree can be easily generated using the auto-generation and editing functions.

To generate a monitoring tree, you simply select a purpose-built template from the Generation Tree list in the Auto-generation - Select Configuration window. The Central Scope automatically collects definition information from the JP1/IM agents, and creates a monitoring tree based on the template.

A template consists of model definition information for producing a monitoring tree in the form of a work-oriented tree or server-oriented tree.

You can edit an automatically generated monitoring tree in the Monitoring Tree (Editing) window to suit your system operation and its requirements.

Alternatively, you can output the monitoring tree definitions to a CSV file and then edit them.

##### ■ Visual monitoring

The icons in a monitoring tree can be mapped on a corporate organizational chart or other image in a Visual Monitoring window.

In addition to the icons provided as standard, you can register images of any size as Visual Icon. Key objects and groups that you particularly want to monitor can be placed on the map. This allows you to easily monitor even a large-scale system from the viewpoints you require.

##### ■ Guide information

You can view guide information relevant to the monitoring nodes and generated JP1 events. Action flows and troubleshooting procedures can be registered as advice for handling problems that might arise during system monitoring, lessening the system administrator's workload at the initial response stage.

Guide information can be preset by the user. As conditions for determining what information to display, you can specify information about a particular monitoring node or about a JP1 event that triggers a change in the status of a monitoring node.

You can also navigate from the Central Scope's Monitoring Tree window to the Event

Console window in the Central Console.

---

## 4.2 Monitoring tree

---

The following describes a monitoring tree.

### 4.2.1 Monitoring tree structure

A monitoring tree consists of monitoring objects, monitoring groups, and a virtual root node.

*Table 4-1:* Elements of a monitoring tree

Item	Description
Monitoring object	An object that you monitor using the Central Scope. A monitoring condition can be set for a monitoring object to change its icon to error status or other status under certain conditions. The icon status changes when a JP1 event related to the object is received by JP1/IM - Manager and is found to match the set monitoring condition.
Monitoring group	A group of monitoring objects. A monitoring group can contain monitoring objects and/or other monitoring groups. When the icon status of a lower-level object or group changes on receipt of a JP1 event, the icon status of the higher-level monitoring group containing that object or group also changes.

Item	Description
Virtual root node	<p>Appears only when the monitoring range settings are enabled for the monitoring tree. For details, see 4.4.3 <i>Setting the monitoring range of a monitoring tree</i>.</p> <p>For example, if the JP1 user <code>jp1ope</code> logs in to JP1/IM - Manager (JP1/IM - Central Scope) while the monitoring range settings are enabled, the virtual root node will appear at the top of the monitoring tree as shown in the figure below.</p> <p><i>Example:</i></p> <p>As shown in the figure, the virtual root node is identified by an icon in the shape of a person. The name of the virtual root node is that of the JP1 user currently logged in to JP1/IM - Manager (JP1/IM - Central Scope). Unlike a monitoring object or monitoring group, the information in a virtual root node cannot be edited (in the Properties window). Neither can you change the node status or perform any other direct operations on the virtual root node. (Its status changes accordingly when the status of a monitoring node below it changes, but you cannot change the virtual root node status directly. To change its status, you must change the status of a lower-level monitoring node.)</p>

Monitoring objects and monitoring groups are referred to generically as *monitoring nodes*.

#### 4.2.2 Statuses of monitoring nodes

The status of monitoring objects and groups is managed on the basis of the JP1 events generated in the particular object.

A monitoring node has two different types of statuses:

- Status

The events occurring on a monitoring node are managed according to the status of the node.

Node statuses, in order of priority, are Emergency, Alert, Critical, Error, Warning, Normal, Debug, and Initial.

For example, if an error occurs on a node, resulting in a JP1 event of Emergency level, the Central Scope manages the event according to the current status of the node.

##### ■ Monitoring status

Information that determines whether to monitor the node status.

There are two monitoring statuses: **Monitor** and **Do not monitor**.

When **Monitor** is set for a node, the status of the node changes when a JP1 event matching the monitoring conditions is received. Statuses are color-coded in the Monitoring Tree window and Visual Monitoring window.

When **Do not monitor** is set for a node, the status of the node does not change even when a JP1 event is received from the node. The node is grayed out in the Monitoring Tree window and Visual Monitoring window.

A node has Initial status when monitoring begins. This means that the Central Scope does not yet have any information about the status of the node.

If **Monitor** is set for an object and a JP1 event of Emergency level occurs because of a failure, for example, the status of the object changes on receipt of the JP1 event by JP1/IM - Manager. Whether a status change occurs in an object is determined by a *status change condition*.

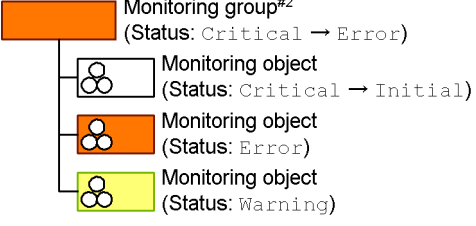
When the status of an object changes, its new status is passed in succession to each of the higher-level groups in the monitoring tree. If the new status has higher priority than the status of the receiving group, or if the status of the lower-level node satisfies the status change condition of the receiving group, the status of that group changes.

If **Do not monitor** is set for an object, the status of the monitoring node does not change, even when a JP1 event is received because of an error on the node. If the object's monitoring status is changed to **Monitor**, the status of the node will change according to JP1 events subsequently received from the object. **Do not monitor** is the default status for an automatically generated monitoring tree.

#### (1) Behavior when changing the status of a monitoring node manually

You can change the status of a monitoring node manually. The statuses that can be set, and the status change behavior, differ according to whether the monitoring node consists of monitoring objects or monitoring groups.

Table 4-2: Specifiable statuses and status change behavior based on monitoring node type

Monitoring node type	Specifiable statuses and status change behavior
Monitoring object	<p>You can change the node status to Emergency, Alert, Critical, Error, Warning, Normal, Debug, or Initial<sup>#1</sup>.</p> <p>When the node status changes, the new information is relayed upward through the tree, and the status of each higher-level monitoring group changes to the status that has highest priority among the statuses of the lower-level monitoring nodes.</p> <p>Example:</p>  <pre> graph TD     A[Monitoring group#2 (Status: Critical → Error)] --- B[Monitoring object (Status: Critical → Initial)]     A --- C[Monitoring object (Status: Error)]     A --- D[Monitoring object (Status: Warning)]   </pre>
Monitoring group	<p>You can change the node status to Initial<sup>#1</sup> only.</p> <p>When the node status changes, the new information is relayed upward through the tree, and the status of each higher-level monitoring group changes to the status that has highest priority among the statuses of the lower-level monitoring nodes (same behavior as for a monitoring object). The status of all lower-level monitoring nodes changes to Initial.</p>

#1: Manually changing the status of a monitoring node deletes the status change events logged for that node (see 4.6.2 *Searching for status change events*).

#2: The status of a monitoring group changes to the highest status among the lower-level nodes. However, when a status change condition is set for a group, that condition takes precedence.

You can change a node status manually using the GUI or the `jcschstat` command (for the command syntax, see `jcschstat` in 1. *Commands* in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*).

When you change a node's monitoring status to **Do not monitor**, the monitoring status of all lower-level nodes is reset to **Do not monitor**. The node itself and all lower-level nodes revert to *Initial* status. Similarly, when you change a node's monitoring status to **Monitor**, all lower-level nodes also change to **Monitor**.

When a higher-level node has been reset to **Do not monitor**, you cannot change the lower-level nodes back to **Monitor** status. To change a lower-level node back to **Monitor** status, you must change the higher-level node from **Do not monitor** to

**Monitor** again.

### 4.2.3 Status change conditions

A status change condition changes the status of a monitoring node. It can be set for both monitoring objects and monitoring groups, but there are differences in each case.

Status change condition for a monitoring object

Determines what types of received JP1 events will trigger a status change in the monitoring object (for example, change the node status to `Warning` when a specific JP1 event of `Warning` level is received).

Status change condition for a monitoring group

Determines what lower-level node statuses will trigger a status change in the monitoring group (for example, change the node status to `Error` when two of three lower-level monitoring nodes have `Error` status).

When no condition has been set, the monitoring group is set to the status that has highest priority among the lower-level monitoring nodes.

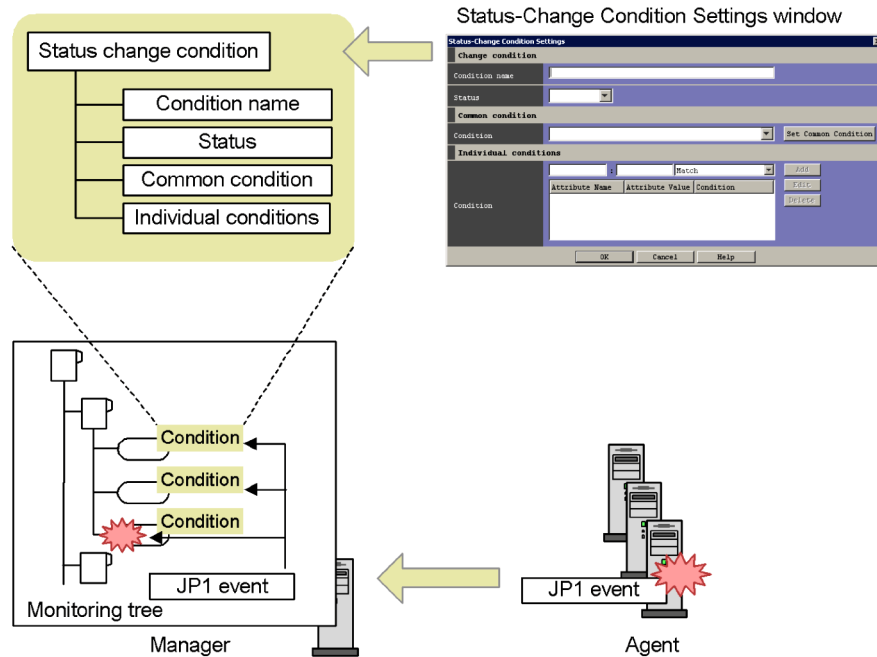
The status change conditions for monitoring objects and groups are further described below.

#### **(1) Status change conditions for monitoring objects**

The following figure shows status change conditions for monitoring objects.



Figure 4-2: Status change conditions for monitoring objects



Each monitoring object in a monitoring tree has its own status change condition. When JP1/IM - Manager receives a JP1 event, it checks the status change condition of each object. If the condition is satisfied, and the status of the received event has higher priority than the object's current status, JP1/IM - Manager changes the object's status accordingly. In this way, generated JP1 events are associated with the relevant objects in the monitoring tree, providing a visual representation of the system status.

A status change condition for a monitoring object consists of a condition name, status, common condition, and individual conditions, as described below. Multiple common conditions and individual conditions can be specified for a JP1 event.

- **Condition name**  
The name of the status change condition.
- **Status**  
The status of the monitoring object when the status change condition is satisfied.  
One of the following can be specified: Emergency, Alert, Critical, Error, Warning, Normal, Debug, or Initial.
- **Common condition**

A status change condition that applies to a number of monitoring objects. For example, for an object that monitors a jobnet, JP1 event ID 4108 (generated when a jobnet ends with a warning) is a common condition and applies to all such monitoring objects.

- Individual condition

A condition whose value is specific to the object concerned. For example, a condition whose value changes for each monitoring object, such as the job name for a jobnet monitoring object, is an individual condition.

The following figure describes how a status change condition is set in practice, taking as an example a system-monitoring object.

Figure 4-3: Example of a system-monitoring object (extract from "AJS Monitoring")

**Overview of the system-monitoring object**

Item	Description	
Monitoring node type	AJS Monitoring	
Purpose	Monitor errors in JP1/AJS and the jobnet execution status.	
Basic information	Object name	Full name of the jobnet ( <i>scheduler-service-name/jobnet-name</i> ). Example: AJSROOT1:/Job_A/Order-processing
	Host name	Host name of the manager on which JP1/AJS - Manager is installed. Example: host01

**Status change condition**

Status change condition		Common conditions# and individual conditions	
Condition name	Status	Condition	Comparison value
Jobnet warning event (AJS)	Warning	Jobnet warning event (AJS)#	Event ID (B.ID)
		Object ID (E.OBJECT_NAME)	Object name in the basic information
		Source event server name (B.SOURCESERVER)	Host name in the basic information

#: Common conditions (applied to all monitoring objects)

This figure is an extract from the description of the system-monitoring object called *AJS Monitoring* in 4. *Lists of System-Monitoring Objects (for Central Scope)* in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.

The example in the figure defines a status change condition with the title *Jobnet*

*warning event (AJS)*. As a common condition for all AJS Monitoring objects, the object status is set to `Warning` when event ID 4108 (indicating that the jobnet ended with a warning) is generated. As an individual condition set for each monitoring object, a condition related to the basic information held by the monitoring object (for identifying the object) identifies which of the objects in the monitoring tree changes its status.

In this way, a common condition related to the type of monitoring object (product name, for example) can be combined with an individual condition for identifying the specific monitoring object whose status will change.

Making status change conditions for monitoring objects resident in memory

When JP1/IM - Manager receives a JP1 event, it checks whether the status change condition of each monitoring object is satisfied. If a large number of JP1 events are received at once, the number of disk accesses increases accordingly and it could take longer to apply the new status to the monitoring objects. By making the status change conditions of the monitoring objects resident in memory, you can reduce the disk accesses during the Central Scope processing on receipt of an event.

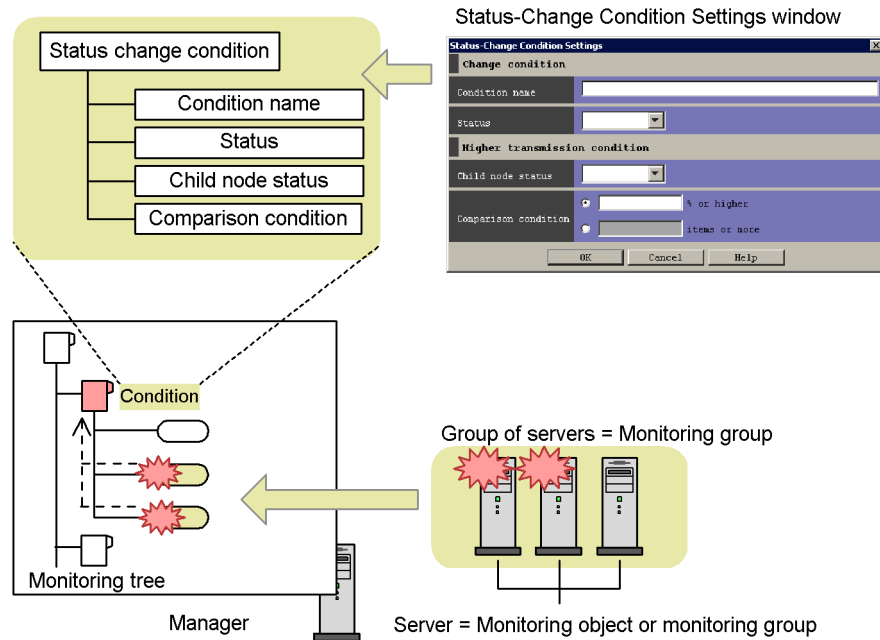
When you use this functionality, the status change conditions for all monitoring objects are kept in memory. Sufficient memory is needed for this purpose. We recommend that you estimate the memory requirements and set up this functionality if sufficient memory can be allocated.

For the equations used when estimating memory requirements, see the *Release Notes* for JP1/IM - Manager. For details about how to set up this functionality, see *5.7.5 Setting the memory-resident status change condition function* in the *Job Management Partner 1/Integrated Management - Manager Configuration Guide*.

## **(2) Status change conditions for monitoring groups**

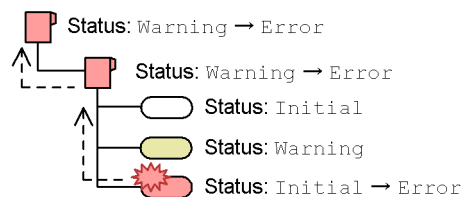
A *monitoring group* is a set of monitoring nodes. Therefore, the status of the monitoring group changes according to the status of its constituent nodes. The following figure shows status change conditions for monitoring groups.

Figure 4-4: Status change conditions for monitoring groups



When JP1/IM - Manager receives a specific JP1 event and changes the status of a monitoring object, the new status is passed to the higher-level monitoring groups. The default behavior is as follows.

Figure 4-5: Status change behavior of a monitoring group (default setting)



As shown in the figure, the monitoring group status changes to the status that has highest priority among the lower-level monitoring nodes. Thus, when the topmost monitoring node has **Error** status, it means that none of the nodes under it has a status of higher priority than **Error**.

While the default settings are appropriate in most cases, more detailed monitoring can be performed by defining a status change condition for the monitoring group in special circumstances (such as a load-balancing system).

A status change condition for a monitoring group consists of a condition name, status, child node status, and comparison condition, as described below.

- Condition name

The name of the status change condition.

- Status

The status of the monitoring group when the status change condition is satisfied.

In order of priority, the specifiable statuses are Emergency, Alert, Critical, Error, Warning, Normal, and Debug. Initial cannot be specified.

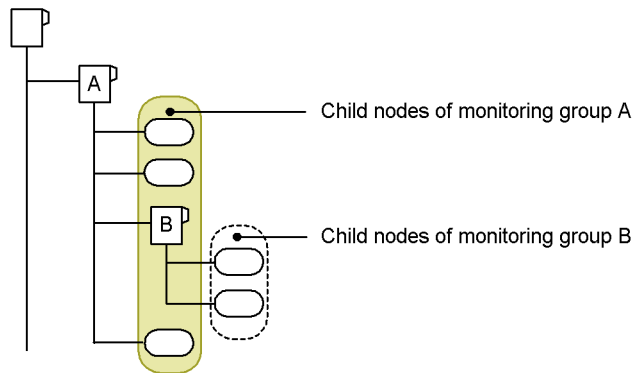
- Child node status

The status of a lower-level monitoring node. Specify the status that will cause a change in the status of the monitoring group to which the node belongs. In order of priority, the specifiable statuses are Emergency, Alert, Critical, Error, Warning, Normal, and Debug. Initial cannot be specified.

The status you specify here includes those of higher priority. For example, Error includes all statuses from Error upward.

The following figure shows the child node concept.

*Figure 4-6: Range of child nodes in a monitoring group*

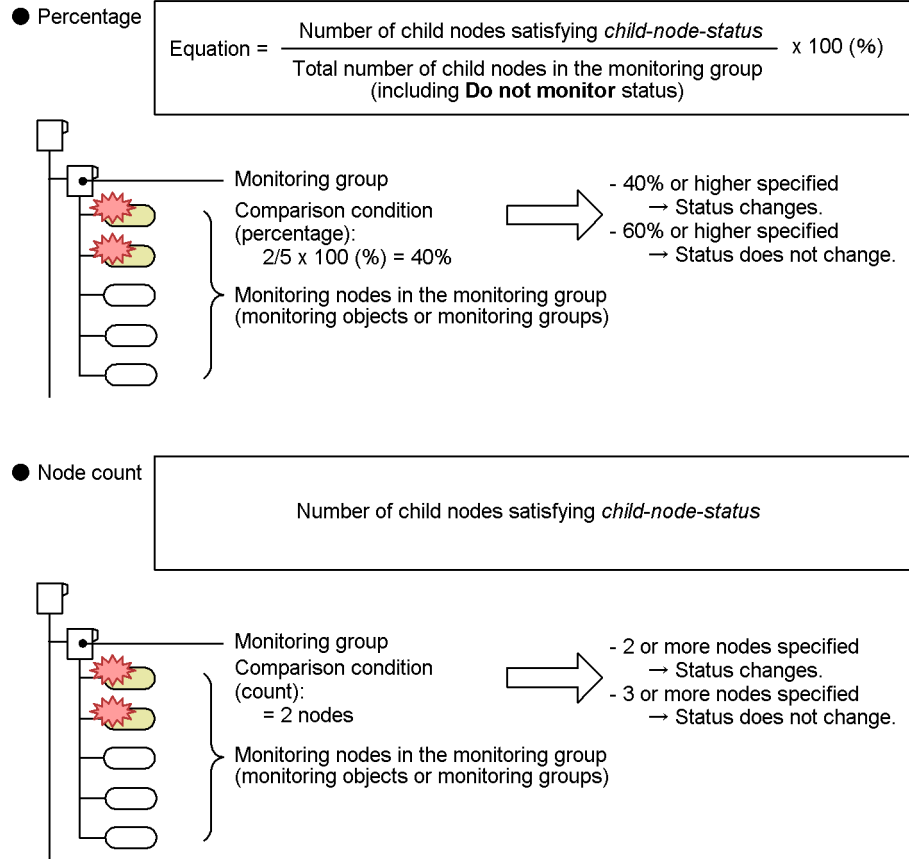


As shown above, monitoring group B is included among the child nodes of monitoring group A, but its own child nodes are not included.

- Comparison condition

A condition for comparing lower-level monitoring nodes within the group. You can specify a percentage ( $x\%$  or higher) or a count ( $x$  nodes or higher), as follows.

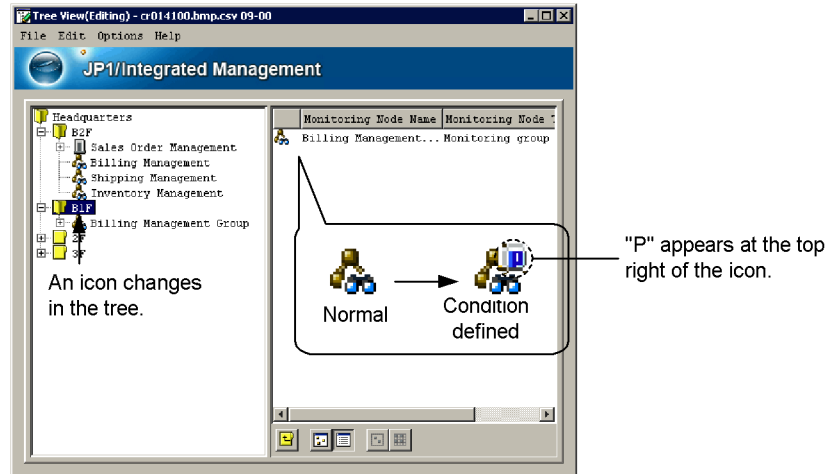
Figure 4-7: Comparison conditions (percentage-based and count-based)



By setting a condition name, status, child node status, and comparison condition in this way, you can customize the conditions that cause the status of a monitoring group to change.

When you define a status change condition, the icon of the monitoring group changes as shown below. From the icon display you can tell whether a status change condition has been set for a particular group.

Figure 4-8: Change in icon display (example)



"P" is not added to Visual Icon registered by the user. Identify whether a status change condition has been defined from the icons in the tree.

#### 4.2.4 Event generation condition

A monitoring node can issue a JP1 event when its status changes.

As an event generation condition, you can specify the type of status change that will cause the node to issue a JP1 event. This JP1 event cannot be issued when the node status changes to *Initial*.

The issued JP1 event has event ID 00003FB0.

Details about this JP1 event are as follows. This information is taken from 3. *JP1 Events* in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.

Table 4-3: Details about event ID 00003FB0 (from the above manual)

Attribute type		Item	Attribute name	Contents
Basic		Source event server name	SOURCESERVER	The name of the event server that issued the JP1 event
		Message	MESSAGE	KAVB7900-I Status of <i>monitoring-node-name</i> is changed <i>status</i> from <i>status</i> .
Extended	Common information	Event level	SEVERITY	Information
		Product name	PRODUCT_NAME	/HITACHI/JP1/IM/SCOPE

Attribute type		Item	Attribute name	Contents
		Object type	OBJECT_TYPE	SERVICE
		Object name	OBJECT_NAME	IM_CS
		Occurrence	OCCURRENCE	STATUS_CHANGE
	Program-specific information	Monitoring node ID	MON_NODE_ID	The ID of the monitoring node
		Monitoring node name	MON_NODE_NAME	The name of the monitoring node
		Monitoring node status <sup>#1</sup>	MON_NODE_STATUS	The StatusID of the monitoring node
		Information about the JP1 event that triggered the status change <sup>#2</sup>	<i>attribute-name</i>	The attribute value (basic attribute value prefixed with JCS_B_ or extended attribute value prefixed with JCS_E_)

#1: The monitoring node status (E.MON\_NODE\_STATUS) is stored as one of the following numeric values, which is called the node's *StatusID*.

- Value of StatusID (monitoring node status):

Emergency: 800, Alert: 700, Critical: 600, Error: 500,

Warning: 400, Normal: 300, Debug: 200, Initial: 100

For example, the JP1 event issued when the status of the monitoring node changes to Emergency has a monitoring node status (E.MON\_NODE\_STATUS) of 800.

#2: You cannot check this information from JP1/IM - View. Every item of information is stored as an attribute name combined with the attribute value. Therefore, when JP1 event 00003FB0 exceeds the maximum length of a JP1 event (10,000 bytes), only the portion within that limit is stored as information about the JP1 event that triggered the status change. Similarly, when the number of extended attributes exceeds 100, only the JP1 event information up to the 100th attribute is stored. Attributes are stored only if the attribute name is within 26 characters; if the attribute name exceeds 26 characters, the attribute is not saved.

#### *Setting an automated action for a monitoring node*

To execute an automated action when the status of a monitoring node changes:

- In the **Event-Issue Conditions** page of the Properties dialog box for the selected monitoring node, select the node status that triggers the JP1 event.
- Add an automated action condition for JP1 event 00003FB0 to the automated action definitions.



Information about the JP1 event resulting in a node status change is included in JP1 event 00003FB0, as shown in *Information about the JP1 event that triggered the status change* in the above table. For example, the original event message (B.MESSAGE) can be used as the attribute name E.JCS\_B\_MESSAGE with the automated action.

---

## 4.3 Automatically generating a monitoring tree

---

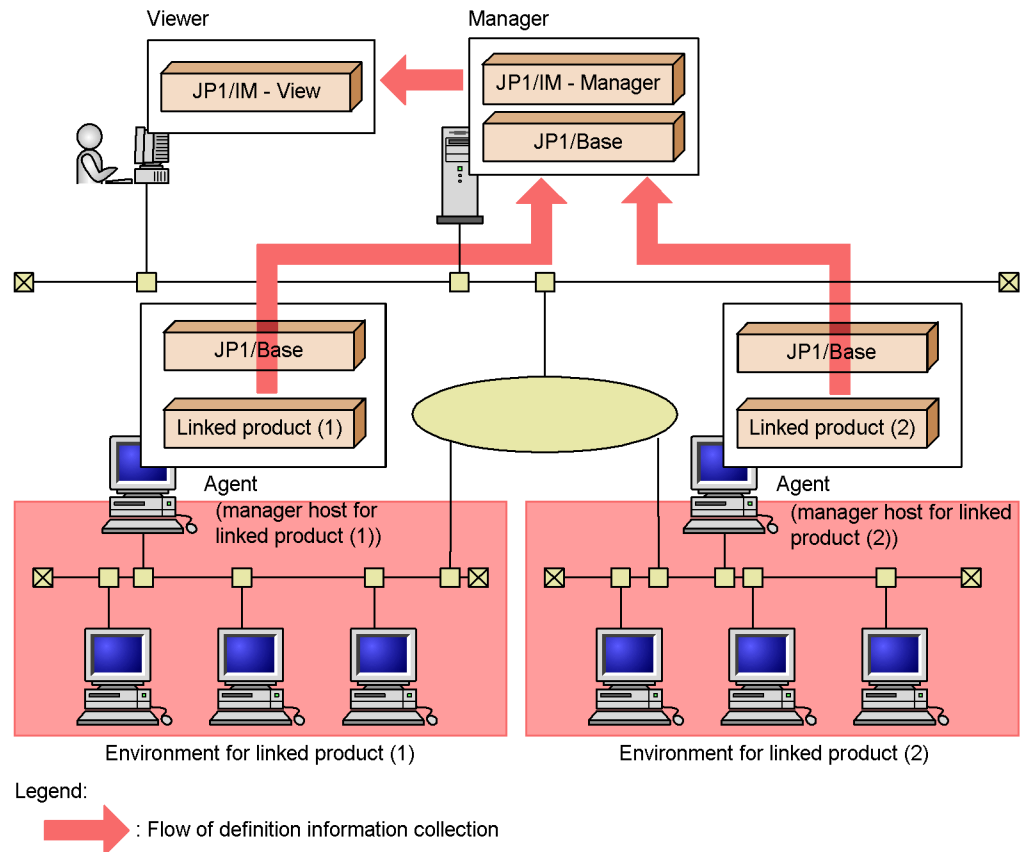
Using the auto-generation function, you can automatically collect definition information from the active hosts in the system and create a monitoring tree. If the system is reconfigured, you can collect difference information and update the monitoring tree.

The auto-generation function substantially simplifies the work involved in configuring a monitoring system. A monitoring tree can help you monitor even a large-scale system efficiently, but it still requires a vast amount of definition information. The tasks at the system configuration stage, and the updates required when the system is modified, mean a huge commitment of time and effort. The function for automatically generating a monitoring tree offers support for this undertaking.

### 4.3.1 Automatically generating a monitoring tree

When you use the auto-generation function, JP1/IM - Manager collects definition information from the agents and automatically generates a monitoring tree as shown below.

Figure 4-9: Overview of auto-generation of a monitoring tree



*Note:*

To generate a monitoring tree automatically, the products to be monitored must support the auto-generation function.

### 4.3.2 Conditions for automatically generating a monitoring tree

The auto-generation function is supported by the JP1 products (JP1/AJS, JP1/PPM, and JP1/IM) and by Cosminexus. If you wish to monitor any other products in your system, you must set the definition information manually.

The following conditions apply when automatically generating a monitoring tree:

- JP1/Base (version 7 or later) is required on each agent.

Definition information is collected using JP1/Base functionality.

- The products to be monitored must support the JP1/Base functionality for collecting definitions.

You must execute the setup command for enabling this functionality in the relevant products on each agent.

- The service for each linked product must be active during auto-generation.

Definition information cannot be collected from products whose service is inactive.

For the procedures to link these products with JP1/IM, see *5.8 Setting up for linked products* in the *Job Management Partner 1/Integrated Management - Manager Configuration Guide* and the documentation for the relevant linked product.

The following table describes the monitoring objects created by the auto-generation function.

*Table 4-4: List of monitoring objects created at auto-generation*

Product	Monitoring node type	Description
JP1/IM - Manager	IM Monitoring	Monitors the status of JP1/IM - Manager. Defined so that its status changes conditional on a JP1 event indicating an error in JP1/IM - Manager.
JP1/AJS - Manager	AJS Monitoring	Monitors the status of JP1/AJS - Manager and the jobnets executed under its control. Defined so that its status changes conditional on a JP1 event indicating an error in JP1/AJS - Manager or a change in the status of a jobnet.
	Jobnet Monitoring (AJS)	Monitors job execution status. Defined so that its status changes conditional on a JP1 event indicating a change in the status of the job.
JP1/PFM - Manager	Agent Monitoring (PFM)	Monitors the status of performance data monitored by an agent that is managed by JP1/PFM - Manager. The auto-generation function creates the same number of Agent Monitoring (PFM) objects as the JP1/PFM - Agents managed by JP1/PFM - Manager. Defined so that its status changes conditional on a JP1 event indicating a change in the status of the performance data.
Cosminexus	Logical Server Monitoring (Cosminexus)	Monitors the status of a Cosminexus logical server (J2EE server, Web server, naming service, CTM, and so on). Defined so that its status changes conditional on a JP1 event indicating that the Cosminexus logical server has started or stopped, or a JP1 event indicating an execution error.

Product	Monitoring node type	Description
	J2EE Application Monitoring (Cosminexus)	Monitors the status of a Cosminexus J2EE application. Defined so that its status changes conditional on a JP1 event indicating that the J2EE application has started or stopped, or a JP1 event indicating an execution error.

*Note:*

Before you begin operation, you should customize the automatically generated monitoring tree to suit the methods you will be using to monitor your system.

A monitoring tree created by the auto-generation function incorporates the collected information in its entirety. It represents the system configuration information as completely as possible, so that the system administrator can delete whatever is unnecessary for monitoring purposes.

For further details about the contents of the automatically generated nodes in a monitoring tree, see 4. *Lists of System-Monitoring Objects (for Central Scope)* in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.

### 4.3.3 Monitoring tree structures

The monitoring trees produced by the auto-generation function are based on a template which you select in the Auto-generation - Select Configuration window. A template is a set of model definitions for managing a system using the Central Scope.

JP1/IM provides the following two templates.

*Table 4-5: Monitoring tree templates*

Generation tree	Description
Work-oriented tree	Use this template to monitor the system from a work-oriented perspective. The generated monitoring tree is based on the jobnet organization in JP1/AJS or logical server configuration in Cosminexus. Typically, jobs are grouped together as jobnets to systematize job execution, and logical servers are defined to systematize the applications used in a Web system. Hence, the generated tree reflects how work tasks are performed. If the linked JP1/AJS is version 8 or later, the function collects from JP1/AJS not only information about the jobnet organization, but also information about the JP1 resource groups set in each JP1/AJS unit. <sup>#</sup>
Server-oriented tree	Use this template to monitor the system from a server-oriented perspective. The generated monitoring tree is based on the system hierarchy in JP1/IM. In JP1/IM, the servers are typically arranged in a hierarchical structure. Hence, the generated tree reflects the manner in which servers are managed.

#: For details about using the acquired JP1 resource groups, see *4.4.3 Setting the monitoring range of a monitoring tree*.

The structure and monitoring objects of an automatically generated monitoring tree differ for each of the two templates. The following table describes the relationships between the type of template and the generated monitoring objects.

*Table 4-6: Template type and generated monitoring objects*

Monitoring object	Template		
	Work-oriented tree		Server-oriented tree
	JP1/AJS management group	Cosminexus management group	
AJS Monitoring	Y	--	Y
Jobnet Monitoring (AJS)	Y	--	Y
Agent Monitoring (PFM)	Y	Y	Y
Metric Monitoring (PAM)	--	--	--
Object Monitoring (PAM)	--	--	--
SD Monitoring	--	--	--
Distribution Job Monitoring (SD)	--	--	--
NNM Monitoring <sup>#</sup>	--	--	--
Node Monitoring (NNM) <sup>#</sup>	--	--	--
IM Monitoring	--	--	Y
Logical Server Monitoring (Cosminexus)	--	Y	Y
J2EE Application Monitoring (Cosminexus)	--	Y	Y
HiRDB Monitoring	--	--	--

Monitoring object	Template		
	Work-oriented tree		Server-oriented tree
	JP1/AJS management group	Cosminexus management group	
Physical Host Monitoring (System Manager)	--	--	--

Legend:

Y: Generated

--: Not generated

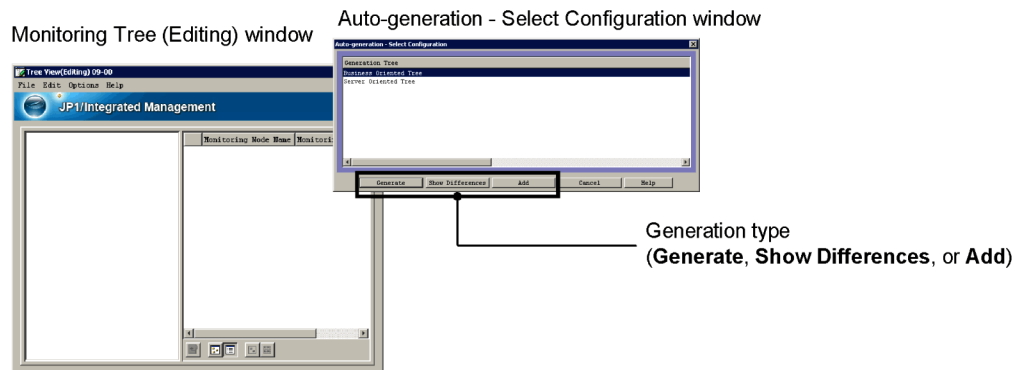
#: HP NNM must be version 7.5 or earlier.

For details about the structure of automatically generated monitoring trees, see 5. *Monitoring Tree Models (for Central Scope)* in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.

#### 4.3.4 Generation types

When generating a monitoring tree automatically, you can select one of three generation types: **Generate**, **Show Differences**, or **Add**.

Figure 4-10: Generation types



##### (1) Processing when you select "Generate" as the generation type

When you select **Generate** to create a monitoring tree, the information displayed in the Monitoring Tree (Editing) window is erased, and then the monitoring tree is redrawn according to the tree structure of the template you selected under **Generation Tree** in the Auto-generation - Select Configuration window.

**(2) Processing when you select "Show Differences" as the generation type**

When you select **Show Differences** to create a monitoring tree, the monitoring conditions set for the monitoring objects stored in the JP1/IM - Manager monitoring objects database are compared with the monitoring conditions in the definition information (monitoring objects) that was collected and collated during the generation processing. Monitoring objects found to have different monitoring conditions than recorded in the database, and all monitoring groups containing those objects up to the topmost level, are created as difference information under a monitoring group called `NEW_OBJECT`.

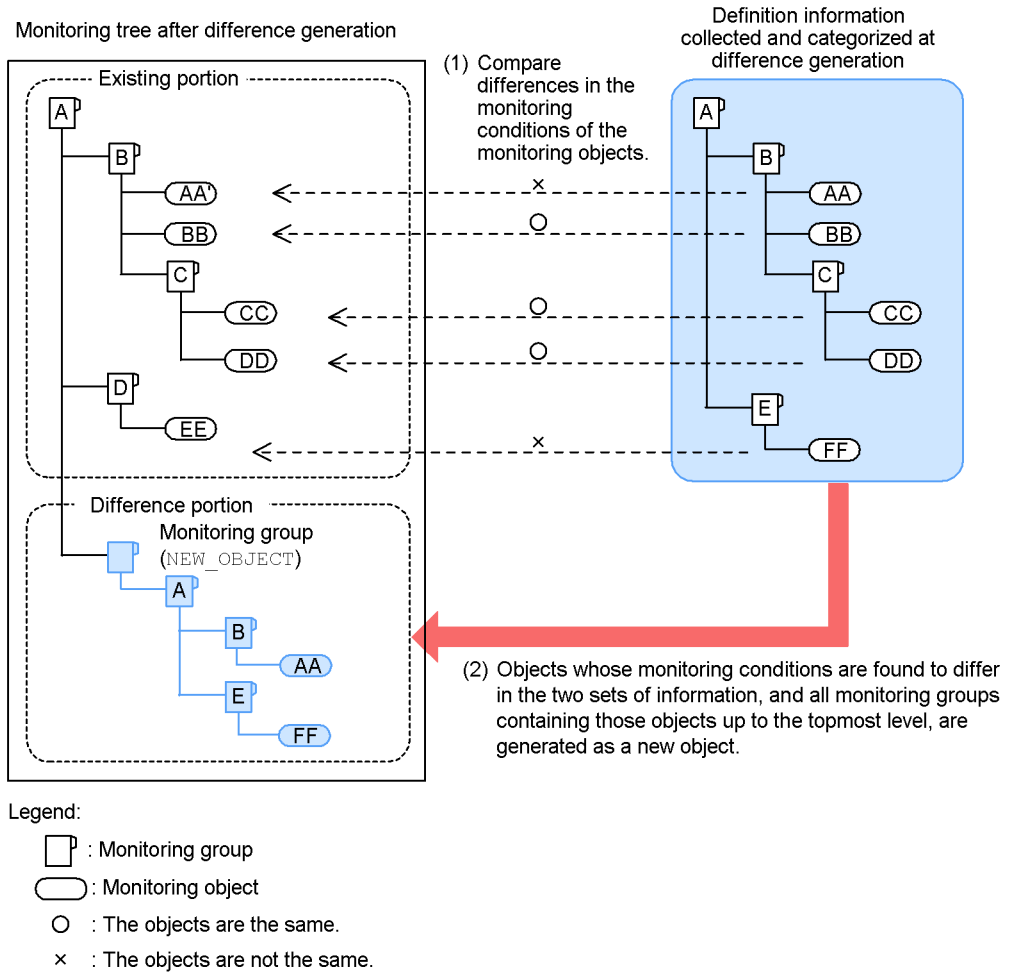
This processing allows you to update a monitoring tree when a system is reconfigured, by collecting only the changed parts of the definition information.

This new monitoring node generated as difference information can be placed in an existing monitoring tree as required.

The following figure shows the generation of a monitoring tree that shows differences.



Figure 4-11: Generation of a 'differences' monitoring tree



Monitoring objects in the *existing portion* of the figure:

AA' is created from the original monitoring object AA. BB, CC, and DD incorporate the auto-generated objects without change. EE is an object added by the user for monitoring purposes.

Definition information collected and collated at difference generation:

This area of the figure shows the definition information collected at difference generation from the products running in the current system, organized into tree form. This information is held internally by JP1/IM - Manager. The generated tree structure depends on the selected template.

*Difference portion of the figure:*

This node contains the monitoring objects AA and FF, which JP1/IM - Manager determined to be absent from the existing portion as a result of comparing the monitoring conditions of the objects in that portion with the monitoring conditions of the objects in the definition information collected and collated at difference generation. A, B, and E are also generated in this node because they are the higher-level monitoring groups containing AA or FF.

**(3) Processing when you select "Add" as the generation type**

When you select **Add** to create a monitoring tree, an additional monitoring tree is added to those in JP1/IM - Manager's monitoring objects database. The structure of the tree follows the template you selected under **Generation Tree** in the Auto-generation - Select Configuration window.

## 4.4 Editing a monitoring tree

You can freely customize a monitoring tree to suit your purpose. Before you start monitoring operations, edit the monitoring tree that you easily created using the auto-generation function, according to the type of monitoring you want to perform.

For details about the actual editing procedure, see 5. *Setting up Central Scope* in the *Job Management Partner 1/Integrated Management - Manager Configuration Guide*.

### 4.4.1 Editing a monitoring tree

Use the Monitoring Tree (Editing) window to edit a monitoring tree. You can add, delete, and move nodes in this window, according to how the tree is to be used.

To create or edit a monitoring node, you must set the following attributes in the node. All these attributes have been discussed earlier in this chapter.

*Table 4-7: Monitoring node attributes defined in the Monitoring Tree (Editing) window*

Attribute	Description
Monitoring node name	The name of the monitoring node.
Monitoring node type	The monitoring group or monitoring object. There are several types of monitoring objects, including system-monitoring objects such as the AJS Monitoring and SSO Monitoring, and general monitoring objects such as a user monitoring object.
Icon	An icon that represents a monitoring node.
Visual Icon	An icon that represents a monitoring node. Visual Icon are displayed only in map views and in the Visual Monitoring window.
Monitoring status	The monitoring status set for a node. The two statuses are <b>Monitor</b> and <b>Do not monitor</b> .
JP1 resource group	Information set for controlling the monitoring range permitted to individual JP1 users, and for exercising precise control over access to the nodes in a monitoring tree. For details about using resource groups, see 4.4.3 <i>Setting the monitoring range of a monitoring tree</i> .

Attribute	Description
Basic information	<p>Basic information for identifying a monitoring node.</p> <p>In the case of a monitoring group, this attribute is a name identifying the group. For example, you can assign a group name to a group of tasks or servers, such as <i>Daily accounting routines</i> or <i>Database server group</i>, according to the monitoring objectives.</p> <p>In the case of a monitoring object, this attribute is information for identifying the object. For example, you can define a combination of information for identifying the object within the system, such as the jobnet name and a host name.</p> <p>For a system-monitoring object, the same attribute as the basic information of the object to be monitored is defined as an individual condition in the status change conditions.</p>
Status change condition	<ul style="list-style-type: none"> <li>• Status change condition for a monitoring object A condition that determines which received JP1 events will change the status of the monitoring object. This attribute defines a JP1 event that triggers a status change, and the resulting status.</li> <li>• Status change condition for a monitoring group A condition that determines what lower-level node statuses will change the status of the monitoring group. The attribute defines the statuses of the lower-level nodes triggering a status change, the resulting status of the monitoring group, and a comparison condition.</li> </ul>
Event generation condition	A condition that specifies the status of a monitoring node that will cause a JP1 event to be issued. The issued JP1 event has event ID 00003FB0.

You can create a monitoring group simply by specifying its name (unless you also need to define a status change condition for the group). However, when you create a monitoring object, you must also carefully consider and define what exactly you need to monitor and how this is to be done.

JP1/IM provides a number of *system-monitoring objects* to facilitate object definition.

The following types of monitoring objects are provided:

■ System-monitoring object

A monitoring object provided by the JP1/IM system. Each product in the JP1 series has its own monitoring object. The basic settings needed for monitoring are pre-defined, so that you can easily set up the monitoring environment.

System-monitoring objects include a variety of types, such as an *AJS Monitoring*, *SSO Monitoring*, and so on. For details about the program products that are monitored by these objects, and how to set them up, see 4. *Lists of System-Monitoring Objects (for Central Scope)* in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.

A system-monitoring object becomes a general monitoring object when edited as follows:

- By changing the basic information on the **Basic Information** page of the Properties window
- By adding, changing, or deleting a status change condition on the **Status-Change Condition** page of the Properties window
- By changing a common condition in the Status-Change Condition Settings window
- By adding, changing, or deleting an individual condition in the Status-Change Condition Settings window

When you alter a system- monitoring object in any of these ways, a confirmation dialog box appears with the following message: *If this operation is continued, the monitoring node type will become User Monitoring Object. Do you want to continue?*

#### ■ General monitoring object

An object for general monitoring purposes, created and customized by the user. This type of object is called a *User Monitoring Object*.

A general monitoring object can be customized very flexibly, allowing precise settings to match the type of monitoring required. On the other hand, the system administrator needs to be well versed in the settings that can be performed. This type of object also takes time to create.

For most purposes, we recommend that you use system-monitoring objects to create your monitoring nodes, and customize the parts that need to be changed.

### 4.4.2 Map display settings

In the detailed view area of the Monitoring Tree window, you can view information in map format just as in the Visual Monitoring window. This allows the system administrator a more intuitive means of monitoring the system.

To display map views in the detailed view area, you must set the background image, arrange the monitoring nodes, and complete other settings. Otherwise, you will see icons without any background when you switch to the map view. Use the Monitoring Tree (Editing) window to enter the required settings.

Differences from the Visual Monitoring window

Unlike the Visual Monitoring window, you cannot use the map view in the detailed view area for the purpose of localized monitoring of a specific node only, such as monitoring a particular regional office or an important job.

For example, if there are three nodes displayed in the detailed view area of the

Monitoring Tree window, all three will be displayed when you switch to a detailed view or map view. (You cannot hide one of them, for example.)

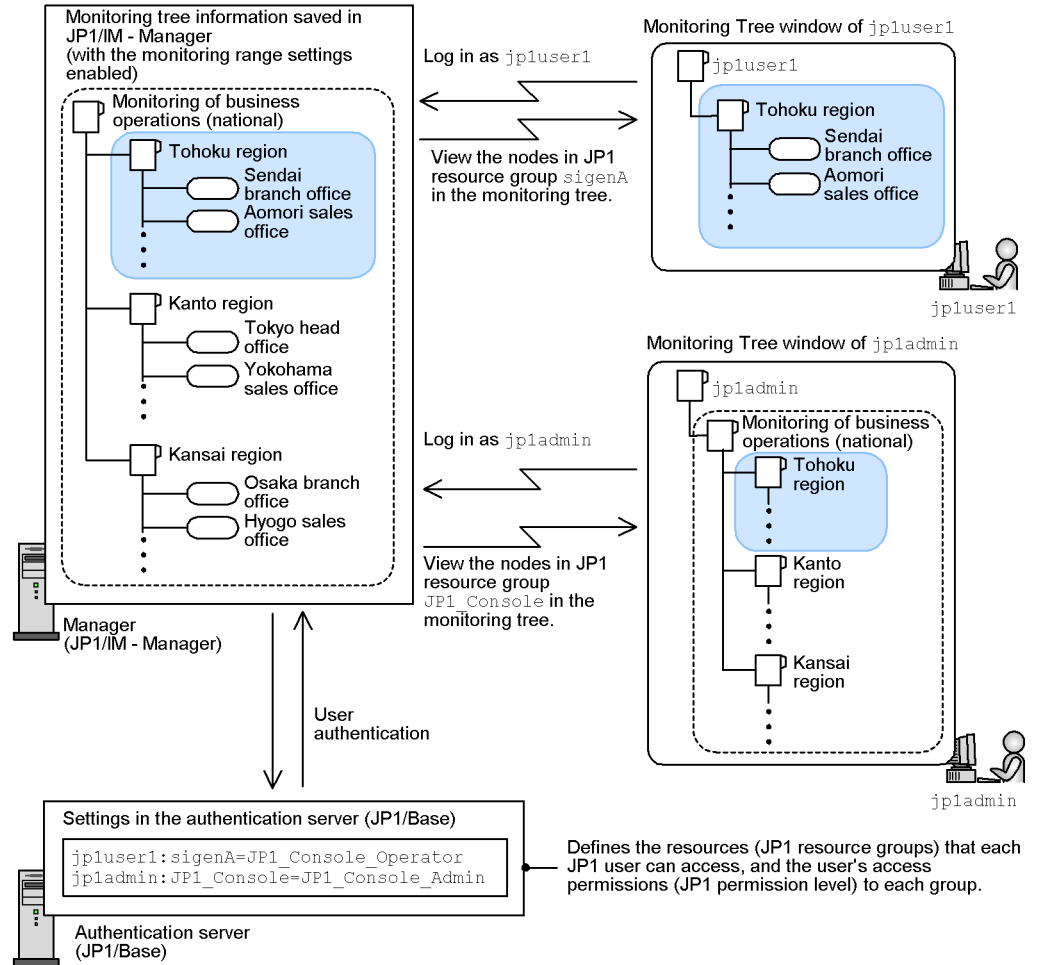
#### **4.4.3 Setting the monitoring range of a monitoring tree**

You can change the monitoring range of a monitoring tree for each JP1 user, by performing the following two settings:

- Enable the monitoring range settings, and then set JP1 resource groups for specific nodes (set in JP1/IM - View and save to JP1/IM - Manager).
- Allocate one or more JP1 resource groups to each JP1 user (set on the JP1/Base authentication server).

For example, by completing the above settings, you can permit a particular user (`jp1user1`) to monitor part of the tree, and another user (`jp1admin`) to monitor the entire tree, as shown in the figure below.

Figure 4-12: Changing the monitoring range using JP1 resource groups (access control to a monitoring tree)



Legend:

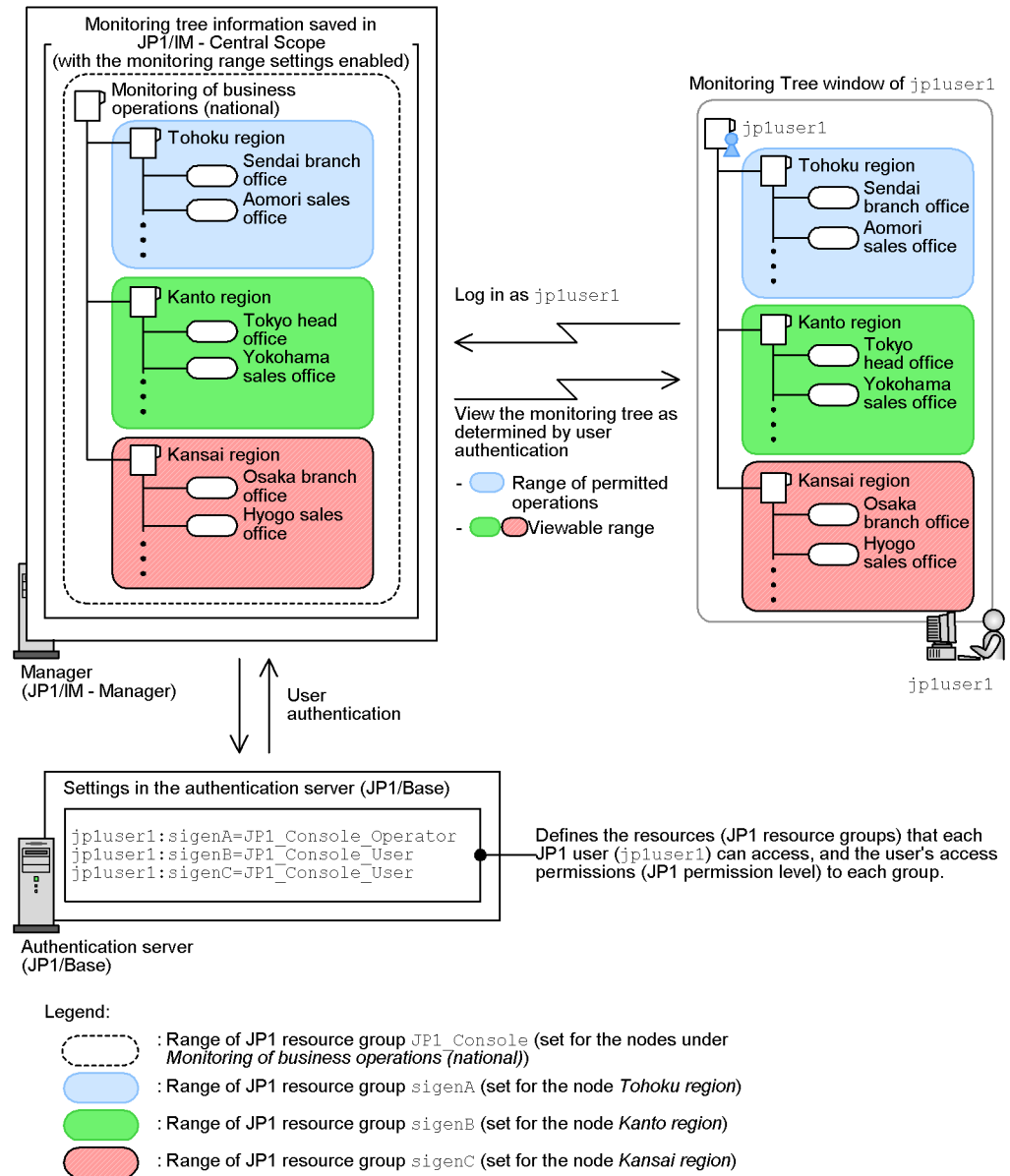
- : Range of resource group *JP1\_Console* (set for the nodes under *Monitoring of business operations (national)*)
- : Range of JP1 resource group *sigenA* (set for the node *Tohoku region*)

When the monitoring range settings are enabled, the topmost node of the tree in the Monitoring Tree window is always the virtual root node. When the monitoring range settings are disabled, all tree information is displayed, regardless of the JP1 resource group settings (the virtual root node is not shown).

By allocating multiple JP1 resource groups to a particular JP1 user, and assigning a

different JP1 permission level for each group, you can allow that JP1 user to operate on one part of a monitoring tree, but only view another part, as shown in the figure below.

Figure 4-13: Example of controlling monitoring tree operation using a combination of JP1 resource groups and JP1 permission levels





### (1) Enabling or disabling monitoring range settings, and setting a JP1 resource group for a monitoring node

To enable or disable the monitoring range settings, in the Monitoring Tree (Editing) window, choose **Options** and then **Monitoring Range Settings**. When **Monitoring Range Settings** is checked, the settings are enabled; when there is no check mark, the settings are disabled.

The monitoring range settings in JP1/IM - View might be automatically enabled or disabled when a monitoring tree is auto-generated, depending on the generation type and the server (JP1/IM - Manager) settings. This occurs in the following two cases:

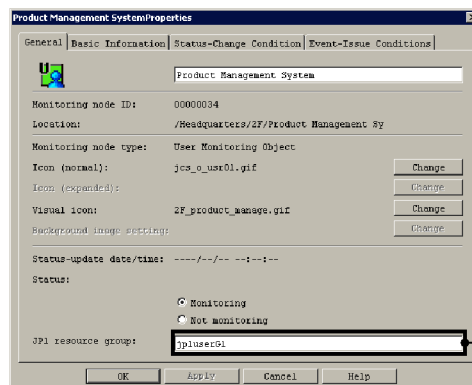
1. The monitoring range settings are disabled in JP1/IM - View but enabled in JP1/IM - Manager, and **Show Differences** or **Add** is set as the generation type.
2. The monitoring range settings are enabled in JP1/IM - View but disabled in JP1/IM - Manager, and **Show Differences** or **Add** is set as the generation type.

In the first case, the JP1/IM - View monitoring range settings are automatically enabled after auto-generation.

In the second case, the JP1/IM - View monitoring range settings are automatically disabled after auto-generation.

When the monitoring range settings are enabled, you can set a JP1 resource group for any monitoring node from the **General** page of the Properties window for that node. The **JP1 resource group** box appears only when the monitoring range settings are enabled.

Figure 4-14: Properties window when the monitoring range settings are enabled



Displayed when the **Monitoring Range Settings** command is checked in the **Options** menu of the Monitoring Tree (Editing) window.

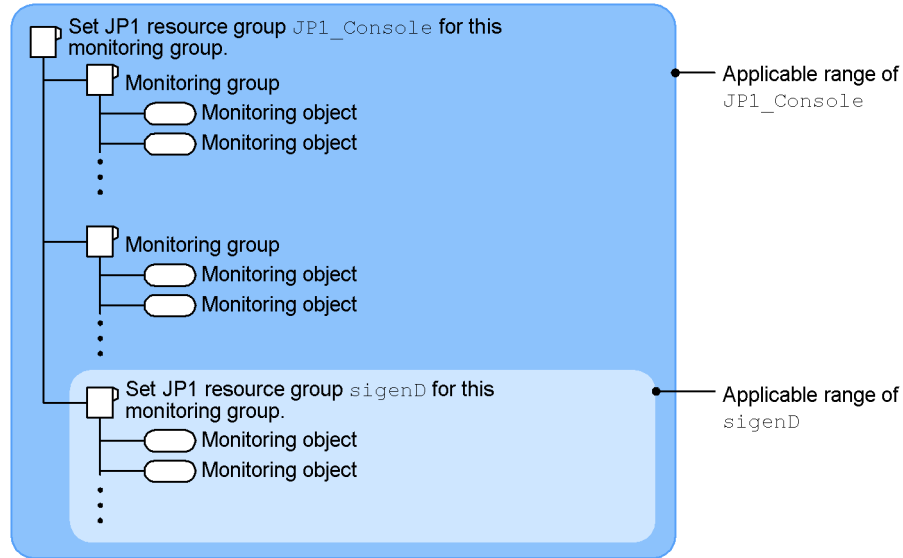
Once set, the JP1 resource group setting is saved as internal information even if you subsequently disable the monitoring range settings. (When you re-enable them, the resource group you set previously is again displayed.)

You can set a JP1 resource group only for the highest node within the range of control

(that is, you do not need to repeat the setting for each child node). The JP1 resource group set for a node applies to all its child nodes.

For example, if you set JP1\_Console as the JP1 resource group for the topmost monitoring group in the tree, all nodes under that group will belong to JP1 resource group JP1\_Console. If you then set JP1 resource group `sigenD` for a monitoring group under the topmost monitoring group, the group itself and all its lower-level nodes will belong to both JP1\_Console and `sigenD`.

Figure 4-15: Applicable range of JP1 resource groups



The JP1 users granted access to JP1\_Console can view the range JP1\_Console (all nodes in the monitoring tree); the JP1 users granted access to `sigenD` can view the range `sigenD`.

#### Initial JP1 resource group setting for a monitoring node

Regardless of whether the monitoring range settings are enabled, the JP1 resource group JP1\_Console is automatically set for the topmost node. You can change this setting, but you cannot make it blank (a value must be entered).

When you auto-generate a monitoring tree under the following conditions, the JP1 resource group already set in the linked product is imported as the initial value for that monitoring node. This applies when:

- You generate a monitoring tree automatically by selecting the work-oriented tree template for JP1/AJS version 8.

The monitoring range settings in JP1/IM - View and JP1/IM - Manager are completed when you finish setting JP1 resource groups for the nodes and save the changes to JP1/

IM - Manager.

## (2) Allocating JP1 resource groups to JP1 users

When you set the monitoring range of a monitoring tree, you must also review the JP1/Base (authentication server) settings and add or edit the JP1 user settings as required.

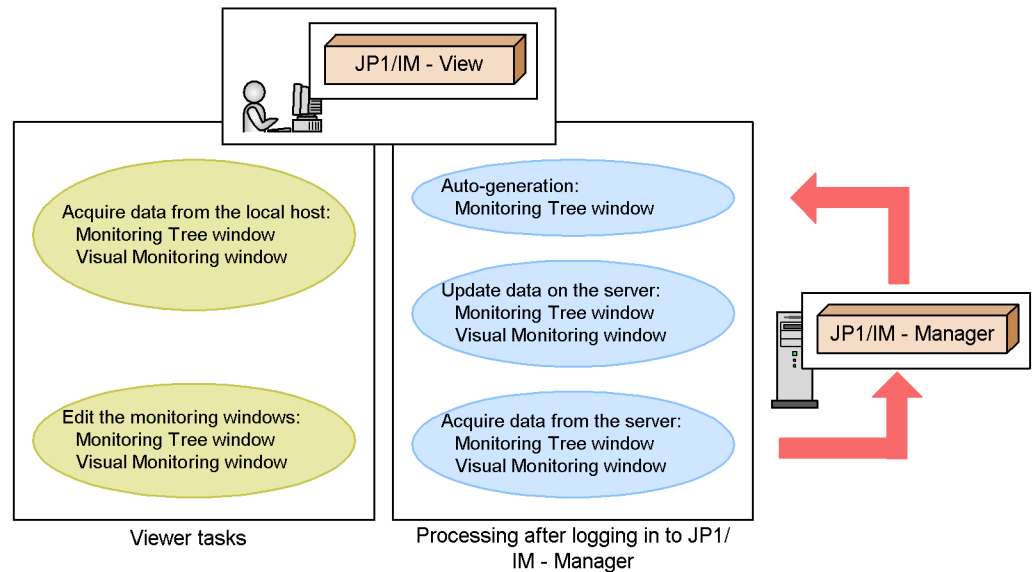
For information about how to manage JP1 users in JP1/Base, see *7.4.1 Managing JP1 users*.

For setting particulars, see the chapter about user management setup in the *Job Management Partner 1/Base User's Guide*.

### 4.4.4 Setting the Central Scope monitoring windows

Two main tasks are involved in setting the monitoring windows of the Central Scope (Monitoring Tree window and Visual Monitoring window): editing the windows on the viewer, and connecting to the manager to update or acquire the existing settings.

Figure 4-16: Setting the Central Scope monitoring windows



#### ■ Editing the monitoring windows (tasks on the viewer host)

Edit information in the Monitoring Tree (Editing) window and Visual Monitoring (Editing) window on a viewer. You do not need to connect to the manager (JP1/IM - Manager (JP1/IM - Central Scope)) to perform these tasks.

Required permissions:

Any user who can log in to the operating system is able to perform editing. No

particular JP1 user permissions are required.

- Acquiring and updating monitoring window settings (processing after connecting to the manager host)

Processing of the following operations is performed after you log in to the server (manager):

- Auto-generate a monitoring tree
- Acquire the existing settings of a monitoring tree
- Save edited monitoring tree settings
- Acquire the existing settings of the Visual Monitoring window
- Save the settings edited in the Visual Monitoring window
- Acquire update data for the common condition of a status change condition

To perform the above operations, you must log in to JP1/IM - Manager (JP1/IM - Central Scope). When the Login window appears, log in as a JP1 user.<sup>#</sup>

Required permissions:

The JP1 user who logs in to JP1/IM - Manager (JP1/IM - Central Scope) requires the following permissions:

- JP1 resource group: JP1\_Console
- JP1 permission level: JP1\_Console\_Admin

A JP1 user who wants to auto-generate a monitoring tree must log in as the `jpladmin` user.

This is because a permission other than `JP1_Console_Admin` might be required to access definition information for a linked product during auto-generation. (If the `jpladmin` user has been deleted for operational reasons, the JP1 user will require a permission level that allows access to the definition information of the linked product. For example, to acquire JP1/AJS jobnet information, the JP1 user will require a permission level that grants jobnet access.)

<sup>#</sup>: If you have checked the **Save Login Information** command in the **File** menu of the Monitoring Tree (Editing) window, your login user name, password, and host name are preserved until you log out, and the Login window does not appear during subsequent operations to connect to the server.

Before you perform settings in a monitoring window of the Central Scope, make sure that you know the `jpladmin` user password, or the password and user name of the JP1 user who has `JP1_Console_Admin` permission.

*Note:*

When you update the server to apply the changed settings in the Monitoring Tree (Editing) window, the status of all monitoring nodes and status change events is initialized.

---

## 4.5 Visual monitoring

---

### Creating and editing Visual Monitoring windows

You can create and edit a Visual Monitoring window to suit your purpose. This is useful for localized monitoring of specific nodes only (such as a node related to operations at the Kyushu branch office, for example).

The Visual Monitoring window supports the display of background images and Visual Icon. We recommend that you use these tools to create highly flexible Visual Monitoring windows.

You can perform the following operations:

- Set or edit a Visual Monitoring window name.
- Set or edit comments about a Visual Monitoring window.
- Arrange nodes, set attributes, change the monitoring status, or perform a search in a Visual Monitoring window.
- Change the background image.

Use the Visual Monitoring (Editing) window for creating or editing a Visual Monitoring window.

### Monitoring operations in the Visual Monitoring window

You can perform the following operations in the Visual Monitoring window:

- Launch a Monitoring Tree window.
- Perform operations from a pop-up menu.

You can also perform the following operations in the same way as in the Monitoring Tree window:

- Change the node status
- Change the monitoring status
- Conduct a search
- Display guidance
- Search for status change events
- Display properties

When the monitoring range settings are enabled for a monitoring tree, they also affect the Visual Monitoring window display. For example, if a Visual Monitoring window contains a node that the user is not permitted to access, it will not appear when the window is displayed.

---

## 4.6 Searching for monitoring nodes or status change events

---

### 4.6.1 Searching for monitoring nodes

You can search for monitoring nodes in the Monitoring Tree window and Visual Monitoring window.

For example, you can execute a search to see whether any monitoring objects have changed their status (indicating that an event has occurred) or to find a specific monitoring object.

When performing a monitoring node search, you can specify various conditions in the displayed Search window. The following items can be specified as search conditions:

- Monitoring node name
- Monitoring node ID
- Monitoring node type
- Status
- Monitoring status
- JP1 resource group<sup>#</sup>
- Basic information
- Status change condition
- Event generation condition

<sup>#</sup>: Appears only when the monitoring range settings are enabled for the monitoring tree. For details, see *4.4.3 Setting the monitoring range of a monitoring tree*.

These conditions are related by an AND condition. Use regular expressions when entering a monitoring node name, basic information, or status change condition.

The search results are displayed in the Search window. You can change the status and monitoring status of a selected node in this window. By double-clicking a displayed node, you can display the node in its selected status in the Monitoring Tree window.

### 4.6.2 Searching for status change events

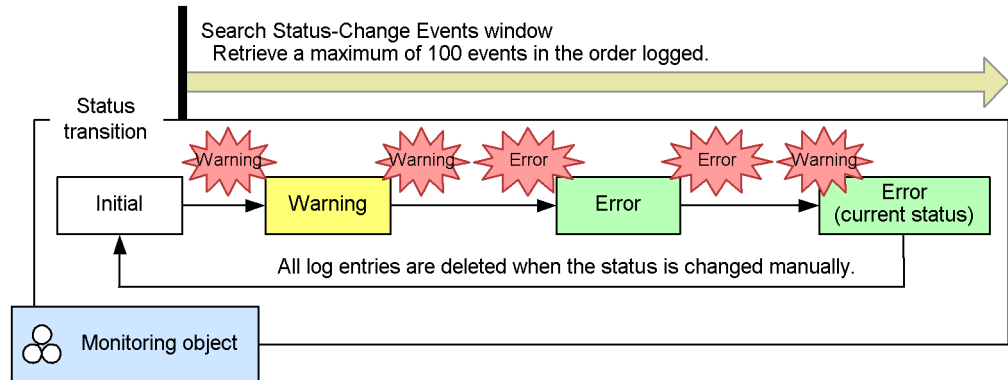
In the Monitoring Tree window and Visual Monitoring window, you can search for status change events in a particular monitoring object. A maximum of 100 events can be retrieved in the order they were logged, starting from the oldest (you cannot search for events exceeding this maximum number). A *status change event* is a JP1 event that acts as a monitoring target (status change condition) in the Central Scope.

**(1) Searching for logged status change events**

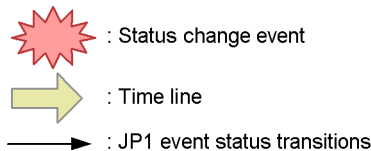
Perform a search when you need to check the logged status change events that have resulted in the present status of a monitoring object or group, or to view detailed information about any of the logged status change events. The JP1 event details appear on the **Search Events** page of the Event Console window.

If you manually change the status of a monitoring node, all status change events are deleted from the log.

*Figure 4-17: Status transition of a monitoring object and searching for status change events*



Legend:

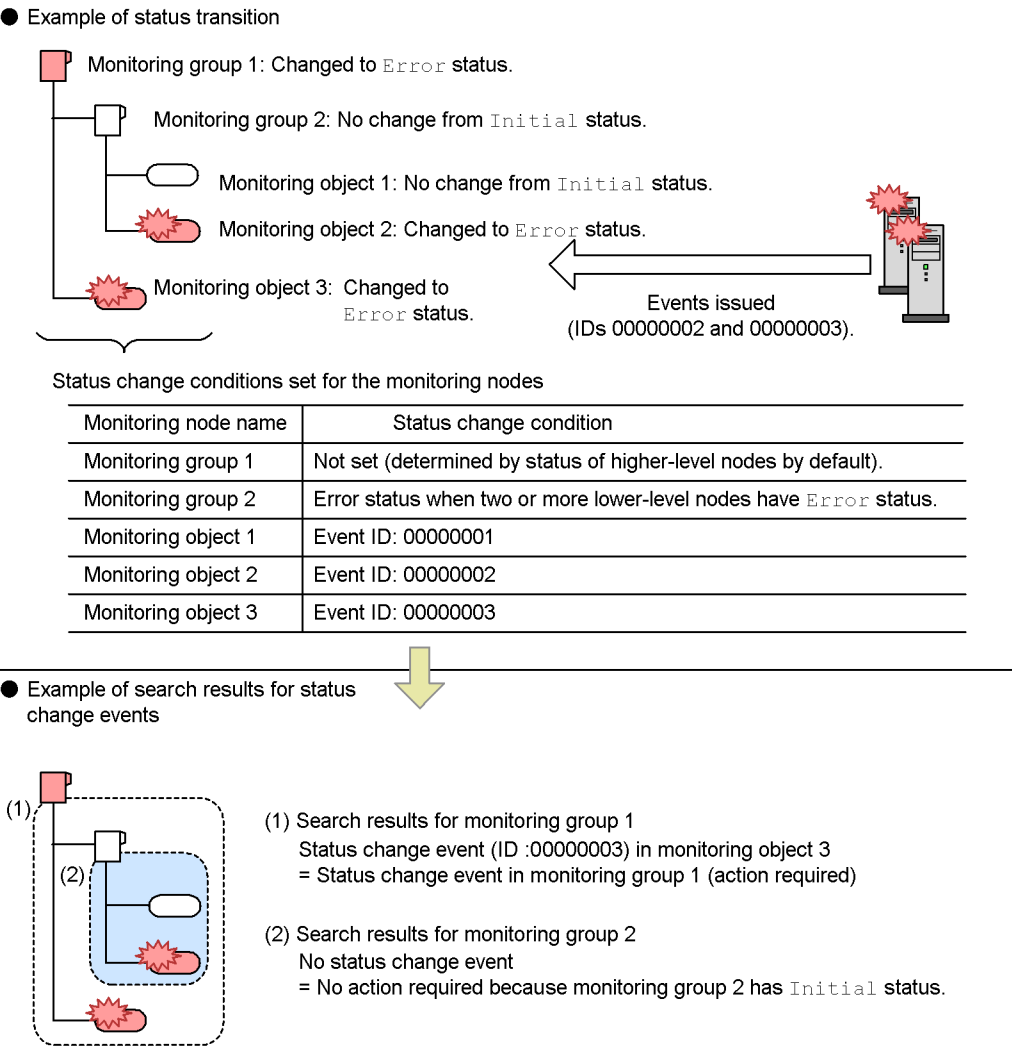


When you search for status change events affecting a monitoring group, the results show the status change events that occurred in the lower-level monitoring nodes, to a maximum of 100 starting from the oldest.

However, if a status change condition is defined for the monitoring group, the status change events that occurred in lower-level nodes are shown in the results only if they require a response, to a maximum of 100 starting from the oldest. The following figure shows an example.



Figure 4-18: Example of searching for status change events in a monitoring group



As shown in the figure, only the status change events that require a response are shown in the search results.

To view the search results for status change events in monitoring object 2, you can drill down the monitoring tree to that object, or you can search for status change events in monitoring object 2 itself. To search for status change events in all nodes from the higher-level monitoring group 2 down to monitoring object 2, you can define one or more child nodes in `Error` status as the condition for changing monitoring object 2 to

Warning status.

Event issued when the number of status change events exceeds 100

When the number of status change events in a monitoring object exceeds 100, a warning JP1 event is issued.

Issued JP1 event

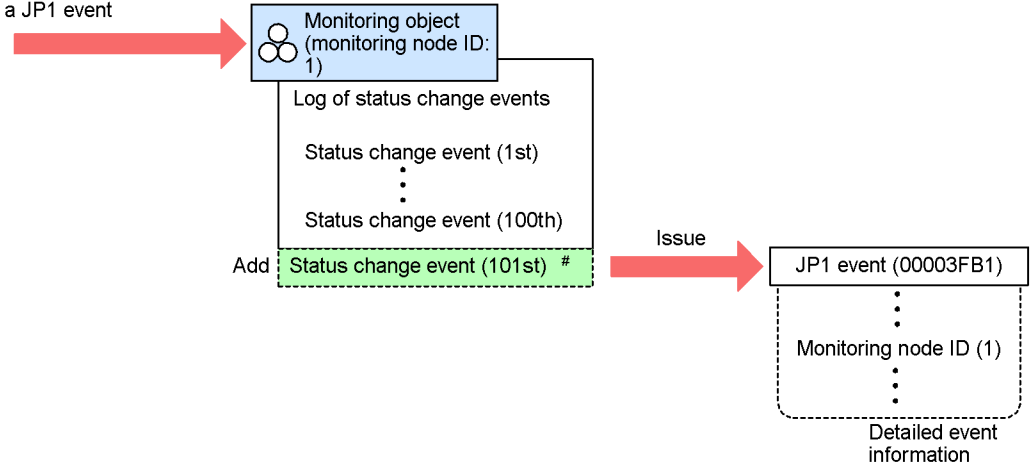
- Event ID: 00003FB1
- Message: KAVB7901-W The number of status change event for the monitored node *monitoring-node-ID* has reached the threshold.

Only one warning JP1 event (ID 00003FB1) is issued even if a single JP1 event causes the number of status change events to exceed 100 in multiple monitoring objects. The IDs of the affected objects are listed in comma-separated form in *monitoring-node-ID* in the message text, to a maximum of 10. If there are more than 10 affected objects, the IDs are followed by an ellipsis (...).

Figure 4-19: Issuing of event ID 00003FB1

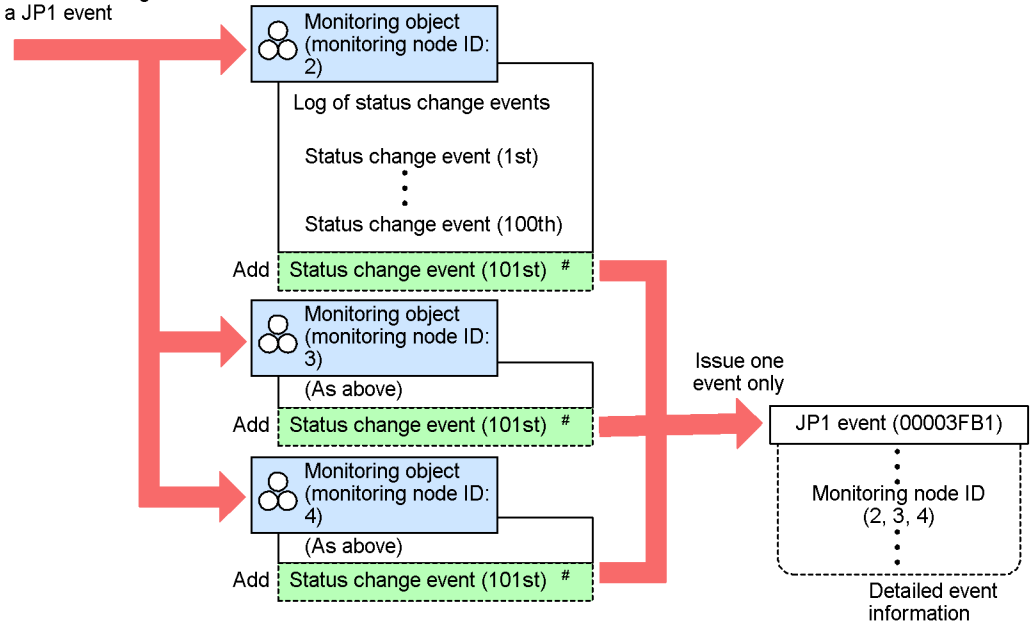
- Maximum number of status change events (100) exceeded in one monitoring object

JP1/IM - Manager receives  
a JP1 event



- Maximum number of status change events (100) exceeded in multiple monitoring objects

JP1/IM - Manager receives  
a JP1 event



#: Not shown in the search results for status change events.

*Reference note:*

The log of status change events for a monitoring object can only be managed to a maximum of 100 events. We recommend that you periodically check the number of logged status change events (by executing a search) and purge the log if it is getting too large. You can do so by manually changing the status of the monitoring object, or you can choose to delete the log automatically.

Before you manually purge a log, make sure that the JP1 events listed in the search results have all been dealt with.

The log can be deleted automatically in either of two ways:

- Set the monitoring object to `Initial` status on receipt of a specific JP1 event.
- Delete the log when the response status of JP1 events changes to **Processed**.

For details about how to change a monitoring object to `Initial` status on receipt of a specific JP1 event, see (2) *Setting a monitoring object to initial status on receipt of a JP1 event*. For details about how to delete a log of status change events when the response status of JP1 events is changed to **Processed**, see 4.8.3 *Automatically deleting processed status change events*.

## **(2) Setting a monitoring object to initial status on receipt of a JP1 event**

A monitoring object can be placed in `Initial` status on receipt of a particular JP1 event. This automatically deletes the log of status change events for that monitoring object. This functionality is referred to as *automatically initializing a monitoring object*. The functionality is disabled by default.

For example, by using a JP1 event that is issued when an error has been resolved, you can automatically initialize a monitoring object based on a recovery notification. To set this up, you would need to define a status change condition which changes the monitoring object to `Initial` status on receipt of a recovery-notification JP1 event.

You can define an `Initial` status change condition only for a monitoring object, not for a monitoring group.

As a note of caution when using this functionality, consider the possibility of two or more different errors being reported as JP1 events for the same monitoring object. If a recovery-notification JP1 event is received for one of these errors, the monitoring object will be forcibly initialized and its log of status change events will be deleted, even if the other error is unresolved. For this reason, we recommend that you use the automatic initialization functionality only under the following conditions:

- The issuing of one notification JP1 event guarantees that all errors occurring in a monitoring object have been resolved.
- Error recovery does not require the user to check the error log for the monitoring

object in question.

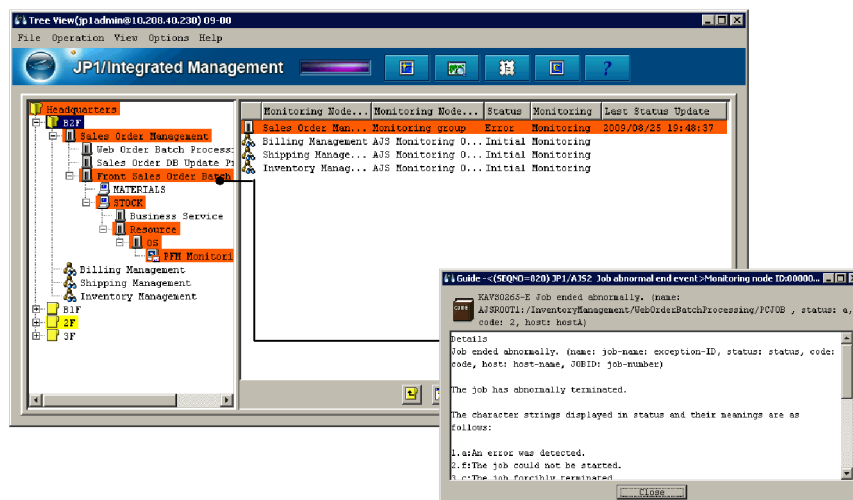
For details about how to set the automatic initialization function, see *5.7.4 Settings for initializing monitoring objects when JPI events are received* in the *Job Management Partner 1/Integrated Management - Manager Configuration Guide*.

## 4.7 Guide function

The guide function displays information relating to the type and status of a monitoring node in the Monitoring Tree window or Visual Monitoring window.

Using this function, you can view troubleshooting advice, such as action procedures and response methods for various errors, in accordance with the type and status of the monitoring object or group. For example, you can register troubleshooting procedures as guide information for each of the jobs in a monitoring group associated with a jobnet. This makes it easy to find pertinent information in a crisis. You can also use the guide function to describe the particular job that a monitoring node is associated with, and the specific aspects it is monitoring, and to accumulate operating know-how as guide information. Utilizing guide information in this way, as reference material when a problem occurs, lessens the system administrator's workload at the initial response stage.

Figure 4-20: Troubleshooting advice displayed as guide information



View guide information to find out methods and procedures for handling the problem.

### Example:

Guide information before a status change: Description of the associated job and the purpose of monitoring.

Guide information after a status change: Explanation of how to handle the error that has occurred.

The information displayed by the guide function is called *guide information*. Its contents and format (text or HTML) can be set by the user.

For details about how to set guide information, see 5.6.1 *How to edit guide information* in the *Job Management Partner 1/Integrated Management - Manager Configuration Guide*.

### 4.7.1 Settings for guide information

The contents displayed as guide information are set in a *guide information file* managed by JP1/IM - Manager.

- Guide information file

Windows: *scope-path*\conf\jcs\_guide.txt

UNIX: /etc/opt/jp1scope/conf/jcs\_guide.txt

For the format of a guide information file, see below.

About the guide information file

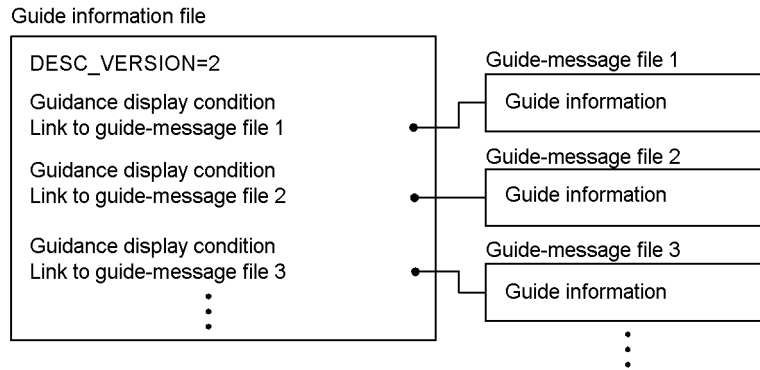
- Format of a guide information file

See *Guide information file (jcs\_guide.txt)* in 2. *Definition Files* in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.

In a guide information file, you can specify the contents to be displayed as guide information and the conditions about when to display the information.

The information to be displayed can be stored and managed in individual files. In JP1/IM, these separate files are known as *guide-message files*.

To use guide-message files, the guide information file must be version 2 (DESC\_VERSION=2). In the guide information file, instead of writing out the information itself, you simply write links to the guide-message files.

*Figure 4-21: Using guide-message files***(1) Conditions for displaying guide information**

Using a condition `EV_COMP_n` (where  $n$  represents a number), you can specify when to display a particular item of guide information. You can specify multiple conditions in the form `EV_COMP_1`, `EV_COMP_2`, and so on. The specified conditions are related by an AND condition.

As the condition, you can specify the type of JP1 event received by the monitoring node, or information about the node itself, as follows:

- Basic attribute or extended attribute of a JP1 event

For example, you can specify the event ID (`B.ID`), event level (`E.SEVERITY`), or other attribute.

You can also specify program-specific information (provided as an extended attribute of JP1 events) for a particular JP1 product. For example, you can specify the host that executes JP1/AJS jobs (`E.CO`).

For the basic attributes and extended attributes of JP1 events, see the appropriate manual for information about JP1 events issued by the product concerned.

- Monitoring node attribute

You can specify a monitoring node ID (`T.MONNODEID`) identifying a specific node. Check the ID in the Properties window or Search window for the monitoring node you want to specify.

When guide information is displayed in JP1/IM - View, the contents of the guide information file are referenced from the top. When an item matching the conditions is found, referencing stops and the applicable information appears in the Guide window.



*Note:*

Because the Guide window displays only the first of possibly multiple items in the guide information file that match the conditions, bear the following in mind when setting display conditions:

- Set multiple display conditions for an item of guide information so that the condition does not duplicate a display condition set for a different guide item.

For example, by setting multiple JP1 event attributes in a display condition, such as the event ID, event level, or message, you can differentiate the display condition from that set for another guide item.

A regular expression can be written as the contents of an attribute, but it must require a complete match.

- Write the contents of the guide information file starting from the highest event level.

For example, if status change conditions have been defined to change the status of a monitoring node to `Warning` and `Error`, respectively, write the information displayed when the node status changes to `Error` before the information displayed when the node status changes to `Warning`.

To display a description of the monitoring node as guide information, simply specify the node ID as the display condition. Write low-priority information of this nature at the very end of the guide information file.

## **(2) Contents displayed as guide information**

To write messages to be displayed as guide information, specify `EV_GUIDE` in the guide information file. To use guide-message files, specify `EV_FILE` instead of `EV_GUIDE`.

Messages can be written in text format or HTML format. The attribute values of JP1 events can also be used as variables in messages (by prefixing the attribute value with `$`). For example, if you write `$B.MESSAGE`, JP1 event messages (`B.MESSAGE`) will be handled as variables, and the attribute value of the JP1 event will be displayed in the guide message.

*Reference note:*

- You cannot format the message layout in a guide information file by inserting linefeed codes. However, you can do so in a guide-message file.

*Figure 4-22: Examples of writing guide information*

Coding in a guide information file (extract)

```

:
EV_GUIDE=Detailed information\nThe jobnet (jobnet name: execution-ID)
terminated abnormally.\n\nThe jobnet terminated abnormally.\n\n(S) \n
Continues processing. The execution ID is output when yes is specified in the
LOGINFOALL parameter in the configuration definition file or when All is specified
for output of information to the scheduler log and event log in the Scheduler Log
Settings page of the Manager Environment Settings dialog box.\n\n(O) \nCheck
the cause of the error and take appropriate action.
:

```

Linefeed codes cannot  
be inserted to format the  
message.

Coding in an event-guide message file

```

Detailed information
The jobnet (jobnet name: execution-ID) terminated abnormally.

The jobnet terminated abnormally.

(S)
Continues processing. The execution ID is output when yes is specified in the
LOGINFOALL parameter in the configuration definition file or when All is
specified for output of information to the scheduler log and event log in the
Scheduler Log Settings page of the Manager Environment Settings dialog box.

(O)
Check the cause of the error and take appropriate action.

```

Linefeed codes can be  
inserted to format the  
message.

Because you can apply formatting, guide-message files are useful when you are preparing messages in HTML format, and there is a large amount of information or you need to periodically review the message contents.

- Only one item of information can be written in a guide-message file. If you are writing a large amount of information, you might end up with a considerable number of files. Bear the following in mind when using guide-message files:
  - Use file names that will be easy to manage.

Name the files based on set conventions, using keywords (event IDs and message IDs, product names (AJS), monitoring node IDs, and so on) that are contained in the display conditions or display contents.

- Include the guide-message file name in the guide title (EV\_TITLE) written in the guide information file.

For example, suppose you are creating a guide-message file with the name `guide001`. Write the title as follows.

```

:
EV_TITLE=guide001: Abnormal job termination
EV_FILE=guide001

```

:

This makes it easier to edit the information later because you can tell from the display in the Guide window which guide-message file is being referenced.

### 4.7.2 Utilizing guide information tailored to the system operation

In the Guide window, you can choose to display any type of information as guide information, according to how the system is to be monitored.

For example, guide information could be utilized in the following ways.

Guide information tailored to system operation (examples)

- Guide information about troubleshooting procedures

First, suggest ways of handling particular problems, and advise what action to take in a crisis. Register these ideas as guide information.

Investigate the problem in detail at the follow-up stage, using all the various JP1/IM functions.

- Guide information about particular problems (JP1 events)

Prepare guide information about the causes of particular problems.

As a display condition, you can use information about the JP1 event that caused a status change in the monitoring node. Register this information as guide information

You can also set different types of guide information for different types of monitoring nodes. For example, you could display troubleshooting procedures for monitoring groups, and details about error causes for monitoring objects.

#### (1) *Guide information about action procedures*

To display guide information about action procedures, you must register information with the relevant monitoring nodes (that is, the monitoring viewpoints associated with a jobnet or other processing).

Each monitoring node has its own ID. Set guide information using the node ID as a condition.

Monitoring node IDs are unique to a node and are assigned automatically when a node is created. The node ID does not change when a node is moved in a monitoring tree.

1. Verify the monitoring node ID.

In the Monitoring Tree window, verify the ID of the node that you want to set guide information for in either of the following ways:

- Select the node, and then right-click and choose **Properties** from the pop-up

menu. View the **General** page in the displayed Properties window. The node ID appears in the **Monitoring node ID** field.

- Execute a node search: Choose **View** and then **Search** to open the Search window, and then search for the monitoring node you require. The node ID appears in the **Monitoring node ID** field in the search results.

2. Write guide information using the monitoring node ID as the condition.

In the guide information file (`jcs_guide.txt`), write guide information specifying the monitoring node ID (`T.MONNODEID`) as the condition (`EV_COMP` specified).

For example, write the guide information as follows.

*Coding example:*

```
[EV_GUIDE_1]

NUM=1

EV_COMP_1=T.MONNODEID: (monitoring-node-ID)

EV_TITLE=Action for error in Accounts_DailyTotals

EV_GUIDE=Action procedure when an error occurs in
Accounts_DailyTotals\nSee: User's Guide 3.11
Troubleshooting\nSummary: (For details, see the User's
Guide.)\nCheck the error cause. If the error has major impact,
suspend related jobs and contact the administrator (contact
route C) .

[END]
```

*Explanation of coding example:*

In `T.MONNODEID: (monitoring-node-ID)`, specify the node ID you verified above.

## (2) Guide information about an error (JP1 event)

To display guide information about an error, you must register information about the JP1 event that caused a status change in the monitoring node.

1. Investigate the JP1 event.

Investigate the JP1 event related to the problem.

As a display condition, you can use the event ID (`B.ID`) or other attribute of the JP1 event.

If you want to include a message (`B.MESSAGE`) or other JP1 event information in the guide information, also check message contents and attribute names.

## 2. Write guide information using the JP1 event as the condition.

In the guide information file (`jcs_guide.txt`), write guide information specifying the JP1 event ID (`B.ID`) or other JP1 event information as the condition (`EV_COMP` specified).

For example, write the guide information as follows.

*Coding example:*

```
[EV_GUIDE_1]

NUM=1

EV_COMP_1=B.ID:00004107

EV_TITLE=Abnormal job termination

EV_GUIDE=The job ended abnormally.\nJob name:
$E.OBJECT_NAME\nJob execution
host:$E.C0\nMessage--\n$B.MESSAGE\n--\n<Case>\nIf job A and
job B are executed concurrently, job B will end abnormally
because there is insufficient work area: Check the log
(jobexe.log) .

[END]
```

---

## 4.8 Completed-action linkage function

---

The completed-action linkage function automatically changes the status of monitoring objects according to the response status of the associated JP1 event. Thus, the status of each monitoring object in the Central Scope is linked to the response status of the corresponding JP1 event in the Central Console, and changes accordingly.

For example, suppose that an object has `Error` status because an error event has been received. When you change the response status of this error event to **Processed**, the status of the object changes from `Error` to `Normal`.

This function saves you from having to manually change the status of monitoring objects and monitoring groups and facilitates Central Scope operations.

The function does not work in reverse: Changing the status of a monitoring object in the Central Scope does not change the response status of the JP1 event matching a status change condition in the Central Console. For example, if you change the status of an object in the Central Scope from `Error` to `Normal`, the JP1 event in the Central Console does not change to **Processed**.

*Note:*

If you change the status of an object in the Central Scope, and then change the JP1 event response status in the Central Console, the status of the object will change again as a result.

However, because the log of status change events managed by the Central Scope is deleted when an object's status is changed manually, the completed-action linkage function is disabled at that point.

If there are any JP1 events not yet set to **Processed** status, the monitoring object will be in a corresponding status. In order of priority, its status will be one of the following: `Emergency`, `Alert`, `Critical`, `Error`, `Warning`, `Normal`, or `Debug`. When the user has changed all the JP1 events in the search results to **Processed** status, the monitoring object changes to `Normal`.

If a JP1 event has been changed from **Processed** to **Processing**, **Held**, or **Unprocessed** status, the object will revert to its previous status accordingly.

### 4.8.1 Behavior of the completed-action linkage function

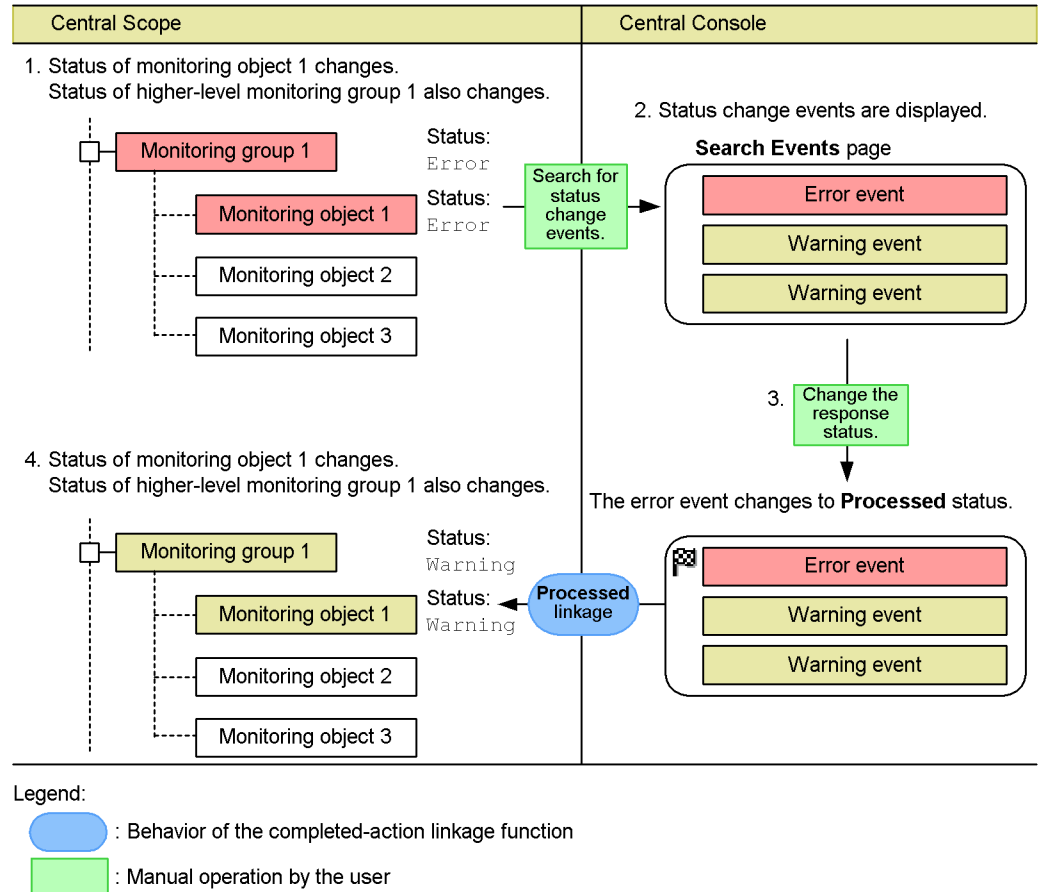
The following describes, by way of examples, how the completed-action linkage function works when the user manually changes the response status of a JP1 event in the Central Console after a monitoring object change status while the system is being monitored from the Central Scope.

The example below is based on the following assumptions:

- Both error events and warning events are set as status change conditions for monitoring object 1.
- Monitoring object 1 is defined so that its status changes to **Error** when an error event occurs, and to **Warning** when a warning event occurs.
- No status change condition is set for monitoring group 1 (the default applies).

The following example shows the behavior of the completed-action linkage function when the user changes the response status of a JP1 event to **Processed**.

Figure 4-23: Example of the completed-action linkage function (1)



The flow of processing is described below, following the numbers in the figure:

1. JP1/IM receives a JP1 event matching a status change condition of monitoring object 1, and the object's status changes to **Error**. The status of the higher-level monitoring group 1 also changes to **Error**.

The user investigates the cause of the error by searching for status change events, for example.

2. The status change events that occurred in monitoring object 1 appear on the **Search Events** page of the Central Console.

In this example, both error events and warning events will change the status of monitoring object 1. The object's status has changed to `Error` here as a result of both types of events.

The user acts on the problem that needs to be resolved first, according to the event level of the JP1 events.

3. The user changes the response status of the error event that caused the status change in monitoring object 1 to **Processed**.

The user sets **Processed** only for the event that has been resolved.

4. In tandem with the JP1 event changing to **Processed**, the `Error` status of monitoring object 1 is cleared, and its status changes to `Warning`. The status of the higher-level monitoring group 1 also changes to `Warning`.

Because the error event has changed to **Processed**, monitoring object 1 changes to the status corresponding to a warning event.

The user investigates and resolves the remaining warning events. When all the JP1 events matching the status change conditions have been changed to **Processed**, the status of the monitoring object changes to `Normal`.

The next example shows the behavior of the completed-action linkage function when the user changes the response status of a JP1 event from **Processed** to a different value.<sup>#</sup>

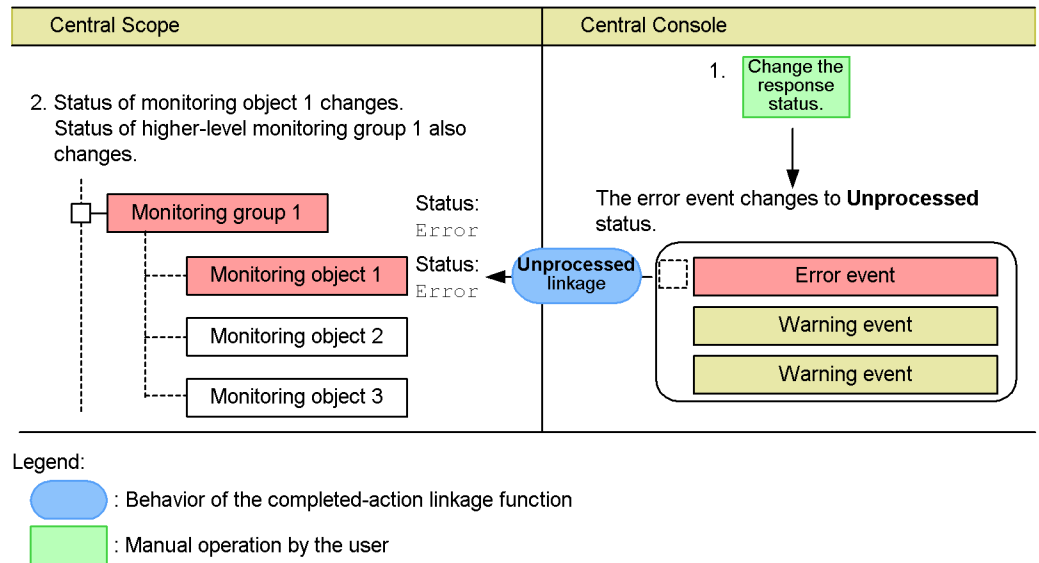
#

Other possible values are **Processing**, **Held**, or **Unprocessed**.

**Delete** is not included. **Delete** simply hides the JP1 event on the **Severe Events** page. JP1 events deleted on this page might still be listed on the **Monitor Events** page and **Search Events** page. Thus, setting the response status of a JP1 event to **Delete** does not change the status of the monitoring object.



Figure 4-24: Example of the completed-action linkage function (2)



The flow of processing is described below, following the numbers in the figure:

1. The user changes the response status of the JP1 event to **Unprocessed**.

A processed JP1 event might need to be changed to another response status if the problem had not been resolved after all, or if the **Processed** status was set by mistake, for example.

2. In tandem with the JP1 event changing to **Unprocessed**, the status of monitoring object 1 changes back to **Error**. The status of the higher-level monitoring group 1 also changes back to **Error**.

Because the error event is now **Unprocessed**, the object's status also changes back to **Error**, which has higher priority than **Warning**.

The user now proceeds to fix the problem.

#### 4.8.2 Disabling the completed-action linkage function

When the number of status change events exceeds the maximum (100), the completed-action linkage function is disabled. This is because integrity cannot be maintained between the log of status change events managed by the Central Scope and the JP1 events displayed in the Central Console.

For this reason, search for status change events on a regular basis and, if number of JP1 events in the search results is approaching the maximum, change the status of the monitoring objects manually to clear the log entries.

Manually changing the status of monitoring objects makes the completed-action linkage function usable once more. It also means that the corresponding JP1 events will not appear on the **Search Events** page, although they might still appear on the **Monitor Events** page and **Severe Events** page. Changing the response status of the JP1 events displayed on these pages has no effect on the status of the monitoring objects.

### 4.8.3 Automatically deleting processed status change events

The log of status change events can be deleted automatically when the response status of a JP1 event is changed to **Processed**. When this functionality is enabled, if all status change events for the monitoring object are changed to **Processed** status, the log is deleted and the monitoring object reverts to *Initial* status.

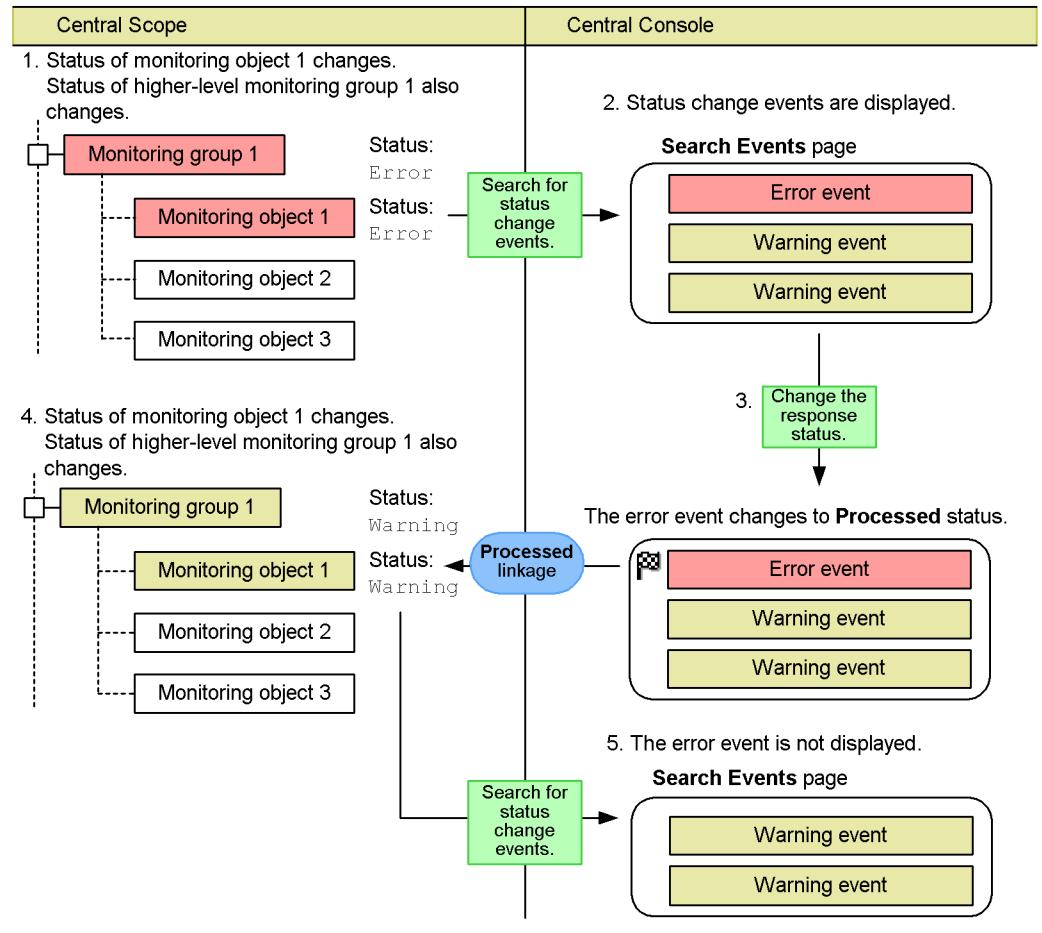
This functionality is disabled by default.

The following describes by way of an example how the log of status change events is automatically deleted. The example is based on the following assumptions:

- Both error events and warning events are set as status change conditions for monitoring object 1.
- Monitoring object 1 is defined so that its status changes to *Error* when an error event occurs, and to *Warning* when a warning event occurs.
- No status change condition is set for monitoring group 1 (the default applies).

The example below shows the behavior of the automatic deletion function when the user changes the response status of a JP1 event to **Processed**.

Figure 4-25: Example of automatically deleting processed status change events



Legend:

- : Behavior of the completed-action linkage function
- : Manual operation by the user

Numbers 1 to 4 in the figure are the same as in Figure 4-23 *Example of the completed-action linkage function (1)*. Of the status change events for monitoring object 1, the error event is set to **Processed**.

At step 5 in the figure, the user opens the **Search Events** page of the Central Console to search for status change events for monitoring object 1. However, because entries about JP1 events whose status was changed to **Processed** at step 3 have already been deleted from the log of status change events, these processed JP1 events do not appear

on the **Search Events** page. Only unprocessed status change events are listed.

Automatic deletion applies only to status change events issued after the function was enabled. Status change events that occurred before the function was enabled and are already set to **Processed** status are not deleted from the log. To delete these events, delete them manually by changing the monitoring node to `Initial` status in the Monitoring Tree window or by using the `jcschstat` command.

For the setup required to delete processed status change events, see 5.7.3 *Settings for automatically deleting status change events when JP1 event handling is completed* in the *Job Management Partner 1/Integrated Management - Manager Configuration Guide*.

*Note:*

If you mistakenly change a JP1 event to **Processed**, and then change it to **Error** or another status, the status of the monitoring object and the log of status change events do not revert to their previous state. Consequently, you cannot search for that JP1 event from the Central Scope. You will need to search for **Processed** JP1 events from the Event Console window.

Do not use automatic deletion in normal circumstances because of the considerable caution is required in performing status operations with this functionality enabled. We recommend that you delete the log of status change events by manually setting the monitoring object to `Initial` status in the Central Scope. Enable automatic deletion only in special circumstances, such as restricting user operations to the Central Console only.

*Reference note:*

Even if you enable automatic deletion of processed status change events, when the number of events exceeds the maximum (100), the completed-action linkage function is disabled. For this reason, periodically change the status change events to **Processed** to clear them from the log.

---

## 4.9 Performing system operations from JP1/IM

---

When a problem is detected during system monitoring, you can investigate using the Tool Launcher.

### 4.9.1 Tool Launcher

From the Tool Launcher window in JP1/IM - View, you can launch the GUI for products in the JP1 series and for many other applications. The Tool Launcher window lists the application functions that are linked with JP1/IM, allowing the windows of the appropriate application to be launched directly from the listing.

For details about the functions available in the Tool Launcher window, see *3.12.2 Tool Launcher*.

## 4.10 Central Scope

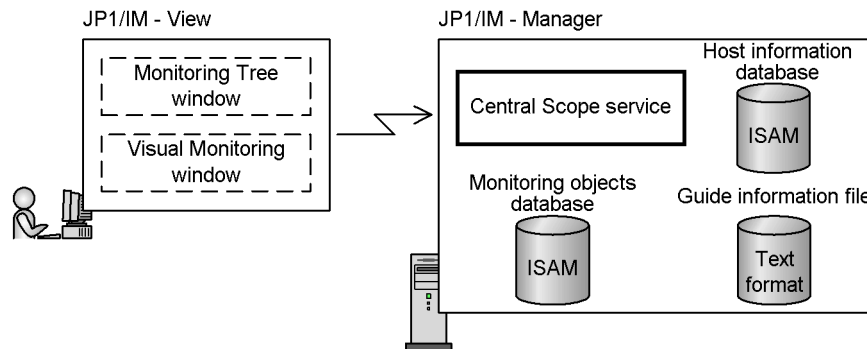
The following describes how the Central Scope works.

The Central Scope is designed so that it can be used without knowing how it works, but an understanding of Central Scope processes is useful if you want to customize settings or design a sophisticated system.

### 4.10.1 Overview of the Central Scope

The Central Scope incorporates the following functionality.

*Figure 4-26: Overview of the Central Scope*



### 4.10.2 Host information

JP1/IM - Manager (JP1/IM - Central Scope) stores host information (IP addresses and corresponding real host names and aliases) in a host information database of its own.

The processing carried out by JP1/IM - Manager (JP1/IM - Central Scope) includes managing the JP1 events occurring on the agents and automatically generating monitoring trees from definition information. JP1/IM - Manager must therefore recognize the host names and IP addresses of the agents correctly, and associate the right information.

To prevent discrepancies between the host names recognized by other products and those recognized by JP1/IM - Manager (JP1/IM - Central Scope), association information can be stored in the JP1/IM host information database.

The host names that need to be registered in the host information are as follows:

- The host name for which **Host name comparison** is selected in individual conditions for monitoring objects

- The following host names when using auto-generation of monitoring trees:
  - The host names managed by JP1/AJS or other linked product
  - The host names defined in the JP1/IM configuration definition

To find host information that is not registered in the host information database, JP1/IM - Manager (JP1/IM - Central Scope) references the settings in the JP1/Base `jp1hosts` information, the OS `hosts` file, and the DNS.

We recommend that you select **Host name comparison** when specifying a host name in an individual condition for a monitoring object.

About host information:

- Format of the host information file

See *Host information file (jcs\_hosts)* in 2. *Definition Files* in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.

- Commands for setting and referencing host information

See *jcshostsimport* in 1. *Commands* in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.

See *jcshostsexport* in 1. *Commands* in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.

- How to specify a host name in an individual condition for a monitoring object

See 3.12 *Status-Change Condition Settings window* in the manual *Job Management Partner 1/Integrated Management - Manager GUI Reference*.

*Reference note:*

When you select **Match**, JP1/IM - Manager (JP1/IM - Central Scope) determines that the individual condition is satisfied only when there is a complete match between the attribute value (string) of a received JP1 event and the string specified as the individual condition.

In contrast, when you select **Host name comparison**, JP1/IM - Manager (JP1/IM - Central Scope) compares the event attribute value with the host information in the database.

For example, suppose that the following is defined in the host information database or in the DNS or `hosts` file of the host on which JP1/IM - Manager (JP1/IM - Central Scope) runs.

```
111.111.111.111 server1 webserver
```

The differences between specifying **Match** and specifying **Host name comparison** in this environment are as follows:

Specified individual condition: `E.OBJECT_ID : server1 : Match`

If `E.OBJECT_ID` of a JP1 event is `server1`: Condition is satisfied.

If `E.OBJECT_ID` of a JP1 event is `webserver`: Condition is not satisfied.

If `E.OBJECT_ID` of a JP1 event is `111.111.111.111`: Condition is not satisfied.

Specified individual condition: `E.OBJECT_ID : server1 : Host name comparison`

If `E.OBJECT_ID` of a JP1 event is `server1`: Condition is satisfied.

If `E.OBJECT_ID` of a JP1 event is `webserver`: Condition is satisfied.

If `E.OBJECT_ID` of a JP1 event is `111.111.111.111`: Condition is satisfied.

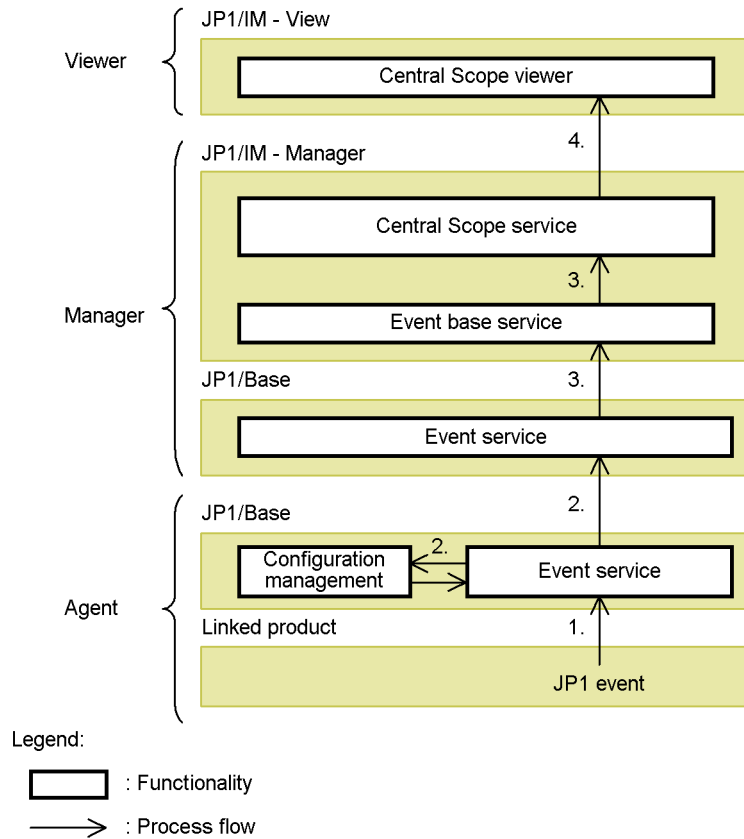
### 4.10.3 System monitoring using the Central Scope

The Central Scope visually represents events occurring in the system by analyzing JP1 events, determining where they occurred in the monitoring tree, and changing the status of the icon at that location.

The following figure shows the flow of processing.



Figure 4-27: Flow of processing to change the status of a monitoring object



The flow of processing is described below, following the numbers in the figure:

1. A JP1 event is generated on the agent and is registered with the event service.
2. The registered JP1 event is forwarded to a higher-level manager. The higher-level manager is determined from the configuration definitions of the configuration management function.

The event base service on the manager acquires the JP1 event from the event service. The event base service is solely responsible for processing JP1 events in JP1/IM. (For details about JP1 event acquisition and JP1 event control within JP1/IM - Manager, see 3.1.3 *Internal control of JP1 events by JP1/IM - Manager*.)

3. The JP1 event is passed to JP1/IM - Manager (Central Scope service), which analyzes the JP1 event, determines its severity, and associates it with a position in the monitoring tree.

The monitoring objects database is used for these processes.

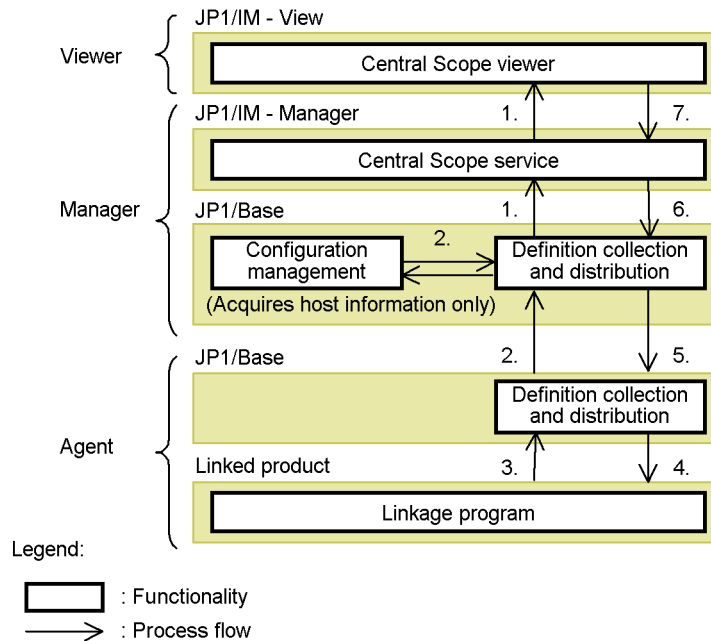
4. The system event is displayed visually in the Central Scope viewer (Monitoring Tree window and Visual Monitoring window) of JP1/IM - View.

In this way, the JP1 events generated on the agents in the system are accumulated on the JP1/IM managers, and the system is represented visually in the monitoring windows.

#### 4.10.4 Automatic generation of a monitoring tree

The flow of processing when automatically generating a monitoring tree is described below using the following figure as an example.

Figure 4-28: Flow of processing to automatically generate a monitoring tree



The flow of processing is described below, following the numbers in the figure:

1. An auto-generation request is sent from a window on the viewer to JP1/IM - Manager on the manager. On receiving the request, JP1/IM - Manager instructs JP1/Base on the manager to collect the monitoring objects (definition information) that will constitute the monitoring tree.
2. On receiving the instruction, JP1/Base (definition collection and distribution function) references the configuration definition information and sends collection requests to JP1/Base on the agents.

3. On receiving the collection request, JP1/Base on each agent requests the linked product (which supports the JP1/Base definition collection and distribution function) on that host to forward the required definition information.
4. On receiving the request, the linked product passes the definition information to JP1/Base on that agent. (This information will be the source data for defining the monitoring objects.)
5. JP1/Base on each agent forwards the transferred definition information to JP1/Base on the manager.
6. JP1/Base on the manager passes the received definition information to JP1/IM - Manager, which re-organizes the data into monitoring objects.

At this point, the definition information is not yet saved to the object database managed by JP1/IM - Manager.

7. JP1/IM - Manager passes the re-organized monitoring object information to JP1/IM - View. The information appears in tree format in the JP1/IM - View windows.

If the generated monitoring tree and objects are adequate for your requirements, you can save them to the manager and immediately begin monitoring from JP1/IM - View. If any adjustments are needed, you can modify the tree configuration and monitoring object definitions, and then save the changes to the manager. (For details about how to modify a monitoring tree, see *4.4 Editing a monitoring tree*.)

#### 4.10.5 Central Scope databases

The Central Scope has two databases: a *monitoring objects database* and a *host information database*.

##### ■ Managing the monitoring objects database

The monitoring objects database is managed by JP1/IM - Manager and contains the object information displayed in JP1/IM - View.

This database is updated on request from JP1/IM - View and on receipt of a JP1 event that changes the status of a monitoring object.

Note that the following processing to update the monitoring objects database might take some time to complete:

- Updating a server tree from the Monitoring Tree (Editing) window
- Importing database information to the monitoring objects database by the `jcsdbimport` command

If the OS shuts down, or if a failover occurs in a cluster system, while this update processing is in progress, the database could become corrupted.

To prevent corruption of the database, JP1/IM provides an automatic backup and recovery function. When this function is enabled, the database is automatically

backed up before either of the above types of update processing is performed, and is automatically restored to its former state if a problem occurs. If the update processing is successful, the backup data is automatically deleted.

This function is enabled for a new installation of JP1/IM, but is disabled when an upgrade installation is performed. To enhance the system's fault tolerance, we recommend that you enable the function if upgrading JP1/IM.

To enable the function, prepare an automatic backup and recovery settings file (`auto_dbbackup_xxx.conf`) for the monitoring objects database, and then apply the setting using the `jbssetcnf` command.

#### ■ Managing the host information database

The host information database contains information specific to JP1/IM - Manager (JP1/IM - Central Scope) and is managed within JP1/IM - Manager (JP1/IM - Central Scope).

You can import and export information to the Central Scope databases using the commands shown in the table below.

*Table 4-8: Commands for importing and exporting database information*

Command name	Purpose
<code>jcsdbexport</code> command	Acquire information from the monitoring objects database.
<code>jcsdbimport</code> command	Save information to the monitoring objects database.
<code>jcshostsexport</code> command	Acquire information from the host information database.
<code>jcshostsimport</code> command	Save information to the host information database.

You can check database information using the `jcsxxexport` commands, and you can migrate the environment to another server using the `jcsxxexport` commands in conjunction with the `jcsxximport` commands.

## Chapter

---

# 5. Command Execution by Automated Action

---

This chapter describes the automated action function provided by JP1/IM - Manager.

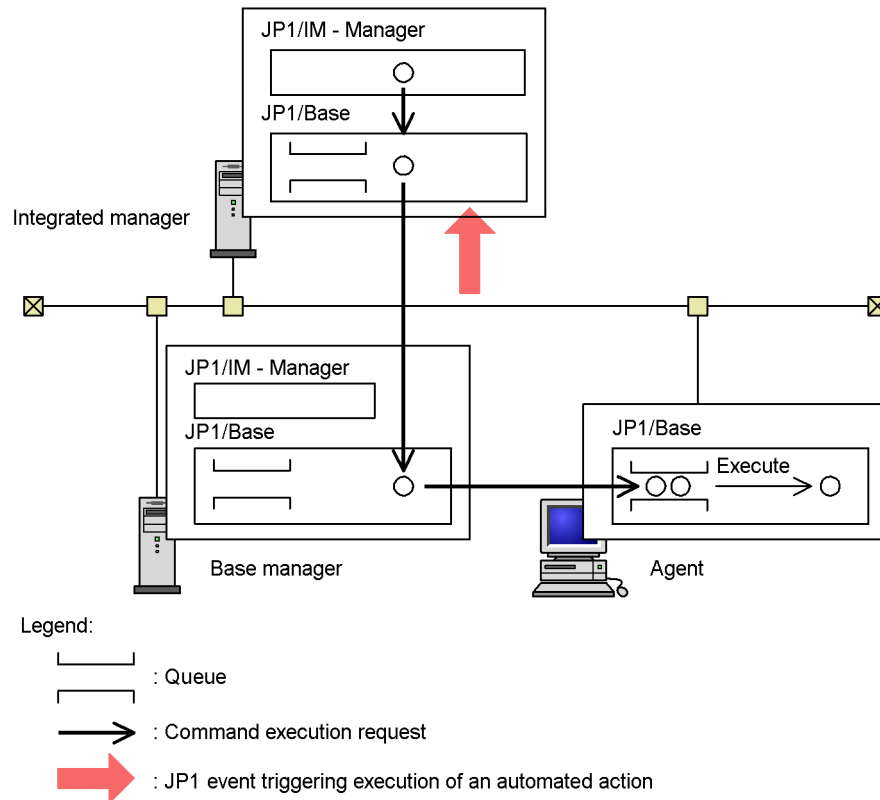
- 5.1 Overview of automated actions
- 5.2 Managing the status of automated actions
- 5.3 Defining an automated action
- 5.4 Specifying a command to be executed as an automated action
- 5.5 Monitoring the execution of an automated action
- 5.6 Checking the execution status and results of automated actions
- 5.7 Canceling automated actions
- 5.8 Re-executing an automated action
- 5.9 Operation settings for automated actions
- 5.10 Flow of automated action execution

## 5.1 Overview of automated actions

In JP1/IM, you can execute a command automatically when a specific JP1 event is received by a manager. This function is called *automated actions*.

By using automated actions, you can advise the system administrator, by executing a command that sends an email or makes a phone call, whenever a JP1 event reporting an error is received, for example.

Figure 5-1: Overview of automated actions



By defining the following items, you can execute a specified command as an automated action under set conditions.

- Define the automated action to be executed:
  - Specify a condition for executing the automated action.
  - Specify the command to be executed as an automated action, the target host,

the user account, and whether identical actions are to be suppressed.

- Set the environment for executing the automated action:
  - Customize the automated action execution environment.
  - Set up user mapping on the target host.

JP1/IM provides the following functionality to enable early detection of any problems during processing of an automated action.

- Automated action execution monitoring
  - Monitoring for delayed automated actions
  - Monitoring of automated action status

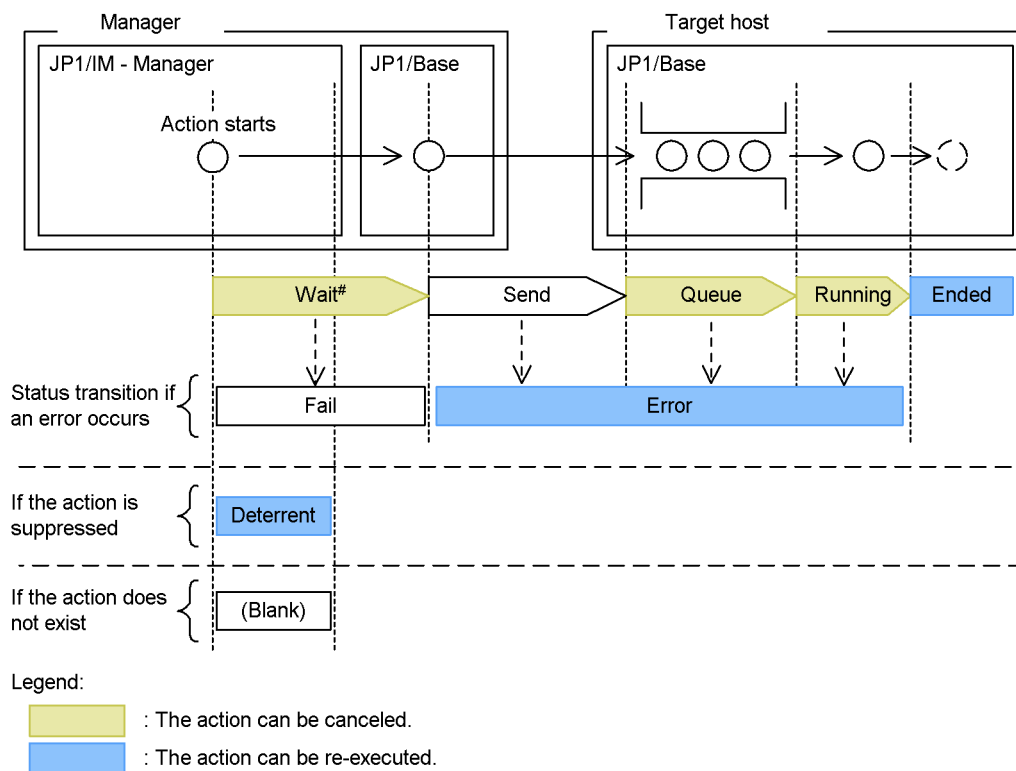
The next section describes how JP1/IM manages the status of automated actions. The following sections describe how to define an automated action, and the processes of monitoring and executing automated actions.

## 5.2 Managing the status of automated actions

When an automated action is executed, the processing is carried out through JP1/IM - Manager and JP1/Base. JP1/IM manages the processing in its domain as the action *status*.

The following figure shows in diagrammatic form the status transition of an automated action.

Figure 5-2: Status transition of an automated action



#: Occurs only if a retry is performed during the transfer of processing from JP1/IM - Manager to JP1/Base.

The flow of processing is always from JP1/IM - Manager to JP1/Base on the manager, and then from JP1/Base on the manager to JP1/Base on the target host. When the processing is successful, the status transition is Send, Queue, Running, and Ended, in that order. When the send buffer to JP1/Base is full, the status transition is Wait, Send, Queue, Running, and Ended, in that order. If an error occurs, the action status is set to Fail or Error, and processing terminates.



In the following cases, the status of the automated action is `Deterrent` or blank, and the processing terminates within JP1/IM - Manager:

- *Suppress* is set and the automated action meets the specified suppression conditions.

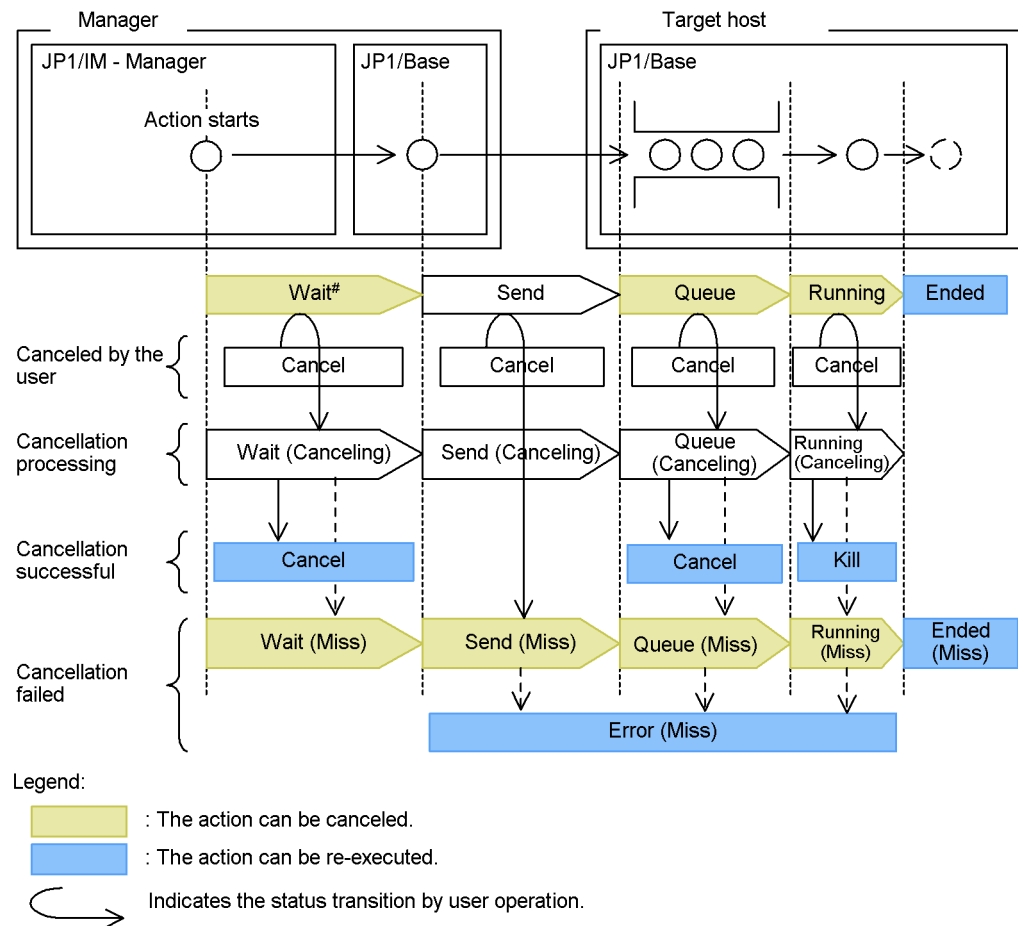
In this case, the status of the automated action is set to `Deterrent`, and processing terminates without the command being executed (for details, see 5.4.4 *Suppressing identical actions*).

- An execution condition has been set for the automated action, but the action definition (command to be executed) has not been set.

In this case, the automated action is executed, but because there is no command to execute, its status is blank and processing ends.

An automated action can be canceled while its status transition is still in progress (`Wait`, `Queue`, or `Running` status), but not while in `Send` status. The following figure shows the status transition when an automated action is canceled.

Figure 5-3: Status transition when an automated action is canceled



#: Occurs only if a retry is performed during the transfer of processing from JP1/IM - Manager to JP1/Base.

When an action in **Wait**, **Queue**, or **Running** status is canceled unsuccessfully, it remains in the same status instead of shifting to **Cancel** or **Kill**.

When an action in **Send** status is canceled unsuccessfully, its status becomes **Send (Miss)**.

When a cancellation request is issued for an action in **Send** status, the deletion processing is not performed until the action execution request is queued in JP1/Base on the target host. Depending on the action status when the cancellation request reaches JP1/Base, the cancellation processing may fail. If the action has reached

Ended or Error status, cancellation fails.

The following table describes details about action statuses.

*Table 5-1: List of automated action statuses*

Status	Description
Wait	<p>Because the send buffer<sup>#</sup> is full, JP1/Base declined the execution request from JP1/IM - Manager, which is now waiting to retry. (This status is cleared as soon as the buffer becomes available.)</p> <p><sup>#</sup>: The buffer used when sending a request to execute an automated action from JP1/IM - Manager to JP1/Base on the manager.</p>
Send	The execution request from JP1/IM - Manager is being sent from JP1/Base on the manager to JP1/Base on the target host.
Queue	<p>The execution request from JP1/IM - Manager is queued in JP1/Base on the target host. If this status persists for some time, the following problem may have occurred in JP1/Base:</p> <ul style="list-style-type: none"> <li>More automated actions are being generated than anticipated at the system design stage, leading to a massive backlog of redundant actions in the queue.</li> </ul> <p>In this situation, you can cancel the redundant automated actions using the JP1/IM cancellation function (for details, see <i>5.7 Canceling automated actions</i>).</p>
Running	<p>The execution request from JP1/IM - Manager is being executed by JP1/Base on the target host. If this status persists for some time, the following problem may have occurred in JP1/Base:</p> <ul style="list-style-type: none"> <li>A command executed by a previous automated action has hung or is taking longer than expected to complete. Subsequent automated actions cannot be executed for that reason.</li> </ul> <p>In this situation, you can cancel the automated action that caused the problem using the JP1/IM cancellation function (for details, see <i>5.7 Canceling automated actions</i>).</p>
Ended	The command has completed execution in JP1/Base, and the action result has been reported to JP1/IM - Manager. The action result has already been logged to the action re-execution file at startup of the automatic action service.
Fail	<p>An error occurred before the execution request was passed to JP1/Base. The reason is:</p> <ul style="list-style-type: none"> <li>An internal error occurred in the automatic action service; or</li> <li>JP1/Base (command execution management) that performs the processing is inactive.</li> </ul>
Error	<p>An error occurred in processing at the JP1/Base side, and command execution failed. In this situation, the text of the message (KAVBxxxx-E) output by JP1/Base is passed to JP1/IM - Manager as the action result. For JP1/Base message details, see <i>2.2 Messages related to command execution (KAVB2001 to KAVB2999)</i> in the manual <i>Job Management Partner 1/Integrated Management - Manager Messages</i>.</p>

## 5. Command Execution by Automated Action

Status	Description
Deterrent	A JP1 event met the condition for executing the automated action, but it occurred within the specified suppression time. Therefore, the action was suppressed (for details, see <i>5.4.4 Suppressing identical actions</i> ).
(blank)	An automated action with a set execution condition, but without a set action definition (command to be executed), has been executed.
Wait (Canceling)	Cancellation processing is being executed for an automated action in Wait status (the cancellation processing is incomplete).
Send (Canceling)	Cancellation processing is being executed for an automated action in Send status (the cancellation processing is incomplete).
Queue (Canceling)	Cancellation processing is being executed for an automated action in Queue status (the cancellation processing is incomplete).
Running (Canceling)	Cancellation processing is being executed for an automated action in Running status (the cancellation processing is incomplete).
Cancel	An automated action was cancelled before it reached Running status.
Kill	An automated action was canceled (killed) while in Running status.
Wait (Miss)	An automated action was canceled while in Wait status, but the processing failed.
Send (Miss)	An automated action was canceled while in Send status, but the processing failed. Or, an automated action was canceled unsuccessfully while in the previous status (Wait), and then shifted to Send status.
Queue (Miss)	An automated action was canceled while in Queue status, but the processing failed. Or, an automated action was canceled unsuccessfully while in a previous status (Wait or Send), and then shifted to Queue status.
Running (Miss)	An automated action was canceled while in Running status, but the processing failed. Or, an automated action was canceled unsuccessfully while in a previous status (Wait, Send, or Queue), and then shifted to Running status.
Ended (Miss)	An unsuccessfully canceled action is in Ended status.
Error (Miss)	An unsuccessfully canceled action is in Error status.
Unknown <sup>#</sup>	<p>The execution result of an automated action cannot be verified because a problem of some sort has caused inconsistencies in the files containing execution results (action information file, action hosts file, and command execution log file).</p> <p>In this case, you must delete the files. Once these files are deleted, the execution results of past automated actions cannot be referenced.</p> <p>For the deletion procedure, see <i>9.5(5) Actions to take when Unknown is displayed as the automated action execution status</i> in the <i>Job Management Partner 1/Integrated Management - Manager Administration Guide</i>.</p>

<sup>#</sup>: This is not an action status, but indicates that JP1/IM - Manager was unable to

acquire the status of the automated action.

You can check the execution status of an automated action in JP1/IM - View or by executing a command. For details, see *5.6 Checking the execution status and results of automated actions*.

### 5.3 Defining an automated action

You can define an automated action in either of two ways: Using the Action Parameter Definitions window in JP1/IM - View, or by creating an automated action definition file and applying its contents using the `jcachange` command.

JP1/IM provides an automated action definition file and an automatic action definition file (for compatibility). The Action Parameter Definitions window differs depending on which of these two files you are using.

For details about the contents you can define in an automated action definition file and automatic action definition file (for compatibility), see the references given in the following table.

Table 5-2: References for defining an automated action

Version information (value of DESC_VERSION)	Version of the automated action definition file	Action Parameter Definitions window	Further details about the automated action definition file	Further details about the Action Parameter Definitions window
1	Indicates that the automated action definition file is version 08-01.	Action Parameter Definitions (for compatibility) window	See <i>Automated action definition file (actdef.conf)</i> (for conversion) in 2. <i>Definition Files</i> in the manual <i>Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference</i> .	See 2.25.2 <i>Action Parameter Detailed Definitions (for compatibility)</i> window in the manual <i>Job Management Partner 1/Integrated Management - Manager GUI Reference</i> .
2	Indicates that the automated action definition file is version 09-00 or later.	Action Parameter Definitions window	See <i>Automated action definition file (actdef.conf)</i> in 2. <i>Definition Files</i> in the manual <i>Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference</i> .	See 2.24 <i>Action Parameter Definitions</i> window in the manual <i>Job Management Partner 1/Integrated Management - Manager GUI Reference</i> .

When a value other than 1 or 2 is specified in DESC\_VERSION, version information "3" is assumed.

When DESC\_VERSION is unspecified, the automatic action definition file (for compatibility) (version information "2") is assumed.

We recommend that you check the contents of the definition file by executing the

jcamakea command.

*Note:*

The action definition file for migration (`replaceactdef.conf`) is supplied for compatibility when using version 5 of the automated action function. You cannot simply edit this file for use with version 09-00 or later. Instead, create an `actdef.conf` file that matches the contents of `replaceactdef.conf`. For details about the automated action definition files, see *Automated action definition file (actdef.conf)* and `ACTIONDEFFILE` in *Automated action environment definition file (action.conf.update)* in 2. Definition Files in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.

You cannot use both `replaceactdef.conf` and `actdef.conf`.

### 5.3.1 Items that can be specified as execution conditions

You can specify any of the following items as a condition for executing an automated action:

- JP1 event ID

Specify the event ID of the JP1 event that triggers the automated action. You can select All IDs or specify a particular event ID.

- Event condition

Specify the event condition of the JP1 event that triggers the automated action. The items you can specify depend on whether you are using an automated action definition file or automatic action definition file (for compatibility).

Table 5-3: Specifiable event conditions

Attribute	Item	Event condition#1	
		Automated action definition file	Automatic action definition file (for compatibility)
Basic attribute	Registered reason	<ul style="list-style-type: none"><li>Match</li><li>Does not match</li></ul>	--
	Event ID	<ul style="list-style-type: none"><li>Match</li><li>Does not match</li><li>Regular expression</li></ul>	<ul style="list-style-type: none"><li>Match</li><li>Regular expression</li></ul>
	Source process ID		<ul style="list-style-type: none"><li>Regular expression</li></ul>
	Source user ID		
	Source group ID		
	Source user name	<ul style="list-style-type: none"><li>Match</li><li>Does not match</li><li>Is contained</li><li>Is not contained</li><li>First characters</li><li>Regular expression</li></ul>	
	Source group name		
	Source event server name		
	Source IP address		
	Event details		
	Message		
	Registered time	<ul style="list-style-type: none"><li>Regular expression</li><li>YYYYMMDDhhmmss format (YYYY: year, MM: month, DD: day, hh: hour, mm: minute, ss: second)</li></ul>	<ul style="list-style-type: none"><li>Regular expression</li><li>YYYY/MM/DD hh:mm:ss format (YYYY: year, MM: month, DD: day, hh: hour, mm: minute, ss: second)</li></ul>
	Arrived time		--



Attribute		Item	Event condition <sup>#1</sup>	
			Automated action definition file	Automatic action definition file (for compatibility)
Extended attribute	Common information	Start time	<ul style="list-style-type: none"> <li>Regular expression (specifying cumulative seconds)</li> </ul>	<ul style="list-style-type: none"> <li>Regular expression (specifying cumulative seconds)</li> </ul>
		End time		
		Product name	<ul style="list-style-type: none"> <li>Match</li> <li>Does not match</li> <li>Is contained</li> <li>Is not contained</li> <li>First characters</li> <li>Regular expression</li> </ul>	<ul style="list-style-type: none"> <li>Regular expression</li> </ul>
		Object type		
		Object name		
		Root object type		
		Root object name		
		Object ID		
		Occurrence		
		User name		
		Return code		
		Event level	<ul style="list-style-type: none"> <li>Match<sup>#2</sup></li> <li>Regular expression</li> </ul>	<ul style="list-style-type: none"> <li>Match<sup>#2</sup></li> <li>Regular expression</li> </ul>
	Program-specific information	E.	<ul style="list-style-type: none"> <li>Match</li> <li>Does not match</li> <li>Is contained</li> <li>Is not contained</li> <li>First characters</li> <li>Regular expression</li> </ul>	<ul style="list-style-type: none"> <li>Regular expression</li> </ul>
	For compatibility	Basic event information	<ul style="list-style-type: none"> <li>Regular expression</li> </ul>	

Legend:

--: None

#1: By default, only extended regular expressions can be specified in comparison conditions. For details about regular expressions, see *G. Regular Expressions*. However, if you have upgraded from a previous version of JP1/IM - Manager or JP1/IM - Central Console, the information set in the previous version is carried over.

If you are using version 8 or earlier of JP1/IM - View, you can edit event conditions only if you are using the automatic action definition file (for compatibility).

#2: You can specify the following attribute values: Emergency, Alert, Critical, Error, Warning, Notice, Information, and Debug.

### 5.3.2 Precedence of execution conditions

When a received JP1 event matches the execution condition for an automated action, the automated action is executed separately for each of the parameter groups in which it is defined.

If the received JP1 event matches multiple conditions for automated actions, the action that has highest precedence is executed.

Set the precedence of automated actions in the ACTIONPRIORITY parameter in the automated action environment definition file. As an option, you can specify DEFAULT or V8COMPATIBLE.

For a new installation of JP1/IM - Manager, specify DEFAULT as the precedence option. You cannot specify a precedence option after performing an upgrade installation. If no option is specified, V8COMPATIBLE is assumed (the action precedence used in JP1/IM - Manager version 8 or earlier apply).

If you specify DEFAULT, actions take precedence in the order in which they are written in the definition file. If you specify V8COMPATIBLE, the automated action targeted to a specific event ID takes precedence. If more than one automated action is targeted to a specific event ID, the actions are executed in the order in which they are written in the file.

The following table shows how the order of precedence differs between DEFAULT and V8COMPATIBLE when the specified event ID is 0000001, 0000002, or All IDs.

*Table 5-4:* Difference in action precedence when the event IDs 0000001, 0000002, and "All IDs" are specified in that order in the definition file

Event ID	Order in the definition file	Parameter group	Precedence with the DEFAULT option	Precedence with the V8COMPATIBLE option
0000001	1	1	1	1
0000002	2	1	2	2
All IDs	3	1	3	3

*Table 5-5:* Difference in action precedence when the event IDs "All IDs", 0000001, and 0000002 are specified in that order in the definition file

Event ID	Order in the definition file	Parameter group	Precedence with the DEFAULT option	Precedence with the V8COMPATIBLE option
All IDs	1	1	1	3
0000001	2	1	2	1
0000002	3	1	3	2

*Table 5-6:* Difference in action precedence when the event IDs 0000001, "All IDs", and 0000002 are specified in that order in the definition file

Event ID	Order in the definition file	Parameter group	Precedence with the DEFAULT option	Precedence with the V8COMPATIBLE option
0000001	1	1	1	1
All IDs	2	1	2	3
0000002	3	1	3	2

### 5.3.3 Parameter groups and AND condition

By using parameter groups and AND conditions, you can set complex conditions for executing automated actions.

- Parameter groups

A parameter group is a set of judgment conditions for executing an automated action. There are 10 parameter groups. Each automated action definition belongs to one parameter group only.

You can use parameter groups to execute multiple actions in response to one event, or to associate multiple execution conditions using an AND condition (as explained later).

When a JP1 event arrives at a JP1/IM manager, it is compared with the action definition parameters and execution conditions in their order of precedence, separately for each parameter group. When an execution condition is satisfied, the action that has the highest precedence in each parameter group is executed.

Each parameter group is assigned a one-digit number (0 to 9). This number is unrelated to the execution order or precedence of the automated actions.

If you do not specify the parameter group when defining an automated action, it will belong to parameter group 0.

- AND condition

An AND condition is a setting that requires all the execution conditions to be satisfied before an action is executed.

When an ampersand (&) is specified instead of a number in a parameter group specification, the relationship with the preceding execution condition in the automated action definition (displayed one line above in the GUI, or written one action block above in the definition file) is handled as an AND condition. You can define a maximum of 10 automated action definitions joined by an AND condition.

When a received event matches one of the execution conditions joined by an AND condition, it waits for another event matching another execution condition to be received. When all the execution conditions joined by the AND condition are satisfied, the automated action is executed. You can specify an AND-event keep limit as a timeout for the AND condition to be satisfied. If the required JP1 event arrives after expiry of the AND-event keep limit, it does not satisfy the AND condition.

Note that when the event base service (`evflow` process) stops, all events waiting for an AND condition to be satisfied are discarded. Take care if the system is restarted, by process management after an error, for example, or in a cluster system when a failover occurs.

### 5.3.4 Inherited event information

When defining an automated action, by using a variable you can specify information about the JP1 event that triggers the action as inherited event information. Inherited event information can be specified for the following items:

- Target host
- Execution user name
- Environment variable file
- Action

The following table lists the inherited event information you can specify.

Table 5-7: Variables that can be specified in an action definition

Attribute	Variable name	Inherited event information
Basic attribute	EVBASE	<ul style="list-style-type: none"> <li>Basic event information</li> </ul>
	EVID	<ul style="list-style-type: none"> <li>Event ID (<i>basic-code:extended-code</i>) Event ID as a character string in the format <i>basic-code:extended-code</i>.</li> </ul>
	EVDATE	<ul style="list-style-type: none"> <li>Date when the event was registered (<i>YYYY/MM/DD</i>) Registered time as a character string in the format <i>YYYY/MM/DD</i>.</li> </ul>
	EVTIME	<ul style="list-style-type: none"> <li>Time when the event was registered (<i>hh:mm:ss</i>) Registered time as a character string in the format <i>hh:mm:ss</i>.</li> </ul>
	EVPID	<ul style="list-style-type: none"> <li>ID of the process that issued the event Value of the source process ID.</li> </ul>
	EVUSRID	<ul style="list-style-type: none"> <li>User ID of the process that issued the event Value of the source user ID.</li> </ul>
	EVGRPID	<ul style="list-style-type: none"> <li>Group ID of the process that issued the event Value of the source group ID.</li> </ul>
	EVUSR	<ul style="list-style-type: none"> <li>User name of the process that issued the event Value of the source user name.</li> </ul>
	EVGRP	<ul style="list-style-type: none"> <li>Group name of the process that issued the event Value of the source group name.</li> </ul>
	EVHOST	<ul style="list-style-type: none"> <li>Host name of the server that issued the event Value of the source event server name.</li> </ul>
	EVIPADDR	<ul style="list-style-type: none"> <li>IP address of the server that issued the event Source IP address as a character string in the format <i>aaa.bbb.ccc.ddd</i>.</li> </ul>
	EVSEQNO	<ul style="list-style-type: none"> <li>Serial number in the event database Value of the serial number.</li> </ul>
	EVARVDATE	<ul style="list-style-type: none"> <li>Date when the event arrived (<i>YYYY/MM/DD</i>) Arrived time as a character string in the format <i>YYYY/MM/DD</i>.</li> </ul>
	EVARVTIME	<ul style="list-style-type: none"> <li>Time when the event arrived (<i>hh:mm:ss</i>) Arrived time as a character string in the format <i>hh:mm:ss</i>.</li> </ul>
	EVSRCNO	<ul style="list-style-type: none"> <li>Serial number in the source event database Value of the source serial number.</li> </ul>

Attribute	Variable name	Inherited event information
	EVMSG	<ul style="list-style-type: none"> <li>Message Text of the message.</li> </ul>
	EVDETAIL	<ul style="list-style-type: none"> <li>Detailed information about the event Event details as character strings in the format <i>Info-1 Δ Info-2 Δ ...Info-n Δ</i> (where <b>Δ</b> represents a space).</li> </ul>
Extended attribute	EVSEV	<ul style="list-style-type: none"> <li>Event level in the extended event information (Emergency, Alert, Critical, Error, Warning, Notice, Information, or Debug) Value of the event level.</li> </ul>
	EV <i>extended-attribute-name</i>	<ul style="list-style-type: none"> <li>User-specified extended attribute Value of the attribute specified in the extended attribute name.</li> </ul>
Other	ACTHOST	<ul style="list-style-type: none"> <li>Host name of the manager that requested execution of the action Manager host name.</li> </ul>
	EVENV1 to EVENV9	<ul style="list-style-type: none"> <li>Data extracted by specifying "(" )" in a regular expression in an action execution condition Can be specified only when extended regular expressions are used on the manager.</li> </ul>

**(a) Specification method**

Inherited event information is specified using a variable. Specify the variable in the form `$variable-name`. To specify a dollar sign as a character, type a backslash (\) before the dollar sign (\\$).

**(b) Converting inherited event information**

You can convert special ASCII characters included in inherited event information into a different character string.

This functionality allows you to convert characters in event information that have a special meaning in the OS into different characters.

Specify the special characters and the characters they are to be converted into using a configuration file for converting information. For details about this file, see *Configuration file for converting information (event\_info\_replace.conf)* in 2. *Definition Files* in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.

---

## 5.4 Specifying a command to be executed as an automated action

---

The following describes how to specify the command to be executed as an action when the execution conditions are fulfilled.

### 5.4.1 Executable commands

The following types of commands can be executed as automated actions:

On a Windows host:

- Executable file (`.com` or `.exe`)
- Batch file (`.bat`)
- Script file of JP1/Script (`.spt`) (provided the `.spt` file extension is associated with JP1/Script so that it can be executed)

On a UNIX host:

- UNIX command
- Shell script

However, the following types of commands cannot be executed:

- Commands that require interactive operation
- Commands that display windows
- Commands that use an escape sequence or control code
- Non-terminating commands such as daemons
- Commands (Windows only) that require interaction with the desktop, such as the Windows message structure or DDE
- Commands that shut down the OS, such as `shutdown` and `halt`

### 5.4.2 Target host

As the target host on which to execute a command as an automated action, you can specify a JP1/IM agent or manager.

The agent must be defined in the configuration management information as a host managed by JP1/IM.

By defining multiple agents in a host group, you can execute the same command on multiple hosts.

### 5.4.3 User account

Specify the JP1 user under whose account the command is to be executed.

The command is executed under the name of the OS user mapped to that JP1 user on the agent.

#### **5.4.4 Suppressing identical actions**

You can suppress the execution of an automated action that is identical to a previous action and occurs within a set time after that action.

This applies to automated actions that only need to be executed once during a set time period, such as actions that flash a signal light or send a notification email to the user. If these sorts of automated actions were allowed to accumulate in the JP1/Base command execution queue, they could delay the execution of urgent actions, such as those that perform error recovery.

You can avoid such situations by suppressing automated actions that do not need to be executed more than once during a set duration.

You can enable or disable suppression, and set the suppression time, for individual actions. This allows you to build an environment that suppresses actions that do not need to be repeated and executes only those that are required.

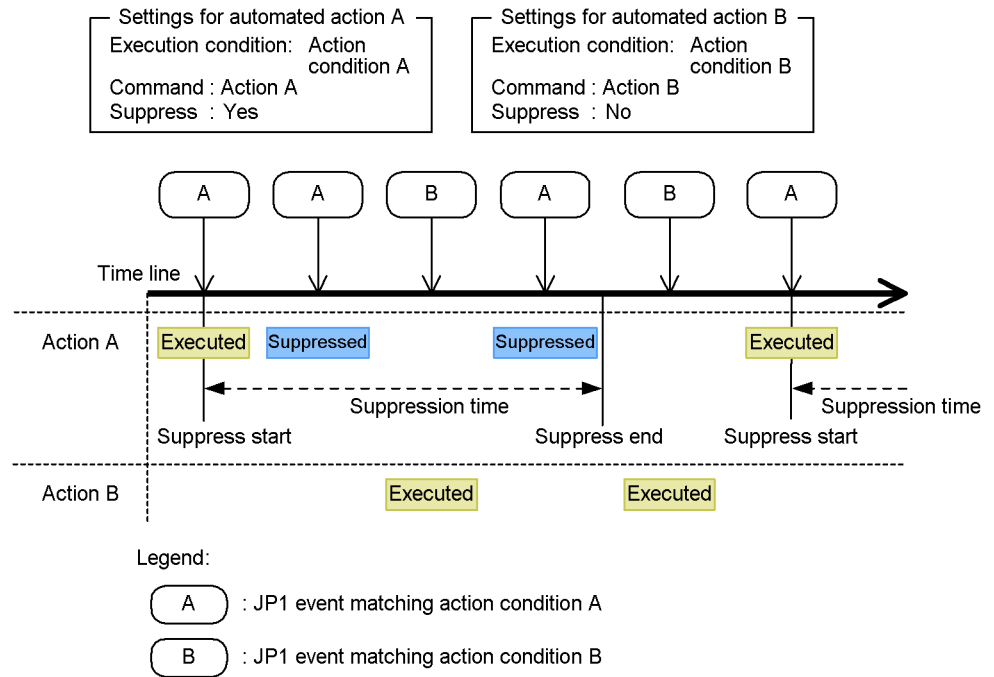
Suppression is cleared for an automated action being suppressed when a process is restarted by the process management functionality or if a failover occurs in a cluster system.

##### **(1) Behavior of an automated action when suppression is enabled**

The following figure shows how an automated action works when suppression is enabled.



Figure 5-4: Behavior of an automated action when suppression is enabled



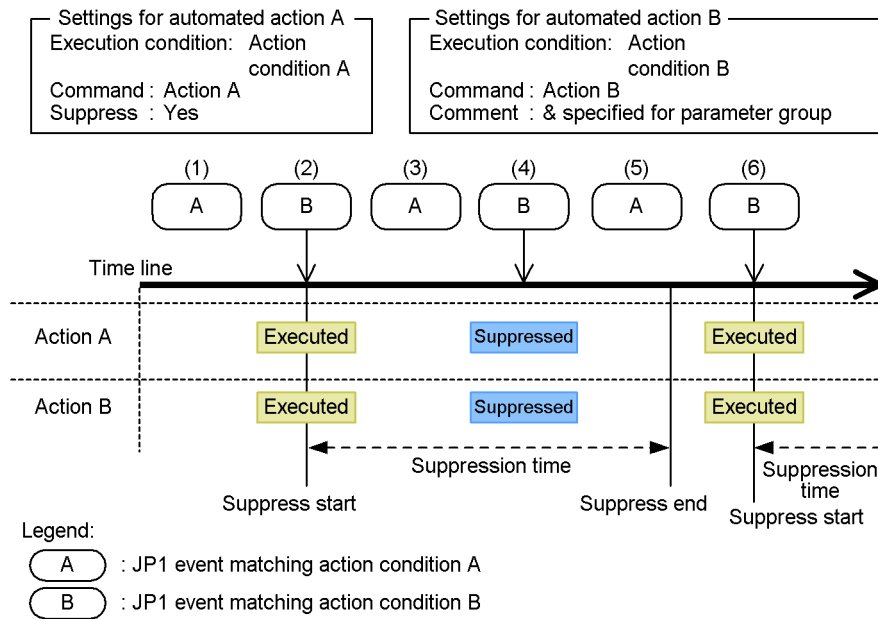
As shown by automated action A in the figure, when *Suppress* is set, the action is executed only in response to the first of multiple JP1 events that match the action's execution condition and occur within the set suppression time. The action is not executed for the second and subsequent identical JP1 events. The status of the unexecuted action is *Deterrent*.

As shown by automated action B in the figure, when *Suppress* is not set, the action is executed in response to every JP1 event that matches the action's execution condition (the behavior is unaffected by other JP1 events that are being suppressed).

**(2) Behavior of automated actions joined by an AND condition when suppression is enabled**

The following figure shows the behavior of automated actions joined by an AND condition when suppression is enabled.

*Figure 5-5: Behavior of automated actions joined by an AND condition when suppression is enabled*



The automated action behavior is described below, following the numbers in the figure:

1. A JP1 event matching execution condition A is received by JP1/IM - Manager. The action is not executed yet because actions A and B are joined by an AND condition.
2. A JP1 event matching execution condition B is received by JP1/IM - Manager. Because a JP1 event matching condition A has been received, the AND condition is satisfied and actions A and B are executed.
3. A JP1 event matching execution condition A is received by JP1/IM - Manager (same situation as 1).
4. A JP1 event matching execution condition B is received by JP1/IM - Manager (same situation as 2). A JP1 event matching condition A has been received and the AND condition is therefore satisfied, but the suppression time set for action A is still in effect. Therefore, actions A and B are not executed; both are set to Deterrent status.
5. A JP1 event matching execution condition A is received by JP1/IM - Manager (same situation as 1).
6. A JP1 event matching execution condition B is received by JP1/IM - Manager

(same situation as 2). Although a JP1 event matching condition A has been received within the suppression time for action A, this new event satisfying the AND condition was received after the suppression time elapsed. Therefore, actions A and B are not suppressed; both are executed.

---

## 5.5 Monitoring the execution of an automated action

---

JP1/IM - Manager provides functionality for monitoring the execution of automated actions so that any problems can be quickly detected. This is realized by the following two functions, which can each be set independently:

- Automated action delay monitoring

Execution is monitored so that if the action fails to complete within a set time, the problem is detected and the user notified.

- Automated action status monitoring

Action status is monitored so that if execution of an action fails, the problem is detected and the user notified.

### 5.5.1 Automated action delay monitoring

The following problems may occur during execution processing of automated actions:

- An action did not complete within the expected time.
- An action has not completed after a considerable time.

These types of problems affect the execution processing not only of the action in question but of subsequent actions too.

By monitoring the execution time of an automated action (delay monitoring), you can reduce the time it takes for the operator to respond to a problem. Any delay will be reported to the operator by a JP1 event or notification command.

For details on setting up delay monitoring, see *5.5.3 Setting up execution monitoring*.

#### (1) Delay monitoring start time and end time

Delay monitoring starts at the time when the JP1 event that triggers execution of the automated action arrives at JP1/Base on the manager.

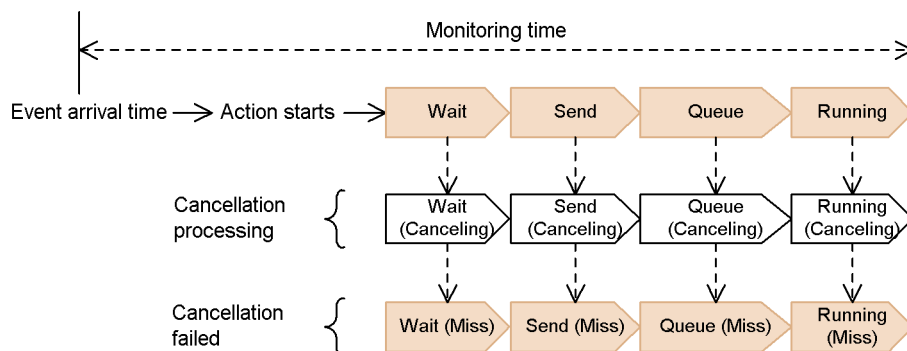
Delay monitoring ends when the action reaches one of the following statuses:

- Ended, Cancel, Kill, Fail, or Error
- Ended (Miss) or Error (Miss)

If the action fails to reach one of the above statuses within the time set for delay monitoring, its status becomes Delay.

The following figure shows the time frame and statuses monitored during delay monitoring.

Figure 5-6: Delay monitoring time and monitored statuses



When an automated action is re-executed at failover in a cluster system, the delay monitoring time and monitored statuses are no different from normal operation (the figure above). If you are using a cluster system, you must consider the time required for failing over the system when you set a delay monitoring time.

*Note:*

Delay monitoring does not apply to an automated action that is re-executed manually. This is because you are re-executing the action yourself, and can see when it starts and how long it takes.

Also, automated actions whose status is displayed as blank or as *Deterrent* are not monitored for execution delays.

## 5.5.2 Automated action status monitoring

The following problem may occur during execution processing of automated actions:

- JP1/IM - Manager or JP1/Base detects an error, the action status consequently changes to *Fail*, *Error*, or *Error (Miss)*, and processing terminates.

Because the automated action fails to complete execution as the user intended, this type of problem has a major impact on monitoring jobs.

By detecting errors in automated action processing, you can reduce the time it takes for the operator to respond to a problem. Errors are reported to the operator by JP1 events and notification commands.

For details on setting up status monitoring, see 5.5.3 *Setting up execution monitoring*.

## 5.5.3 Setting up execution monitoring

The functions for delay monitoring and status monitoring of automated actions are not enabled at installation and must be set up as required.

The following table describes the settings required to perform automated action delay monitoring and status monitoring. The defaults are shown in parentheses.

*Table 5-8: Settings required for delay monitoring and status monitoring*

Function	Setting	Where
Delay monitoring	<ul style="list-style-type: none"> <li>• Enable or disable delay monitoring (disable)</li> <li>• Delay monitoring time (600 seconds)</li> </ul>	Action Parameter Detailed Definitions window or the automated action definition file
	<ul style="list-style-type: none"> <li>• Issue JP1 event (true)</li> </ul>	Automatic action notification definition file
	<ul style="list-style-type: none"> <li>• Execute notification command (false)</li> </ul>	
Status monitoring	<ul style="list-style-type: none"> <li>• Enable or disable status monitoring (disable)</li> </ul>	Action Parameter Definitions window or automated action definition file
	<ul style="list-style-type: none"> <li>• Issue JP1 event (true)</li> </ul>	Automatic action notification definition file
	<ul style="list-style-type: none"> <li>• Execute notification command (false)</li> </ul>	

Delay monitoring can be set for an individual action, whereas status monitoring is set for the whole system (JP1/IM - Manager). JP1 events are issued by default: When monitoring is enabled, a JP1 event is issued on detection of an error. Notification commands are not executed by default: To execute a notification command on detection of an error, you must edit the automatic action notification definition file.

If you disable both JP1 events and notification commands, detected errors will not be reported to the user even if you set *Apply* for **Delay monitoring** or **Status monitoring**. You must specify either means of notification to perform delay monitoring or status monitoring.

#### 5.5.4 Automated action error monitoring using the execution monitoring function

When delay monitoring or status monitoring is enabled, detected errors are reported to the user by means of a JP1 event or notification command.

However, notification via these monitoring functions is performed once only. Further notification is suppressed and any subsequent errors are not reported.

For this reason, when you have finished dealing with a problem reported by an automated action, you must re-enable notification: In the Event Console window of JP1/IM - View, choose **Options** and then **Function-Status Notification Return**.

---

## 5.6 Checking the execution status and results of automated actions

---

You can check the execution status and result of an automated action using the following:

- List of Action Results window, Action Log window, and Action Log Details window (for further specifics) in JP1/IM - View
- `jcashowa` command

To check the contents of the command execution log, use the `jcocmdlog` command.

A JP1 event can be issued to report the execution status of an automated action. Because JP1 events are not issued by default, you must change the settings for issuing JP1 events by specifying the `-actevent` option of the `jcocmddef` command.

---

## 5.7 Canceling automated actions

---

You can cancel automated actions whose status is any of the following:

- Wait, Queue, or Running
- Send (Miss)<sup>#</sup>, Wait (Miss)<sup>#</sup>, Queue (Miss)<sup>#</sup>, or Running (Miss)<sup>#</sup>

<sup>#</sup>: Before you cancel an automated action in a status tagged (Miss), you should identify and fix whatever caused the cancellation failure (Miss), by examining the execution result in detail (error log) or by conducting an event search to check what happened on the target host, for example.

When you cancel an automated action, its status is tagged as (Canceling), and then becomes Cancel or Kill. If the cancellation processing fails, the action status is tagged as (Miss), and then proceeds through the usual status transitions (for details, see *5.2 Managing the status of automated actions*).

You can cancel an automated action and check whether cancellation was successful using the following:

- List of Action Results window, Action Log window, and Action Log Details window (cancel only) in JP1/IM - View
- jccancel command (cancel), jccashowa command (cancellation status check)

*Note:*

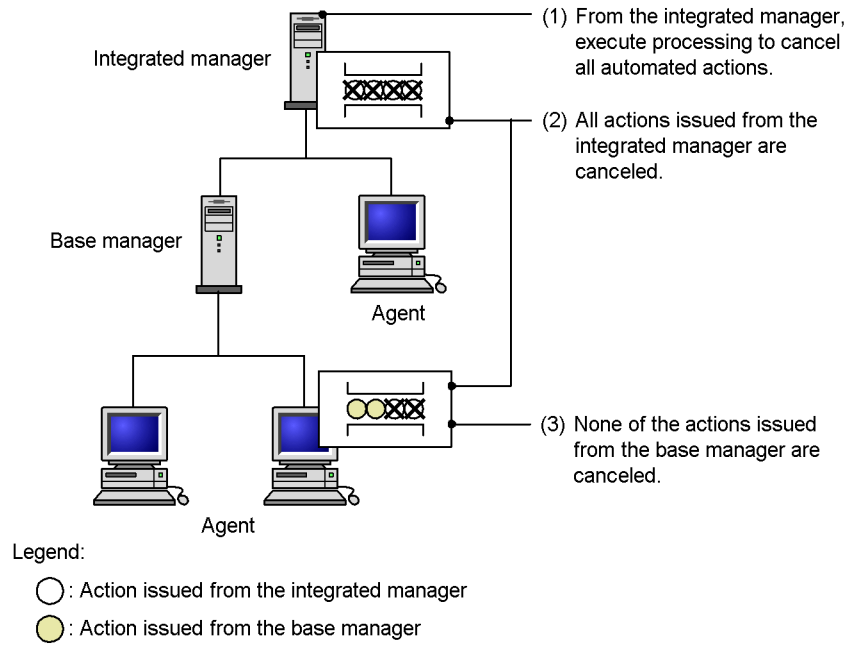
Automated actions can only be canceled when JP1/Base on the target host executing the action is version 07-51 or later. Cancellation is not possible if JP1/Base is earlier than version 07-51.

Range of actions that can be canceled

Only actions issued from the manager on which you are executing the cancellation processing can be canceled. That is, actions issued from a base manager cannot be canceled from the integrated manager.

The following figure shows the range of actions that can be canceled.



*Figure 5-7: Range of actions that can be canceled*

As shown in the figure, when action cancellation processing is executed from the integrated manager, only those action issued from the integrated manager are affected. Because actions executed from the base manager are not affected, they are processed as usual on the agent. To cancel actions issued from the base manager, you must execute the cancellation processing from that host.

---

## 5.8 Re-executing an automated action

---

You can re-execute an automated action whose status is any of the following:

- Deterrent, Ended, Error<sup>#</sup>, Cancel, or Kill
- Ended (Miss) or Error (Miss)<sup>#</sup>

<sup>#</sup>: Before you re-execute an automated action in Error or Error (Miss) status, you should identify and fix whatever caused the error, by examining the execution result in detail (error log) or by conducting an event search to check what happened on the target host, for example.

When you re-execute an automated action, it proceeds through the same status transitions as when processed by the system (for details, see *5.2 Managing the status of automated actions*).

You can re-execute an automated action and check whether execution was successful using the following:

- List of Action Results window, Action Log window, and Action Log Details window (re-execute only) in JP1/IM - View
- `jcashowa` command (re-execution status check)

---

## 5.9 Operation settings for automated actions

---

As internal processing, JP1/IM acquires events from JP1/Base, judges whether each event is a JP1 event that triggers an automated action, and executes the appropriate action if so. There is usually no need to change this internal processing, but you can halt it temporarily when a large number of redundant automated actions have been generated due to maintenance or some other activity.

To change JP1/IM settings, use the `jcachange` command. To check the settings, use the `jcastatus` command.

If you suspend internal processing, no automated actions will be executed after the system is operational again for any events that may have been received while processing was suspended. Do not suspend internal processing if there is an automated action that needs to be executed.

### *Reference note:*

About the `jcachange` command and `jcastatus` command:

See `jcachange` and `jcastatus` in *1. Commands* in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.

---

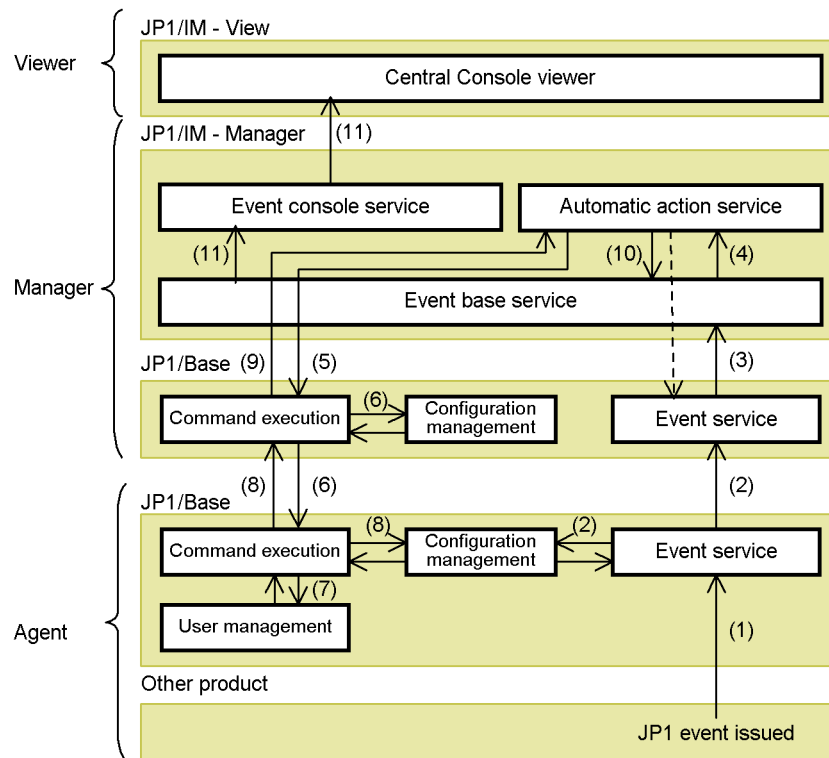
## 5.10 Flow of automated action execution

---

The following describes how the JP1/IM and JP1/Base functionality are inter-linked in automated action execution, taking as an example the flow of processing from the time a manager receives a JP1 event that triggers an automated action until the action is executed on an agent.

The description below assumes that the definition of the automated action has been completed. (For details on defining an automated action, see *5.3 Defining an automated action*).

Figure 5-8: Flow of processing for automated action execution (command executed on an agent by an automated action)



Legend:

□ : Functionality

→ : Process flow

---> : The action execution status is notified as a JP1 event (not issued by default).

The flow of processing is described below, following the numbers in the figure:

1. A JP1 event that triggers an automated action occurs on the agent and is registered with the event service.
2. The registered JP1 event is forwarded to a higher-level host in accordance with the configuration management definitions, and is registered with that manager's event service.
3. JP1/IM - Manager (event base service) acquires the registered JP1 event from the event service.

4. The acquired JP1 event is compared with the automated action definitions, and is passed to the automatic action service if a match is found.
5. On receiving the JP1 event, the automatic action service passes a command execution request to JP1/Base on the manager.
6. On receiving the command execution request, JP1/Base on the manager references the configuration information and sends a command execution request to the target host.
7. JP1/Base on the agent that received the request references the user mapping definitions and then executes the command using the permissions of the mapped OS user.<sup>#</sup>

<sup>#</sup>: User mapping (JP1/Base user management) is processed on the target host where the command is to be executed. Thus, user mapping must be set up in advance on the agent where the automated action is to be executed, or on the manager if the automated action is to be executed on the manager.

8. After the command has been executed, JP1/Base on the agent reports the result to the higher-level host defined in the configuration definitions.
9. On receiving the command execution result, JP1/Base on the manager records the result in a command execution log (ISAM) file, and then reports the result to the automatic action service.
10. The automatic action service outputs the execution result received from JP1/Base to a log, and then passes the execution result to the event base service.
11. The JP1 event information held by the event base service is displayed in JP1/IM - View through the event console service.

Automated actions are executed by the JP1/Base command execution function. See also 7.4.4 *Managing command execution*.

*Note:*

If any of the following events occurs during the execution processing of an automated action, the action ceases to proceed through the usual status transition (this applies only to actions whose status is `Wait`, `Send`, `Queue`, `Running`, `Wait (Canceling)`, `Send (Canceling)`, `Queue (Canceling)`, or `Running (Canceling)`):

- The manager, action relay host, or action target host is shut down or otherwise stopped.
- Network error
- JP1/Base failure

In such cases, check the status of the automated actions as follows.

Using the JP1/Base `jcocmdshow` command (supported in version 07-51):

You can check the action status using this command if the automated action was being processed by JP1/Base (command execution management) on the target host.<sup>#</sup>

<sup>#</sup>: If the processing request has not yet been received or if processing has ended, you cannot use this command to check the action status.

If an automated action ceases to progress and the `jcocmdshow` command cannot be used to check its status, evaluate whether it needs to be re-executed, and do so if necessary from the Execute Command window.





## Chapter

---

# 6. System Hierarchy Management Using IM Configuration Management

---

This chapter describes the functionality for centrally managing the system hierarchy by using IM Configuration Management. To manage the system hierarchy, you must first set up the IM Configuration Management database.

For information about defining the system hierarchy and collecting and distributing definition information using the functionality provided by JP1/Base, see 7.4.3 *Managing the system hierarchy* and 7.4.5 *Collecting and distributing definition information*.

- 6.1 Host management
- 6.2 System hierarchy management
- 6.3 Profile management
- 6.4 Management of service activity information
- 6.5 Importing and exporting IM Configuration Management information
- 6.6 Virtualization configuration management

## 6.1 Host management

Using IM Configuration Management - View, you can register and delete hosts on the network. You can also list registered hosts, and manage the host name and IP address of each host (hereafter, *host information*).

To manage hosts, JP1/Base must be active on the managed hosts.

This section describes the host information you can manage by using IM Configuration Management, and the functionality provided for this purpose.

### 6.1.1 Host information managed by IM Configuration Management

The following table lists the host information managed by IM Configuration Management.

*Table 6-1:* Host information managed by IM Configuration Management

Item	Description	Method of specification
Host	The host name registered in IM Configuration Management. You cannot register identical host names.	Specified directly when you register a host or change host information.
Comment	Comment about the host.	
IP address	The IP address of a host recognized by the manager. A maximum of four IP addresses can be registered. IP addresses cannot be specified directly. Be aware, especially if using NAT or with multiple LANs configured in the system, that this is not necessarily the IP address actually set for the host.	Acquired automatically when you register a host, change host information, or collect host information. Cannot be specified directly.
Host name list	A list of the authoritative names and aliases of the hosts recognized by the manager. A maximum of four aliases can be registered per host, but only one for a Windows host.	
Actual host name	The host name actually set for the host.	Acquired automatically when host information is collected. Cannot be specified directly.

Item	Description	Method of specification
Host type	The type of host, registered as one of the following: <ul style="list-style-type: none"> <li>Physical host</li> <li>Virtual host</li> <li>Logical host</li> <li>Unknown</li> </ul>	Specified directly when you register a host or change host information. Can be acquired when host information is collected.
Active host	The host name of the physical host used as the active node of a logical host. Registered when you select <b>Logical host</b> as the host type at registration. You cannot register the same host name as a standby host.	Specified directly when you register a host or change host information.
Standby host	The host name of the physical host used as the standby node of a logical host. A maximum of four host names can be registered. Registered when you select <b>Logical host</b> as the host type at registration. You cannot register the same host name as an active host.	
VMM host	The host name of the host running a VMware ESX or other virtual machine monitor. Registered when you select <b>Virtual host</b> as the host type at registration.	
OS	The name of the OS on the physical host.	
Collection status	The status of the host when host information is collected, registered as one of the following: <ul style="list-style-type: none"> <li>Not collected</li> <li>Collected</li> <li>Collection failed</li> </ul>	Acquired automatically when host information is collected. Cannot be specified directly.
Collection date/time	The date and time at which collection of host information was last completed.	
Configuration type	The type of host in a system managed by JP1/IM, registered as one of the following: <ul style="list-style-type: none"> <li>Integrated manager</li> <li>Base manager</li> <li>Relay manager</li> <li>Agent</li> <li>Not set</li> </ul>	Registered automatically when host information is read from the system definitions at addition or deletion of a host in the system hierarchy. Cannot be specified directly.
Configuration application date/time	The date and time at which a host was added to the system hierarchy.	

Item	Description	Method of specification
Configuration application status	<p>The configuration status when a host is added to the system hierarchy, registered as one of the following:</p> <ul style="list-style-type: none"> <li>• Not applied The change has not been applied to the system hierarchy (the host has not been added).</li> <li>• Applied The change has been applied to the system hierarchy.</li> <li>• Application failed The host has been added, but the change has not been applied to the system hierarchy.</li> </ul>	Registered automatically when host information is read from the system definitions at addition or deletion of a host in the system hierarchy. Cannot be specified directly.
Configuration verification date and time	The date and time at which the system hierarchy was verified.	
Configuration verification status	<p>The host status at the time the system hierarchy was verified, registered as one of the following:</p> <ul style="list-style-type: none"> <li>• Not yet verified The host's configuration definition information has not yet been verified.</li> <li>• Match The configuration definition information in the IM Configuration Management database matches the information in the host.</li> <li>• Does not match The configuration definition information in the IM Configuration Management database does not match the information in the host.</li> <li>• Verification failed The host's configuration definition information could not be verified because JP1/Base could not be reached.</li> <li>• Not supported The host does not support IM Configuration Management because it is running a version of JP1/Base earlier than version 9.</li> </ul>	
Product information	<p>A list of information about the JP1 products installed on the physical host. The following information is registered:</p> <ul style="list-style-type: none"> <li>• Product name</li> <li>• Product module</li> <li>• Version</li> <li>• Installation path</li> </ul>	Acquired automatically when host information is collected. Cannot be specified directly.

### 6.1.2 Registering hosts

Using IM Configuration Management, you can register hosts in the network as hosts to be managed in the IM Configuration Management database.

By registering hosts, you can then perform the following operations in IM Configuration Management:

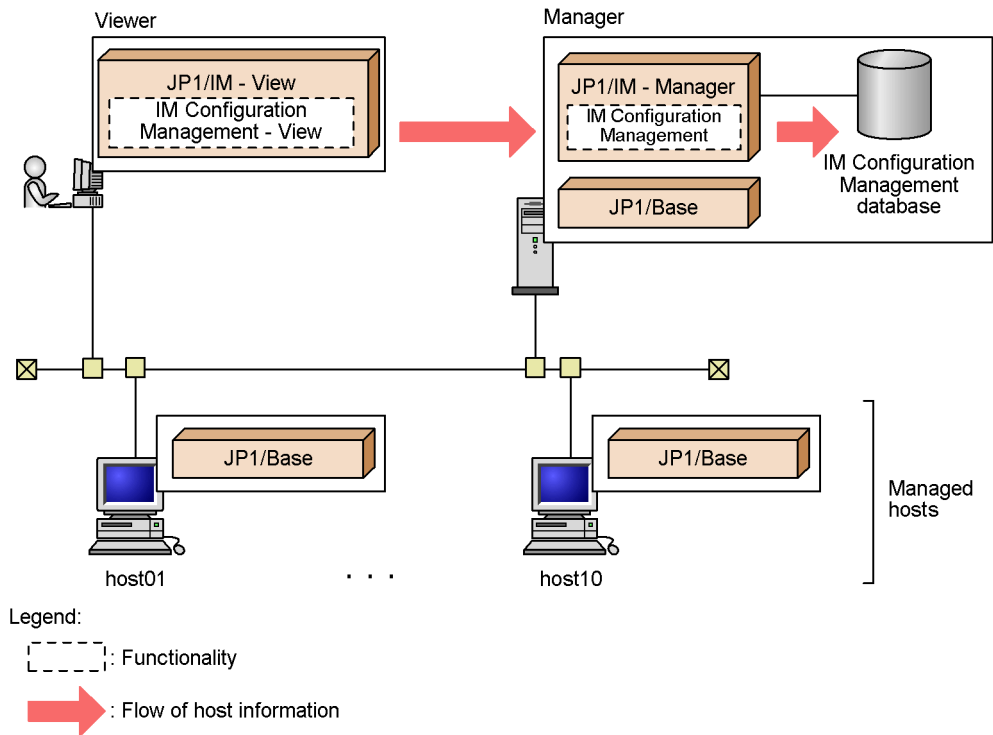
- Add a host to the system hierarchy.
- Check whether services on a host are active.

When IM Configuration Management starts, if there are no hosts registered in its database, information about the host (physical or logical host) running IM Configuration Management is registered automatically in the database.

Note that when the `jcfimport` command is executed on the manager running IM Configuration Management, the host information relating to that manager is overwritten.

To register host information, use the Register Host window.

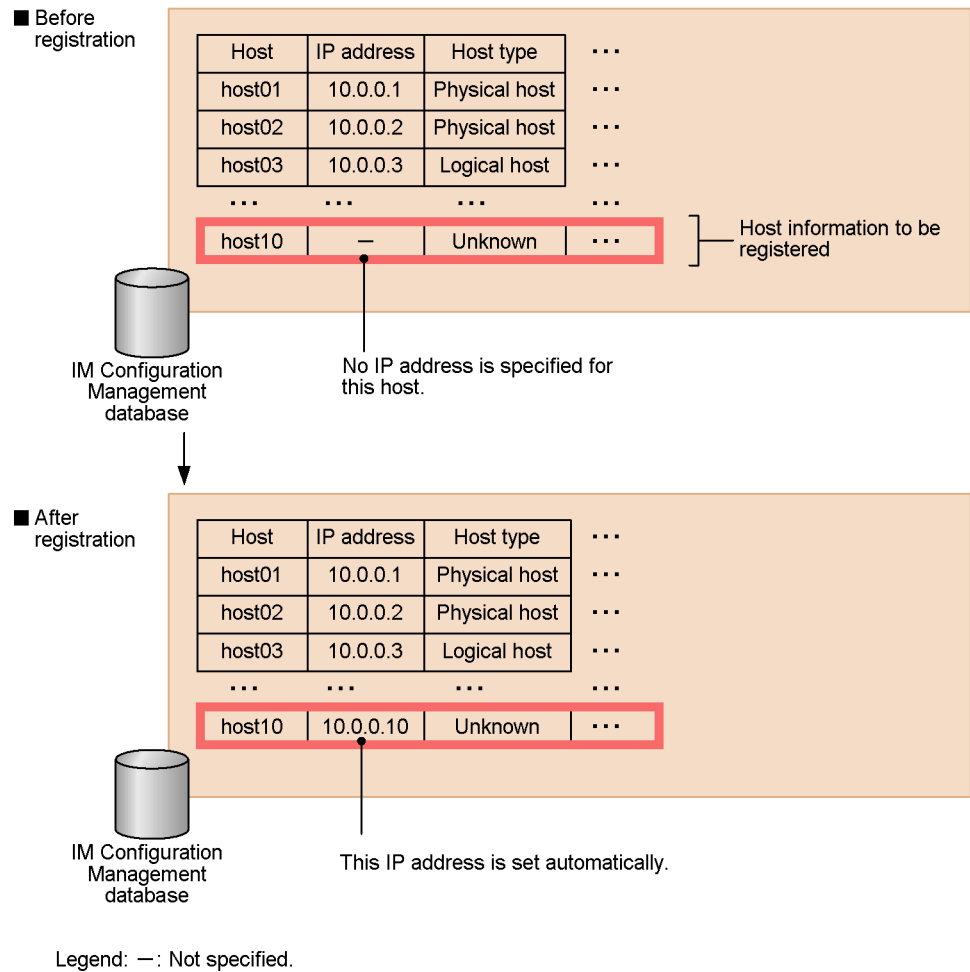
The figure below shows the flow of processing when registering hosts in IM Configuration Management.

*Figure 6-1: Registering hosts in IM Configuration Management*

When you register hosts, the information entered in the Register Host window is saved to the IM Configuration Management database. At this time, the IP address set for each host is registered automatically.

The figure below shows an example of the host information registered in the database at host registration.

*Figure 6-2:* Example of host information registered in the IM Configuration Management database at host registration



Any unregistered hosts in the system hierarchy are automatically registered in the IM Configuration Management database when configuration definition information is collected from the hosts.

Automatically acquiring host information from the system hierarchy definitions

Host information contained in the system hierarchy definitions (configuration definition information) is automatically registered in the IM Configuration Management database when you perform any of the following operations:

- Acquire the system hierarchy by using IM Configuration Management -

View.

For details, see *6.2.2 Acquiring the system hierarchy*.

- Load the system hierarchy from a configuration definition file by using IM Configuration Management - View.

For details, see *6.2.5(6) Loading the system hierarchy*.

- Import the system hierarchy on the server running IM Configuration Management.

For details, see *6.5.3 Importing IM Configuration Management information*.

If the number of hosts to be read from the system hierarchy exceeds the maximum number of hosts that can be registered in the IM Configuration Management database, only hosts equal to the maximum number are registered in the database.

The following checks are performed on the acquired system hierarchy when the acquisition is performed by IM Configuration Management - View is used:

- Whether the local host name in the acquired system hierarchy matches the local host name registered in the IM Configuration Management database. If different, the following message is output and processing is canceled:  
Collection of the IM configuration failed because the local host name "host1" is different from the registered host name "host2".
- Whether two or more hosts with the same host name exist in the acquired system hierarchy. If so, a message reports that the host name is duplicated and processing is canceled.

After these checks, if there is no higher-level host in the acquired system hierarchy, the configuration type of the local host changes to **Integrated manager**. If there is a higher-level host in the acquired system hierarchy, the configuration type of the local host changes to **Relay manager**.

When you import the system hierarchy on the server running IM Configuration Management, the hosts' IP addresses are not registered in the IM Configuration Management database even if set in the export file (`host_input_data.csv`).

### 6.1.3 Collecting host information

Using IM Configuration Management, you can collect the host information held by JP1/Base on each of the managed hosts, and register it in the IM Configuration Management database.

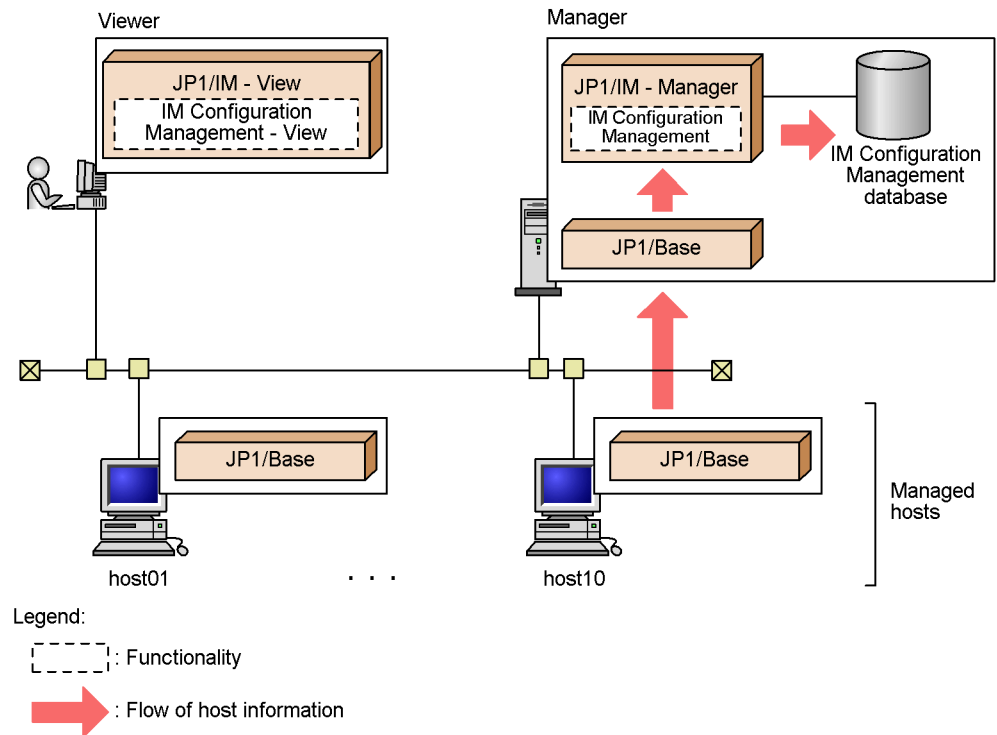
Collect host information on the **Host List** page or **IM Configuration** page of the IM Configuration Management window.

The figure below shows the flow of processing when collecting host information with



## IM Configuration Management.

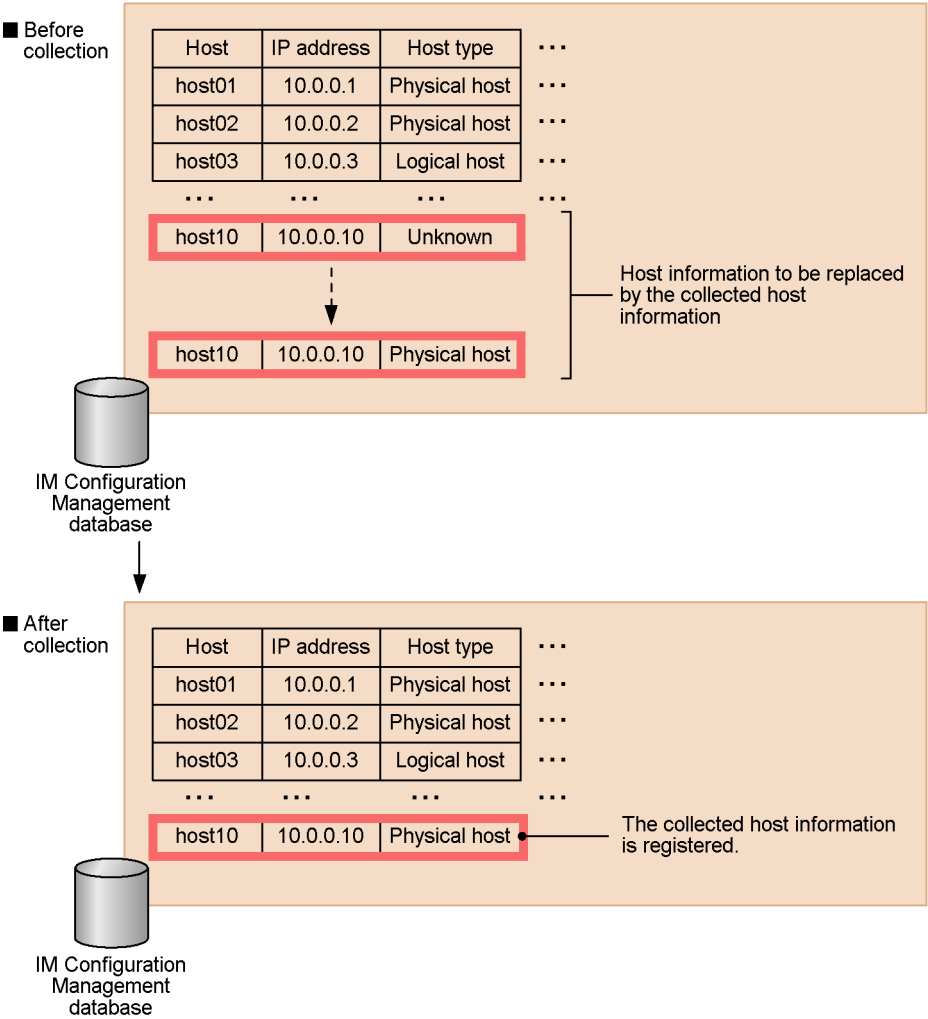
Figure 6-3: Collecting host information with IM Configuration Management



The collected host information is saved to the IM Configuration Management database, replacing the existing data.

The figure below shows an example of the host information registered in the IM Configuration Management database when collection is performed.

Figure 6-4: Example of host information registered in the IM Configuration Management database when collection is performed



The following table describes the correspondence between the version of JP1/Base on the managed hosts and the host information you can collect.

Table 6-2: JP1/Base version and host information that can be collected

Host information	JP1/Base version	
	Version 9	Versions 7 and 8
IP address	Y	Y

Host information		JP1/Base version	
		Version 9	Versions 7 and 8
Host name list		Y	Y
Host type		Y	N
Actual host name		Y	N
OS		Y	Y
Product information	Product name	Y	Y
	Product module	Y	N
	Version	Y	N
	Installation path	Y	N

Legend:

Y: Can be collected.

N: Cannot be collected.

The following table lists the JP1 products from which product information can be collected.

*Table 6-3: JP1 products from which product information can be collected*

Product name	Product version		
	Version 7	Version 8	Version 9
JP1/Base	Y	Y	Y
JP1/IM - Manager	N	N	Y

Legend:

Y: Can be collected.

N: Cannot be collected.

After host information is successfully collected from a host running JP1/Base version 9, JP1/IM performs either of the following checks on the collected information, as applicable:

- Host type determination

If the host information was collected from a host registered as **Unknown** type in the IM Configuration Management database, the host type is determined

automatically. The registered host type is changed to the host type contained in the collected host information.

Host type determination does not distinguish between a physical host and a virtual host. If the host is actually a virtual host, after the determination you must change the host type to Virtual host and set a VMM host in IM Configuration Management - View.

For details about how to set the host type, see *6.1.5 Changing host information*.

#### ■ Host type check

If the host information was collected from a host registered as other than **Unknown** type in the IM Configuration Management database, its host type is verified. The registered host type is compared with the host type contained in the collected host information. If a mismatch is found, the host type registered in the database is judged to be incorrect and an error message is displayed.

The host type check does not distinguish between a physical host and a virtual host. The host is assumed to be a physical host in all cases. The table below describes the results of a host type check.

*Table 6-4: Results of a host type check*

Host type of the collection target host	Host type registered in the IM Configuration Management database	Check result
Physical host	Physical host or virtual host	Y
Physical host	Logical host	N
Logical host	Physical host or virtual host	N
Logical host	Logical host	Y

Legend:

Y: Correct

N: Incorrect

*Note:*

If the host type is incorrectly specified as a physical host or virtual host in the IM Configuration Management database, the setting is not regarded as incorrect by the host type check.

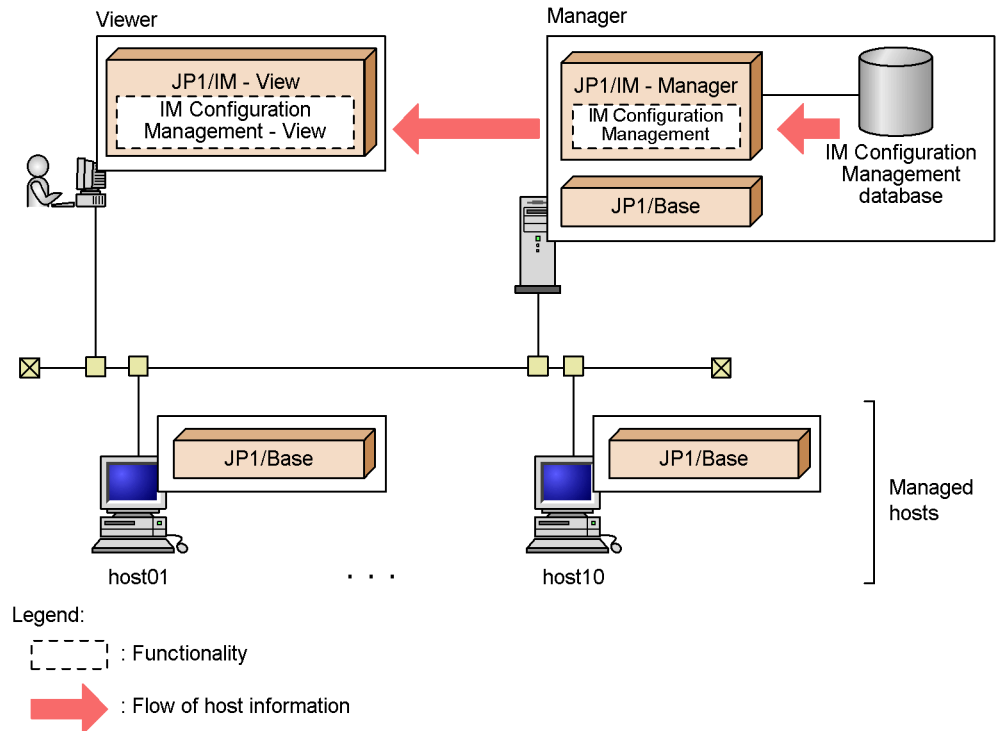
On the **Host List** page of the IM Configuration Management window, you can check the status of the hosts after host information is collected. If collection fails for any host, the host's icon appears grayed in the tree display area. To see more details, click the **Basic Information** button in the node display area on the **Host List** page.

### 6.1.4 Displaying host information

On the **Host List** page of the IM Configuration Management window, you can display a list of hosts registered in the IM Configuration Management database. On the **IM Configuration** page, you can view information about a particular host.

The figure below shows the flow of processing when displaying host information with IM Configuration Management.

Figure 6-5: Displaying host information with IM Configuration Management

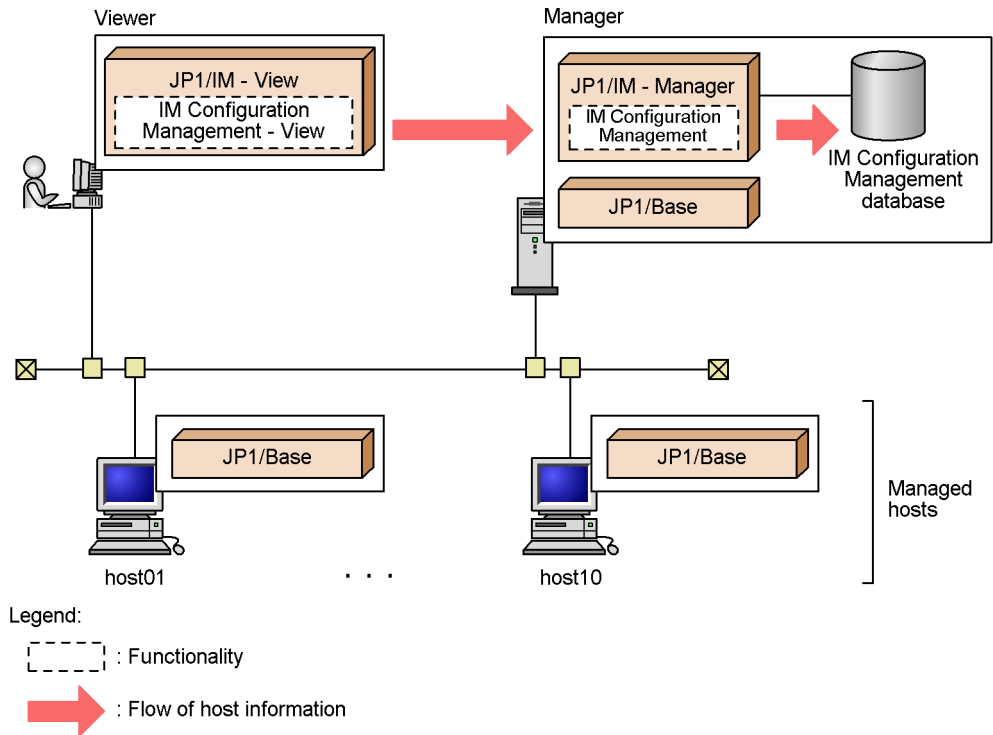


### 6.1.5 Changing host information

Using IM Configuration Management, you can change the host information registered in the IM Configuration Management database.

To change host information, use the Edit Host Properties window.

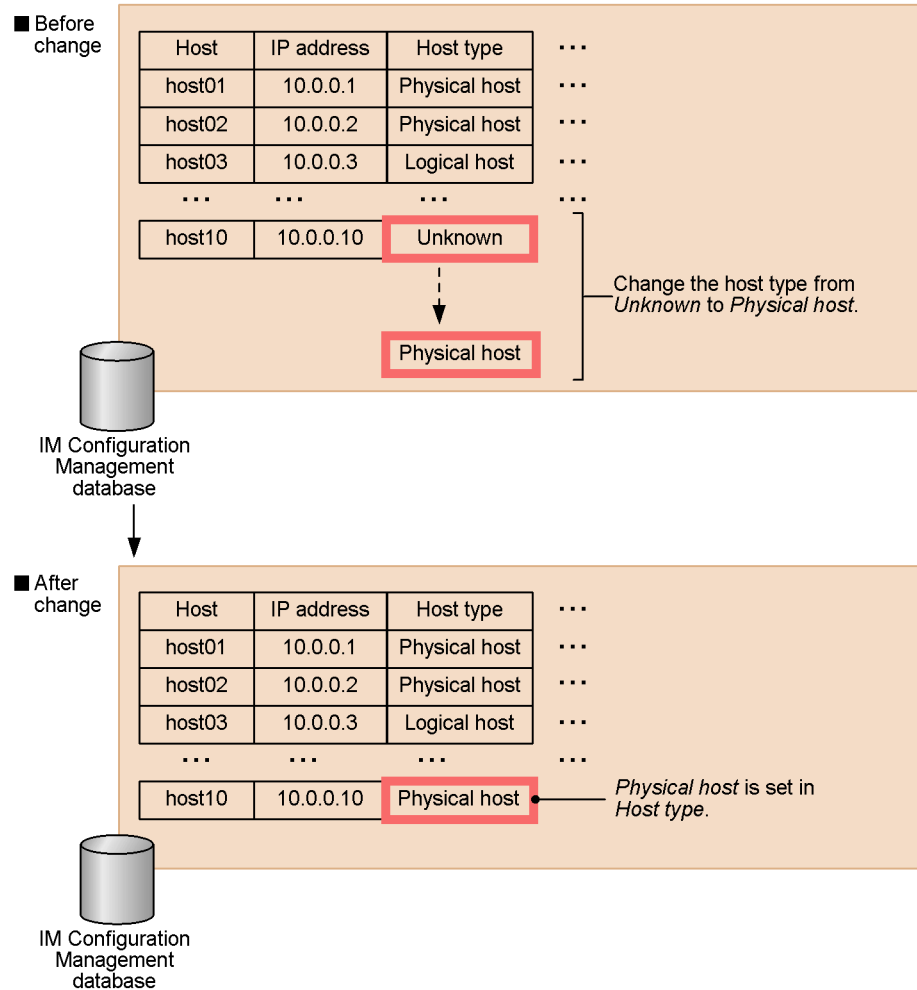
The figure below shows the flow of processing when changing host information with IM Configuration Management.

*Figure 6-6: Changing host information with IM Configuration Management*

The host and host information that you change in the Edit Host Properties window is registered in the IM Configuration Management database.

The figure below shows an example of the host information registered in the IM Configuration Management database after a property is changed.

Figure 6-7: Example of host information registered in the IM Configuration Management database after a property is changed



You cannot change the host type in the following cases:

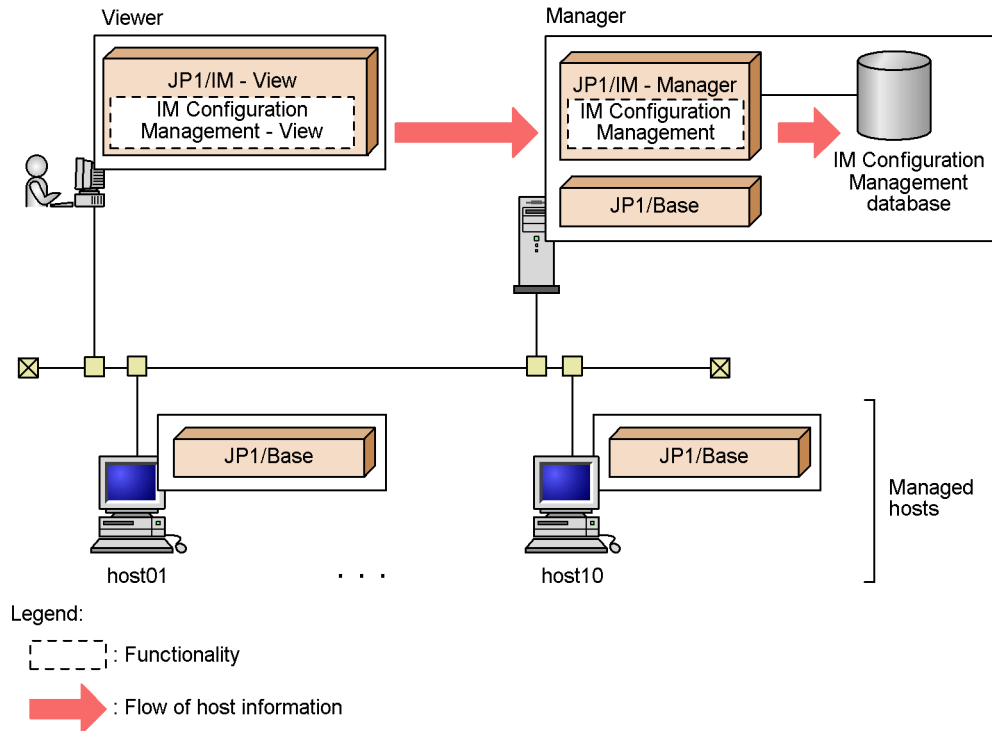
- Physical host  
If the physical host is being used as a VMM host in a virtual host, you cannot change its host type.
- Physical host or Virtual host  
If the host is being used as an active host or standby host in a logical host, you cannot change its host type to **Logical host** or **Unknown**.

### 6.1.6 Deleting hosts

Using IM Configuration Management, you can delete a host registered in the IM Configuration Management database.

Delete the host on the **Host List** page of the IM Configuration Management window. The figure below shows the flow of processing when deleting a host with IM Configuration Management.

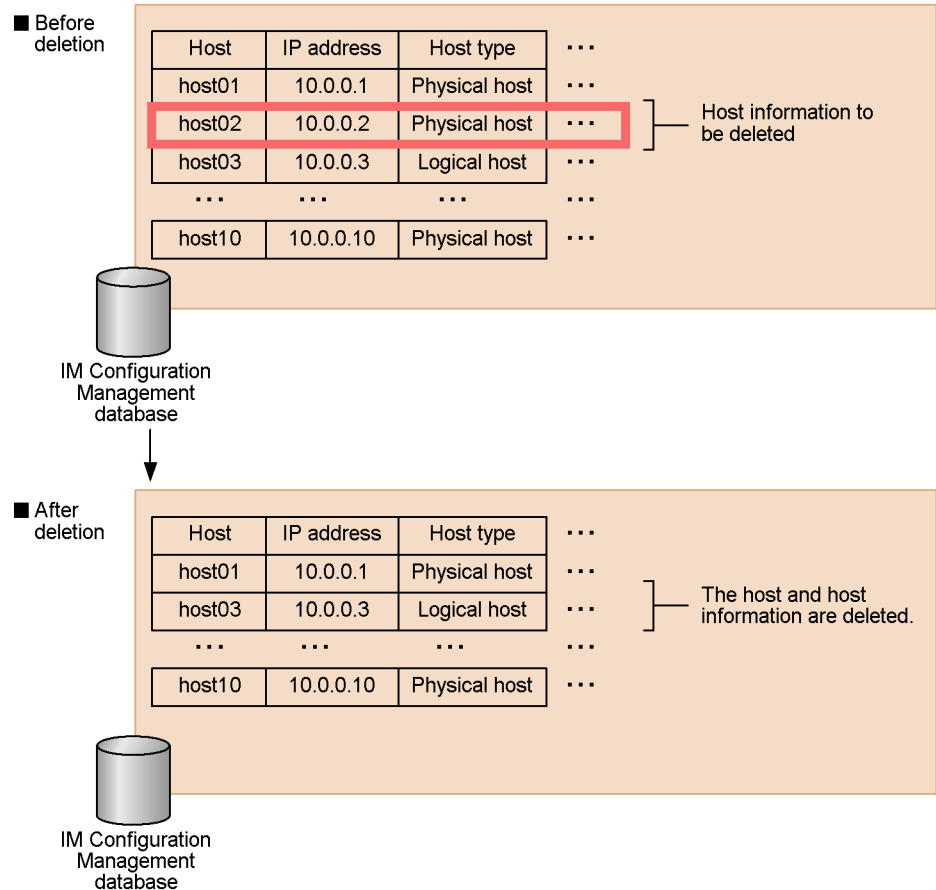
Figure 6-8: Deleting a host with IM Configuration Management



The figure below shows an example of host information erased from the IM Configuration Management database after a host is deleted.



Figure 6-9: Example of host information erased from the IM Configuration Management database when a host is deleted



The host and host information that you specify in the IM Configuration Management window are erased from the IM Configuration Management database. In addition to the host information, the profile information in JP1/Base (profile list and profile configuration files) are also erased. For details about profile information, see 6.3 *Profile management*. Note that the manager running IM Configuration Management cannot be erased from the IM Configuration Management database.

You cannot delete a host from the IM Configuration Management database in the following cases:

- Host registered in the configuration definition information

Before you delete the host from the IM Configuration Management database, you must first delete it from the system hierarchy in the Edit IM Configuration

window.

- Host of **Physical host** type being used as a VMM host in a virtual host

Before you delete the physical host, you must first perform either of the following:

- Change the VMM host used by the virtual host to a different physical host.
- Delete the virtual host.

- Host of **Physical host** type being used as an active or standby host in a logical host

Before you delete the physical host, you must first perform either of the following:

- Delete the physical host from the active host or standby host used by the logical host.
- Delete the logical host.

- Host of **Virtual host** type being used as an active or standby host in a logical host

Before you delete the virtual host, you must first perform either of the following:

- Delete the virtual host from the active host or standby host used by the logical host.
- Delete the logical host.

---

## 6.2 System hierarchy management

---

Using IM Configuration Management - View, you can centrally manage the system hierarchy.

To manage the system hierarchy, you must first register the hosts configured in the system in the IM Configuration Management database. JP1/Base must also be active on the managed hosts.

This section describes the hierarchical configurations you can manage using IM Configuration Management, and the functionality provided for this purpose.

### 6.2.1 Hierarchical configurations managed by IM Configuration Management

Using IM Configuration Management, you can define the host relationships and manage the JP1/IM system configuration as a hierarchy.

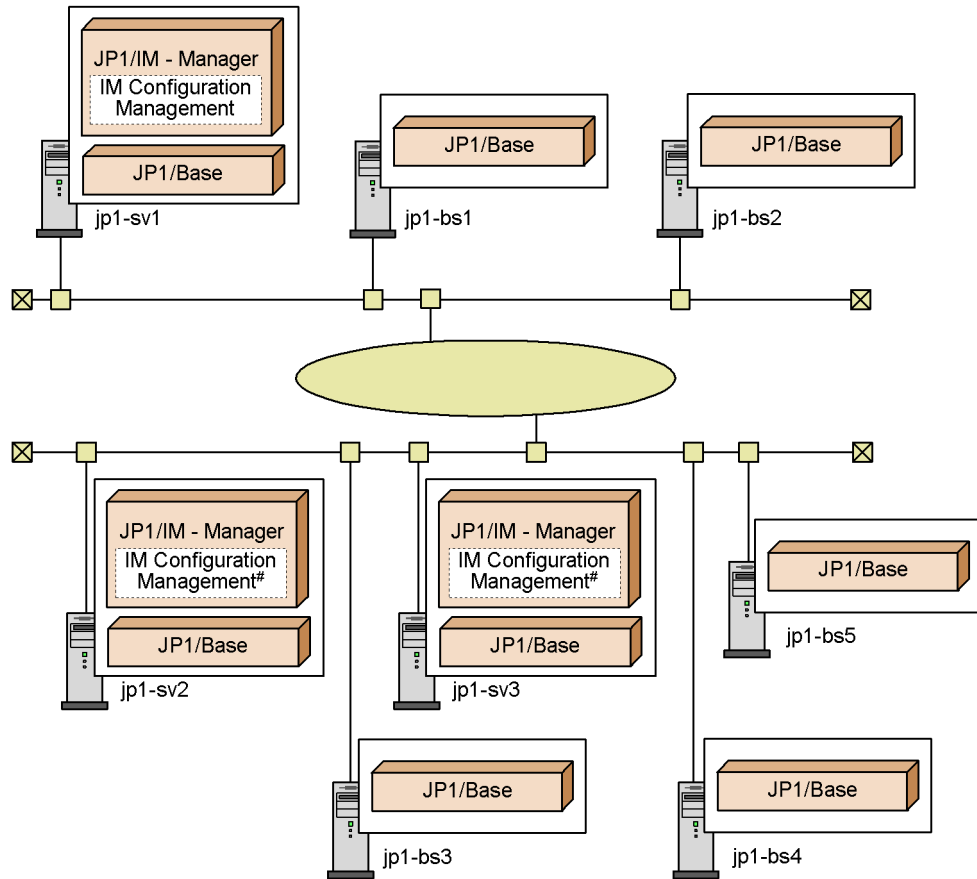
Defining the system hierarchy in IM Configuration Management allows you to perform the following operations in JP1/IM:

- Forward JP1 events to a higher-level host
- Execute commands from JP1/IM - View
- Execute automated actions from JP1/IM
- Collect and distribute definition information

In addition, by using IM Configuration Management, you can manage the JP1/Base profiles on the hosts added to the system hierarchy.

The figure below shows an example of defining a system hierarchy using IM Configuration Management.

Figure 6-10: System hierarchy example (physical configuration)



#: Required to use the node as a base manager. Not required for a relay manager.

Two types of 3-tier system configurations can be defined in IM Configuration Management:

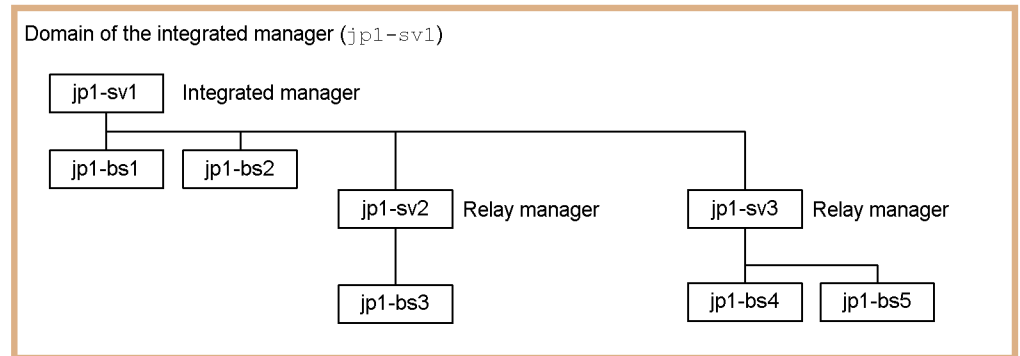
- A configuration where the agents are centrally managed by an integrated manager
- A configuration where the agents are managed by base managers in separate domains

### (1) Centralized management by an integrated manager

In a configuration where the agents in the JP1/IM system are centrally managed by an integrated manager, agent information is collected by relay managers placed in the middle tier.

The relay managers do not provide the IM Configuration Management functionality.

*Figure 6-11:* System hierarchy example (centralized management by an integrated manager)



The table below describes the operations that can be performed from the integrated manager on the hosts in the above configuration example.

*Table 6-5:* Operations that can be performed from the integrated manager (with relay managers in the middle tier)

Target host		Operation			
		View the system configuration	Change the system configuration	View host information	View and change profile information
Integrated manager (jp1-sv1)		Y	Y	Y	Y
Relay manager (jp1-sv2 and jp1-sv3)		Y	Y	Y	Y
Agent	Under the integrated manager (jp1-bs1 and jp1-bs2)	Y	Y	Y	Y
	Under a relay manager (jp1-bs3, jp1-bs4, and jp1-bs5)	Y	Y	Y	Y

Legend:

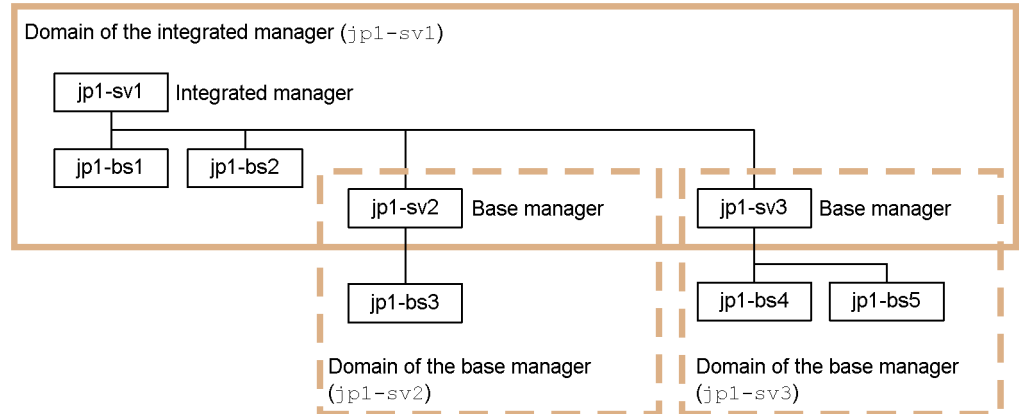
Y: Can be performed.

**(2) Agent management in separate domains**

In a configuration where the agents are managed by base managers in separate domains, base managers are placed in the middle tier.

The base managers provide the IM Configuration Management functionality.

*Figure 6-12: System hierarchy example (agent management in separate domains)*



The table below describes the operations that can be performed from the integrated manager on the hosts in the above configuration example.

*Table 6-6: Operations that can be performed from the integrated manager (with base managers in the middle tier)*

Target host		Operation			
		View the system configuration	Change the system configuration	View host information	View and change profile information
Integrated manager (jp1-sv1)		Y	Y	Y	Y
Base manager (jp1-sv2 and jp1-sv3)		Y	Y	Y	Y
Agent	Under the integrated manager (jp1-bs1 and jp1-bs2)	Y	Y	Y	Y

Target host		Operation			
		View the system configuration	Change the system configuration	View host information	View and change profile information
	Under a base manager (jp1-bs3, jp1-bs4, and jp1-bs5)	Y	N	N	N

Legend:

Y: Can be performed.

N: Cannot be performed.

The table below describes the operations that can be performed from a base manager on the hosts in the configuration example shown in Figure 6-12 *System hierarchy example (agent management in separate domains)*.

*Table 6-7: Operations that can be performed from a base manager (base managers in the middle tier)*

Target host		Operation			
		View the system configuration	Change the system configuration	View host information	View and change profile information
Integrated manager (JP1-sv1)		Y <sup>#</sup>	N	N	N
Base manager (local host)		Y	Y	Y	Y
Base manager (remote host)		N	N	N	N
Agent	Under the integrated manager (jp1-bs1 and jp1-bs2)	N	N	N	N
	Under a base manager (local host)	Y	Y	Y	Y
	Under a base manager (remote host)	N	N	N	N

Legend:

Y: Can be performed.

N: Cannot be performed.

#

Viewable only when the integrated manager is a level above the base managers.

### 6.2.2 Acquiring the system hierarchy

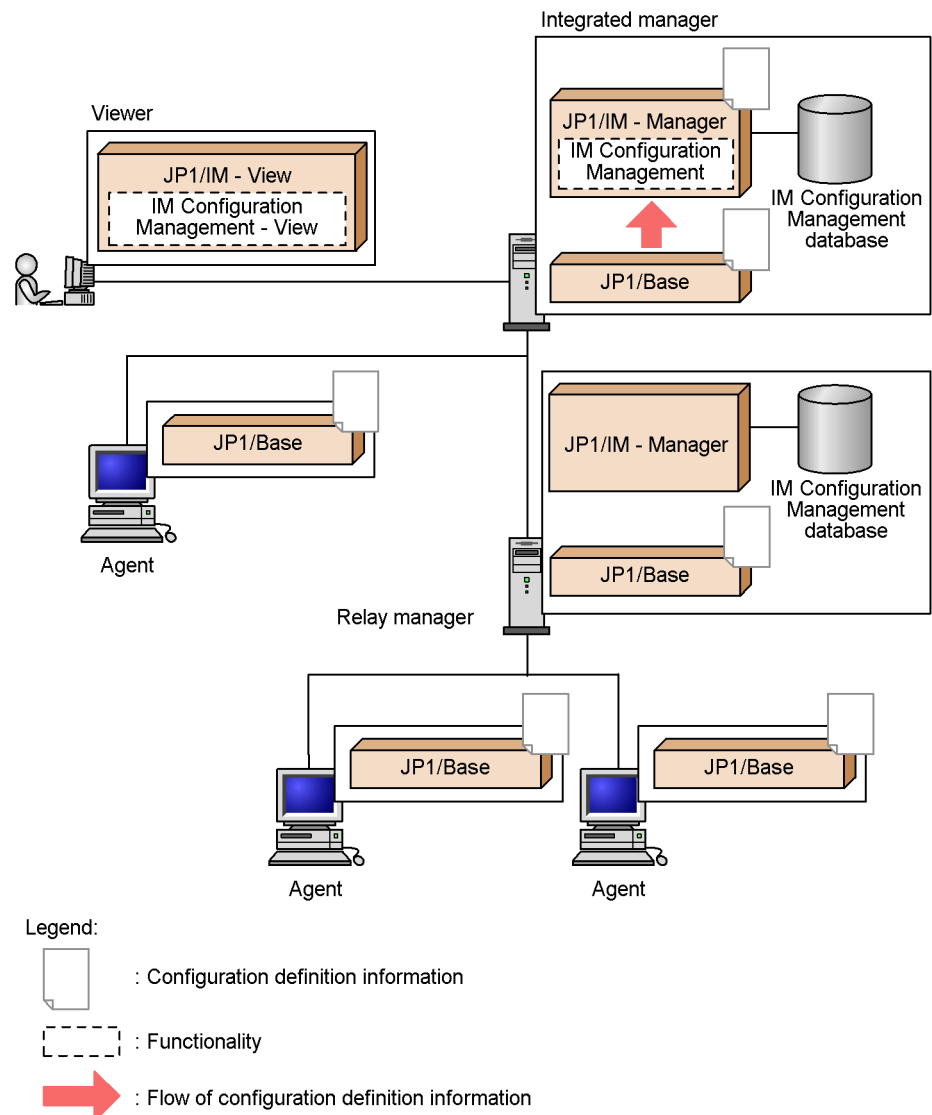
You can collect the system hierarchy definitions (configuration definition information) held by JP1/Base on the manager running IM Configuration Management and register them as configuration definition information in the manager's IM Configuration Management database.

Acquire the system hierarchy on the configuration definition information on the **IM Configuration** page of the IM Configuration Management window.

The figure below shows the flow of processing when acquiring the system hierarchy with IM Configuration Management.



Figure 6-13: Acquiring the system hierarchy with IM Configuration Management



Acquire the system hierarchy when it has been changed, other than by using IM Configuration Management, as in the following situations:

- When IM Configuration Management is deployed in an existing JP1/IM system
- When the system hierarchy is altered by executing the `jbsrt_distrib`

command on the manager running IM Configuration Management

The configuration definition information held in the IM Configuration Management database is updated when the system hierarchy is acquired. If you want to save the existing information before it is updated, you must export it in advance on the manager running IM Configuration Management.

After the acquisition, the system hierarchy is displayed as follows in IM Configuration Management:

- Any unregistered hosts included in the acquired information are automatically registered in the IM Configuration Management database. No host information is acquired for these hosts, however. Instead, you must collect the information manually on the **Host List** page or **IM Configuration** page of the IM Configuration Management window.

If duplicated host names exist in the acquired information, an error message appears and the acquired information is not applied in the configuration definition information held in the IM Configuration Management database.

Make sure no hosts with the same host name exist in the configuration definition information.

- Acquired information containing duplicated host names is discarded and the IM configuration tree appears grayed on the **IM Configuration** page.
- If the acquired information differs from the information in the IM Configuration Management database, the affected host is represented by an error-status icon in the tree display area of the **IM Configuration** page.
- If the configuration definition information held by JP1/Base on the manager running IM Configuration Management has been deleted, the following message appears: IM configuration does not exist. Do you want to reflect to the IM configuration maintained in server?

Click the **Yes** button to erase the deleted information from the IM Configuration Management database. Click the **No** button to keep the deleted information. This will make the system hierarchy appear grayed on the **IM Configuration** page.

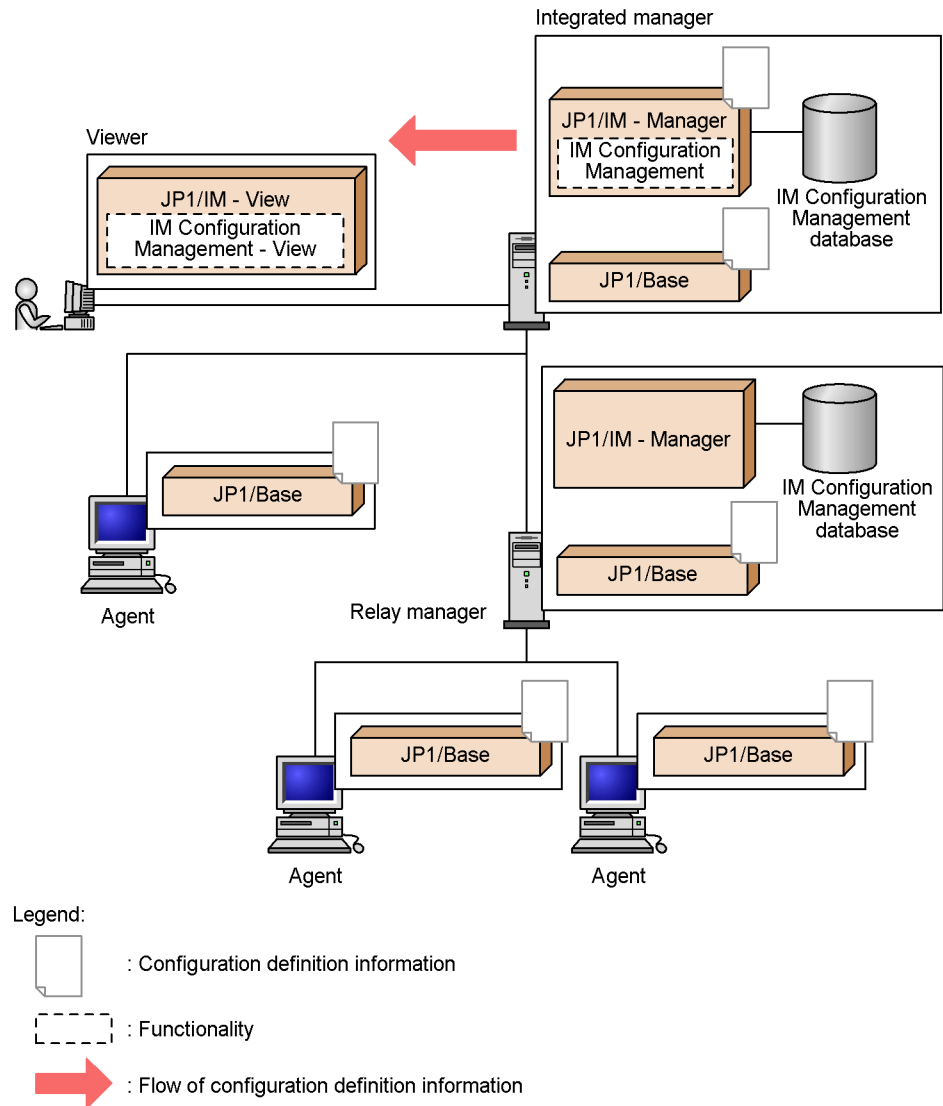
When IM Configuration Management starts, configuration definition information is acquired automatically so that the information held by JP1/Base on the manager running IM Configuration Management can be checked for consistency with the definitions in the IM Configuration Management database.

### 6.2.3 Displaying the system hierarchy

Using IM Configuration Management, you can display the configuration definition information held in the IM Configuration Management database. The information appears on the **IM Configuration** page of the IM Configuration Management window.

The figure below shows the flow of processing when displaying the system hierarchy with IM Configuration Management.

*Figure 6-14:* Displaying the system hierarchy with IM Configuration Management



#### 6.2.4 Verifying the system hierarchy

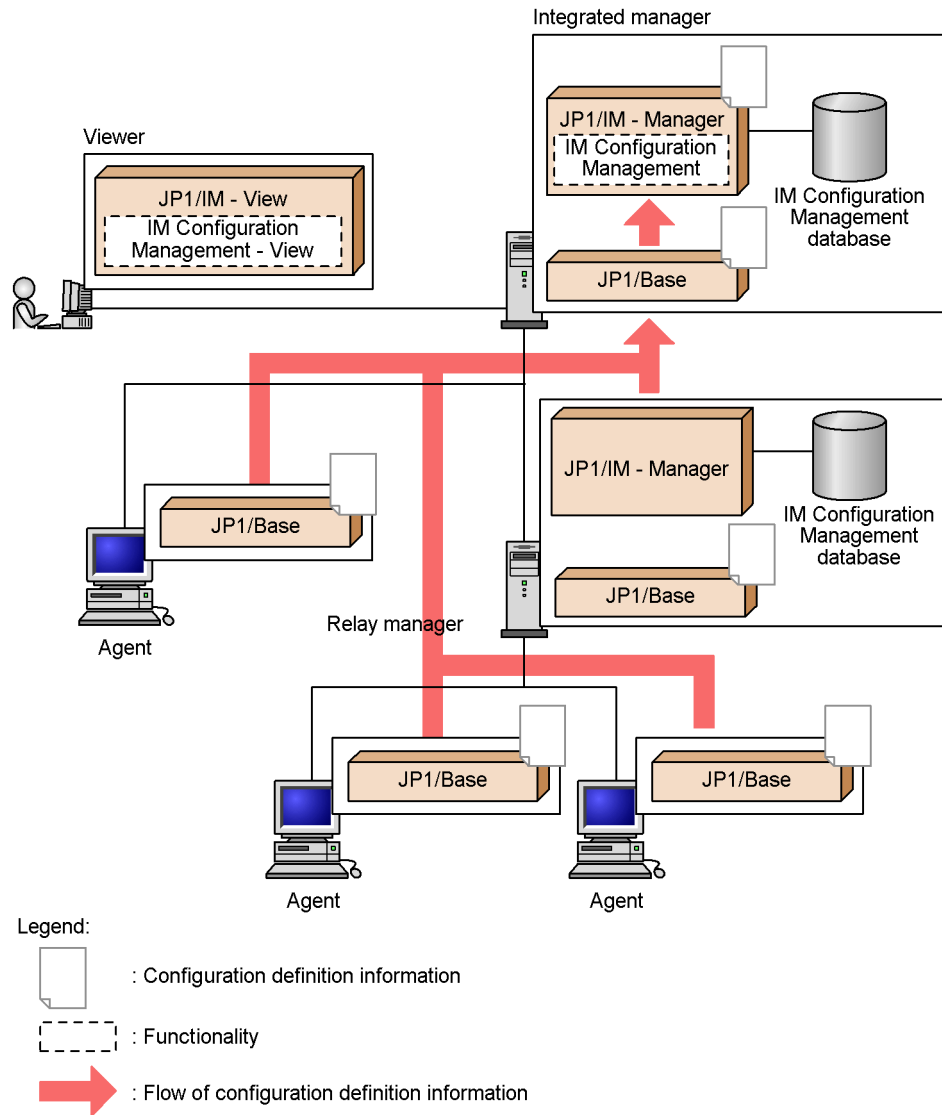
Using IM Configuration Management, you can check whether the configuration definition information held by JP1/Base on each of the hosts in the JP1/IM system

matches the information in the IM Configuration Management database.

Verify the system hierarchy on the **IM Configuration** page of the IM Configuration Management window.

The figure below shows the flow of processing when verifying the system hierarchy with IM Configuration Management.

*Figure 6-15: Verifying the system hierarchy with IM Configuration Management*



The table below describes the range of hosts whose system configuration information you can verify from the integrated manager.

*Table 6-8:* Range of hosts whose system configuration information can be verified from the integrated manager

Host type		Verify
Local host		Y
Relay manager		Y
Base manager		Y
Agent	Directly under the local host	Y
	Under a relay manager	Y
	Under a base manager	N <sup>#</sup>

Legend:

Y: The information can be verified.

N: The information cannot be verified.

#

An agent under a base manager might not be reachable from the integrated manager if it is behind a firewall. For this type of agent, verify the configuration definition information from the base manager.

The table below describes the range of hosts whose system configuration information you can verify from a base manager.

*Table 6-9:* Range of hosts whose system configuration information can be verified from a base manager

Host type		Verify
Local host		Y
Parent host		N
Relay manager		Y <sup>#1</sup>
Base manager		Y <sup>#1</sup>
Agent	Directly under the local host	Y <sup>#1</sup>
	Under a relay manager	Y <sup>#1</sup>

Host type		Verify
	Under a lower-level base manager	N <sup>#2</sup>

Legend:

Y: The information can be verified.

N: The information cannot be verified.

#1

Not recommended because the system configuration, including the integrated manager, would be more than three tiers.

#2

An agent under a lower-level base manager might not be reachable from the integrated manager if it is behind a firewall. For this type of agent, verify the configuration definition information from the lower-level base manager.

You can check the verification results in the following windows:

- **Host List** page or **IM Configuration** page of the IM Configuration Management window
- Execution Results window

If the information held by JP1/Base on the manager running IM Configuration Management differs from the information in the IM Configuration Management database, the affected hosts are represented by error-status icons in the tree display area of the **IM Configuration** page.

If verification fails, an error-status icon is displayed for the affected host in the tree display area of the **IM Configuration** page.

Configuration definition information cannot be verified on hosts running a version of JP1/Base earlier than version 9. In this case, the affected hosts are represented by error-status icons in the tree display area of the **IM Configuration** page.

If no configuration definition information exists on the manager, or if the information is corrupted, manager verification generates an error and the processing is canceled.

### 6.2.5 Editing the system hierarchy

Using IM Configuration Management, you can create and edit configuration definition information by adding, moving, or deleting hosts.

Edit the system hierarchy in the Edit IM Configuration window of IM Configuration Management - View.

The functions for editing the system hierarchy using IM Configuration Management

are described next.

### **(1) Obtaining update rights**

To edit the system hierarchy, you must have update rights to the configuration definition information. This prevents anyone else from editing the information, using IM Configuration Management - View on another host, while you are doing so.

To obtain update rights to the configuration definition information, in the Edit IM Configuration window select the **Acquire update right** check box.

If you attempt to obtain update rights while IM Configuration Management - View on another host has exclusive rights to the configuration definition information and profiles, an error message appears and the attempt fails. In this case, you must find out which user has exclusive rights in the Login User List window and revoke those rights.

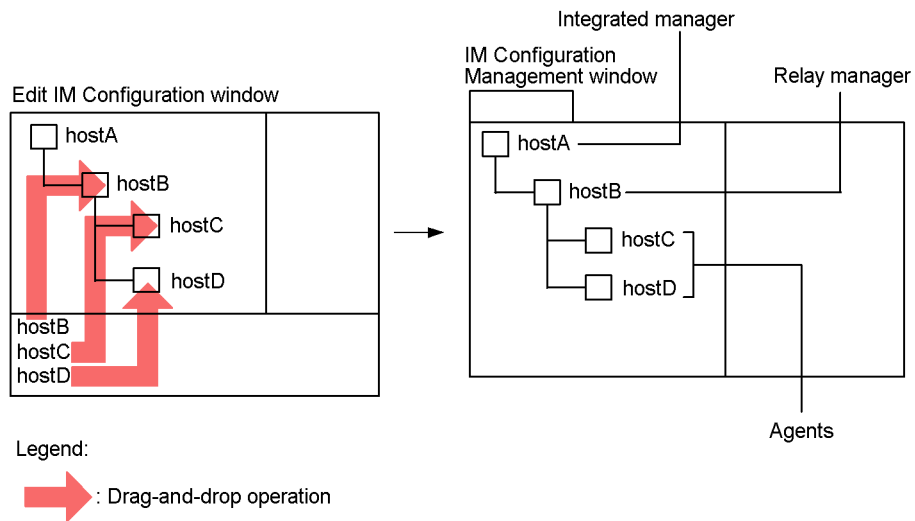
### **(2) Adding hosts**

You can add hosts to the system hierarchy by performing either of the following operations in the Edit IM Configuration window:

- Select a host in the **Host List**, and then move it to the tree display area by drag-and-drop operation.
- Select a host in the tree display area, and then choose **Edit** and **Add Host**.

When you define a 3-tier configuration in the tree display area of the Edit IM Configuration window and apply the configuration to the system hierarchy, the managers defined in the middle tier will be displayed as relay managers in the tree display area of the **IM Configuration** page of the IM Configuration Management window.

*Figure 6-16:* Adding hosts to the system hierarchy with IM Configuration Management



### (3) Moving hosts

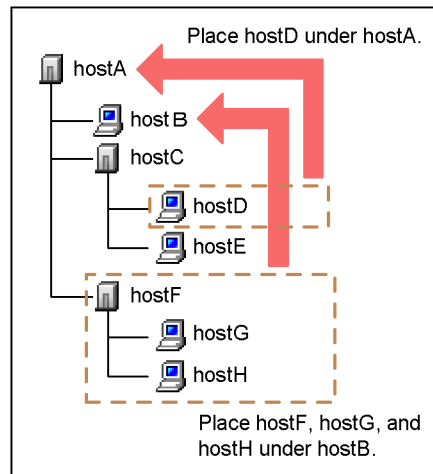
You can move hosts to another level in the system hierarchy by performing either of the following operations in the Edit IM Configuration window:

- Select a host in the tree display area, and then move it to another level by drag-and-drop operation.
- Select a host in the tree display area and choose **Edit** and **Cut**. Then select a higher-level host to place the selected host under, and choose **Edit** and **Paste**.


When you move a relay manager, the agents in its domain are also moved.



*Figure 6-17: Moving a host in the system hierarchy with IM Configuration Management*



Legend:

 : Drag-and-drop operation

The following table describes the types of higher-level hosts you can specify for each type of target host.

*Table 6-10: Types of higher-level hosts that can be specified when moving a target host*

Target host	Specifiable higher-level host	Moved hosts
Integrated manager	--	--
Base manager	<ul style="list-style-type: none"> <li>Integrated manager</li> <li>Relay manager</li> </ul>	The selected base manager
Relay manager	<ul style="list-style-type: none"> <li>Integrated manager</li> <li>Relay manager</li> </ul>	The selected relay manager and the agents in its domain
Agent	<ul style="list-style-type: none"> <li>Integrated manager</li> <li>Relay manager</li> </ul>	The selected agent

Legend:

--: Cannot be moved.

#### **(4) Deleting hosts**

You can delete hosts from the system hierarchy by performing either of the following operations in the Edit IM Configuration window:

- Select a host in the tree display area, and then move it the **Host List** by drag-and-drop operation.
- Select a host in the tree display area, and then choose **Edit** and **Delete Host**.

When you delete a base manager or relay manager, the agents in its domain are also deleted from the system hierarchy. An integrated manager cannot be deleted.

If you want to delete the entire system hierarchy, choose **File** and then **New**.

#### **(5) Saving edited information**

You can save edited configuration definition information in a configuration definition file (`jbs_route.conf`) on the host where IM Configuration Management - View is active. To do so, choose **File** and then **Save IM Configuration** in the Edit IM Configuration window.

Use the **Save** command to temporarily save a system hierarchy you are creating, or to manage records of a system configuration.

#### **(6) Loading the system hierarchy**

You can load the following configuration definition information in the Edit IM Configuration window:

- Information in the IM Configuration Management database

In the Edit IM Configuration window, choose **File** and then **Acquire IM Configuration from Server** to load the configuration definition information held in the IM Configuration Management database.

- Information on the IM Configuration Management - View host

In the Edit IM Configuration window, choose **File** and then **Open IM Configuration** to load configuration definition information as a configuration definition file (`jbs_route.conf`) on the host where IM Configuration Management - View is active.

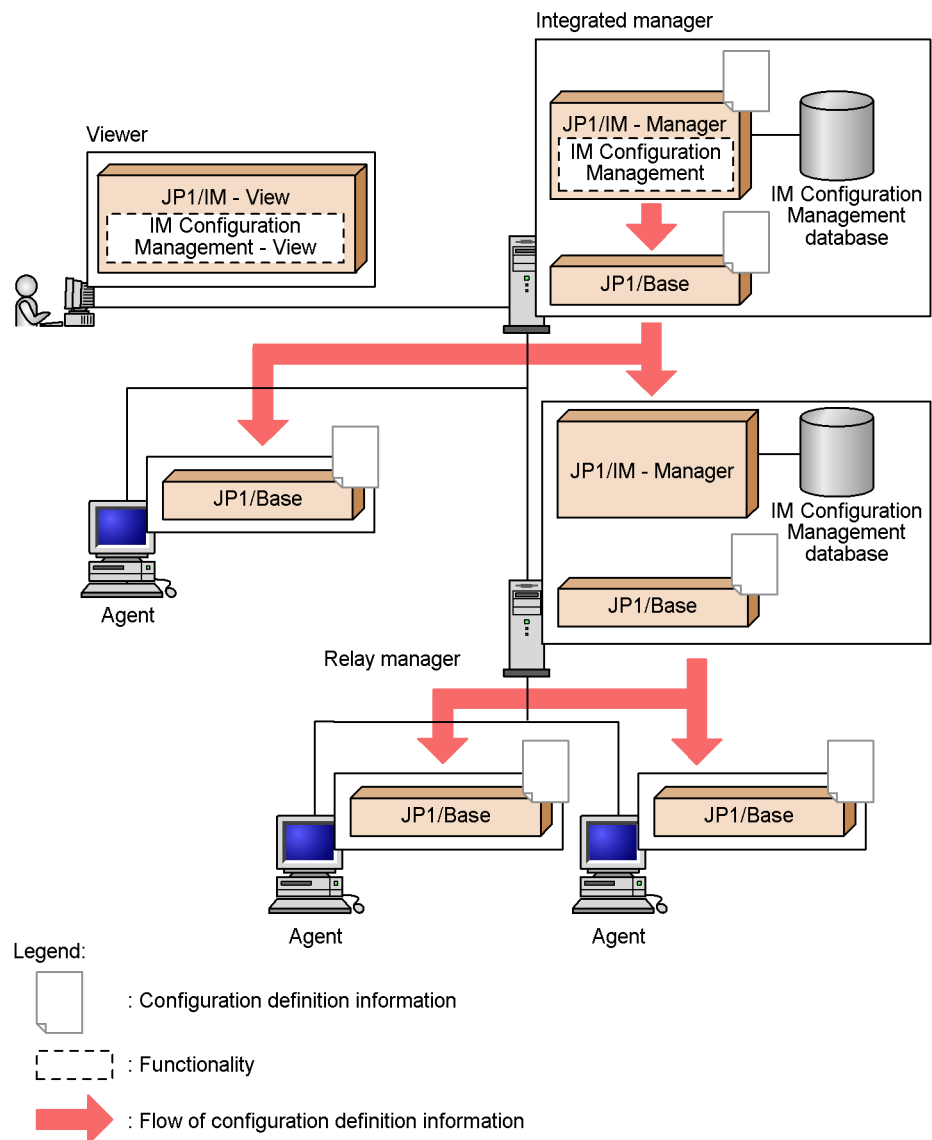
### **6.2.6 Applying the system hierarchy**

Using IM Configuration Management, you can apply edited configuration definition information to all the hosts in the system hierarchy.

To apply configuration definition information, use the Edit IM Configuration window.

The figure below shows the flow of processing when applying configuration definition information with IM Configuration Management.

Figure 6-18: Applying configuration definition information with IM Configuration Management



When you apply configuration definition information, the `jbsrt_distrib` command is executed on the manager running IM Configuration Management. This command first deletes the information on all the hosts in the system, and then distributes the edited information to the hosts.

The applied information replaces the existing information in the configuration definition file (`jbs_route.conf`) on the host running IM Configuration Management. If you want to save the file contents before they are replaced, you must take a backup by saving the file under another name or by other means.

If processing fails for any host, its host name is displayed in a dialog box.

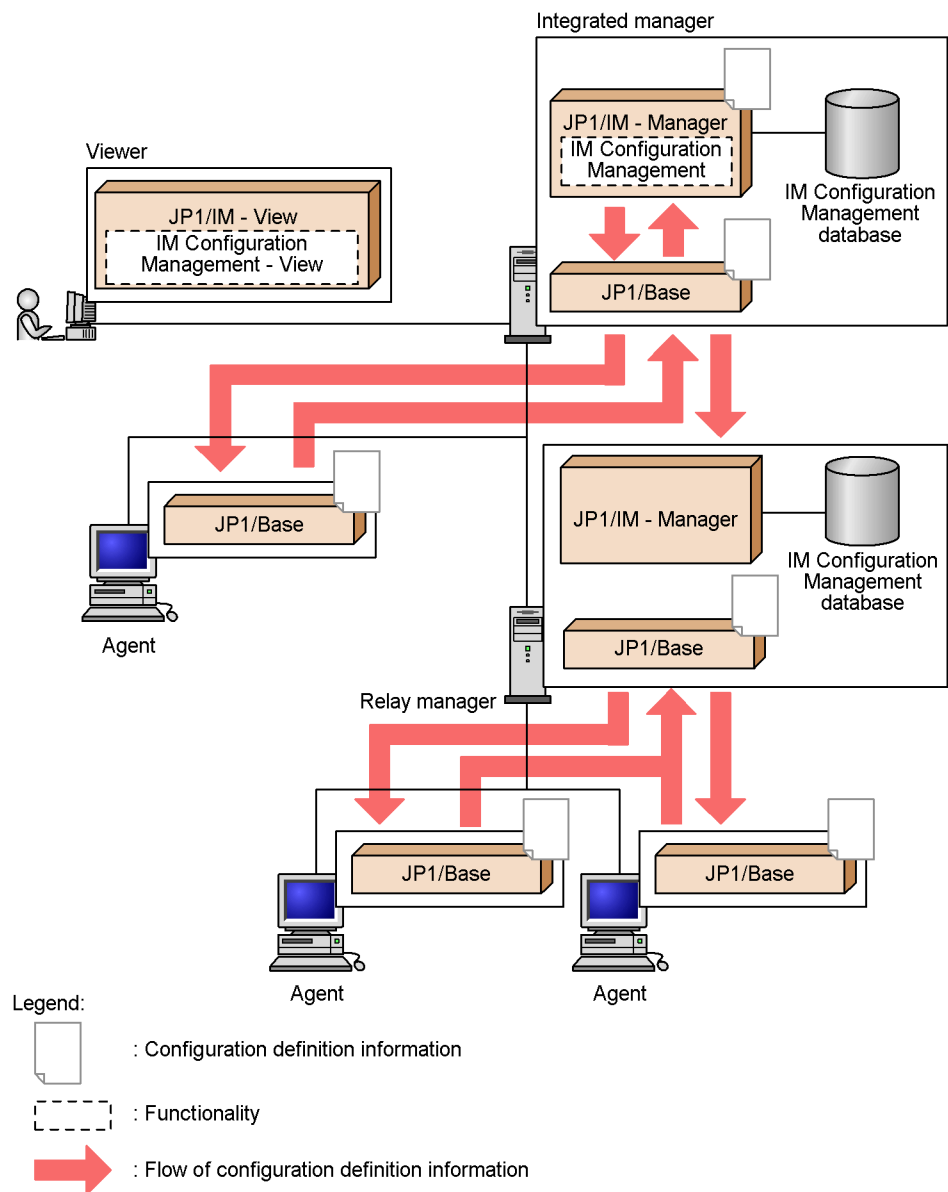
The result of applying a system hierarchy are shown in a dialog box. Also, you can check the new system hierarchy on the **IM Configuration** page of the IM Configuration Management window. If processing failed, the affected host is represented by an error-status icon in the tree display area of the **IM Configuration** page. To view further details, click the **Basic Information** button in the node display area of the **IM Configuration** page.

### 6.2.7 Synchronizing the system hierarchy

Configuration definition information must be synchronized between the integrated manager and base managers if information was defined separately on each manager system in IM Configuration Management. Perform the synchronization from the integrated manager.

To synchronize information among the systems, use the **Host List** page or **IM Configuration** page of the IM Configuration Management window.

Figure 6-19: Synchronizing configuration definition information with IM Configuration Management



When you synchronize configuration definition information, the `jbsrt_sync` command is executed on the integrated manager. This command collects and synchronizes the information on the integrated manager, and then updates the

configuration definition information on all the hosts in the system hierarchy.

If no base managers are defined under the integrated manager, an error message is displayed and the system hierarchy is not synchronized among the hosts.

---

## 6.3 Profile management

---

Using IM Configuration Management - View, you can centrally manage the JP1/Base profiles on the hosts in the system hierarchy.

To manage profiles with IM Configuration Management, the hosts must be added to the system hierarchy and JP1/Base must be active on each host.

This section describes the profiles you can manage by using IM Configuration Management, and the functionality provided for this purpose.

### 6.3.1 Types of profiles that can be managed

Using IM Configuration Management, you can manage the profiles set in JP1/Base on the hosts in the system hierarchy.

You can manage the following JP1/Base profiles:

- Valid configuration information

The settings information that is currently valid in JP1/Base (read from a configuration file at startup of the JP1/Base service). To manage this information, JP1/Base on the target host must be version 9.

- Configuration file contents

The information set in a profile configuration file in JP1/Base. This information will differ from the valid configuration information if you made any changes to the configuration file after startup of the JP1/Base service but did not apply the edited file contents.

Using IM Configuration Management, you can manage profiles in JP1/Base version 7 or later.

Profile management can be used for the following purposes:

- To check the status of the hosts on a routine basis or in the event of an error
- To change a profile during a system upgrade or maintenance
- To apply the contents of a profile to the JP1/Base profiles on other hosts

The table below describes the types of profiles you can manage with IM Configuration Management.

*Table 6-11:* Types of profiles that can be managed with IM Configuration Management

Profile type	Description
Event Forwarding	Profile about the functionality for forwarding JP1 events to a higher-level host in accordance with the system hierarchy.
Log File Trapping	Profile about the functionality for converting information output to a log file by an application program into JP1 events. Configuration files cannot have identical file names. A different file name must be assigned to the configuration file for each process, even when the files are stored in different directories.
Event Log Trapping	Profile about the functionality for converting Windows events into JP1 events.
Local Action <sup>#1</sup>	Profile about actions executed on an agent without going through a manager.
Authentication Server <sup>#1</sup>	Profile about the server for centrally managing the users of a system configured in JP1/IM or JP1/AJS.
JP1 User-Permissions Level <sup>#1, #2</sup>	Profile about the permission levels of JP1 users (users of a JP1 system such as JP1/IM or JP1/AJS).
Registered JP1 Users <sup>#1, #2</sup>	Profile about the list of JP1 users.
OS User Mapping <sup>#1, #2</sup>	Profile about the mapping between OS users who have permission to execute jobs and commands and JP1 users.

#1

Only information in JP1/Base version 9 can be managed.

#2

If the local host is used as the authentication server, information can be displayed only when the service of the authentication server is active.

If the local host is used as the authentication server, the display area appears grayed when the service of the authentication server is stopped.

The profiles in JP1/Base version 9 that can be managed by IM Configuration Management are the contents of configuration files stored in each host's `conf` directory. Configuration files located in other directories, such as those for log file trapping, cannot be managed by IM Configuration Management. If you want to include such files in the profile management functionality, you must move them to the



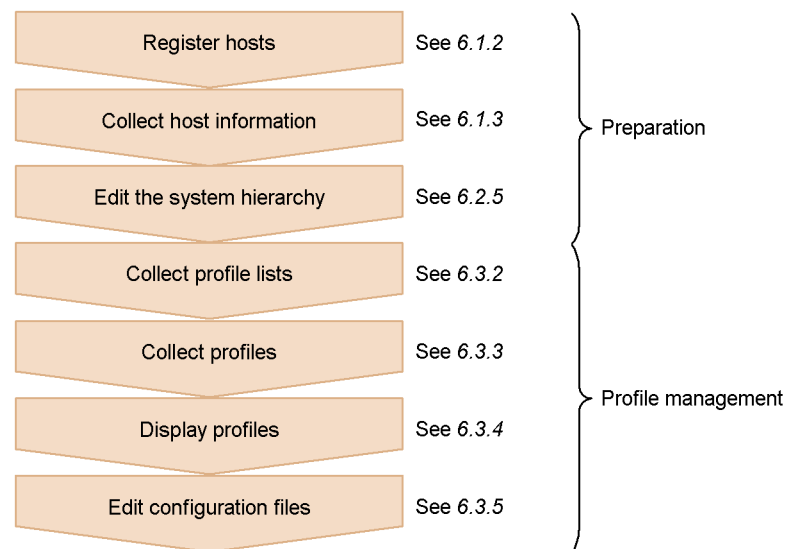
`conf` directory.

IM Configuration Management manages JP1/Base event log traps and log file traps on a physical host basis, not on a logical host basis. To display or edit profiles about event log traps or log file traps in a logical host, you must do so on a physical host basis, identifying the physical host associated with the logical host.

All valid configuration information can be displayed, however, even for services that start with a configuration file located in a directory other than the `conf` directory. From the displayed information you can find out whether a service's configuration file is located in the `conf` directory.

The figure below shows the flow of operations required to manage profiles with IM Configuration Management.

*Figure 6-20:* Flow of operations for managing profiles with IM Configuration Management



Profiles on a host whose host name is defined by its IP address in the IM Configuration Management database cannot be managed using IM Configuration Management. Operations attempted on a target host defined in this way might result in the following message: Profile management failed because the host name is defined with IP address. Please define real host name. This message appears when you perform any of the following operations on a host defined by its IP address:

- Open the Display/Edit Profiles window.
- Collect profiles as a batch operation in the IM Configuration Management window.

You cannot collect profiles from hosts defined by their IP addresses, but processing succeeds for the other hosts.

- Apply profiles as a batch operation in the IM Configuration Management window.

You cannot apply profiles to hosts defined by their IP addresses, but processing succeeds for the other hosts.

### 6.3.2 Collecting profile lists

Using IM Configuration Management, you can collect a list of profiles (hereafter, *profile list*) from each host.

The collected profile list appears in the tree display area of the Display/Edit Profiles window.

If the service for which the profile is set (event log trapping service, event service, and so on) is inactive on a target host, the collected profile list is displayed as follows:

- In the tree display area of the Display/Edit Profiles window, profiles from the host where the service is inactive appear grayed and cannot be selected in the profile list.
- In the node display area of the Display/Edit Profiles window, the configuration file's **Collection status** remains unchanged.
- When you click the **Basic Information** button in the node display area of the **Host List** page or **IM Configuration** page of the IM Configuration Management window, the profile collection status is shown as **Collected**.

The service for local actions is inactive by default because there is no configuration file (`jbslact.conf`) in the host. As a result, when you collect a profile list in the Display/Edit Profiles window, the KNAN20333-I message is displayed and **Collected** appears as the **Collection status** in the node display area.

You can start the service for local actions by creating a configuration file (`jbslact.conf`) and applying it to the host in question.

For details about creating a configuration file (`jbslact.conf`) and applying it to a host, see 3.3.5(2) *Applying edited information in configuration files to individual hosts* in the *Job Management Partner 1/Integrated Management - Manager Configuration Guide*.

To create or update the profile list for a host, perform either of the following:

- In the tree display area of the Display/Edit Profiles window, click the JP1 product name (**JP1/Base**) and then choose **Operation** and **Rebuild Profile Tree**.
- In the tree display area of the Display/Edit Profiles window, right-click the JP1 product name (**JP1/Base**) and then choose **Rebuild Profile Tree**.

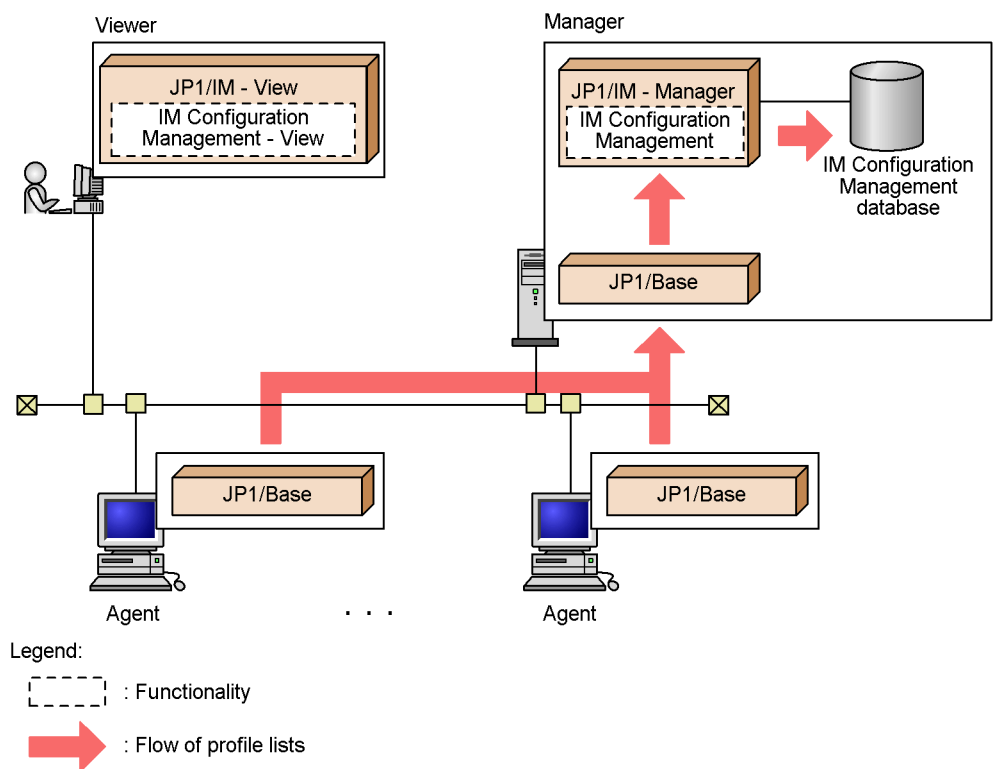
If the IM Configuration Management database does not contain a profile list for a particular host, performing either of the following operations will generate a profile list or update the system hierarchy:

- Open the Display/Edit Profiles window.
- On the **Host List** page or **IM Configuration** page of the IM Configuration Management window, choose **Operation** and **Batch Collect Profiles**.

When a host is restarted, or when JP1/Base is restarted on a host, you must update the profile lists. In the Display/Edit Profiles window, choose **Operation** and **Rebuild Profile Tree**.

The figure below shows the flow of processing when collecting profile lists with IM Configuration Management.

Figure 6-21: Collecting profile lists with IM Configuration Management



If a host is deleted from the system hierarchy or is no longer managed by IM Configuration Management, the profile list collected from that host is deleted. Profile lists are also deleted when you perform any of the following operations:

- Collect host information on the **Host List** page or **IM Configuration** page of the IM Configuration Management window.
- Apply new or edited configuration definition information in the Edit IM Configuration window.
- Import configuration definition information on the manager running IM Configuration Management.

The following table describes the profile lists you can collect for each version of JP1/Base on the target host.

*Table 6-12:* Profile lists that can be collected by JP1/Base version

JP1/Base version	Profile type	Description
Versions 7 and 8	Event Forwarding	--
	Log File Trapping	--
	Event Log Trapping	Can be collected from a Windows host only.
Version 9	Event Forwarding	--
	Log File Trapping	Multiple profile configuration files can be collected. <sup>#</sup>
	Event Log Trapping	--
	Local Action	--
	Authentication Server	Limited to display of valid configuration information.
	JP1 User-Permissions Level	<ul style="list-style-type: none"> <li>• Limited to display of valid configuration information.</li> <li>• Supported only for an authentication server on the local host.</li> </ul>
	Registered JP1 Users	<ul style="list-style-type: none"> <li>• Limited to display of valid configuration information.</li> <li>• Supported only for an authentication server on the local host.</li> </ul>
	OS User Mapping	Limited to display of valid configuration information.

Legend:

--: Not applicable.

#

A maximum of 100 profile configuration files for log file trapping can be collected from JP1/Base on each host.

When a host is restarted, or when JP1/Base is restarted on a host, you must update the host's profile list.

You must also update the profile list in the following cases:

- When changes are made to the index file for the event forwarding settings on a host

Unless you update the profile list, the contents of the superceded configuration file will be displayed, or an error message will appear, when you collect the host's configuration file.

- When the service for which the profile is set (event log trapping service, event service, and so on) starts or stops on the host

Unless you update the profile list, the following problems occur:

- An error message appears when you display valid configuration information, or when you collect or apply configuration files.
- In the tree display area of the Display/Edit Profiles window, the profiles that you want to view appear grayed in the profile list.
- When log file trapping starts or stops on the host, an error message appears when you display valid configuration information, or when you collect or apply configuration files.

### 6.3.3 Collecting profiles

Using IM Configuration Management, you can collect valid configuration information and configuration files from the hosts.

Collect this information in the Display/Edit Profiles window.

#### (1) *Collecting valid configuration information*

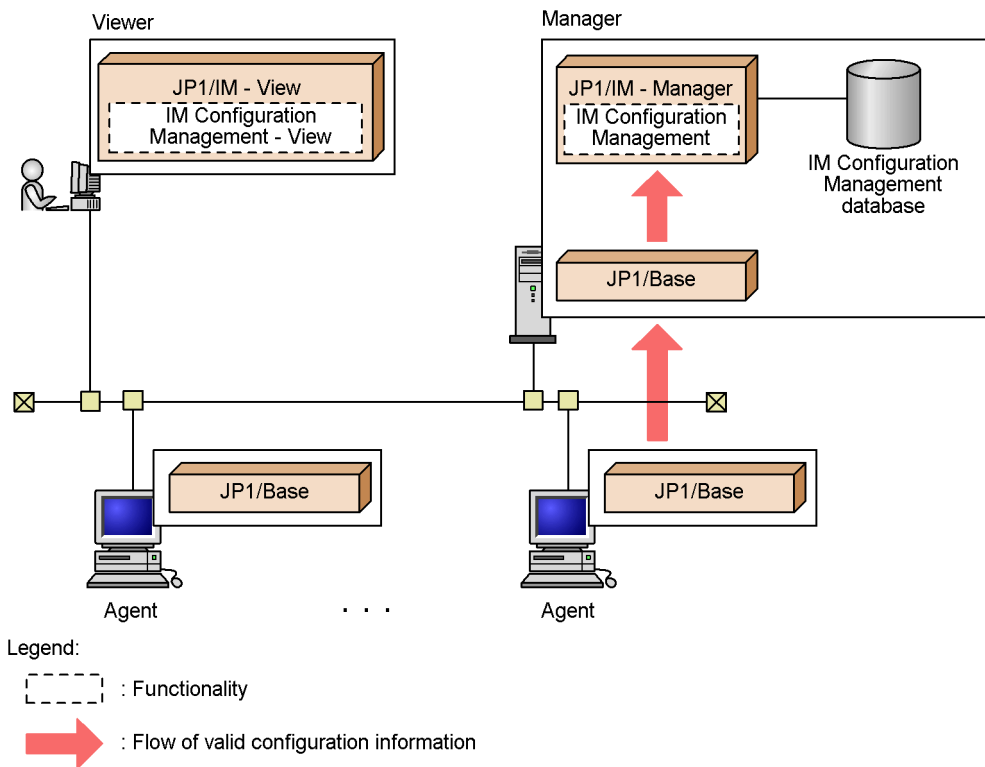
Valid configuration information can be collected from hosts running JP1/Base version 9.

To collect valid configuration information:

1. Open the Display/Edit Profiles window.
2. In the tree display area, select a profile.
3. Click the **Valid Configuration Information** button.

The figure below shows the flow of processing when collecting valid configuration information with IM Configuration Management.

*Figure 6-22: Collecting valid configuration information with IM Configuration Management*



If collection fails, the possible causes are as follows:

*Table 6-13: Causes of failures to obtain valid configuration information*

Status	Cause	Action
No valid configuration information could be obtained in the event forwarding, from the forwarding filter entry onward.	The possible cause is that a higher-level host is set in the forwarding setting file ( <code>forward</code> ) as the destination host for forwarded events, but no higher-level host exists for the source host in the system hierarchy.	Check whether the system hierarchy is correct.

Status	Cause	Action
No valid configuration information could be obtained in the log file trapping.	The process ID might have changed when log file trapping was restarted on the host, resulting in a mismatch with the process ID managed by IM Configuration Management. The process ID changes each time log file trapping starts.	Update the profile list: In the tree display area of the Display/Edit Profiles window, click the JP1 product name ( <b>JP1/Base</b> ) and then choose <b>Operation</b> and <b>Rebuild Profile Tree</b> .
No valid configuration information could be obtained in the JP1 user-permissions level or Registered JP1 Users.	The local host might not be acting as the authentication server.	Check whether the authentication service is active on the local host.
Other status	The target service might be inactive on the host.	Execute the <code>jbs_spmc_status</code> command to check whether the service started successfully. Alternatively, in a Windows system, check the service status from the Computer Management window.

## (2) Collecting configuration files per host

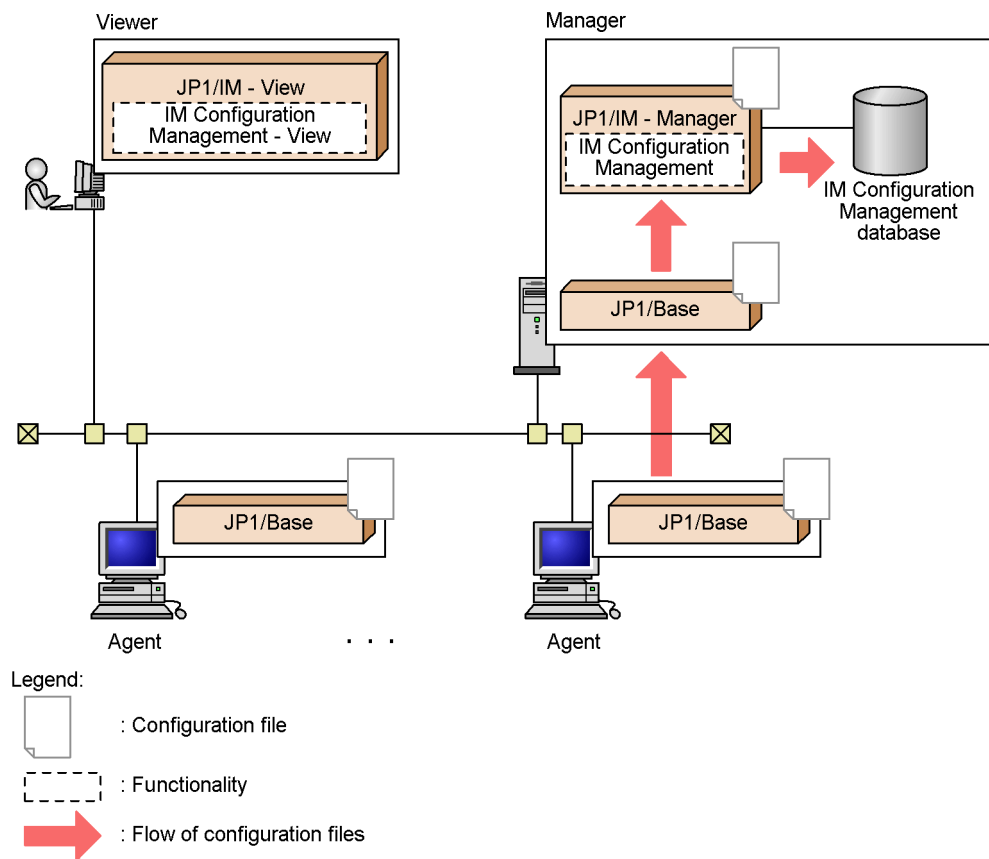
Profile configuration files can be collected from hosts running JP1/Base version 9.

To collect configuration files from a host, perform either of the following:

- In the Display/Edit Profiles window, make sure the **Exclusive Editing Settings** command is checked in the **Edit** menu, or look at the icons in the tree display area to make sure you have exclusive editing rights to the profiles on the target host. Then choose **Operation** and **Collect Profiles**.
- In the IM Configuration Management window, choose **Operation** and **Batch Collect Profiles**.

The figure below shows the flow of processing when collecting configuration files from a host with IM Configuration Management.

*Figure 6-23: Collecting configuration files with IM Configuration Management (per host)*



The table below describes the configuration files you can collect per host.

*Table 6-14: Configuration files that can be collected per host*

Profile type	Configuration file	Notes
Event Forwarding	Event forwarding setting file ( <i>forward</i> )	Files such as the event server index file ( <i>index</i> ) and event server settings file ( <i>conf</i> ) are not collected.



Profile type	Configuration file	Notes
Log File Trapping	Action definition file for log file trapping (any file) <sup>#1, #2</sup>	You must restart the service if you edited parameters other than MARKSTRS and ACTDEFS, or if the start command has been changed. If the number of files collected during batch collection exceeds the maximum number of log file traps that can be managed, a message appears and batch collection is canceled.
Event Log Trapping	Action definition file for event log trapping (ntevent.conf) <sup>#2</sup>	Collected only from a Windows host. The event server name (server) cannot be edited.
Local Action	Local action execution definition file (jbslact.conf)	--

Legend:

--: Not applicable.

#1

Of the currently valid log file trapping profiles on the host, IM Configuration Management collects only the configuration files in the `conf` directory.

#2

JP1/Base event log traps and log file traps cannot be activated on a logical host basis. To manage trap information in a Display/Edit Profiles window connected to the logical host, the physical host corresponding to the logical host must be placed in the same system hierarchy as the logical host.

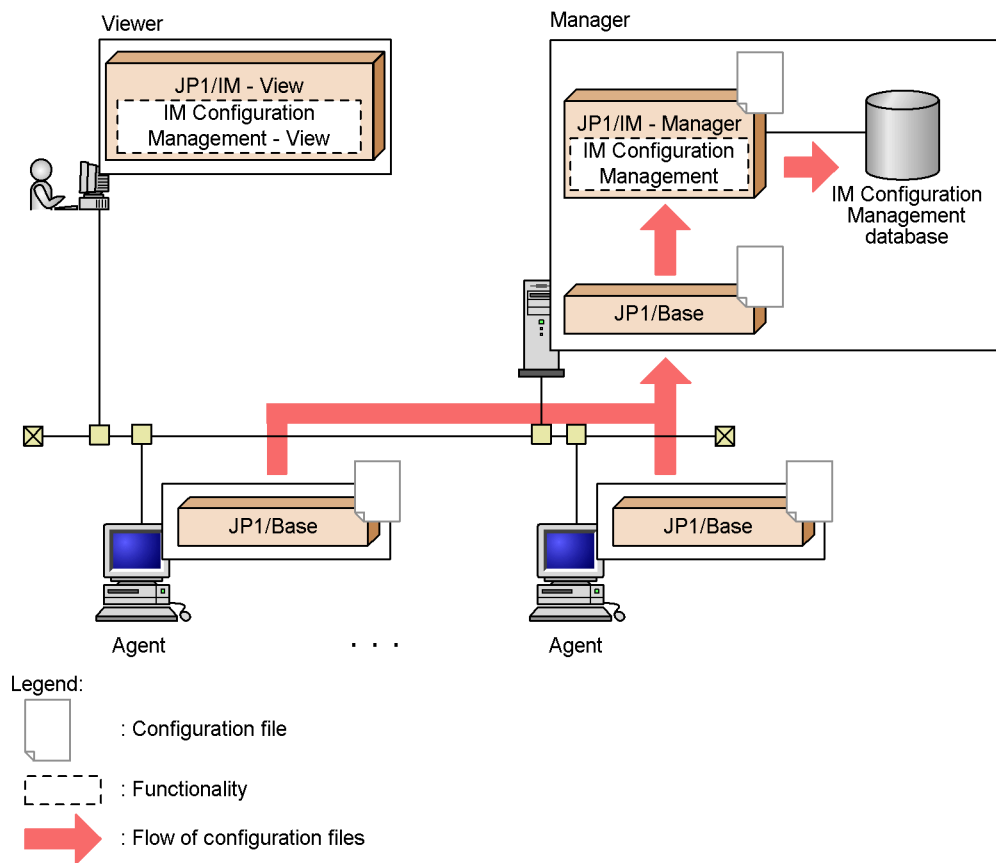
### (3) **Batch-collecting configuration files**

You can collect profile configuration files from all the hosts in one operation. On the **Host List** page or **IM Configuration** page of the IM Configuration Management window, choose **Operation** and then **Batch Collect Profiles**.

You cannot collect profiles in a batch if another user has exclusive editing rights to any of the configuration files. To obtain these rights, see *6.3.6 Obtaining and releasing exclusive editing rights for a configuration file*.

The figure below shows the flow of processing when collecting configuration files from all hosts as a batch operation with IM Configuration Management.

*Figure 6-24: Collecting configuration files with IM Configuration Management (all hosts)*



The following table describes the configuration files you can collect in a batch for each version of JP1/Base on the target hosts.

*Table 6-15: Configuration files that can be batch-collected by JP1/Base version*

JP1/Base version	Profile type
Earlier than version 9	Event Forwarding
	Log File Trapping
	Event Log Trapping
Version 9	Event Forwarding
	Log File Trapping

JP1/Base version	Profile type
	Event Log Trapping
	Local Action

In the Display/Edit Profiles window, you can check whether all the configuration files were successfully collected. If any file could not be collected, **Configuration file contents** is unavailable and the file status appears in **Status** in the node display area.

On the **IM Configuration** page of the IM Configuration Management window, you can check whether the configuration files were successfully collected from all the hosts. If files could not be collected from any host, an error-status icon is displayed for the affected host in the tree display area. To view further details, click the **Basic Information** button in the node display area.

If batch collection fails for any host, processing continues and the profiles on the other hosts are collected. Also, if the maximum number of profile configuration files for log file trapping is exceeded on a host, a message appears and collection processing is canceled for that host.

At batch collection, the profile list on each host is updated automatically. For this reason, configuration files are not collected for services and processes that were inactive at the time the profile list was updated.

When batch collection is completed, a message to that effect appears.

The following limitations apply to collection of configuration files for log file trapping from a host running JP1/Base version 7 or 8:

- Only one configuration file is collected.
- The action definition file that has the default file name (`jevlog.conf`) and is located in the default location (`conf` directory) is regarded as the valid action definition file for log file trapping.

#### (4) Saving configuration files

Configuration files collected from the hosts, or edited in IM Configuration Management - View, can be saved to the manager running IM Configuration Management.

Configuration files are saved when you perform any of the following operations:

- In the Display/Edit Profiles window, choose **Operation** and **Collect Profiles** (provided no one has obtained exclusive editing rights to the configuration files).
- On the **Host List** page or **IM Configuration** page of the IM Configuration Management window, choose **Operation** and **Batch Collect Profiles**.
- In the node display area (settings information) of the Display/Edit Profiles

window, select the **Save** check box and then click the **Execute** button.

- In the node display area (settings information) of the Display/Edit Profiles window, select the **Apply** check box and then click the **Execute** button.
- Import configuration definition information on the manager running IM Configuration Management.

IM Configuration Management stores only one configuration file per profile. The saved profile information will be overwritten if the same configuration file is collected by another user before the saved information is applied to the host.

Configuration files that could not be collected during batch collection of profiles from all hosts cannot be saved.

Valid configuration information cannot be saved in IM Configuration Management. Also, the file names and location of files saved by IM Configuration Management cannot be specified by the user.

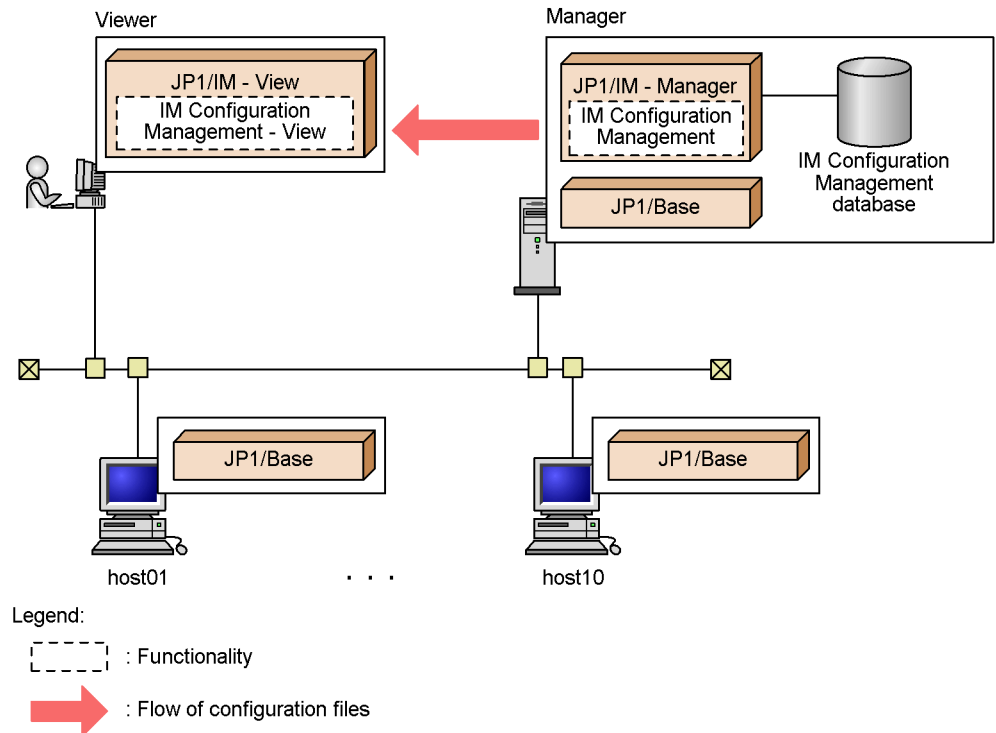
When you delete a host, the host's configuration files are also deleted from the manager running IM Configuration Management. When you delete host information on the **Host List** page of the IM Configuration Management window, the host's configuration files are also deleted.

#### 6.3.4 Displaying profiles

Using IM Configuration Management, the profiles collected from hosts can be displayed in the Display/Edit Profiles window.

The figure below shows the flow of processing when displaying profiles with IM Configuration Management.

Figure 6-25: Displaying profiles with IM Configuration Management



The table below describes the profile information you can display according to whether the service is active or inactive.

Table 6-16: Profile information that can be displayed according to the service's activity status

Profile type	Service activity status	Display of valid configuration information	Display of configuration file contents
Event Forwarding	Running	Y	Y
	Stopped	N	Y
Log File Trapping	Running	Y	Y
	Stopped	N	N
Event Log Trapping	Running	Y	Y
	Stopped	N	Y

Profile type	Service activity status	Display of valid configuration information	Display of configuration file contents
Local Action	Running	Y	Y
	Inactive	N	Y
	Stopped	N	Y

Legend:

Y: Can be displayed.

N: Cannot be displayed.

### 6.3.5 Editing configuration files

Using IM Configuration Management, you can edit the configuration files for the JP1/Base profiles on a host.

The following describes the functionality for editing configuration files.

#### (1) *Editing configuration file contents*

In the Display/Edit Profiles window, you can edit the contents of a displayed configuration file.

The following configuration files can be edited in IM Configuration Management:

- Event forwarding setting file
- Action definition file for log file trapping
- Action definition file for event log trapping
- Local action execution definition file

You can perform the following operations on these files in the Display/Edit Profiles window.

#### Copy text

You can copy text from a configuration file. Exclusive editing rights are not required.

In the file contents shown in the node display area, select the text that you want to copy and then perform either of the following:

- Choose **Edit** and **Copy**.
- Right-click and choose **Copy**.

#### Cut text

You can cut text from a configuration file. To do so, you must first obtain exclusive editing rights.

In the file contents shown in the node display area, select the text that you want to cut and then perform either of the following:

- Choose **Edit** and **Cut**.
- Right-click and choose **Cut**.

Paste text

You can paste copied or cut text into a configuration file. To do so, you must first obtain exclusive editing rights.

In the file contents shown in the node display area, select the position where you want to paste the text and then perform either of the following:

- Choose **Edit** and **Paste**.
- Right-click and choose **Paste**.

The changes you make while editing a configuration file are not checked. If you quit or forcibly terminate IM Configuration Management - View during editing, the changes will not be saved.

## **(2) Saving edited file contents**

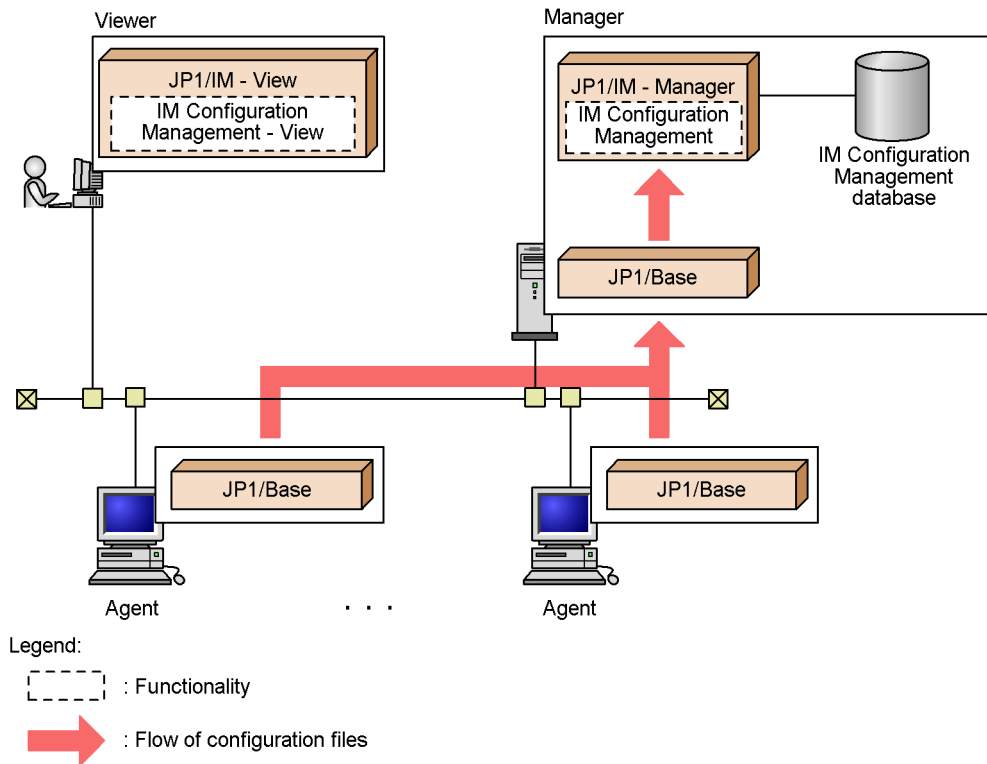
The contents of edited configuration files can be saved to the manager running IM Configuration Management.

Edited file contents are saved when you perform any of the following operations:

- In the node display area (settings information) of the Display/Edit Profiles window, select the **Save** check box and then click the **Execute** button.
- In the node display area (settings information) of the Display/Edit Profiles window, select the **Apply** check box and then click the **Execute** button.
- In the Display/Edit Profiles window, choose **Operation, Save/Apply Profiles**, and then **Save on the Server**.
- Import configuration files on the manager running IM Configuration Management.

The figure below shows the flow of processing when saving the contents of edited configuration files with IM Configuration Management.

Figure 6-26: Saving edited file contents with IM Configuration Management



The following configuration files can be saved:

- Event forwarding setting file
- Action definition file for log file trapping (not exported by IM Configuration Management)
- Action definition file for event log trapping
- Local action execution definition file

The edited file contents saved to the manager running IM Configuration Management cannot be forwarded to hosts.

Edited file contents saved to the manager will be overwritten when profiles are collected from the hosts.

### (3) Applying edited file contents

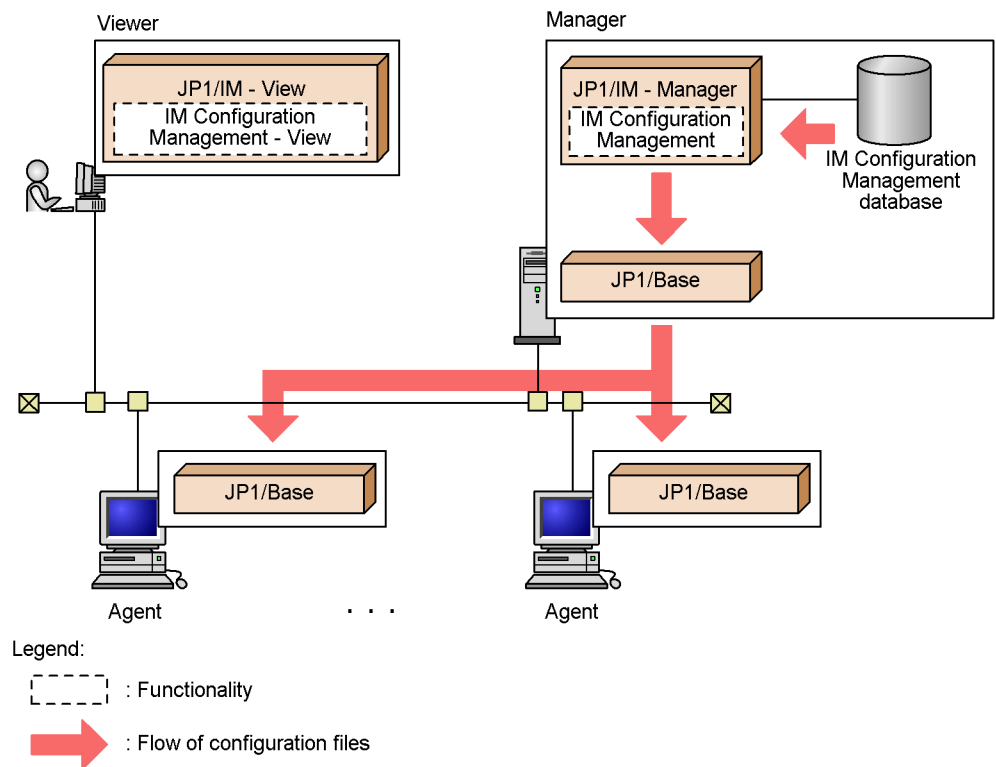
You can apply the contents of edited configuration files to JP1/Base on the hosts.

The figure below shows the flow of processing when applying the contents of edited



configuration files with IM Configuration Management.

Figure 6-27: Applying edited file contents with IM Configuration Management



You can apply edited configuration files in either of two ways, as described below.

In JP1/Base version 9, if the processing fails, the configuration files on the agent are rolled back to their previous state.

#### Apply per host

You can apply edited configuration files to a particular host by performing either of the following:

- In the node display area of the Display/Edit Profiles window, select the **Apply** check box next to **Applied contents** in the **Saving/application** area and then click the **Execute** button.
- In the tree display area of the Display/Edit Profiles window, first make sure you have exclusive editing rights to the profiles. Then choose **Operation**, **Save/Apply Profiles**, and **Apply by Reloading**.

The following configuration files can be applied to a host:

- Event forwarding setting file
- Action definition file for log file trapping
- Action definition file for event log trapping
- Local action execution definition file

Apply to all hosts

You can apply edited configuration files to all hosts in the system hierarchy in one operation. To do so, on the **Host List** page or **IM Configuration** page of the IM Configuration Management window, choose **Operation** and then **Batch Reflect Profiles**.

The following configuration files can be applied in one operation with IM Configuration Management:

- Event forwarding setting file
- Action definition file for event log trapping
- Local action execution definition file

In the Display/Edit Profiles window, you can check whether all the configuration files were successfully applied. If any file could not be applied or has **Saved on the server** status, the file is represented by an editing icon in the tree display area.

If there are no configuration files on the server, message KNAN22497-I appears and the file contents are not applied.

On the **IM Configuration** page of the IM Configuration Management window, you can check whether the configuration files were successfully applied to all the hosts. If any files could not be applied or have **Saved on the server** status, the affected host is represented by an error-status icon in the tree display area. To view further details, click the **Basic Information** button in the node display area.

### 6.3.6 Obtaining and releasing exclusive editing rights for a configuration file

Before you collect or edit configuration files, you must obtain exclusive editing rights to the files so that they cannot be edited from another instance of IM Configuration Management - View.

This section describes how to set and release exclusive editing rights for configuration files.

#### (1) *Obtaining exclusive editing rights*

Exclusive editing rights are required to perform the following operations:

- Edit a configuration file

- Collect configuration file information from lower-level hosts
- Update information in a profile tree

To obtain exclusive editing rights for configuration files, perform either of the following:

- In the tree display area of the Display/Edit Profiles window, click the JP1 product name (**JP1/Base**) and then choose **Edit** and **Exclusive Editing Settings**.
- In the tree display area of the Display/Edit Profiles window, right-click the JP1 product name (**JP1/Base**) and then choose **Exclusive Editing Settings**.

## **(2) Releasing exclusive editing rights**

To release exclusive editing rights for configuration files, perform either of the following:

- In the tree display area of the Display/Edit Profiles window, right-click the JP1 product name (**JP1/Base**) and then choose **Release Exclusive Editing**.
- In the tree display area of the Display/Edit Profiles window, click the JP1 product name (**JP1/Base**) and then choose **Edit** and **Release Exclusive Editing**.

## 6.4 Management of service activity information

Using IM Configuration Management - View, you can check whether services are active on the managed hosts.

This functionality allows you to monitor service activity on each host, and to investigate the service status if an error occurs on a host.

This section describes the service activity information you can manage using IM Configuration Management, and the functionality provided for checking the status of JP1 services.

### 6.4.1 Services whose activity information can be obtained

Using IM Configuration Management, of the JP1 product services on a managed host, you can view service activity information related to the system hierarchy.

When you collect service activity information with IM Configuration Management, a collection command is executed on the target host. The command outputs an execution log on the host.

The table below lists the services whose activity information you can view in IM Configuration Management, and the corresponding status collection command.

*Table 6-17: Services and commands for viewing service activity information*

Product name	Service name	Status collection command
JP1/Base	JP1/Base	jbs_spmc_status
	Event service	jevstat
	Log file trapping	jevlogstat ALL
JP1/IM - Manager	JP1/IM-Manager	jco_spmc_status

### 6.4.2 Collecting service activity information

Using IM Configuration Management, you can collect service activity information from any of the managed hosts.

To collect service activity information, the target host must be registered in the IM Configuration Management database and its host information must have been collected. In addition, JP1/Base must be active on the target host. Service activity information cannot be collected from a host running a version of JP1/Base earlier than version 9.

#### (1) Procedure for collecting service activity information

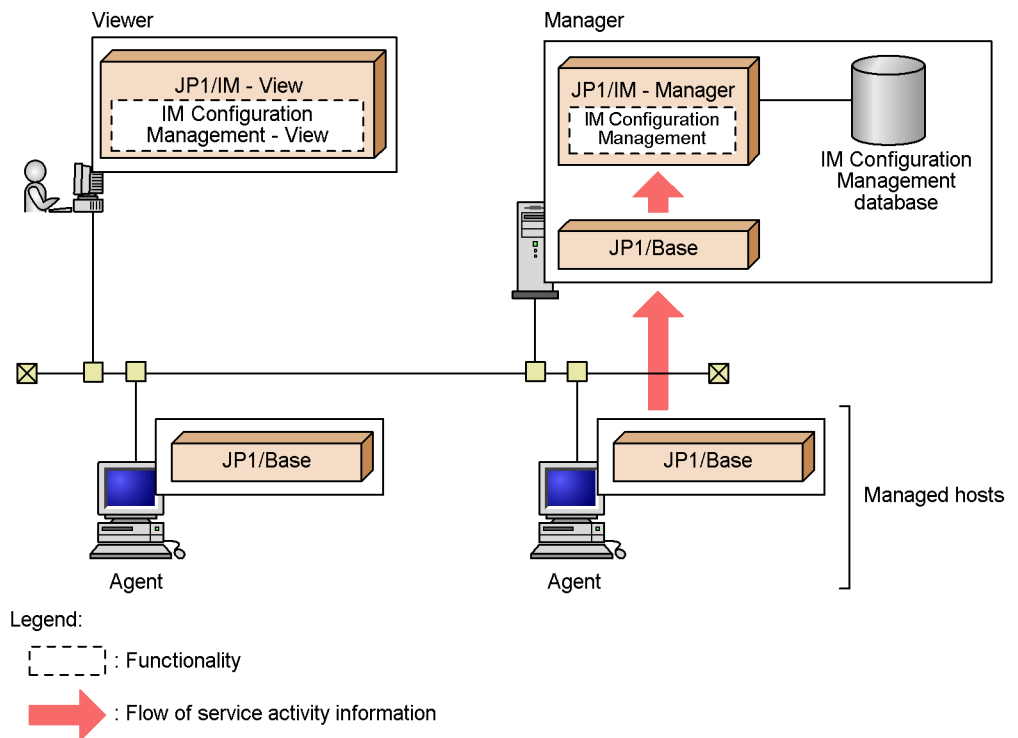
To collect service activity information, perform either of the following operations in

## IM Configuration Management - View:

- On the **Host List** page or **IM Configuration** page of the IM Configuration Management window, select a host and then click the **Service Information** button.
- On the **IM Configuration** page, click the **Refresh** button (to refresh the displayed information).

The figure below shows the flow of processing when collecting service activity information.

Figure 6-28: Collecting service activity information



The collected service activity information is saved to memory on the manager running IM Configuration Management, not to the manager's IM Configuration Management database.

## (2) Hosts from which service activity information can be collected

You can collect service activity information from only one host at a time. The range of hosts from which you can collect activity information depends on which host IM Configuration Management is installed on.

The table below describes the range of hosts whose service activity information you can collect from the integrated manager.

*Table 6-18:* Range of hosts whose service activity information can be collected from the integrated manager

Host type		Collect
Local host		Y
Relay manager		Y
Base manager		Y
Agent	Directly under the local host	Y
	Under a relay manager	Y
	Under a base manager	N <sup>#</sup>

Legend:

Y: The information can be collected.

N: The information cannot be collected.

#

An agent under a base manager might not be reachable from the integrated manager if it is behind a firewall. For this type of agent, collect the service activity information from the base manager.

The table below describes the range of hosts whose service activity information you can collect from a base manager.

*Table 6-19:* Range of hosts whose service activity information can be collected from a base manager

Host type		Collect
Local host		Y
Parent host		N <sup>#1</sup>
Relay manager		Y <sup>#2</sup>
Base manager		Y <sup>#2</sup>
Agent	Directly under the local host	Y
	Under a relay manager	Y <sup>#2</sup>

Host type		Collect
	Under a lower-level base manager	N <sup>#3</sup>

Legend:

Y: The information can be collected.

N: The information cannot be collected.

#1

You cannot collect service activity information from a parent host because its host information cannot be collected.

#2

Not recommended because the system configuration, including the integrated manager, would be more than three tiers.

#3

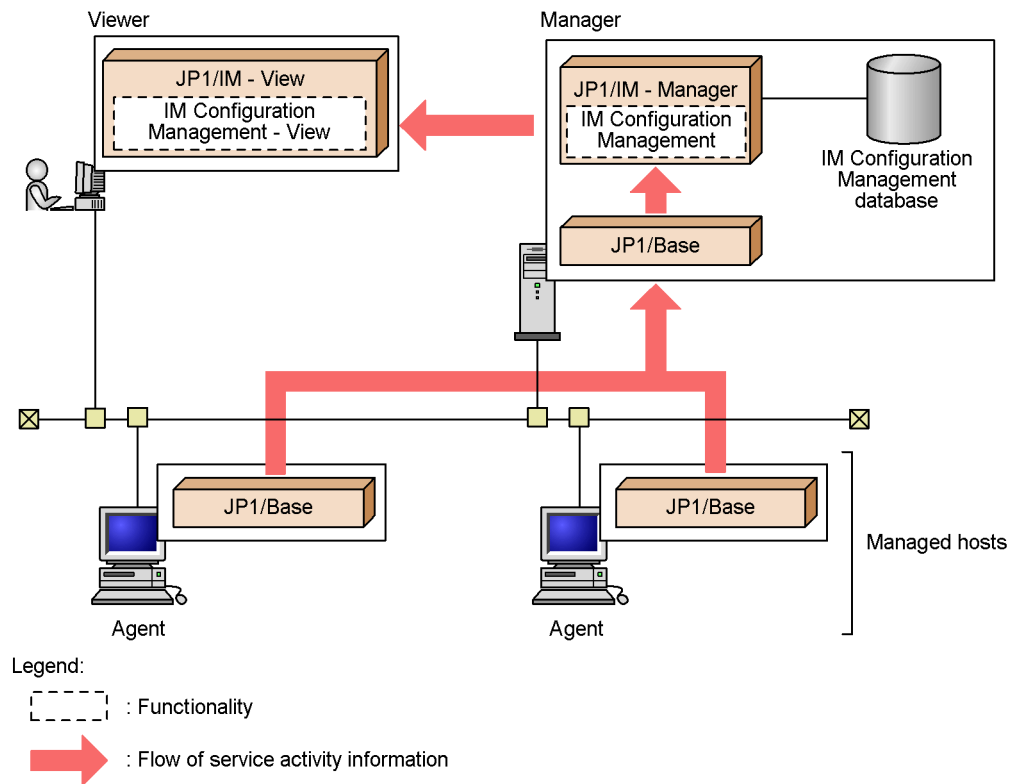
An agent under a lower-level base manager might not be reachable from the integrated manager if it is behind a firewall. For this type of agent, collect the service activity information from the lower-level base manager.

### 6.4.3 Displaying service activity information

You can display service activity information collected from a managed host on the **IM Configuration** page (service information) of the IM Configuration Management window.

The figure below shows the flow of processing when displaying service activity information with IM Configuration Management.

*Figure 6-29:* Displaying service activity information with IM Configuration Management





## 6.5 Importing and exporting IM Configuration Management information

Using IM Configuration Management, you can export information managed by IM Configuration Management and import management information that has been exported.

The import/export functionality can be used for the following purposes:

- To transfer a system hierarchy from a test environment to a real-world environment, or from a legacy environment to a new environment
- To import management information from another manager server on which IM Configuration Management is installed
- To temporarily or periodically change the system hierarchy
- To change settings back to a previous status after a failure

This section describes the information you can import or export using IM Configuration Management, and the functionality provided for this purpose.

### 6.5.1 Types of information that can be imported or exported

The following table describes the range of information managed by IM Configuration Management that can be imported or exported.

*Table 6-20:* Range of IM Configuration Management information that can be imported or exported

Information managed by IM Configuration Management		Export	Import
Host information	User-specified items	Y	Y
	OS information	Y	N
	Product information	Y	N
System hierarchy		Y	Y
Profiles	Event forwarding setting file	Y	Y
	Action definition file for event log trapping	Y	Y
	Action definition file for log file trapping	N	N
	Local action execution definition file	Y	Y
	Authentication server settings file	N	N
	JP1 user settings file	N	N

Information managed by IM Configuration Management		Export	Import
	User mapping settings file	N	N
Service activity information		N	N

Legend:

Y: Can be imported or exported.

N: Cannot be imported or exported.

The table below lists the export file names used in IM Configuration Management and the operations that can be performed on each file.

*Table 6-21: Export file names and supported operations*

Management information		Export file name	Operation	
			Import	Edit
Information about exported data		data_information.txt	N	--
Host information	User-specified items	host_input_data.csv <sup>#2</sup>	Y	Y
	Information collected automatically <sup>#1</sup>	host_collect_data.csv <sup>#2</sup>	N	--
System hierarchy		system_tree_information.txt	Y	Y
Profiles	Event forwarding setting file	forward	Y	Y
	Action definition file for event log trapping	ntevent.conf	Y	Y
	Local action execution definition file	jbslcact.conf	Y	Y

Legend:

Y: Can be performed.

N: Cannot be performed.

--: Cannot be edited because not imported.

<sup>#1</sup>

Host information must be collected after an import operation.

#2

When the host information contains a comma, line feed code, or double quotation mark, the output value is enclosed with double quotation marks (for example, aaa,aaa is output as "aaa,aaa"). A double quotation mark occurring in the output value itself is replaced with two double quotation marks (for example, aaa"bbb is output as "aaa" "bbb").

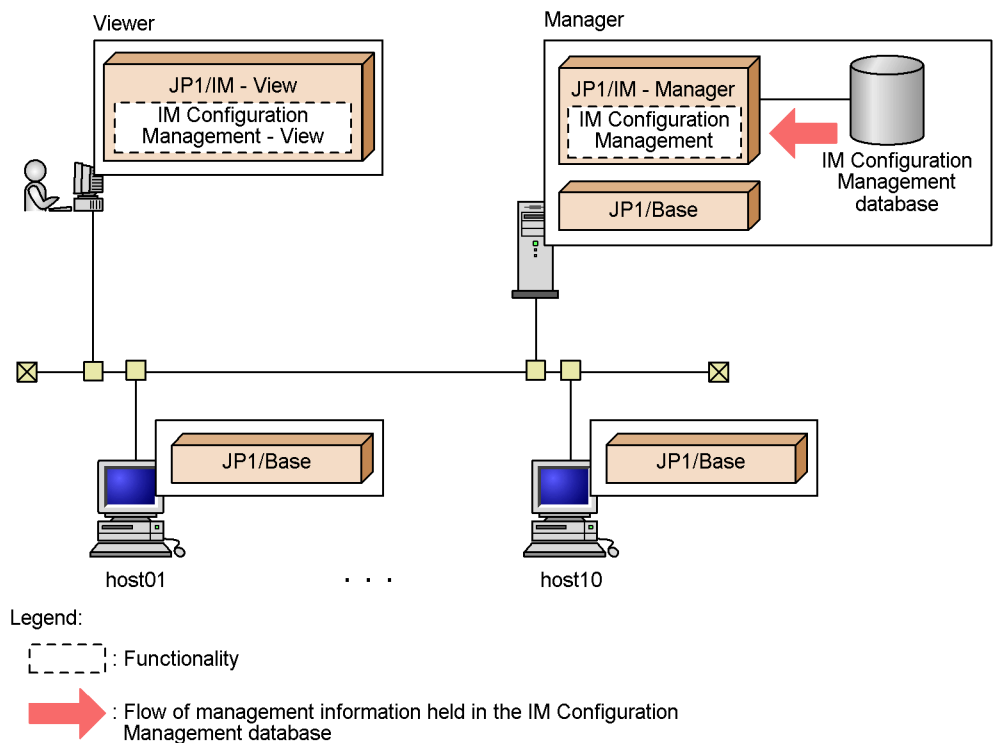
### 6.5.2 Exporting IM Configuration Management information

Using IM Configuration Management, you can export information held in the IM Configuration Management database to multiple files.

To export management information, execute the `jcfexport` command on the manager running IM Configuration Management.

The figure below shows the flow of processing when exporting management information with IM Configuration Management.

*Figure 6-30: Exporting management information with IM Configuration Management*



Before executing the command, make sure you check the information to be exported

in case the IM Configuration Management database contains management information that has not been applied in the actual system.

You can specify options in the `jcfexport` command to select the types of management information to export. For the command syntax, see *jcfexport* in *1. Commands* in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.

The table below describes the range of information you can specify for export.

*Table 6-22: Range of specifiable management information for export*

Type of management information (for export)		Export		
		Host information	System hierarchy	Profiles (all hosts)
Information about exported data		Y	Y	Y
Host information		Y	Y	Y
System hierarchy		N	Y	Y
Profiles	Event forwarding setting file	N	N	Y
	Action definition file for event log trapping	N	N	Y
	Local action execution definition file	N	N	Y

Legend:

Y: Can be specified.

N: Cannot be specified.

The table below describes the output formats of exported management information.

*Table 6-23: Output formats of exported management information*

Management information	Output format
Information about exported data	Information about exported data is output to one file.
Host information	Information about managed hosts is output to two files.
System hierarchy	Information about the system hierarchy is output to one file.
Profiles	JP1/Base profiles on the hosts are output to multiple files.

Information cannot be exported while import is in progress.

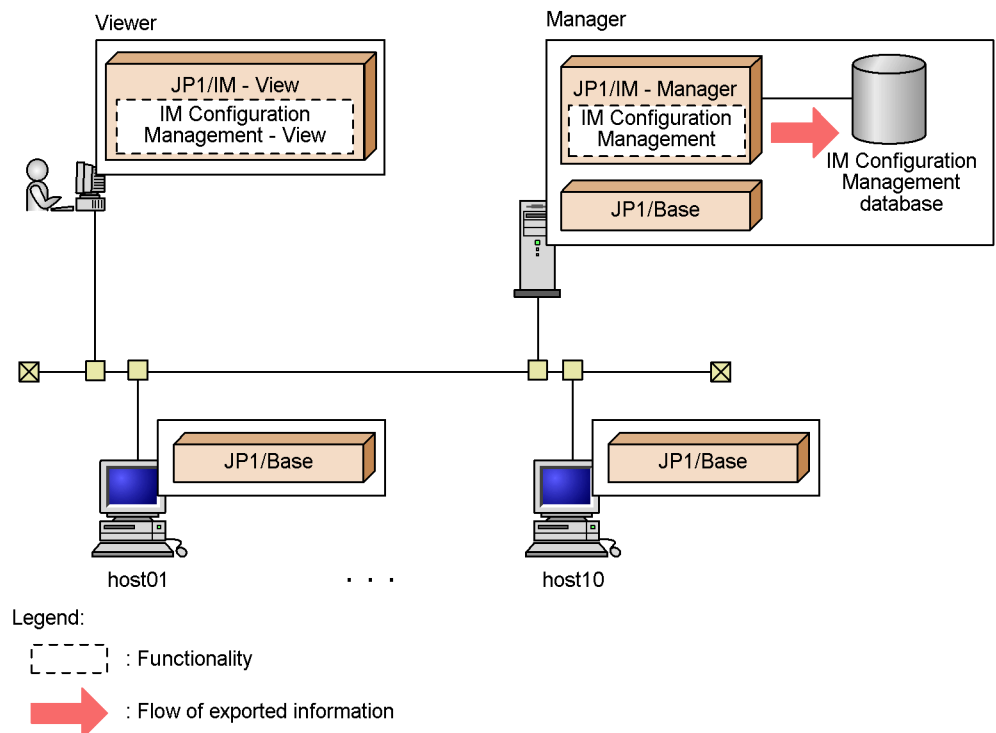
### 6.5.3 Importing IM Configuration Management information

Using IM Configuration Management, you can import exported management information.

To import management information, execute the `jcfimport` command on the manager running IM Configuration Management.

The figure below shows the flow of processing when importing management information with IM Configuration Management.

*Figure 6-31: Importing management information with IM Configuration Management*



Because importing information changes the data held by the IM Configuration Management database, we recommend that you back up the existing data in the database before performing an import operation. If an error occurs during import, the data will be rolled back to its previous state.

You can specify options in the `jcfimport` command to select the types of management information to import. For the command syntax, see *jcfimport* in *1. Commands* in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.

The table below describes the range of information you can specify for import.

*Table 6-24: Range of specifiable management information for import*

Type of management information (for import)		Import		
		Host information	System hierarchy	Profiles (all hosts)
Information about exported data		N	N	N
Host information		Y	Y	Y
System hierarchy		N	Y	Y
Profiles	Event forwarding setting file	N	N	Y
	Action definition file for event log trapping	N	N	Y
	Local action execution definition file	N	N	Y

Legend:

Y: Can be specified.

N: Cannot be specified.

To apply imported IM Configuration Management information to the actual system, you must apply the system hierarchy from the Edit IM Configuration window. For the procedure, see 8.2.5 *Applying the system hierarchy* in the *Job Management Partner 1/ Integrated Management - Manager Administration Guide*.

Management information cannot be imported while any of the following operations are in progress in IM Configuration Management:

- Collect, verify, synchronize, or apply the system hierarchy; obtain or release update rights to the system hierarchy
- Collect, edit, or delete host information
- Collect, edit, save, apply, or batch-distribute profiles
- Export or import management information

---

## 6.6 Virtualization configuration management

---

Using IM Configuration Management, you can manage a system hierarchy that includes virtual hosts running VMware ESX or another type of virtual machine monitor. Hereafter, this type of system hierarchy is called a *virtualization configuration*.

Virtualization configurations managed by IM Configuration Management can be monitored from Central Scope.

This section describes the functionality for managing virtualization configurations with IM Configuration Management.

### 6.6.1 Setting virtual host information

To manage a virtualization system with IM Configuration Management, you must set information about the virtual hosts.

You can set virtual host information using IM Configuration Management. If you are using VMware ESX, virtual host information can be collected from VMware ESX and imported to IM Configuration Management.

#### (1) *Entering virtual host information with IM Configuration Management*

To enter virtual host information in IM Configuration Management, you must first register the virtual hosts as managed hosts, setting **Virtual host** as their host type.

#### (2) *Importing host information from a VMware ESX virtualization configuration*

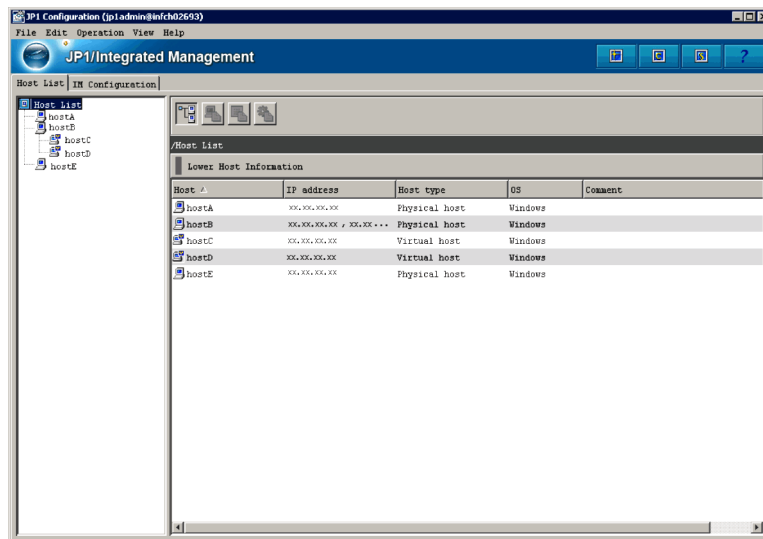
If you are using VMware ESX, you can collect host information from the VMware ESX virtualization configuration, and then import it to IM Configuration Management by merging it with the host input information file output from IM Configuration Management.

### 6.6.2 Displaying a virtualization configuration

You can display a virtualization configuration in the tree display area on the **Host List** page of the IM Configuration Management window.

The figure below shows an example of displaying a virtualization configuration in IM Configuration Management - View.

*Figure 6-32: Example of displaying a virtualization configuration in IM Configuration Management - View*



When you import host information from a VMware ESX virtualization configuration, the host information, IM configurations, and profiles held by IM Configuration Management are deleted. To manage profiles, you must collect the host information, IM configurations, and profiles after importing the VMware ESX information.

To collect this information:

1. Navigate to the **Host List** page of the IM Configuration Management window.
2. In the tree display area, click **Host List** and select all the hosts in the **Lower Host List**.
3. From the **Operation** menu, choose **Collect Host Information**.
4. From the **Operation** menu, choose **Collect IM Configuration**.
5. From the **Operation** menu, choose **Batch Collect Profiles**.

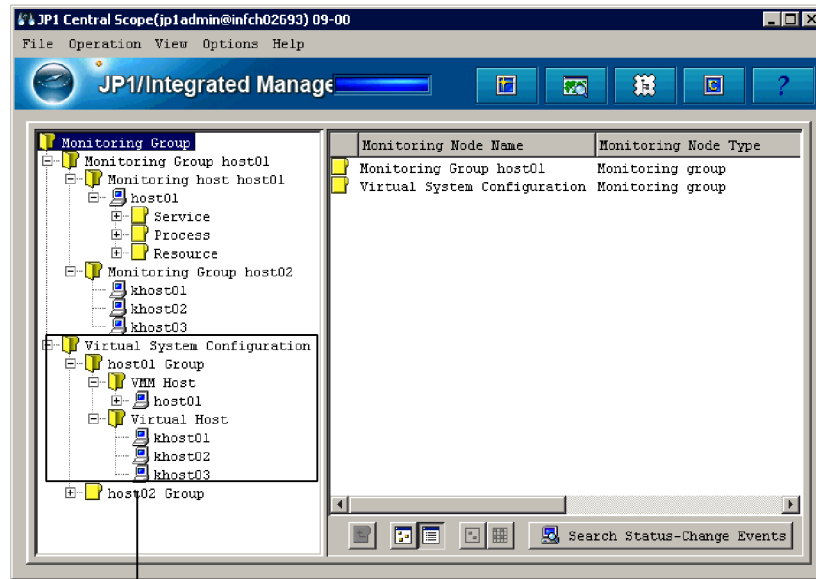
### 6.6.3 Importing a virtualization configuration to Central Scope

To monitor a virtualization configuration in Central Scope, export the virtualization configuration information managed by IM Configuration Management, and import it to Central Scope by converting it with the `jcfmkcsdata` command.

The figure below shows an example of displaying a virtualization configuration in the Central Scope viewer.



*Figure 6-33: Example of displaying a virtualization configuration in the Central Scope viewer*



Represents the virtualization configuration monitoring tree

For the syntax of the `jcfmkcsdata` command, see `jcfmkcsdata` in *1. Commands* in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.



## Chapter

---

# 7. JP1/IM Operation Control

---

This chapter describes the operation control in JP1/IM, and the communication that takes place in the JP1/IM system environment.

- 7.1 JP1/IM - Manager process management
- 7.2 JP1/IM - Manager health check function
- 7.3 Communication performed in the JP1/IM system environment
- 7.4 Core functionality provided by JP1/Base

## 7.1 JP1/IM - Manager process management

Process management is a core functionality of JP1/IM - Manager, used to control startup and termination of the manager functions. Another responsibility of process management is to issue instructions for checking the status of JP1/IM - Manager functions.

JP1/IM - Manager provides the following functions, the processes of which are controlled by process management:

- Event console service (evtcon)
- Event base service (evflow)
- Automatic action service (jcmain)
- Event generation service (evgen)<sup>#1, #2</sup>
- Central Scope service (jcsmain)<sup>#2</sup>
- IM Configuration Management service (jcfmain)<sup>#2</sup>

#1: Not started by default. Applicable when not using the integrated monitoring database.

#2: Not started by default.

Process management is realized by the following commands:

Table 7-1: Process management commands

Functionality	Command	Description
Start JP1/IM - Manager <sup>#</sup> (UNIX only)	jco_start	Controls JP1/IM - Manager startup and termination.
Stop JP1/IM - Manager <sup>#</sup> (UNIX only)	jco_stop	
JP1/IM - Manager status check	jco_spmd_status	Checks the activity status of JP1/IM - Manager.
Reload JP1/IM - Manager definition information	jco_spmd_reload	When definition information is updated in JP1/IM - Manager, this command reloads and applies the new definitions.

#: In Windows, JP1/IM - Manager is started and stopped by a Windows service registered under the service name JP1/IM-Manager. Use this service to start and stop

JP1/IM - Manager.

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

JP1/IM - Manager process management can also detect and troubleshoot abnormal process startup and termination using the following functionality:

- Automatically restarting an abnormally ended process
- Issuing a JP1 event when an error is detected at process startup or termination

For details about this functionality, see *7.1.1 Restarting abnormally ended processes* and *7.1.2 Issuing JP1 events at detection of process errors*.

### 7.1.1 Restarting abnormally ended processes

When a process that provides a function in JP1/IM - Manager ends abnormally, JP1/IM - Manager can attempt to recover the process.

JP1/IM processes are controlled by the process management, which detects when a process terminates abnormally and automatically restarts it. This allows JP1/IM - Manager to recover automatically from some temporary errors.

Process restarting is not enabled at installation. To enable process restarting, enable the restart parameter in the extended startup process definition file (`jp1co_service.conf`).

The operation of process restarting is described below. This example is based on settings for the `jcmain` process (automatic action service) being made in the extended startup process definition file. For details about the definition file, see *Extended startup process definition file (jp1co\_service.conf)* in *2. Definition Files* in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.

*Setting example*

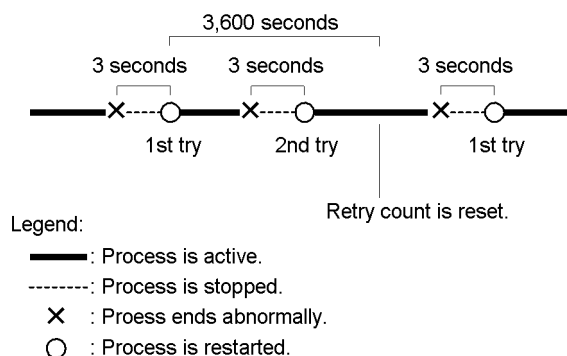
```
jcmain|1|3|3|3600|
```

*Explanation*

```
Process name: jcmain
Restart: 1 (1: Restart; 0: Do not restart (default))
Retry count: 3 (default)
Retry interval: 3 seconds (default)
Retry count reset time: 3,600 seconds (default)
```

In this definition, only the restart parameter is changed. There is typically no need to change the other values as the defaults will be suitable in most situations. With these settings, process restarting operates as follows:

Figure 7-1: Behavior when a process ends abnormally



In this example, if the process does not end abnormally within 3,600 seconds of restarting as specified by the retry count reset time, the retry count is reset. On the other hand, if the process terminates within 3,600 seconds of restarting, the retry count is incremented by one. No more attempts are made to restart the process after the retry count reaches the specified number.

In Windows, a Dr. Watson dialog box or a dialog box for reporting the error to Microsoft (Windows Server 2003 only) appears when a process results in an application error. Because these dialog boxes wait for user input, they can prevent processes from restarting automatically. For this reason, you must disable error reporting using dialog boxes.

*Note:*

If you are using JP1/IM - Manager in a cluster system, do not set up process management to restart abnormally ended processes because the error in the JP1/IM - Manager process may also affect the function that restarts processes. To ensure a more reliable restart, restart JP1/IM - Manager processes under the control of the clustering software.

### 7.1.2 Issuing JP1 events at detection of process errors

When JP1/IM - Manager detects an error in process startup or shutdown processing, it outputs an error message to the integrated trace log. However, this error message can also be issued as a JP1 event.

By default, JP1 events are not issued when a process error is detected. To enable this feature, enable the relevant parameters

(SEND\_PROCESS\_TERMINATED\_ABNORMALLY\_EVENT and SEND\_PROCESS\_RESTART\_EVENT) in the IM parameter definition file (jplco\_param\_V7.conf). For details about the definition file, see *IM parameter definition file (jplco\_param\_V7.conf)* in 2. Definition Files in the manual *Job*

*Management Partner 1/Integrated Management - Manager Command and Definition File Reference.*

If JP1 event issuance is enabled, a JP1 event is issued when:

- A process ends abnormally.
- No startup notification is received and a timeout occurs at process startup.
- Restart of a process that ended abnormally is completed (if process restarting is enabled).

## 7.2 JP1/IM - Manager health check function

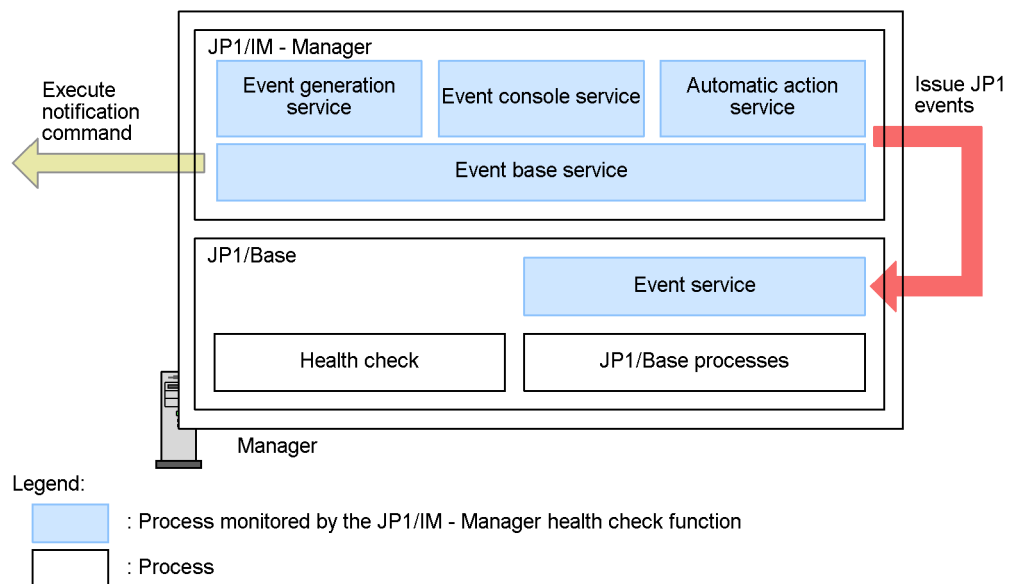
JP1/IM - Manager provides a feature to detect when a process goes into an infinite loop or deadlock (hangup<sup>#</sup>) and ceases processing, and to notify the operator by issuing a JP1 event or executing a notification command. In JP1/IM - Manager, this is called the *health check function*.

<sup>#</sup>: Hangups are caused by a deadlock or infinite loop. This means that the process can no longer accept processing requests.

Use of the health check function enables early detection and response to process errors that can often go unnoticed, such as deadlocks and infinite loops, by issuing a message or JP1 event to report the error and prompt the operator to take recovery action.

The following figure gives an overview of the JP1/IM - Manager health check function.

Figure 7-2: Overview of process monitoring using the JP1/IM - Manager health check function



If enabled, the health check function outputs message information to the OS log (the Windows event log or UNIX syslog) and the integrated trace log when a process hangs. By making the appropriate settings in the health check definition file (`jcohc.conf`), you can also have the health check function issue a JP1 event or notification command when a process hangs.



JP1/Base also provides a health check function for monitoring the various JP1/Base processes. Used in conjunction, the JP1/IM - Manager and JP1/Base health check functions enable early detection and response for process errors in JP1/IM - Manager and instances of JP1/Base in the JP1/IM system.

The following describes the processes monitored by the health check function, how to enable and disable the function, and how the function monitors processes.

### 7.2.1 Processes monitored by the health check function

The following table shows which processes are monitored by the JP1/IM - Manager health check function.

*Table 7-2: Processes monitored by the health check function*

Product	Process	Process name	Monitor
JP1/IM - Manager	Event console service	evtcon	Y
	Automatic action service	jcmain	Y
	Event base service	evflow	Y
	Event generation service <sup>#1</sup>	evgen	Y
	Central Scope service <sup>#2</sup>	jcsmain	--
	Process management <sup>#2</sup>	jco_spm	--
	Windows service control <sup>#2</sup>	jco_service	--
	IM Configuration Management service	jcfmain	--
JP1/Base	Event service <sup>#3</sup>	jevservice	Y
	Functions other than the event service	jbsplugin and others	--

Legend:

Y: Monitored by the health check function.

--: Not monitored by the health check function.

<sup>#1</sup>

The event generation service is disabled by default. It is applicable in a system that does not use the integrated monitoring database, and is not monitored otherwise. To monitor this process, enable the event generation service and the health check function (use the `jcoimdef` command to enable or disable the service).

#2

The Central Scope service (`jcsmain`) and IM Configuration Management service (`jcfmain`) do not support the health check function. The process management (`jco_spm`) is not monitored because it does not affect JP1/IM - Manager services. The process that starts and stops JP1/IM - Manager (`jco_service`) is not monitored because its role is limited to starting and stopping services.

#3

The JP1/IM - Manager health check function monitors the event service on the manager. All other JP1/Base processes are the responsibility of the health check function provided by JP1/Base.

*Reference note:*

The other JP1/Base processes on the manager can be monitored by the JP1/Base health check function. JP1/Base processes on agents are also monitored for errors by the JP1/Base health check function, through the forwarding and registration of error information to the manager as JP1 events.

For details, see the chapter on setting the health check function in the *Job Management Partner 1/Base User's Guide*.

## 7.2.2 Enabling and disabling the health check function

The health check function is not enabled at installation.

In the health check definition file, set the parameter that enables or disables health checking (`ENABLE`) to true. To issue a JP1 event or execute a notification command when a process hangs, enable the `EVENT` parameter, and specify the command to be executed using the `COMMAND` parameter.

To initiate a failover in a cluster system when the health check function detects a process error, you must enable the `FAILOVER` parameter in the health check setup file (the parameter is disabled by default). When this setting is enabled, JP1/IM - Manager is stopped when the health check function detects a process error, allowing failover to take place.

For details about the definition file, see *Health check definition file (`jcohc.conf`)* in 2. *Definition Files* in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.

## 7.2.3 How the health check function works

The JP1/IM - Manager health check function is realized by having processes monitor one another.

The following table describes the correspondence between the processes that perform

monitoring in the JP1/IM - Manager health check function, and the processes they monitor.

*Table 7-3: Correspondence between monitoring processes and monitored processes*

Monitoring processes	Monitored processes
Event console service (evtcon)	Event base service (evflow)
	Automatic action service (jcamain)
	Event generation service (evgen) <sup>#1</sup>
	Event service (jevservice) <sup>#2</sup>
Event base service (evflow)	Event console service (evtcon)

#1: Applicable when not using the integrated monitoring database.

#2: A JP1/Base service that runs on the manager.

### (1) Detecting process errors

In the JP1/IM - Manager health check function, a process that performs monitoring communicates over the network with the processes it monitors, to check whether the processes are working normally.

To detect process errors, the health check function sends polling signals to the monitored processes at regular intervals. If a process has not responded to the signal within a set time, the health check function regards the process as being in an abnormal state.

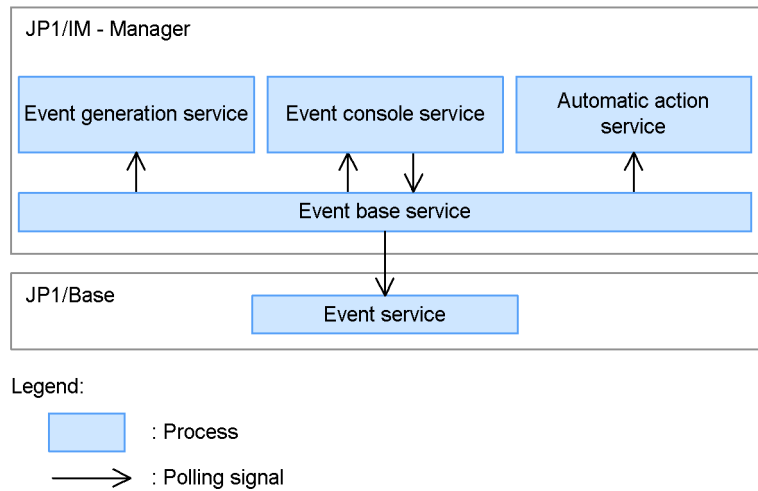
The interval at which processes are polled, and the number of non-responses for a process to be judged abnormal, differ according to the monitored process, as follows:

*Table 7-4: Differences in non-response count*

Monitored process	Polling interval	Non-response count
Event service (jevservice)	60 to 3,600 seconds (default: 300 seconds)	1 to 60 (default: 2)
Process other than the event service	60 to 3,600 seconds (default: 60 seconds)	1 to 60 (default: 3)

The figure below shows in diagrammatic form how process errors are detected.

Figure 7-3: Communication between processes



## (2) Reporting process errors

When the JP1/IM - Manager health check function is enabled, on detection of a process error, JP1/IM - Manager executes the following processing to report that an error has occurred:

- If the error occurred in a process being monitored by JP1/IM - Manager (*evtcon*, *jcmain*, *evflow*, *evgen*, or *jcdmain*), message KAVB8060-E is output to the integrated trace log and to the Windows event log or UNIX syslog.
- If the error occurred in the JP1/Base event service, message KAVB8062-E is output to the integrated trace log and to the Windows event log or UNIX syslog.
- If a notification command has been set, the command is executed.

When the failed process has been restored to normal status, message KAVB8061-I is output to the integrated trace log and to the Windows event log or UNIX syslog. If JP1 event issuance is enabled, a JP1 event (event ID: 00002014) is issued.

*Reference note:*

- The JP1 event with event ID 00002013 is a dummy event (an event not registered in the event database) issued to JP1/IM - View. A dummy event is issued when an error occurs in the event service in which JP1 events are registered.
- We recommend that you set up the functionality for executing a notification command when using the JP1/IM - Manager health check function.

Execution of a notification command is recommended because if errors are reported only by issuing JP1 events, the user may fail to respond promptly when not monitoring services in JP1/IM - View or if a problem occurs in the event console service (that is, the user is not made aware that an error has been detected by JP1/IM).

## 7.3 Communication performed in the JP1/IM system environment

When you monitor the system operation using JP1/IM, communication based on the TCP/IP protocol takes place between the hosts in the system, using port numbers and IP addresses. The port numbers used by JP1/IM and JP1/Base are registered in the `services` file automatically when the product is installed. For details about the port numbers registered at JP1/IM installation, see *C. Port Numbers*. For details about the port numbers registered at JP1/Base installation, see the appendixes in the *Job Management Partner 1/Base User's Guide*. For details about the concept of communication in JP1 series products, see the section on the communication protocol of JP1/Base in the overview chapter in the *Job Management Partner 1/Base User's Guide*.

### 7.3.1 Communication between the viewer and manager

Typically, communication is established between the viewer and manager when a user logs in to JP1/IM - Manager from JP1/IM - View, and is terminated when the user logs out. Communication is also terminated according to the timeout period set in JP1/IM (default 2,500 milliseconds) when communication processing between the viewer and manager takes too long or the manager goes down and fails to respond to requests. To change the communication timeout period, you must change the setting for the viewer (JP1/IM - View) and the manager (JP1/IM - Manager (JP1/IM - Central Console)). You do not need to do so for JP1/IM - Manager (JP1/IM - Central Scope).

The following table lists the ports used for communication between JP1/IM - View and JP1/IM - Manager.

*Table 7-5: Ports used for communication between JP1/IM - View and JP1/IM - Manager*

Service	Port number	Description
jplimevtcon	20115/tcp	Used to connect to JP1/IM - Manager (event console service) from JP1/IM - View.
jplimcmda	20238/tcp	Used to execute commands from JP1/IM - View.
jplimcss	20305/tcp	Used to connect to JP1/IM - Manager (Central Scope service) from JP1/IM - View.
jplimcf	20702/tcp <sup>#</sup>	Used to connect to JP1/IM - Manager (IM Configuration Management service) from JP1/IM - View.

<sup>#</sup>

Port used for communication between JP1/IM - View and JP1/IM - Manager

when using IM Configuration Management.

If you use the Web-based JP1/IM - View, the following ports are used for communication between the viewer and manager.

*Table 7-6:* Ports used for communication between the viewer and manager when using the Web-based JP1/IM - View

Service	Port number	Description
http	80/tcp <sup>#</sup>	Used to connect to the Web server (to download <code>console.html</code> from JP1/IM - Manager).
jp1imevtcon	20115/tcp	Used to connect to JP1/IM - Manager (event console service) from the Web-based JP1/IM - View (through a Web browser).

<sup>#</sup>: The port number may differ depending on how the Web server is set up.

### 7.3.2 Communication between the manager and authentication server

Communication takes place between the manager and authentication server when a user logs in to JP1/IM - Manager from JP1/IM - View.

The following table lists the ports used for communication between the manager and the authentication server.

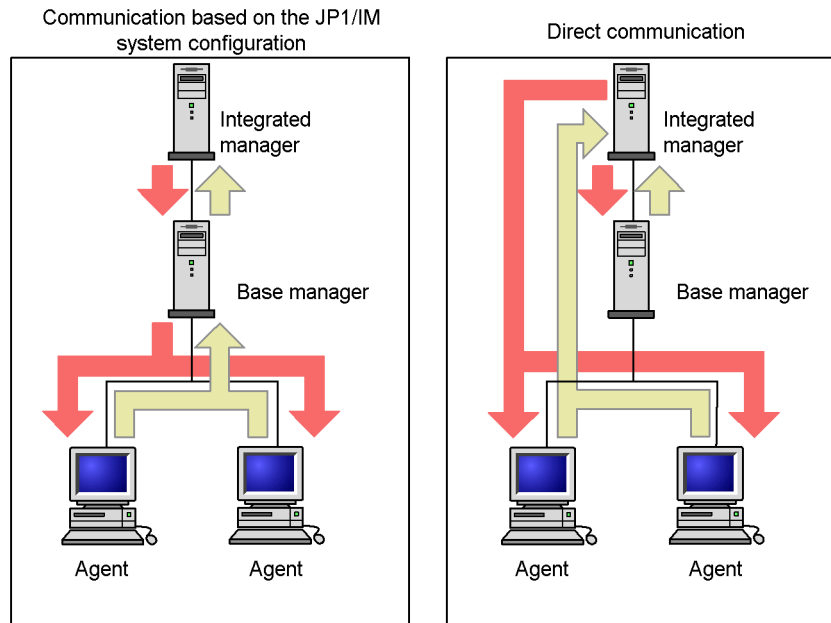
*Table 7-7:* Ports used for communication between the manager and authentication server

Service	Port number	Description
jp1bsuser	20240/tcp	Used for user authentication.

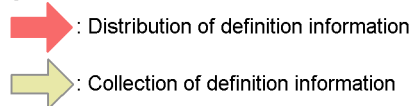
### 7.3.3 Communication between the manager and agent

Communication takes place between the manager and agent when the manager sends an instruction to the agent, or the agent sends processing results to the manager.

There are two forms of communication between the manager and agent. In one form, managers communicate with agents according to the hierarchy defined in the JP1/IM system configuration. In the other, the manager communicates directly with the target host. For this reason, take care when using JP1/IM and JP1/Base in a firewall environment or a system made up of multiple LANs.

*Figure 7-4: Types of communication between manager and agent*

Legend:



The communication that takes place between manager and agent is described below, categorized according to the form of communication involved.

#### Communication based on the system hierarchy

- **Distributing configuration definitions**  
Configuration definition information is distributed to each host in the system, according to the hierarchy defined in the configuration definition file.
- **Executing commands from JP1/IM - View**  
Command execution requests are sent down through lower-level hosts according to the system hierarchy, and the execution results are forwarded through higher-level hosts as defined in the hierarchy.
- **Executing commands by automated action**  
Command execution requests are sent down through lower-level hosts



according to the system hierarchy, and the execution results are forwarded through higher-level hosts as defined in the hierarchy.

- Forwarding JP1 events

Under the default settings, JP1 events are forwarded through higher-level hosts according to the system hierarchy.

The following table lists the ports used when communication is based on the system hierarchy.

*Table 7-8:* Port numbers used for communication based on the system hierarchy

Service	Port number	Description
jp1imrt	20237/tcp	Used to distribute configuration definitions.
jp1imcmdc	20239/tcp	Used for the following tasks: <ul style="list-style-type: none"> <li>• Executing commands from JP1/IM - View</li> <li>• Executing commands by automated action</li> </ul>
jp1imevt	20098/tcp	Used to forward JP1 events.

#### Communicating directly with the target host

- Searching for events

The manager communicates directly with the target host.

- Collecting and distributing event service definitions

Definition information is collected and distributed by communicating directly with all the hosts in the configuration definition file.

- Auto-generating a monitoring tree

Definition information is collected from all products that support the auto-generation function of JP1/IM - Manager (JP1/IM - Central Scope), by communicating directly with each host.

- Using the `jcochstat` command

The manager communicates directly with the host specified as the command argument.

- Canceling an automated action from JP1/IM - View or using the `jcacancel` command

The manager communicates directly with the host where the action is to be cancelled.

- Using the `jcocmdshow` and `jcocmddel` commands

The manager communicates directly with the host specified as the command

argument.

The following table lists the ports used for direct communication with a target host.

*Table 7-9: Ports used for direct communication with target hosts*

Service	Port number	Description
jplimevtapi	20099/tcp	Used to conduct an event search.
jplbsplugin	20306/tcp	Used for the following tasks: <ul style="list-style-type: none"> <li>Collecting and distributing event service definitions</li> <li>Auto-generating a monitoring tree</li> <li>Canceling an automated action from JP1/IM - View</li> <li>jcacancel command</li> <li>jcocmdshow and jcocmdel commands</li> </ul>
jplimevtcon	20115/tcp	Used by the jcochstat command.

### 7.3.4 Communicating within a local host

JP1/IM and JP1/Base use ports to communicate even when the communication takes place within a local host (between the processes on that host).

The following table lists the ports used for communication within a local host.

*Table 7-10: Ports used for communication within a local host*

Service	Port number	Description
jplimevtapi	20099/tcp	Used to acquire JP1 events from JP1/Base and to register JP1 events in JP1/Base.
jplimevtcon	20115/tcp	Used by JP1/IM - Manager internal processing.
jplimfcs	20701/tcp	Used by JP1/IM - Manager internal processing.
jplimcmdda	20238/tcp	Used to execute automated actions.
jplimegs	20383/tcp	Used by JP1/IM - Manager (event generation service) internal processing.
jplimcss	20305/tcp	Used by JP1/IM - Manager (Central Scope service) internal processing.
JP1/IM-Manager DB Server	20700/tcp <sup>#</sup>	Used by JP1/IM - Manager (IM database) internal processing.
jplimcf	20702/tcp	Used by JP1/IM - Manager (IM Configuration Management service) internal processing.

#

The port number for the JP1/IM-Manager DB Server is not written in the `services` file. The port number increases with each logical host configured in the system. The default is 20700/tcp. The port number for the IM database is set in the setup information file. For details, see *Setup information file (jimdbsetupinfo.conf)* in 2. *Definition Files* in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.

### 7.3.5 Communicating with JP1/IM - Rule Operation

In a system linked with JP1/IM - Rule Operation, communication takes place according to the JP1/IM system configuration in the following situation:

- When a rule startup request is sent automatically

The rule startup request is sent from the JP1/IM - Manager (JP1/IM - Central Console) host to the JP1/IM - Rule Operation host.

The following table lists the ports used for communication between the JP1/IM - Manager (JP1/IM - Central Console) host and JP1/IM - Rule Operation.

*Table 7-11:* Ports used for communication between JP1/IM - Manager (JP1/IM - Central Console) hosts and JP1/IM - Rule Operation

Service	Port number	Description
jp1imcmdc	20239/tcp	Used to send rule startup requests to JP1/IM - Rule Operation by automated action.
jp1imevt	20098/tcp	Used to forward JP1 events issued by JP1/IM - Rule Operation.

---

## 7.4 Core functionality provided by JP1/Base

---

JP1/Base is a prerequisite product for JP1/IM - Manager, providing the core functionality for monitoring the system operation using JP1/IM. This section describes the role of JP1/Base in the JP1/IM system environment.

### 7.4.1 Managing JP1 users

JP1/IM performs user authentication and access control based on dedicated **JP1 user** accounts, designed to allow JP1/IM to operate securely in a multi-platform environment. JP1 users are managed via JP1/Base user management.

JP1/Base provides three user management functions:

- User authentication
- Access control
- User mapping

These functions are described below.

#### (1) *User authentication*

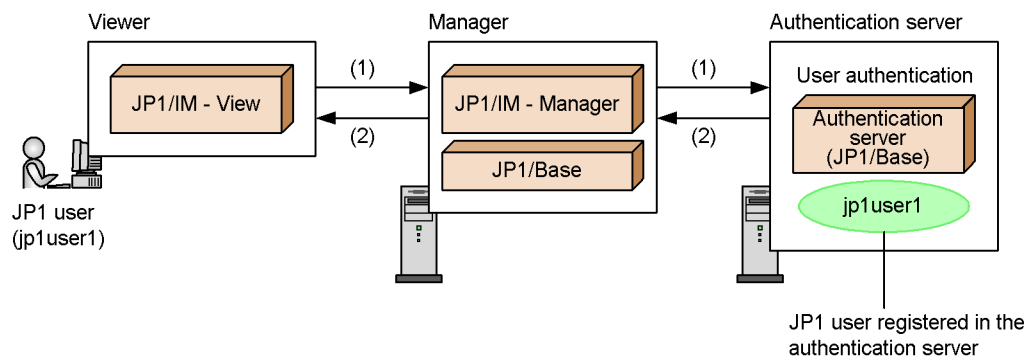
JP1/IM monitors the system by accessing JP1/IM on the manager from JP1/IM - View on the viewer. To prevent access by unauthorized users, user authentication is performed by a login processing when JP1/IM is accessed from JP1/IM - View.

In JP1/IM, user authentication is carried out by the JP1/Base user authentication function when a user attempts to log in to JP1/IM from JP1/IM - View. The JP1/Base that performs this user authentication is called an *authentication server*.

At login, the JP1 user is authenticated by the authentication server assigned to the JP1/IM host.

The following figure shows the flow of user authentication when a user logs in to the JP1/IM host from JP1/IM - View.

Figure 7-5: Flow of processing for user authentication



The flow of processing is described below, following the numbers in the figure:

1. When a user logs in to the JP1/IM host from JP1/IM - View, user authentication is carried out by the authentication server associated with JP1/Base on the JP1/IM host.

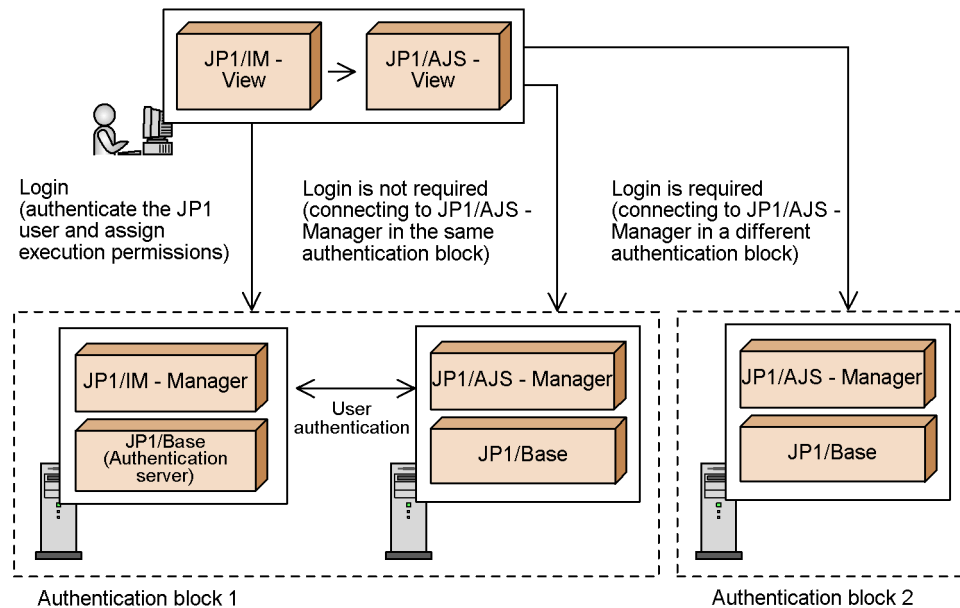
The authentication server used by the JP1/IM host is set up in JP1/Base on that host.

2. The authentication server checks whether the JP1 user who made the login attempt is registered. If the JP1 user is registered, information about the operating permissions for that JP1 user is returned to JP1/IM - View via the JP1/IM host. (For details about operating permissions for JP1 users, see 7.4.1(2) *Access control*.)

JP1 users must be registered in the authentication server in advance.

A group of hosts that use the same authentication server for JP1 user authentication is called an *authentication block*. Users can access JP1/AJS - View windows from JP1/IM - View without needing to log in to JP1/AJS - View if the associated JP1/AJS - Manager is in the same authentication block as JP1/IM - View, as shown in the following figure. (In a system that switches between authentication servers, login will be required after a switch has taken place.) If the JP1/AJS - Manager is in a different authentication block, login is required.

Figure 7-6: Authentication blocks



You can set up two authentication servers in the same authentication block. If connection to one authentication server fails, the JP1 user can connect to and be authenticated by the other authentication server. This prevents any interruption of job processing due to an authentication server error or other such problem. The authentication server used routinely is called the *primary authentication server*, and the authentication server in reserve is called the *secondary authentication server*. Both servers must be running the same JP1/Base version.

## (2) Access control

Only users authenticated by the authentication server are able to log in to JP1/IM. However, there are problems inherent in giving all logged-in users unrestricted access to reference or operate on the management information of JP1/IM. For this reason, JP1/IM allows you to assign access permissions and operating permissions to individual JP1 users that restrict the operations and information available to them in JP1/IM - View.

The access permissions and operating permissions for JP1 users are managed by the authentication server. When user authentication is performed at login, information about the access permissions and operating permissions of the logged-in user (JP1 user) is returned to JP1/IM. JP1/IM uses this information to control what information is displayed and what operations the user may perform in JP1/IM - View.

Access permissions and operating permissions are set when JP1 users are registered in

the authentication server. The access permission for a JP1 user is called a *JP1 resource group*, and the operating permission is called a *JP1 permission level*. The range of tasks a JP1 user can perform in JP1/IM - View is determined by assigned JP1 resource group and JP1 permission level.

The JP1 resource group for JP1/IM is `JP1_Console`. You do not need to change the JP1 resource group if you intend to use the Central Console and IM Configuration Management functionality. However, if you want to control the range of Central Scope information displayed to individual users in a monitoring tree, you must change the JP1 resource group set in the authentication server to match the setting in the Central Scope. For details, see 4.4.3 *Setting the monitoring range of a monitoring tree*.

JP1/IM and IM Configuration Management provide three JP1 permission levels, as listed below. To each JP1 user, assign the permission level that matches their responsibilities (the range of tasks the user performs in JP1/IM - View).

Table 7-12: JP1 permission levels

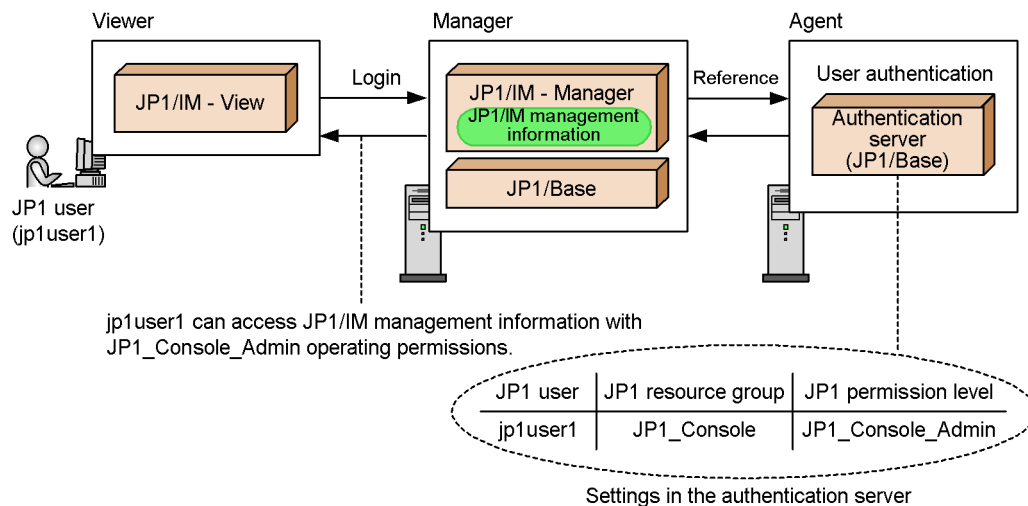
JP1/IM - Manager component	Permission level	Permitted operations
JP1/IM	JP1_Console_Admin	<ul style="list-style-type: none"> <li>Use the Central Console and Central Scope (set the system environment, perform system operations, reference information, set the user environment, and start linked products).</li> <li>Reference the system hierarchy and host information in IM Configuration Management.</li> </ul>
	JP1_Console_Operator	<ul style="list-style-type: none"> <li>Use the Central Console and Central Scope, reference information, set the user environment, and start linked products.</li> <li>Reference the system hierarchy and host information in IM Configuration Management.</li> </ul>
	JP1_Console_User	<ul style="list-style-type: none"> <li>Perform reference operations in the Central Console and Central Scope, set the user environment, and start linked products.</li> <li>Reference the system hierarchy and host information in IM Configuration Management.</li> </ul>
IM Configuration Management	JP1_CF_Admin	Perform all operations in IM Configuration Management, including changing the system hierarchy, changing profiles, and so on.
	JP1_CF_Manager	Reference and collect the system hierarchy and host information.
	JP1_CF_User	Reference and collect the system hierarchy and host information.

Users who work with IM Configuration Management must have both a JP1/IM permission level and an IM Configuration Management permission level.

For details about the operations that the different JP1 permission levels allow JP1 users to perform in JP1/IM - View, see *E. Operating Permissions*.

The following figure shows an example of controlling a JP1 user's access.

Figure 7-7: Example of JP1 user access control



### (3) User mapping

When a command is executed from JP1/IM, either by automated action or from JP1/IM - View, the OS user permissions for the target host are required to actually execute the command on that host. For this reason, the OS user permissions associated with the JP1 user are acquired at command execution.

The functionality that associates JP1 users with OS users is called *user mapping* and is provided by JP1/Base.

User mapping must be defined on all target hosts at which commands are to be executed.

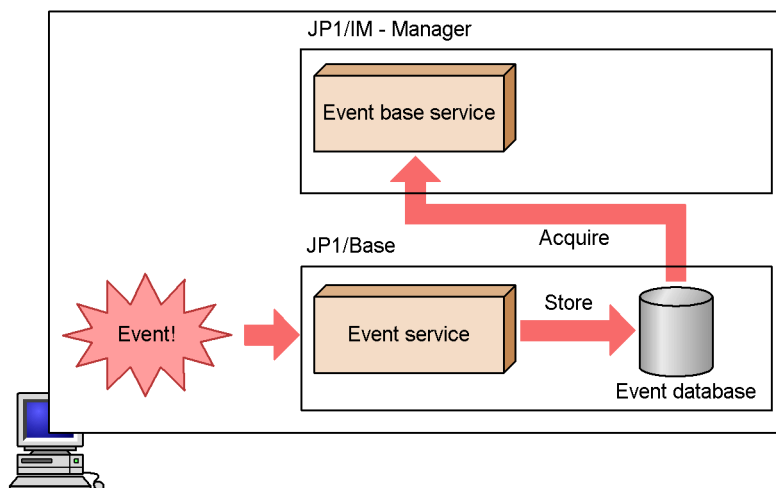
To use IM Configuration Management, you do not need to define user mapping on the manager running IM Configuration Management or on its managed hosts.

## 7.4.2 Managing JP1 events using JP1/Base

JP1 events are controlled by the JP1 event service and recorded in an event database unique to JP1/Base.



Figure 7-8: Overview of JP1 event management



The information recorded in a JP1 event is categorized by attribute as follows:

- Basic attributes (held by all JP1 events)
- Extended attributes (optionally set by the program that issued the JP1 event, and consisting of common information and program-specific information)
  - Common information (information in a format shared by all JP1 programs)
  - Program-specific information (other information in a format specific to the program issuing the event)

To distinguish between attribute types, basic attribute names begin with B. (for example, B.ID), and extended attribute names begin with E. (for example, E.SEVERITY).

Information is recorded for each attribute type as follows:

Example: JP1 event generated when execution of an automated action is requested (partial only)

```

Basic attributes
- Event ID (B.ID): 000020E0
- Message (B.MESSAGE):
KAVB4430-I Execution of the action for an event was
requested.
:
Extended attributes - Common information
- Event ID (E.SEVERITY): Information
- Product name (E.PRODUCT_NAME): /HITACHI/JP1/IM/JCAMAIN
:

```

```
Extended attributes - Program-specific information
- Executing host (E.EXECHOST): jp1-manager
:
```

In this manner, events generated in the system are recorded as JP1 events.

For details about JP1 events, see 3. *JP1 Events* in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*. See also the description of JP1 events in the *Job Management Partner 1/Base User's Guide*.

### (1) Centrally managing events using JP1 events

JP1/Base manages events occurring in the system as JP1 events.

Events being managed outside JP1, such as by log files and SNMP traps, can be converted into JP1 events and handled in JP1/Base.

By using JP1 events in this manner, events handled by a wide variety of products can be managed by JP1/Base in the same way as events issued by products in the JP1 series.

Events issued as JP1 events

- JP1 events (issued by JP1 products)

The products in the JP1 series enable system operation management from a variety of angles. By managing the JP1 events that each product issues, you can comprehensively manage the events occurring in the system.

For details about the JP1 events issued by individual products in the JP1 series, see the relevant manual.

- JP1 events (issued by commands)

JP1/Base provides commands for issuing JP1 events (`jevsend` and `jevsendd`). By placing these commands in a shell script or similar, users can use the issued JP1 events to monitor system operation. Since JP1/IM only monitors JP1 events that have an event level, specify the event level in the command arguments (for example `-e SEVERITY=Error`).

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

- Events in JP1/SES format

JP1/Base can manage events in JP1/SES format (events that can be acquired by the programs JP1/SES and JP1/AJS provided in version 5 and earlier of the JP1 series.)

In its default state, JP1/IM cannot monitor events in the JP1/SES format. This is because JP1/IM uses the event level, an extended attribute, in monitoring events;

events in the JP1/SES format have basic attributes only.

To allow JP1/IM to monitor events in the JP1/SES format, either set up an event acquisition filter to acquire JP1/SES format events, or use the extended functions provided by JP1/Base to enable extended attributes for JP1/SES-format events.

See 3.2 *Filtering of JP1 events*.

See the description of JP1/SES event conversion in the manual *Job Management Partner 1/Base Function Reference*.

- JP1 events (using the event issuing function)

JP1/Base provides functions that allow user application programs to issue JP1 events directly.

See the description of user-defined events in the manual *Job Management Partner 1/Base Function Reference*.

Events converted to JP1 events by the event converters

- Log file information

The JP1/Base log file trapping function converts the information that application programs output to log files into JP1 events for management by JP1/Base.

- Windows event log information

The JP1/Base event log trapping function converts the information output to the Windows event log into JP1 events for management by JP1/Base.

- SNMP traps

The JP1/Base SNMP trap converter converts SNMP traps managed by HP NNM version 7.5 or earlier into JP1 events for management by JP1/Base.

See the chapter on setting the event converters in the *Job Management Partner 1/Base User's Guide*.

*Reference note:*

For details about NNMi incident conversion in HP NNMi, see the manual *Job Management Partner 1/Integrated Management - Event Gateway for Network Node Manager i Description, User's Guide and Reference*.

## **(2) Using JP1 event forwarding to centralize event management**

JP1/IM monitors the system by acquiring from JP1/Base the JP1 events recorded in the event databases on the managers.

Of the JP1 events generated at each host in the system, important events that need to be addresses can be forwarded to the JP1/IM manager by the event forwarding function of JP1/Base. In this manner, JP1/IM can centrally manage the events

occurring in the system (important events needing management follow-up).

**(a) Forwarding JP1 events**

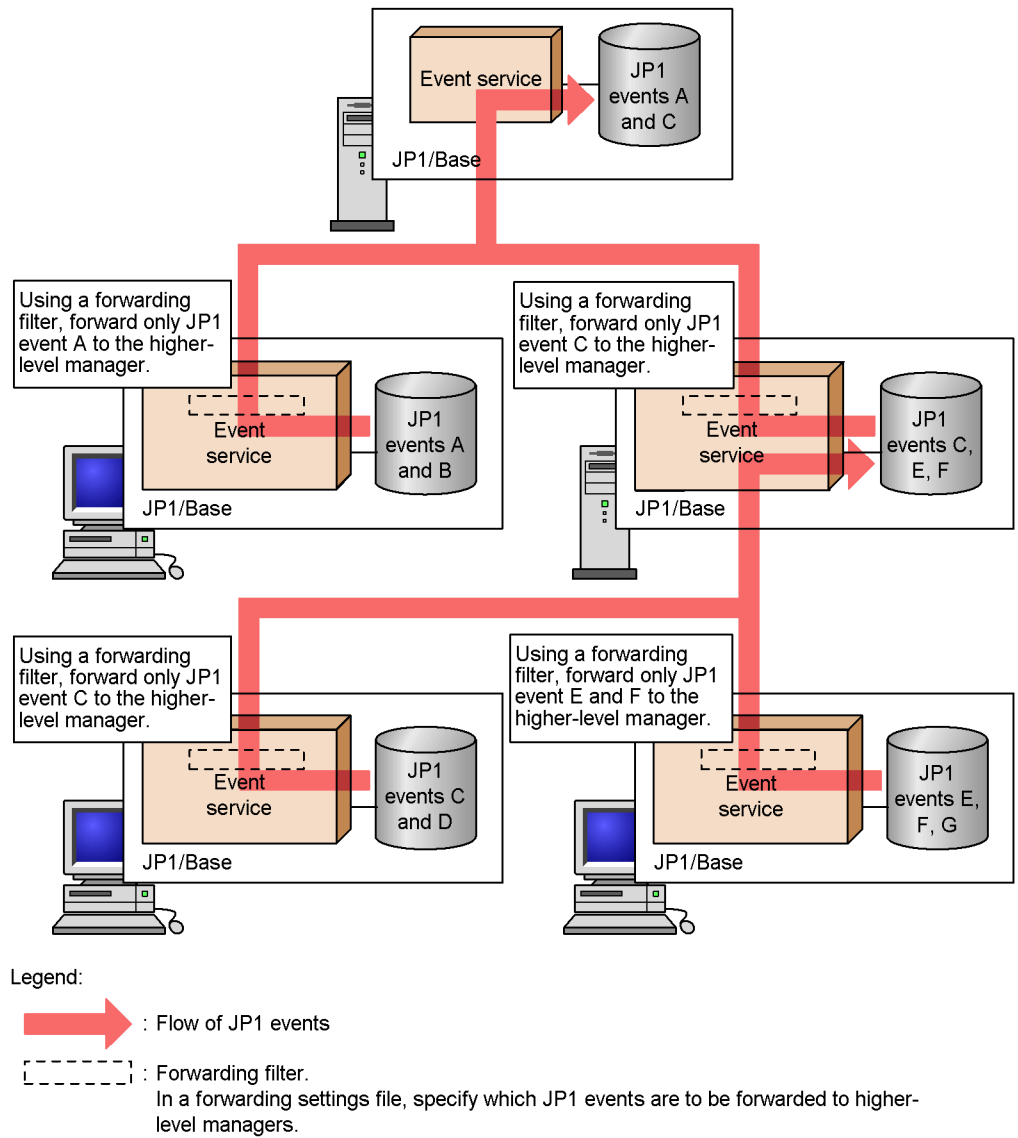
The JP1/Base event forwarding function forwards JP1 events from one host to another. By using this function, JP1/IM can forward JP1 events to a manager where they can be centrally managed.

To define which JP1 events to forward, use the forwarding settings file (`forward`) of the JP1/Base event service. This file is called a *forwarding filter* in JP1/IM.

Only important JP1 events needing management follow-up should be forwarded to a manager. Do not set up event forwarding to send all JP1 events that occur in the system. Under the default settings, JP1 events whose event level is `Emergency`, `Alert`, `Critical`, `Error`, or `Warning` are forwarded to higher-level managers according to the hierarchy defined in the configuration definition.

The following figure shows an example of how JP1 events are forwarded to higher-level managers.

Figure 7-9: JP1 event forwarding



You can change the forwarding settings by editing the forwarding settings file directly on each host. Alternatively, by using the JP1/Base functionality for collecting and distributing definitions, you can distribute the new settings from a higher-level host in a batch operation.

**(b) Retry setting for JP1 event forwarding**

The JP1/Base event service can automatically retry forwarding a JP1 event if transmission fails because of a network error or because the destination event server has stopped. Enter this setting in the JP1/Base event server settings file (`conf`).

See the chapter on setting the event service environment in the *Job Management Partner 1/Base User's Guide*.

**(c) Event forwarding according to configuration management**

When you define the hierarchy of managers and agents using the JP1/Base configuration management functions, each host is automatically set up to forward JP1 events to the higher-level manager according to the resulting configuration definition. When you change a definition in the configuration definition file, the JP1 event forwarding settings are updated automatically on each host.

See 7.4.3 *Managing the system hierarchy*.

**(d) Using the definition collection and distribution function**

By using the definition collection and distribution function, you can distribute JP1 event forwarding settings from a higher-level host defined in the system hierarchy to lower-level hosts (for an overview of configuring a system hierarchy, see 7.4.3 *Managing the system hierarchy*). You can use this function to halt event forwarding from another host when you need to temporarily stop a host for maintenance, for example, or you do not want a flood of events sent from a host on which numerous errors have occurred. By distributing the settings from the manager using a JP1/Base command, you can update the forwarding settings file (`forward`) at all the lower-level hosts. The forwarding settings are reloaded at each host when distribution is successful, and events are forwarded thereafter based on the updated information.

See 7.4.5 *Collecting and distributing definition information*.

**(3) Using JP1 events as historical and statistical information by CSV file output**

You can check the JP1 events stored in an event database by outputting the database contents to a CSV file using the JP1/Base `jevexport` command.

JP1/IM manages the system operation by collecting important JP1 events that require urgent attention on a manager where they can be monitored from JP1/IM - View. Non-urgent JP1 events, on the other hand, are recorded in the event databases of their respective hosts, but are not forwarded to a manager or displayed in JP1/IM - View.

However, information about non-urgent JP1 events (indicating that a job has ended normally, for example) may occasionally be required in order to compile statistical information or an operating history. In this case, use the JP1/Base command `jevexport` to output the database contents to a CSV file.

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

When you use the integrated monitoring database, you can output the JP1 events stored in the integrated monitoring database by using the JP1/IM `jcoevtreport` command.

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

### 7.4.3 Managing the system hierarchy

If you choose not to use IM Configuration Management, the system hierarchy is managed by JP1/IM through the configuration definition functions provided by JP1/Base. On the manager, define the host relationships in a configuration definition file (`jbs_route.conf`), and then apply the configuration definitions by executing the `jbsrt_distrib` command.

By defining the system hierarchy, you can perform the following operations in JP1/IM:

- Forward JP1 events to a higher-level host
- Execute commands from JP1/IM - View
- Execute automated actions from JP1/IM
- Collect and distribute definition information

If you wish to use IM Configuration Management to centrally manage the system hierarchy from JP1/IM - Manager, see *6. System Hierarchy Management Using IM Configuration Management*.

#### **(1) System hierarchy defined with the configuration definition functions**

In a 3-tier configuration defined using the JP1/IM configuration management functions, the managers in the middle tier serve as base managers.

You can define the system hierarchy in one operation on the top-level manager, or divide it into a number of parts and define them separately on the respective managers.

The following figure shows an example of a system hierarchy defined with the configuration management functions.

Figure 7-10: System hierarchy example (physical configuration)

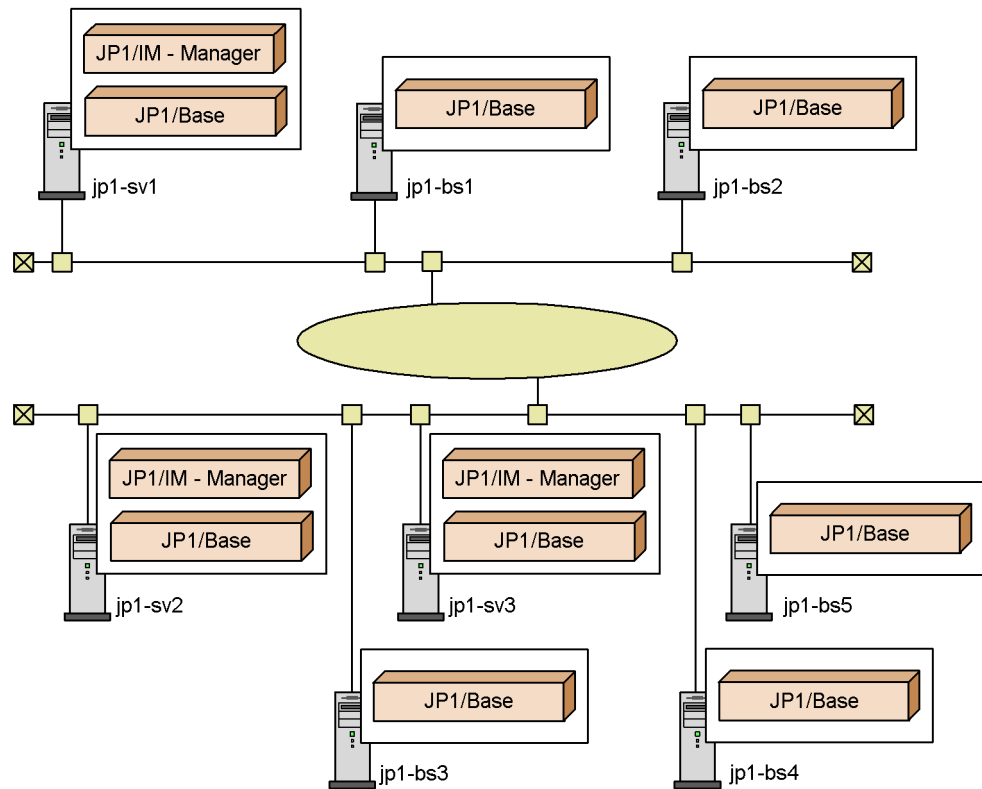


Figure 7-11: System hierarchy example (hierarchical relationships defined in one operation)

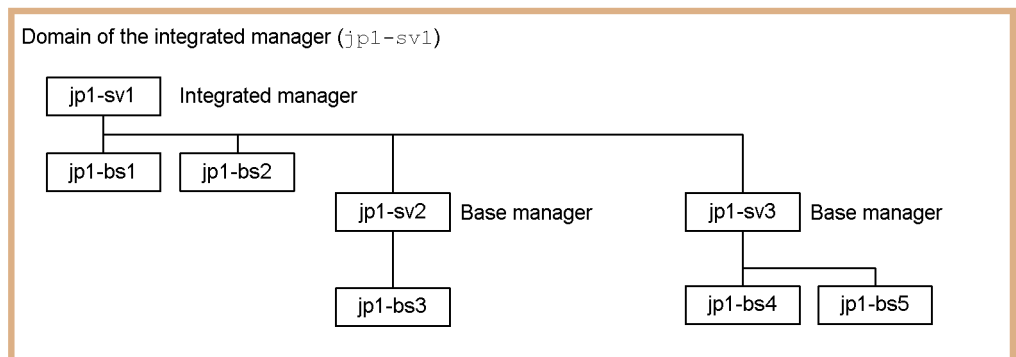
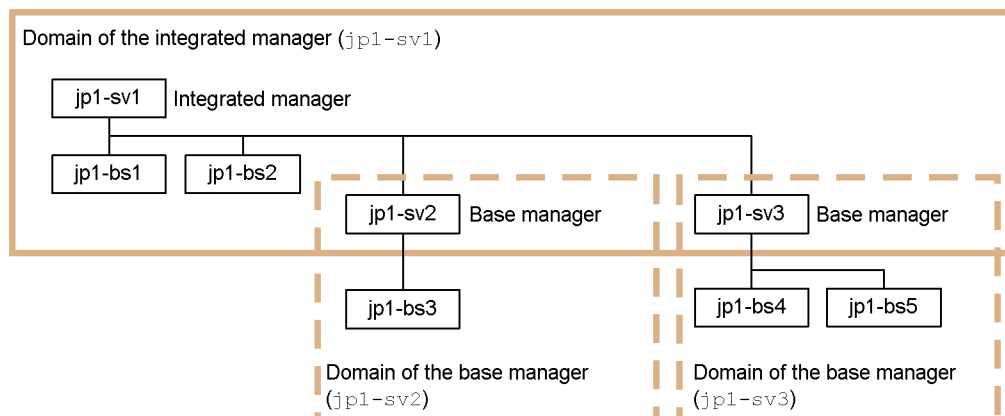


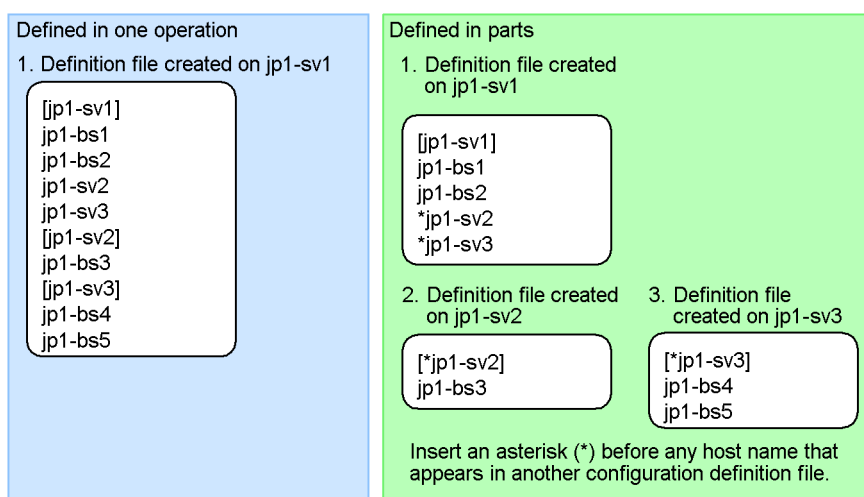


Figure 7-12: System hierarchy example (hierarchical relationships defined in parts)



Define the system hierarchy in the above example in the configuration definition file (`jbbs_route.conf`) as follows:

Figure 7-13: System hierarchy definition example



## (2) Procedure for defining a system hierarchy with the configuration management functions

The following is an overview of defining a system hierarchy using the configuration management functions:

1. Define the configuration definition file on the manager.

In the configuration definition file (`jbs_route.conf`), define the system configuration from the manager down to the lower-level managers and agents.

To define the system hierarchy in one operation, define the entire system configuration in the definition file. To define the system hierarchy in parts, write the configuration for each of the base managers and their lower-level hosts.

2. Execute the `jbsrt_distrib` command on the manager.

This command distributes the definition information to the hosts defined in the configuration definition file, and applies the configuration definition.

To define the system hierarchy in parts, perform steps 1 and 2 on each manager. Then, perform the following procedure at the top-level manager to create the definition for the entire system:

1. Define the configuration definition file on the top-level manager.

Create a configuration definition file (`jbs_route.conf`) that includes the top-level manager host and the managers directly below it in the hierarchy.

2. Execute the `jbsrt_sync` command on the top-level manager.

This command collects the configuration information from all managers defined in the configuration definition file, and creates configuration information for the entire system.

To check the system configuration definitions, execute the `jbsrt_get` command on each host.

For details about the format of the configuration definition file, see *Configuration definition file (jbs\_route.conf)* in 2. *Definition Files* in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*. For details about how to set configuration definition information, see 1.10 *Setting the system hierarchy (when IM Configuration Management is not used)* (for a Windows system) or 2.9 *Setting the system hierarchy (when IM Configuration Management is not used)* (for a UNIX system) in the *Job Management Partner 1/Integrated Management - Manager Configuration Guide*.

#### 7.4.4 Managing command execution

The JP1/Base command execution function controls the following modes of command execution in JP1/IM:

- Command execution from the Execute Command window of JP1/IM - View
- Command execution by automated action

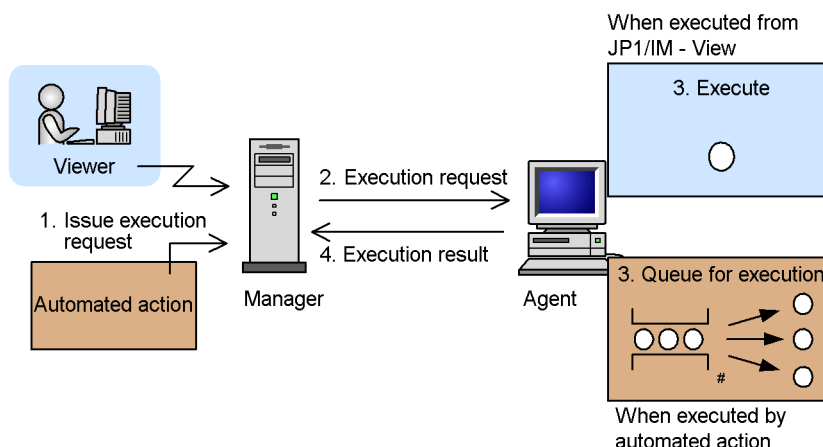
The following describes the JP1/Base command execution function.

### (1) Executing commands

When you execute a command in JP1/IM, JP1/IM on the manager directs the JP1/Base command execution function to execute the command. The command execution function then executes the command by sending a request to the agent specified as the execution target.

Commands executed by the user from JP1/IM - View or by an automated action are both processed by the command execution function. However, they differ in how the execution request is controlled (whether the request is queued or not queued).

Figure 7-14: Command execution



#: By default, commands are executed one at a time.

As shown in the above figure, when you execute a command from JP1/IM - View, the command is executed immediately without being queued. When you execute multiple commands, each command is executed without any controls being placed on the execution order or the number of commands that can be executed concurrently.

Commands executed by automated actions are queued up to the specified *command-queue-count*. Also, the system does not execute more commands at any one time than the specified *command-concurrent-execution-count*.

The flow of processing is described below, following the numbers in the figure:

1. A command is executed.
  - By an operation from JP1/IM - View

When you execute a command from JP1/IM - View, a request for command execution is sent to JP1/IM on the manager that you are logged in to. That instance of JP1/IM then passes the request to the command execution function of JP1/Base on the local host.

- By automated action

The automated action function of JP1/IM automatically executes an action upon receiving a JP1 event specified as a condition in an action definition. When this occurs, the command defined as the action in the action definition is passed by JP1/IM as an execution request to the command execution function of JP1/Base on the local host.

2. The manager requests the agent to execute the command.

The JP1/Base on the manager sends a request to the JP1/Base on the agent specified as the execution target, directing it to execute the command. If there is no response from the agent within the time period specified by *response-monitoring-time*, an error is returned to JP1/IM indicating that the host is unreachable.

3. The command is executed by JP1/Base on the agent.

The command execution function of JP1/Base on the agent executes the command using the OS shell or `cmd.exe`. The command is handled differently depending on how the command execution was requested:

- By an operation from JP1/IM - View

The command is executed immediately.

- By automated action

Command execution requests are queued by the command execution control of JP1/Base on the agent, and executed in order. The maximum number of commands in the queue is determined by the specified *command-queue-count*, and the number of commands that are executed in parallel is determined by the specified *command-concurrent-execution-count*. Although the number of commands being executed at any one time differs according to the duration of commands and the execution environment, it will never exceed *command-concurrent-execution-count* (under the default setting, *command-concurrent-execution-count* is set to 1, and commands are executed one at a time.)

Command execution may be delayed when a command executed by an automated action takes a long time to execute and commands are set to be executed serially (the default setting). In this case, you can reduce delays by setting the command execution function to execute commands in parallel.

Delays can also be introduced when a large number of commands are executed by automated actions, leading to a backlog of commands in the queue. You can gain advance notice of execution delays by setting the *command-queue-count-threshold* parameter (supported in JP1/Base 07-51). Under the default settings, a warning event is issued when the number of

commands in the queue reaches 10, and a recovery event is issued when the number returns to 0.

4. The command execution result is sent from the agent to the manager.

JP1/Base on the agent sends the command execution result (command output) to the JP1/Base on the manager. When the command finishes executing, JP1/Base on the agent reports the execution results to JP1/IM via JP1/Base on the manager.

At this time, log information for the command is recorded in a command execution log file on the manager. The maximum number of records that can be contained in the execution log is defined by the `-record` option of the `jccmddef` command.

You can view these command execution logs in the Execute Command window if the command was executed from JP1/IM - View, or in the Action Log Details window if the command was executed by an automated action.

In the description above, *response-monitoring-time*, *command-queue-count*, *command-concurrent-execution-count*, and *command-queue-count-threshold* are parameters of the JP1/Base command execution function. You can set these parameters using the `jccmddef` command.

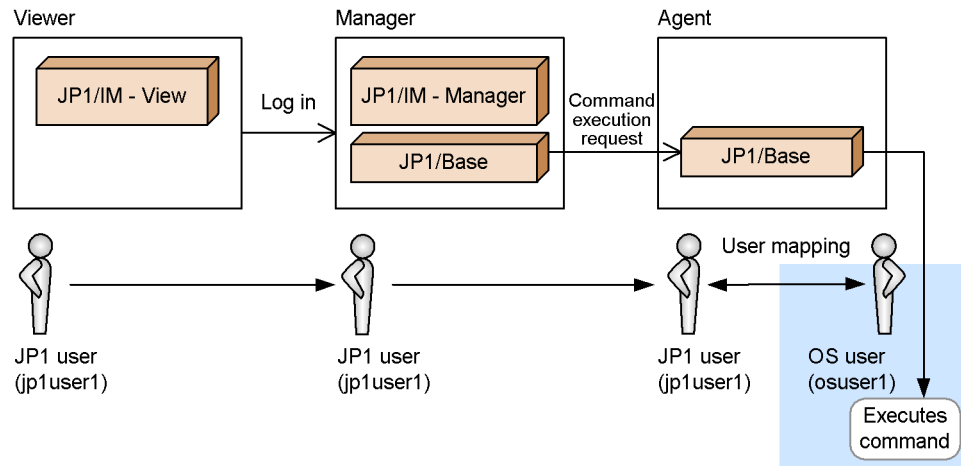
The flow of processing is described in 3.12.3 *Executing commands from JP1/IM - View* and 5. *Command Execution by Automated Action*. Refer to both of these descriptions as required.

## **(2) Users permitted to execute commands**

To execute commands in the OS environment of the agent, you must have the appropriate OS user permissions.

At command execution, user mapping associates the JP1 user with an OS user on the agent, and the command is executed under the OS user permission associated with that JP1 user account.

Figure 7-15: Command execution and user mapping



The command execution function directs the agent to use the following JP1 user accounts when executing commands:

- Command execution from JP1/IM - View

The JP1 user who is currently logged in to JP1/IM - View

- Command execution by automated action

The JP1 user specified in a definition with the highest priority based on the following ranking:

1. The JP1 user specified by the `u=` parameter in the automated action definition (`actdef.conf`)
2. The JP1 user specified by the `ACTIONEXECUSER` parameter in the automated action environment definition (`action.conf`)
3. `jp1admin`

At command execution, the JP1 user is mapped to the OS user defined in the user mapping at the agent where the command is to be executed.

### (3) OS-based command execution

The JP1/Base command execution function uses the following methods for command execution requested by JP1/IM - View or an automated action.

#### (a) Users permitted to execute commands

The command is executed by the OS user mapped to the JP1 user.

**(b) Method of command execution**

The command execution function uses the following methods to execute commands:

- In Windows

The command execution function executes `cmd.exe /c command`.

- In UNIX

The command execution function uses the login shell of the OS user to execute the command, for example `/bin/sh -c command` (where the login shell is `/bin/sh`).

When you execute a command that creates a child process, JP1/Base will be unable to process the next command until the child process has terminated. This is because command execution management recognizes the command as still running.

**(c) Environment for command execution**

The environment used for command execution is described below.

- Environment variables

You can use an environment variable file in JP1/IM to specify the environment variables used at command execution. Specify the environment variable file in the Execute Command window of JP1/IM - View or in the automated action definition file (`actdef.conf`).

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

If you do not set up an environment variable file, the following environment variables are used.

- In Windows

The Windows system environment variables are used at command execution.

- In UNIX

The environment variables of the command execution process (the environment variables specified in the JP1/Base start command `jbs_start`, for example) are used at command execution. The OS user profile is not loaded in UNIX systems.

- OS user profile (Windows only)

You can load the OS user profile when you execute a command on the target host. You can enable this function using the `-loaduserprofile` option of the `jccmddef` command (it is disabled by default).

*Note:*

The environment on the target host must allow the commands to execute normally. Note the following, for example:

- Each command requires a certain amount of resources, such as memory, to execute. When you execute a large number of commands concurrently, the system may have insufficient resources to execute the commands. When there are insufficient system resources in Windows, for example, a dialog box is displayed with the message **cmd.exe - DLL initialization failed**.

If this occurs, adjust the number of commands that are executed concurrently to ensure that sufficient resources are available for each command.

- Commands that cannot be executed in the format `cmd.exe /c command` or `shell -c command` cannot be executed by the JP1/Base command execution function.

**(d) Command execution results**

The execution results for commands executed by the command execution control are handled as follows:

## Outputting command execution results

Command execution results (such as messages) are recorded<sup>#</sup> in a command execution log file managed by the command execution control on the manager. Log information for commands executed from JP1/IM - View appears in the Execute Command window, and log information for commands executed by automated actions appears in the Action Log Details window.

When multiple commands are executed, the results may be output in a different order from the execution order. The result output timing is affected by such things as the time required to execute each command, performance and workload differences among the hosts on which the commands are executed, and retry after a communication error.

#

By changing settings in JP1/Base, you can limit the amount of execution result data output to the command execution log file when commands are executed from JP1/IM - View or by automated actions. You can either restrict the amount of transferred data or prevent registration of detailed information. Both are performed by specifying options in the `jcocmddef` command. Choose whichever method best suits your system operation.

- Restricting the amount of transferred data

You can restrict the amount of execution log data by setting an upper



limit (as a number of lines) for the amount of data that can be transferred from the execution-target host to the manager. This helps control the size of the command execution log file and reduces congestion on the communication lines between the hosts.

You can set separate limits for the execution results of commands executed from JP1/IM - View and for those executed by automated actions.

If you performed a new installation of version 8 of JP1/Base, data transfer will be restricted to a maximum of 1,000 lines by default. If you are running version 7 of JP1/Base, or if you upgraded from version 7 to version 8, data transfer will not be restricted by default.

- Preventing registration of detailed information (applies to commands executed by automated actions only)

For the execution results of commands executed by automated actions, you can choose to register only information indicating the success or failure of the command, and discard detailed information such as message information. By doing so, you can improve the processing speed of the underlying JP1/Base components (and hence the speed with which automated actions are processed). However, when you prevent registration of detailed information, the message KAVB2401-I appears in the **Message** area of the Action Log Details dialog box, and no detailed log information is displayed (the **Log** area is unaffected). Do not enable this setting if you need to view detailed information (the setting is disabled by default).

#### Command execution results (return code)

The following return codes appear in the command execution results:

- In Windows

The return code passed to the command execution function by `cmd.exe`.

- In UNIX

The return code passed to the command execution function by the shell that executed the command.

The command will not execute if an error occurs leading up to command execution (for example user mapping fails or the target host cannot be contacted).

#### **(4) Using host groups to execute commands on multiple hosts**

You can define a number of hosts together as a single group.

You can specify a host group as the target host at command execution. By doing so, you can execute the command on all the hosts in that group in a single operation.

For details about defining host groups, see *Host group definition file* in 2. *Definition Files* in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.

### **(5) Issuing JP1 events based on the command execution status**

You can issue JP1 events that indicate the execution status of commands, such as when command execution starts and stops. JP1 events can be issued in the following cases:

- Command execution from JP1/IM - View  
When a command starts executing, finishes executing, or terminates abnormally.
- Action (command) execution by automated action  
When a command starts executing, finishes executing, terminates abnormally, or fails to execute (due to a failed request).

By enabling this functionality, you can use JP1 events to manage information about when commands are executed, by which users, and on which hosts. You can then display and monitor this information in the Event Console window of JP1/IM - View.

Use the `jcocmddef` command to set up issuing of these JP1 events.

The JP1/Base command execution function also provides for other JP1 events, examples of which are given below. These JP1 events do not require setup as above.

- JP1 events issued based on how long a command takes to execute  
This function is supported from version 07-51 of JP1/Base. A JP1 event is issued when a command has not finished executing within a predetermined period of time. This JP1 event helps you to identify hangups or undue delays in commands executed from JP1/IM - View or by automated action.  
By default, this JP1 event is issued at 10-minute intervals. You can change this setting using the `jcocmddef` command.
- JP1 events issued when the queuing threshold is exceeded  
This function is supported from version 07-51 of JP1/Base. A JP1 event is issued when the number of commands in the queue reaches or exceeds a predetermined number, and another event is issued when the number returns to an acceptable level. These JP1 events allow you to gain advance notice of execution delays when a large number of commands are executed by automated actions, and let you know when the situation has recovered.  
Under the default settings, a warning event is issued when the number of commands in the queue reaches 10, and a recovery event is issued when the number returns to 0. Use the `jcocmddef` command to modify these settings.

### **(6) Commands for troubleshooting**

You may encounter the following problems when using the JP1/Base command

execution function from JP1/IM.

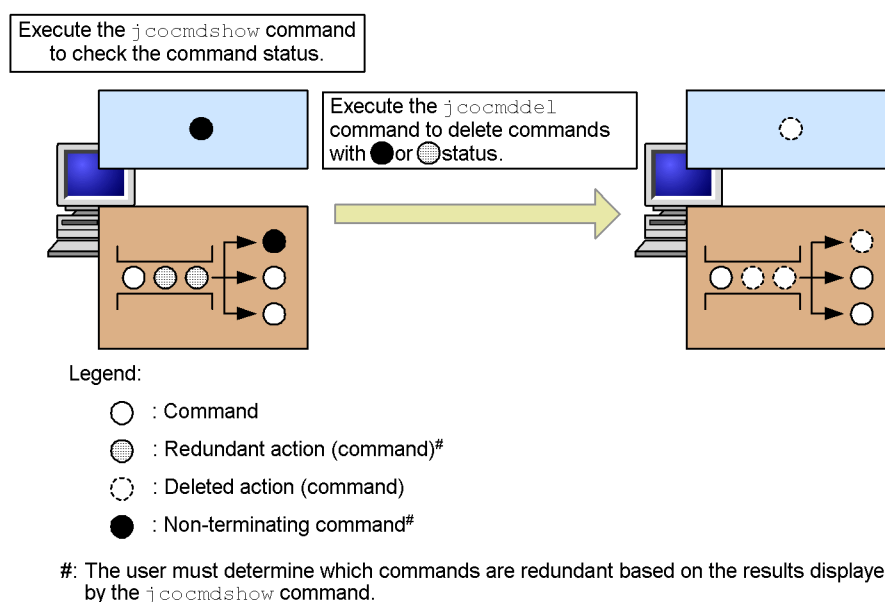
- A command whose execution is not supported in JP1/IM - View (see 3.12.3(1) *Executable commands*) is executed and remains stuck in executing status.
- A greater number of automated actions occur than was anticipated at the design stage, leading to a massive backlog of redundant actions in the queue.
- A command executed by an automated action hangs or takes longer than expected to execute, preventing succeeding commands (actions) from executing.

To allow you to recover quickly from these errors, JP1/Base provides a command for checking the status of queuing or executing commands (`jcocmdshow`), and a command for deleting queuing or executing commands (`jcocmdel`)<sup>#</sup>.

#

JP1/IM can cancel automated actions when command execution results in an error. When an error occurs in a command executed by an automated action, use this function where possible (for details, see 5.7 *Canceling automated actions*).

Figure 7-16: Overview of `jcocmdshow` and `jcocmdel` commands



The `jcocmdshow` command displays the following information. Based on this information, determine which commands need to be deleted, and then delete them using the `jcocmdel` command.

Table 7-13: Information displayed by the `jcocmdshow` command

Display item	Description
ID	The unique ID assigned to commands that are executing or queuing in the command execution function. When you use the <code>jcocmddel</code> command to delete a command, use this ID as the key.
STATUS	The execution status of the command in the command execution function, shown as either Running or Queuing.
TYPE	Whether the command was executed by JP1/IM - View or an automated action.
USER	The name of the JP1 user who issued the command execution request.
STIME	The time at which the command execution function received the instruction from JP1/IM to execute the command.
ETIME	The length of time that has elapsed since the command started execution.
COMMAND	The name of the executing or queuing command.

The `jcocmdshow` and `jcocmddel` command functionality is provided by JP1/Base and may not be supported depending on the version of JP1/Base on the host where the problem occurred. For details, see the *Job Management Partner 1/Base User's Guide*.

The `jcocmdshow` and `jcocmddel` commands can be executed in any of three ways:

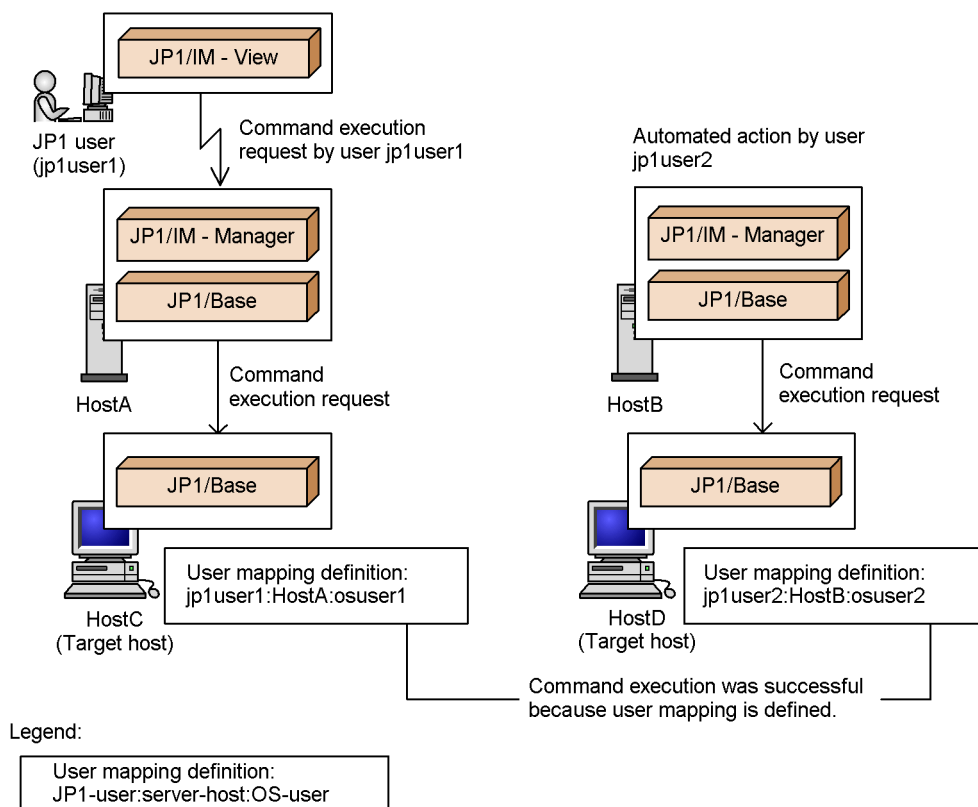
- From JP1/IM - View  
You must specify the `-f` option when you execute the `jcocmddel` command from JP1/IM - View.
- From the manager to an agent target host  
You must specify the `-s` option. Note that in order to execute these commands, the manager must also be running JP1/Base version 07-51 or later.  
Take care when using this option, as communication will take place directly between the manager and agent (using the same communication path as the definition collection and distribution function).
- Directly on the host where the problem occurred

For details about these commands, see the command descriptions in the *Job Management Partner 1/Base User's Guide*.

### (7) Conditions for command execution

The following figure summarizes the conditions for executing commands from JP1/IM - View and by automated actions.

Figure 7-17: Conditions for executing commands and automated actions



Conditions for executing commands from JP1/IM - View:

1. The logged-in JP1 user has permission to execute commands.

JP1 users with JP1\_Console\_Admin or JP1\_Console\_Operator permissions are permitted to execute commands.

2. User mapping is defined on the target host.

User mapping is defined as follows:

*JP1-user:server-host:OS-user*

*JP1-user* is the user who is operating JP1/IM - View, *server-host* is the name of the server host the JP1 user is logged in to, and *OS-user* is the user name of a user or domain user registered on the target host.

3. The system configuration definition is set up (when executing commands on another host).

If the system configuration is not defined, you will be unable to execute commands on another host from JP1/IM - View.

Conditions for executing commands by automated action from the manager:

1. User mapping is defined on the target host.

User mapping is defined as follows:

*JP1-user:server-host:OS-user*

*JP1-user* is the user who executes the automated action, *server-host* is the name of the server host that issues the instruction to execute the automated action, and *OS-user* is the user name of a user or domain user registered on the target host.

2. The system configuration definition is set up (when executing commands on another host).

If the system configuration is not defined, you will be unable to execute a command on another host by automated action.

### 7.4.5 Collecting and distributing definition information

If you choose not to use IM Configuration Management, the information defined in JP1/Base on the hosts is collected and distributed using the definition collection and distribution functions provided by JP1/Base. Using these functions, you can perform the following operations:

- Collect and distribute event service definitions
- Auto-generate a monitoring tree (by collecting definition information)

Definition collection and distribution is functionality specific to JP1/IM - Manager and provided through JP1/Base. Depending on the JP1/Base version, this functionality may not be supported. For details, see the *Job Management Partner 1/Base User's Guide*.

Note that these definition collection and distribution functions are sometimes called plug-in functions. When you use the JP1/Base `jbs_spmc_status` command to verify the status of the service, look for the displayed name `jbsplugin`.

#### (1) Collecting and distributing event service definitions

When using JP1/IM to monitor the system operation, you must consider, for each host, which events should be managed as JP1 events and which events should be forwarded to higher-level hosts, and define the event service accordingly. Although you can check and modify definitions in JP1/Base on each host individually, this is highly inefficient and can lead to mistakes in the definitions.

Using the definition collection and distribution functions of JP1/Base, you can batch-collect information defined in JP1/Base on the hosts, and manage the

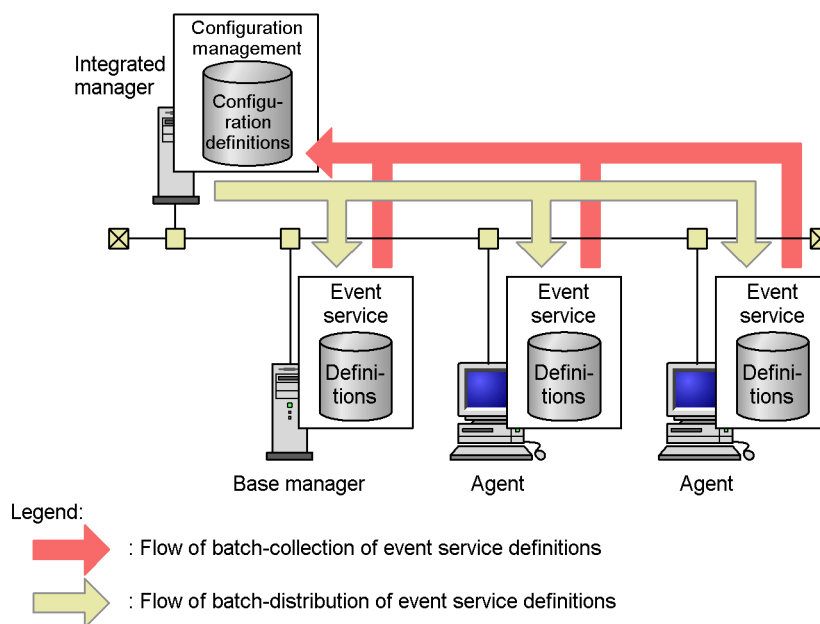
information on the manager. You can also update the definition information on each host by editing and distributing the definition information from the manager. Hence, these functions provide an efficient way of centrally managing definitions related to the event service.

You can collect and distribute definitions from the following files:

- Forwarding setting file (`forward`)
- Action definition file for log file trapping (any file)
- Action definition file for event log trapping (`ntevent.conf`)

The following figure shows the flow of processing when event service definitions are collected from or distributed to all the hosts in the system as a batch operation.

Figure 7-18: Batch-collection and batch-distribution of event service definitions



Working in conjunction with configuration management, the definition collection and distribution functions collect and distribute definitions to the hosts defined in the configuration definition as a batch operation (for details about defining the system configuration, see *7.4.3 Managing the system hierarchy*). When the manager collects definitions from or distributes definitions to managed hosts, it communicates with the hosts directly without regard to the system hierarchy defined in the configuration definition. For this reason, take care when using these functions in a firewall environment.

To collect and distribute event service definitions as a batch operation, use the

commands provided by JP1/Base. For details about the procedures and a description of the batch-collection and batch-distribution commands, see the chapter on collecting and distributing event service definitions (JP1/IM only) in the *Job Management Partner 1/Base User's Guide*.

## **(2) Auto-generation of monitoring trees (Central Scope)**

JP1/IM provides the Monitoring Tree window and Visual Monitoring window to allow objective-oriented system monitoring in accordance with the needs of the system administrator. When you create a Monitoring Tree window, you can use the auto-generation function to generate a monitoring tree automatically, and then customize the tree to suit your needs.

The auto-generation function collects definitions relating to specific linked products from each server, and uses a template to create a monitoring tree from the collected information. The collection of definitions is performed as functionality specific to JP1/IM - Manager, realized through the definition collection and distribution functions provided by JP1/Base.

When directed by JP1/IM - Manager to collect definitions from linked products, JP1/Base collects the definitions from the linked products on that host, and passes the information to JP1/IM. This functionality is supported from JP1/Base version 07-00. To collect definitions, the Central Scope service of JP1/IM - Manager must be active (ON).

The following are examples of the definition information that can be collected and distributed:

- Information about jobs that are being executed automatically by JP1/AJS
- Performance data being monitored by JP1/PFM
- System information in a Cosminexus environment (logical servers, J2EE applications, and so on)

A monitoring tree is created automatically from this information collected from the hosts defined in the system hierarchy.

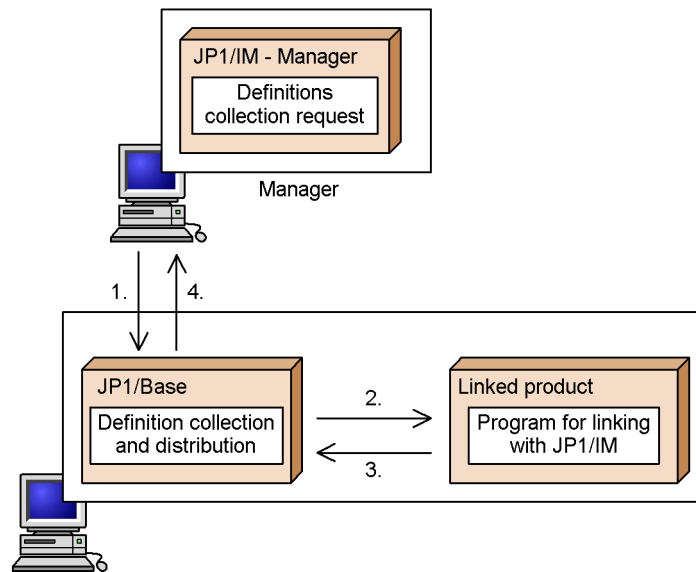
The collection of definition information from linked products is realized by interaction between the JP1/IM functionality and the configuration management and definition collection and distribution functions of JP1/Base. For details about how the JP1/IM functionality works in conjunction with the JP1/Base configuration management functions, see *4.10.4 Automatic generation of a monitoring tree*.

The following describes the behavior of JP1/Base on a target host when directed by JP1/IM to collect definition information.

The following figure shows the flow of the processing to collect definition information within each host.



Figure 7-19: Collection of definition information within a host



The flow of processing is described below, following the numbers in the figure:

1. The host receives a definitions collection request from the manager.
2. On receiving the request, JP1/Base requests definition information from any linked product on that host that supports the JP1/IM definition collection and distribution functions.
3. The linked product that receives the request starts the JP1/IM linkage program to send back the relevant information to JP1/Base.

To start the JP1/IM linkage program, a command that sets up JP1/IM linkage must have been executed on the linked product. For details about the command that sets up JP1/IM linkage, see the documentation for the linked product.

4. On receiving the definitions from the linked product, JP1/Base passes the information back to the manager that issued the request.

#### 7.4.6 Managing service startup (Windows only)

JP1/Base provides startup control for services.

In Windows, the functions of JP1/IM - Manager and JP1/Base are registered as Windows services at installation. By using the Windows service control manager, you can set services to start automatically when the OS starts. However, you cannot set services to start in a particular order (for example, JP1/Base before JP1/IM - Manager) because Windows does not monitor service dependencies. In some cases, a product

that issues JP1 events may start before JP1/Base starts. Because JP1/Base is inactive, such JP1 events cannot be managed. To avoid such situations, use the startup control provided by JP1/Base in Windows systems.

For details about JP1/Base startup control, see the chapter on setting the service start and stop sequences (for Windows only) in the *Job Management Partner 1/Base User's Guide*.

In UNIX-based operating systems, you can use an OS function to control the sequence in which services such as JP1/Base and JP1/IM - Manager start and stop, by registering the services in scripts.

#### 7.4.7 Hitachi Network Objectplaza Trace Library (HNTRLib2)

JP1/Base and JP1/IM provide the Hitachi Network Objectplaza Trace Library (HNTRLib2) to help investigate the cause of errors.

The Hitachi Network Objectplaza Trace Library (HNTRLib2) outputs trace information from the various functions of JP1/Base and JP1/IM to a single *integrated trace log*. The collection of trace information for related products in a coherent manner allows you to gain an overview of what is happening throughout the system, which is of particular value in the initial stages of tracking down a problem. As follows are potential applications of the trace library:

1. Investigating the entire system  
Investigate each host machine based on entries in the Windows event log or UNIX syslog.
2. Investigating JP1 products in the JP1 series  
Investigate JP1 products by checking the flow of operations in the Hitachi Network Objectplaza Trace Library (HNTRLib2).

Each of the JP1 product functions make use of an internal log in addition to the integrated trace log. In combination, these logs allow you to investigate problems in detail. To facilitate the collection of this data in the event of a problem, prepare the JP1/Base and JP1/IM data collection tools when you set up the system.

The Hitachi Network Objectplaza Trace Library (HNTRLib2) is installed when you install JP1/Base or JP1/IM - View, but is also used by JP1/AJS and other Hitachi products. For details about whether a product uses the Hitachi Network Objectplaza Trace Library (HNTRLib2), see the relevant product manual.

#### 7.4.8 JP1/Base health check function

The JP1/Base health check function monitors JP1/Base processes for hangups<sup>#</sup>, abnormal termination, and other problems, and issues a message or JP1 event to report the error and prompt the operator to take recovery action. By using this function, JP1/IM can check whether the instances of JP1/Base in the JP1/IM system are operating

normally. The health check function is disabled by default. Enable the function by changing the setting in the common definition information.

#: Hangups are caused by a deadlock or infinite loop, and mean that the process can no longer accept processing requests.

This subsection gives an overview of the JP1/Base health check function. For details about how the function works and how to set it up, see the chapter on setting the health check function in the *Job Management Partner 1/Base User's Guide*.

Broadly classified, the JP1/Base health check function has two roles:

- Monitoring the status of JP1/Base processes on the local host
- Monitoring the status of JP1/Base processes on remote hosts

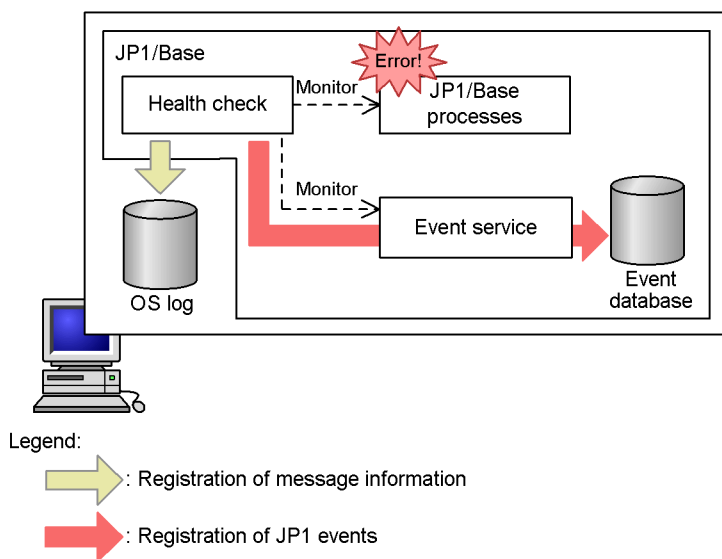
Depending on the JP1/Base version, this functionality may not be supported. For details, see the *Job Management Partner 1/Base User's Guide*.

### (1) Monitoring the status of JP1/Base processes on the local host

By enabling the health check function, you can detect hangups and abnormal terminations in JP1/Base processes on the local host. This information is registered in the operating system's log (the Windows event log or UNIX syslog) as message information, or in the event database as JP1 events, depending on how JP1/Base is set up.

The figure below shows how JP1/Base processes are monitored on the local host.

Figure 7-20: Monitoring the status of JP1/Base processes on the local host



By recording errors that affect JP1/Base as JP1 events in the event database, you can use JP1/IM to monitor JP1/Base for errors.

The health check function is unable to monitor the status of other processes if the function itself hangs or terminates abnormally. Also, JP1 events cannot be registered if an error occurs in the event service.

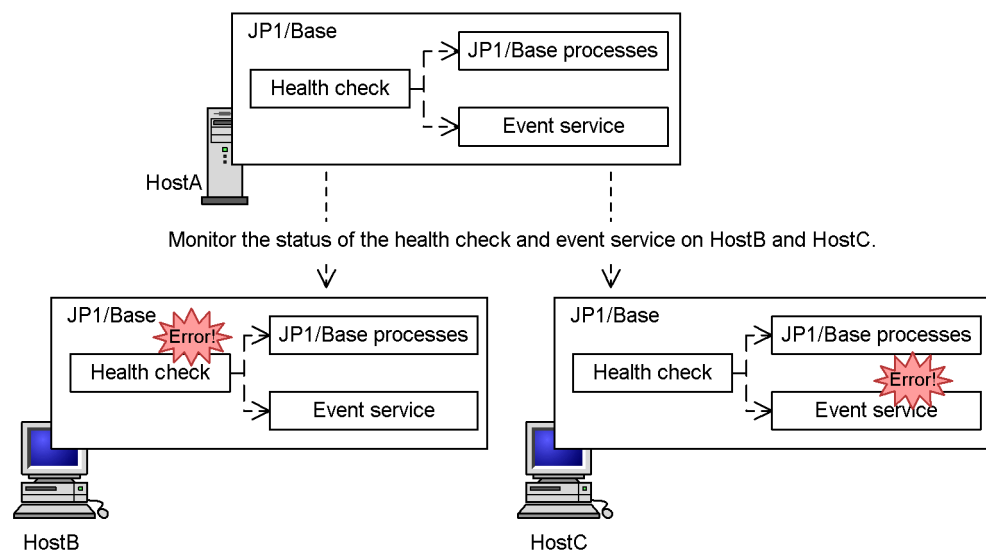
To avoid this type of situation, the health check function and the event service must be monitored by the health check function of JP1/Base on a remote host.

## (2) Monitoring the status of JP1/Base processes on remote hosts

The JP1/Base health check function can monitor the status of the JP1/Base health check function and the event service on remote hosts, as well as the JP1/Base processes on the local host. Thus, you can prevent situations in which errors in JP1/Base processes are overlooked because of an error in the health check function, or JP1 events are not registered because of an error in the event service.

The figure below shows how JP1/Base processes are monitored on remote hosts.

Figure 7-21: Monitoring the status of JP1/Base processes on remote hosts



The above figure shows a configuration in which the health check functions and event services of HostB and HostC are monitored from HostA. When an error occurs in the health check function on HostB, HostA detects the error and records the particulars in its own OS log or event database. When an error occurs in the event service on HostC, HostA detects the error and records the particulars in its own OS log or event database<sup>#</sup>.

#: In this situation, JP1 events cannot be registered in the event database on HostC. However, log information can still be registered in the OS log provided that the health check function is working normally.

In this manner, JP1/Base detects errors in JP1/Base processes.

### 7.4.9 JP1/Base process management

Process management is a core functionality of JP1/Base that starts and stops the processes that make up JP1/Base. Another responsibility of process management is to issue instructions for checking the status of JP1/Base functions and reloading definition information.

JP1/Base process management controls the following functions:

- User management (jbssessionmgr) (also referred to as the authentication server)
- Configuration management (jbsroute)
- Command execution (jcocmd)
- Definition collection and distribution (jbsplugin)
- Health check (jbshcd and jbschostd)

The event service, event converters, and Hitachi Network Objectplaza Trace Library (HNTRLib2) operate independently of the process management functionality. For details, see the *Job Management Partner I/Base User's Guide*.

Process management is realized by the following commands:

Table 7-14: Process management commands

Functionality	Command	Description
Start JP1/Base (internal command)	jbs_spmd	Internal commands used to start and stop JP1/Base processes. These commands apply to the processes managed by process management. Do not execute these commands directly to start or stop JP1/Base process management. In Windows, JP1/Base process management is started and stopped by the Windows service control manager. In UNIX, use the start and stop commands (jbs_start and jbs_stop).
Stop JP1/Base (internal command)	jbs_spmd_stop	
JP1/Base status check	jbs_spmd_status	Checks the activity status of the processes managed by process management.
Reload JP1/Base definition information	jbs_spmd_reload	When definition information is updated for a process managed by process management, this command reloads and applies the new definitions.

Process management also provides the following functionality to help detect and deal with errors in JP1/Base.

- Automatically restarting an abnormally ended process
- Issuing a JP1 event when a process error is detected

This functionality applies to the processes under the control of process management, and is supported from JP1/Base version 07-00.

*Note:*

If you are using JP1/Base in a cluster system, do not set up process management to restart processes at abnormal termination, as the error in the JP1/Base process may also affect the function that restarts processes. To ensure a more reliable restart, restart JP1 under the control of the clustering software.

For details about the commands in the table and how to deal with process management errors, see the description of the settings for dealing with JP1/Base errors in the chapter on installation and setup in the *Job Management Partner 1/Base User's Guide*.

## Chapter

---

# 8. Linking with the JP1/IM Series

---

As well as collecting and centrally managing the management information of other software products and the events that occur in the system, JP1/IM provides functionality for using JP1/IM management information in JP1/IM - Rule Operation, another integrated management product.

JP1/IM - Rule Operation executes troubleshooting processes automatically. When the system generates a JP1 event being monitored by JP1/IM, JP1/IM - Rule Operation judges the JP1 event against a rule startup condition. If the condition is met, JP1/IM - Rule Operation invokes the rule and executes the process prescribed in the rule definition.

This chapter describes the functionality provided by JP1/IM for linking with JP1/IM - Rule Operation.

### 8.1 Linking with JP1/IM - Rule Operation

---

## 8.1 Linking with JP1/IM - Rule Operation

---

The Central Console provides the following functionality used for linking with JP1/IM - Rule Operation:

- Automatically sending rule startup requests to JP1/IM - Rule Operation
- Checking the notification progress and result of such rule startup requests

This functionality is used only for linking with JP1/IM - Rule Operation, and is thus disabled by default.

This section describes this functionality. For details on JP1/IM - Rule Operation, see the *Job Management Partner 1/Integrated Management - Rule Operation System Configuration and User's Guide*.

*Note:*

The JP1/IM - Rule Operation linkage function is provided as an extension of the automated action function. For the most part, the setup procedures and flow of processing are the same as for automated actions.

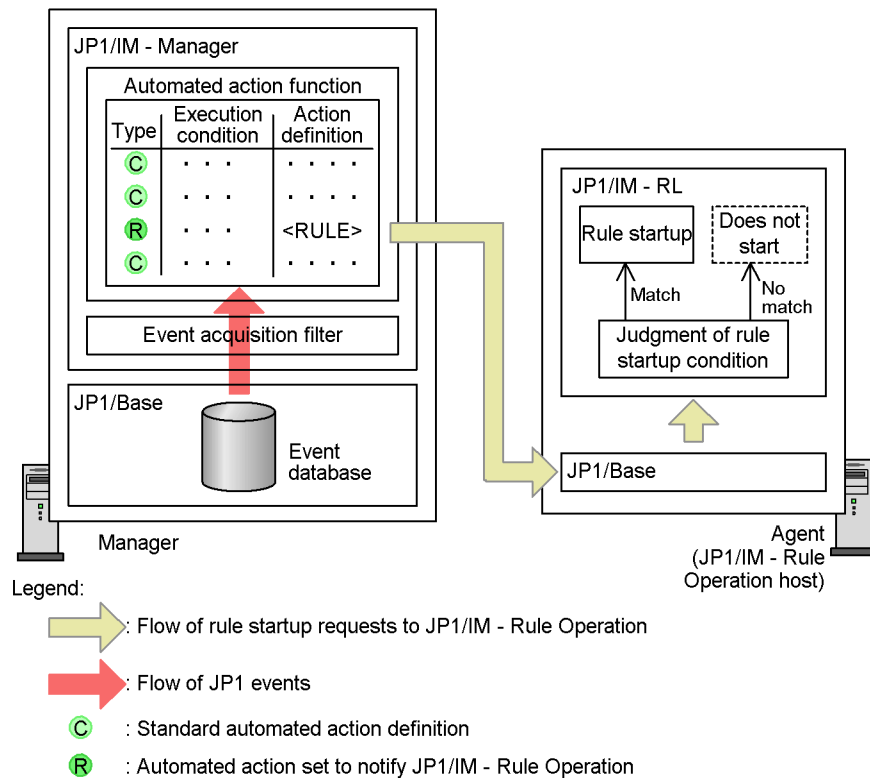
This chapter describes only the characteristics of the JP1/IM - Rule Operation linkage function that differ from automated actions. For details on those that are shared with standard automated actions, see 5. *Command Execution by Automated Action*.

### 8.1.1 Sending rule startup requests to JP1/IM - Rule Operation

When JP1/IM - Rule Operation linkage is enabled, rule startup requests are sent to JP1/IM - Rule Operation automatically via automated actions.



Figure 8-1: Overview of JP1/IM - Rule Operation linkage



When JP1/IM - Rule Operation linkage is enabled, display items related to JP1/IM - Rule Operation appear in the Action Parameter Detailed Definitions window of JP1/IM - View. This allows you to set the conditions for notifying JP1/IM - Rule Operation.

Once a notification condition has been set, whenever a JP1 event triggers a rule startup request, JP1/IM - Manager automatically sends the request to JP1/IM - Rule Operation.

In JP1/IM - Rule Operation, if the received rule startup request is found to match a rule startup condition, the rule is judged valid and executed.

### (1) Enabling and disabling JP1/IM - Rule Operation linkage

To enable or disable JP1/IM - Rule Operation linkage, use the `jcoimdef` command. For details, see `jcoimdef` in 1. *Commands* in the manual *Job Management Partner 1/ Integrated Management - Manager Command and Definition File Reference*.

When you connect from JP1/IM - View to a JP1/IM - Manager with JP1/IM - Rule Operation linkage enabled, display items related to JP1/IM - Rule Operation linkage appear in the following windows:

Additional setup items appear in:

- Action Parameter Definitions window
- Action Parameter Detailed Definitions window

Additional display items appear in:

- Action Log window
- Action Log Details window
- List of Action Results window
- **Search Events** page
- Settings for View Filter window
- Severe Event Definitions window
- Detailed Settings for Event Receiver Filter window

For details about these windows, see 2. *Event Console Window* in the manual *Job Management Partner 1/Integrated Management - Manager GUI Reference*.

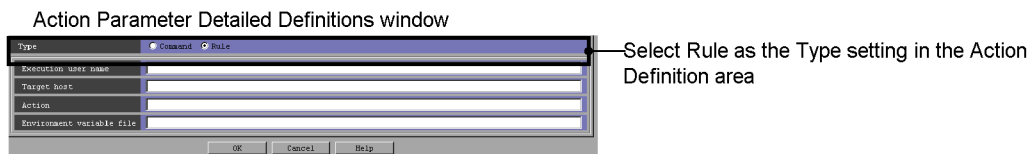
## **(2) Setting notification conditions for sending rule startup requests to JP1/IM - Rule Operation**

As with standard automated actions, you can set conditions for sending rule startup requests to JP1/IM - Rule Operation in the Action Parameter Detailed Definitions window or in the automated action definition file (`actdef.conf`).

When setting a notification condition to send a rule startup request, include only the JP1 events specified as the rule startup conditions. This ensures that no more than the minimum necessary automated actions will be executed.

Perform the same settings as for a standard automated action, except for the parts shown in the figure below.

Figure 8-2: Condition for sending a startup request to JP1/IM - Rule Operation



Automated action definition file (actdef.conf)

DESC\_VERSION=3

```
cmn
  sta false
end-cmn
```

act Action 1

```
  prm 0
  eid 123
```

```
  cnd
    E.SEVERITY IN Error
  end-cnd
```

```
  cmd C:\temp\sample.exe
```

end-act

act Action 2

```
  prm 0
  eid 777
```

```
  cnd
    E.SEVERITY IN Critical
  end-cnd
```

```
  cmd C:\temp\sample2.exe
```

end-act

act Action 3

```
  prm 0
  eid 555
```

```
  cnd
    E.SEVERITY IN Emergency Alert Critical Error Warning
  end-cnd
```

```
  rul
```

end-act

Legend:

: Event monitoring condition

: Action definition

#: The definition sends a startup request to JP1/IM - Rule Operation under the following conditions:

- Event ID: 555
- Event level of JP1 event: Warning, Error, Critical, Alert, or Emergency

The following items, although used when setting an automated action, must be set in

a particular way when setting a condition for sending a startup request to JP1/IM - Rule Operation:

- Execution user: Specify a JP1 user mapped to an OS user on the target JP1/IM - Rule Operation host. Set this user by the `jcoimdef` command.
- Target host: Specify the target JP1/IM - Rule Operation host. Set this host by the `jcoimdef` command. Unlike automated actions, you cannot specify a host group.
- Action: Fixed as `<RULE>`. When JP1/IM - Rule Operation receives a startup request, it executes an internal command using as arguments the JP1/IM - Manager host name, the serial number of the JP1 event that triggered the request, and the arrived time.
- Environment variable file: You cannot specify an environment variable file.

For details about the Action Parameter Detailed Definitions window, see 2.25.1 *Action Parameter Detailed Definitions window* in the manual *Job Management Partner 1/Integrated Management - Manager GUI Reference*. For details about the definition file, see *Automated action definition file (actdef.conf)* in 2. *Definition Files* in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.

### (3) Flow of notification processing

Rule startup requests are sent to JP1/IM - Rule Operation based on the system hierarchy definition, as for a standard automated action. The status transitions of the communication processing are the same as for a standard automated action.


## 8.1.2 Checking the status and result of notification to JP1/IM - Rule Operation

You can check the status and result of notification to JP1/IM - Rule Operation using the following windows and command:

- Action Log window
- Action Log Details window
- List of Action Results window
- `jcashowa` command

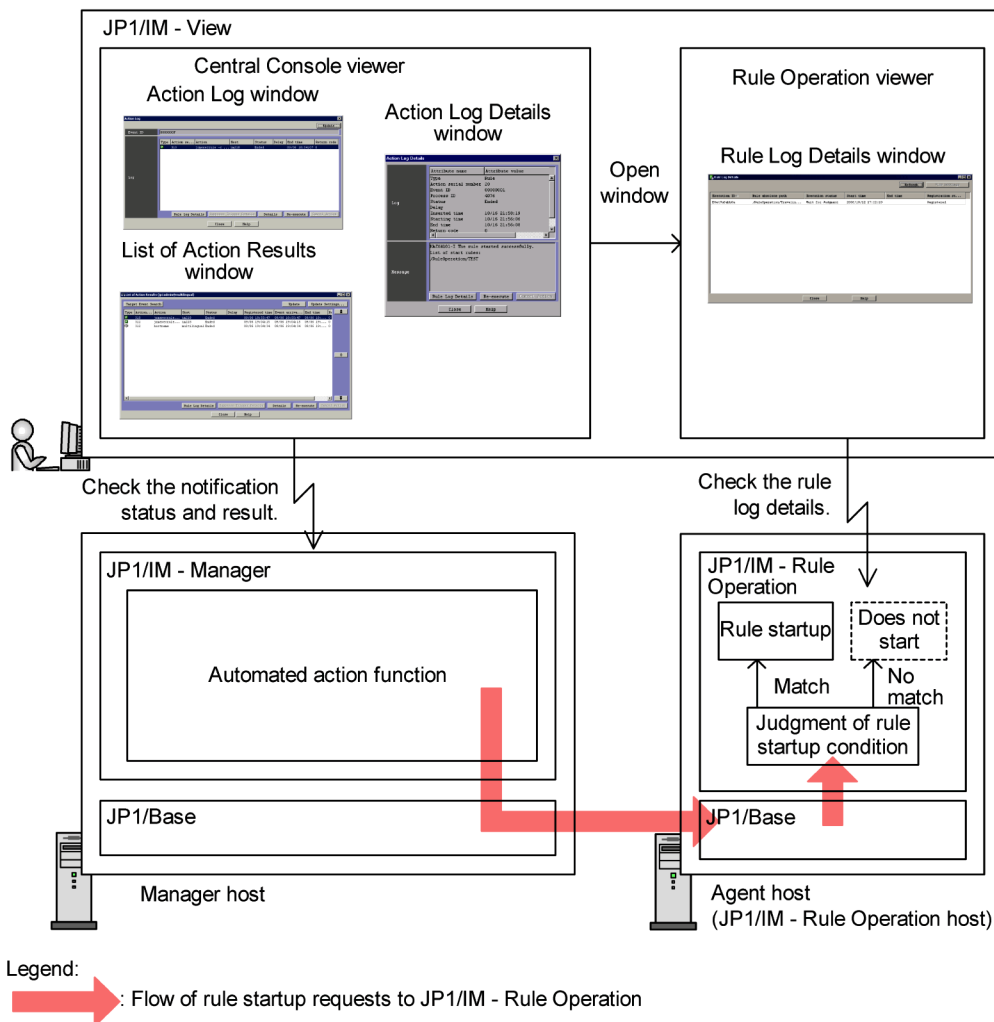
For details about how to interpret the notification status and result, see 2. *Event Console Window* in the manual *Job Management Partner 1/Integrated Management - Manager GUI Reference* and 1. *Commands* in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.

When the following conditions are satisfied, you can open the Rule Log Details window, which serves as the GUI for JP1/IM - Rule Operation, from any of the three windows listed above. You can then view the execution status of the rule:

- The **Type** of the automated action is  (**Rule**).
- The **Return code** of the automated action is 0.

You cannot open the Rule Log Details window when the return code is non-zero as rule startup will not have occurred.

Figure 8-3: Checking the notification status and result and checking the rule log details



When you open the JP1/IM - Rule Operation window from JP1/IM - View, you are logged in according to the authentication information in JP1/IM - View. Note that JP1/IM - View authentication information is invalidated when:

- The authentication server that you are logged in to is restarted.
- The information is reloaded by the `jbs_spmc_reload` command on the authentication server that you are logged in to.
- The primary authentication server that you are logged in to is switched to the secondary authentication server.

When the authentication information in JP1/IM - View is invalid, the operations you can perform depend on the product versions, as follows:

- When JP1/IM - Manager and JP1/IM - View are both version 09-00 or later, you are automatically re-authenticated and authentication information is re-acquired in JP1/IM - View.
- When either JP1/IM - Manager or JP1/IM - View is version 08-01 or earlier, authentication fails on the JP1/IM - Rule Operation side.

### 8.1.3 Monitor startup of JP1/IM - Rule Operation

JP1/IM - Rule Operation issues a JP1 event whenever a rule starts, ends, or ends abnormally. In JP1/IM, you can launch the Rule Operation viewer from these types of JP1 events displayed in JP1/IM - View by choosing the `Monitor` command or **Monitor** button.

## Chapter

---

# 9. JP1/IM Configuration

---

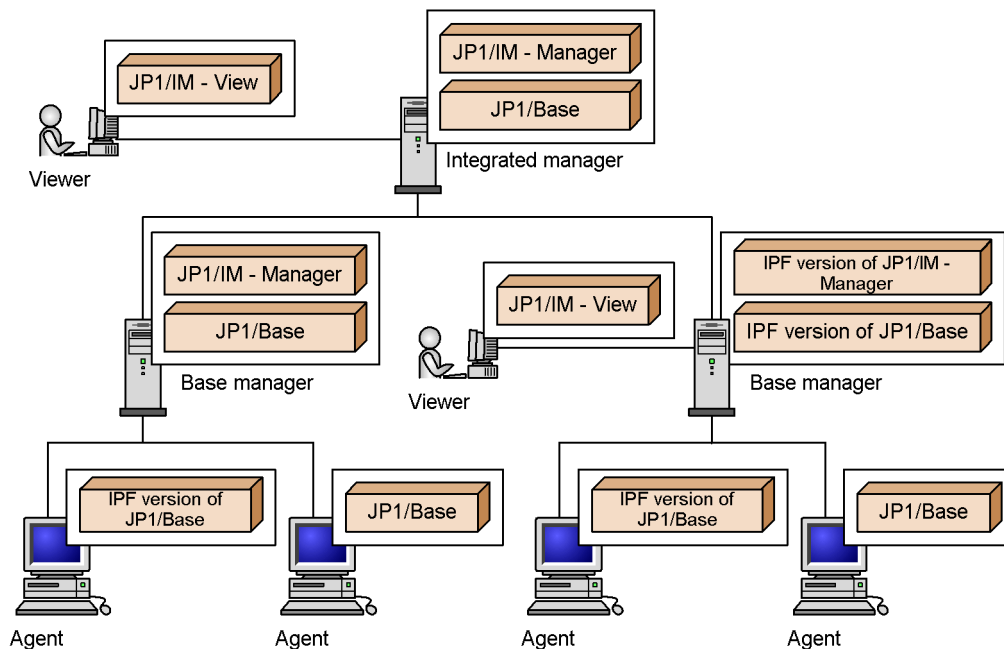
This chapter describes the configuration and functionality of JP1/IM, and the role played by JP1/Base in the JP1/IM system environment.

- 9.1 JP1/IM configuration example
- 9.2 Product structure
- 9.3 Prerequisite operating systems and programs
- 9.4 Support for various system configurations

## 9.1 JP1/IM configuration example

This section describes how to configure JP1/IM to perform system operations management.

*Figure 9-1:* Example of JP1/IM configuration





---

## 9.2 Product structure

---

This section describes the JP1/IM product structure.

### 9.2.1 JP1/IM product structure

JP1/IM consists of the following products:

- JP1/IM - View
- JP1/IM - Manager
- JP1/Base<sup>#</sup>

<sup>#</sup>: JP1/Base is a prerequisite product for the system that is to be monitored by JP1/IM.

#### JP1/IM - View

JP1/IM - View is for connecting to JP1/IM - Manager to view or operate on the management information of JP1/IM - Manager.

Some of the functions provided by JP1/IM - Manager for efficient system monitoring can only be set from JP1/IM - View. This includes setting filtering conditions and generating monitoring trees.

#### JP1/IM - Manager

JP1/IM - Manager provides the components for monitoring the system operation, including the Central Console, Central Scope, and IM Configuration Management.

The following restrictions apply:

- JP1/Base version 9 is a prerequisite program.

#### Web-based JP1/IM - View

This is a light version of JP1/IM - View, provided as a function of the JP1/IM - Manager's Central Console.

The following restrictions apply when you use the Web-based JP1/IM - View in a Web browser:

- You cannot use the Central Scope or IM Configuration Management.
- Some windows, including the Execute Command window and Tool Launcher window, are unavailable. There are also restrictions that disable

some operations, such as monitor startup and saving event lists (CSV snapshots). For details, see *1. Window Transitions and Login Window* in the manual *Job Management Partner 1/Integrated Management - Manager GUI Reference*.

- Some limits are different. See *D. Limits*.

## 9.2.2 Connectivity between JP1/IM products

The following table describes the connectivity, or management relationships, between JP1/IM products.

*Table 9-1: Connectivity between viewer and manager products*

Viewer product	Manager products that can be connected
JP1/IM - View (version 9)	JP1/IM - Manager (versions 9 and 8) JP1/IM - Central Console (version 7)
JP1/IM - View (version 8)	JP1/IM - Manager (version 9) For connectivity to version 8 or earlier manager products, see the previously published version 8 manuals.
JP1/IM - View (version 7)	JP1/IM - Manager (version 9) For connectivity to version 8 or earlier manager products, see the previously published version 8 manuals.

*Table 9-2: Connectivity between manager and agent products*

Higher-level manager	Manager and agent products that can be connected or managed
JP1/IM - Manager (version 9)	JP1/IM - Manager (versions 9 and 8) JP1/IM - Central Console (version 7) JP1/Base (versions 9, 8, 7, and 6 <sup>#</sup> )
JP1/IM - Manager (version 8)	JP1/IM - Manager (version 9) JP1/Base (version 9) For connectivity to version 8 or earlier manager and agent products, see the previously published version 8 manuals.
JP1/IM - Central Console (version 7)	JP1/IM - Manager (version 9) JP1/Base (version 9) For connectivity to version 8 or earlier manager and agent products, see the previously published version 8 manuals.

<sup>#</sup>: JP1/Base version 6 supports only the event forwarding function. For details about this function, see *7.4.2(2) Using JP1 event forwarding to centralize event*

*management.*

## 9.3 Prerequisite operating systems and programs

This section describes the prerequisite operating systems and programs for JP1/IM and JP1/Base.

### 9.3.1 Prerequisite operating systems

The following table lists the prerequisite operating systems for JP1/IM and JP1/Base.

*Table 9-3: Prerequisite operating systems for JP1/IM*

OS	JP1/IM - View	JP1/IM - Manager	JP1/ Base <sup>#1</sup>
Windows XP Professional	Y <sup>#2</sup>	--	Y
Windows Server 2003	Y <sup>#2</sup>	Y <sup>#2</sup>	Y
Windows Server 2003 (IPF)	--	--	Y <sup>#3</sup>
Windows Vista	Y	--	Y
Windows Server 2008	Y	Y	Y
Windows Server 2008 (IPF)	--	--	Y <sup>#3</sup>
HP-UX (IPF)	--	--	Y <sup>#3</sup>
Solaris	--	Y	Y
AIX	--	Y	Y

Legend:

Y: Supported.

-- Not supported.

#1: The range of supported JP1/Base functionality is OS-dependent. For details, see the *Job Management Partner 1/Base User's Guide*.

#2: The following restrictions apply when you use the Remote Desktop for Administration to perform installation and setup tasks:

(a) The Remote Desktop for Administration can only be used for installation, setup, uninstallation, and maintenance purposes.

(b) To perform the tasks in (a), you must connect to Session 0, not the usual Remote Desktop Connection. To establish a connection to Session 0, specify the `/console` option as follows when starting the Remote Desktop Connection application:

```
mstsc.exe /console
```

mstsc.exe is the executable file of the Remote Desktop Connection application.

Only one user belonging to the Administrators group can connect to Session 0 at one time.

#3: Only the IPF version of JP1/Base can be used on a system running Windows Server 2003 (IPF), Windows Server 2008 (IPF), or HP-UX (IPF).

For details about the supported OS versions and types (for example, Enterprise Edition), see the *Release Notes* for the product.

### 9.3.2 Prerequisite programs

The following table lists the prerequisite programs for JP1/IM and JP1/Base.

Table 9-4: Prerequisite programs for JP1/IM and JP1/Base

Product	Prerequisite programs
JP1/IM - View	To display the windows of a linked program in JP1/IM - View, either of the following is required (depending on the type of linked product): <ul style="list-style-type: none"> <li>• A JP1 program or other application program to be launched from JP1/IM - View</li> <li>• Web browser</li> </ul>
JP1/IM - Manager	<ul style="list-style-type: none"> <li>• JP1/Base</li> <li>• Web server<sup>#</sup></li> </ul>
JP1/Base	--

Legend:

--: Not required.

#: Required for the Web-based JP1/IM - View. The Java Runtime Environment (JRE) and the plug-ins bundled with JRE are required in the Web browser (used on the viewer side). For details on the versions and types of Web browser, required JRE, and HTTP server, see the *Release Notes* for JP1/IM - Manager.

---

## 9.4 Support for various system configurations

---

This section describes the various system configurations supported by JP1/IM and JP1/Base.

### 9.4.1 Firewall support

JP1/IM and JP1/Base can operate in a firewall environment if you perform the appropriate settings in the firewall. Network environments behind packet-filtering and NAT (static mode)-based firewalls are supported. When setting the firewall, see the lists of port numbers in the appendixes of the manuals for JP1/IM and JP1/Base. Also note the following points when setting the firewall:

- There are two forms of communication between the manager and agent. In one form, communication takes place according to the system hierarchy definition; in the other, the manager communicates directly with the target host (see 7.3 *Communication performed in the JP1/IM system environment*). You must set up the firewall in a manner that allows both types of communication.
- JP1/IM and JP1/Base use ports to communicate even when that communication takes place within a local host. If you use JP1/IM and JP1/Base on a host set up as a firewall, the firewall must permit local traffic through all ports used by JP1/IM and JP1/Base.

### 9.4.2 Support for multiple LANs

You can deploy JP1/IM and JP1/Base in network configurations with specific requirements such as the following, by changing the communication settings of JP1/IM and JP1/Base (in a network that allows unrestricted communication between machines, these changes will not be necessary).

Specific requirements:

- Specific communication network  
The JP1/IM - Manager and JP1/Base hosts are connected to multiple LANs, but you require them to communicate over a specific LAN only (using IP addresses other than those associated with the host names).
- Separate network  
The JP1/IM - Manager and JP1/Base hosts are connected to multiple LANs, but you do not want them to communicate across LANs (they cannot communicate using the IP address associated with the destination host name).

### 9.4.3 Operation in a cluster system

JP1/IM can be used in a cluster system.

When JP1/IM is used in a cluster system, a secondary node can take over system operation management if a failure occurs on the primary node.

For details, see 6. *Operation and Environment Configuration in a Cluster System* in the *Job Management Partner 1/Integrated Management - Manager Configuration Guide*.

#### **9.4.4 Logical host operation in a non-cluster environment**

A JP1/IM system based on logical hosts is typically a cluster system where JP1/IM is linked with cluster software. However, if you have set up logical hosts running JP1/IM, and have allocated the necessary IP addresses and disk space, JP1/IM can be used in a logical host environment that does not provide failover redundancy or involve linkage with cluster software.

For details, see 6.5 *Logical host operation and environment configuration in a non-cluster system* in the *Job Management Partner 1/Integrated Management - Manager Configuration Guide*.





## **Chapter**

---

# **10. Overview of Design**

---

This chapter gives an overview of the flow of JP1/IM deployment and the design tasks involved.

System operation management takes many forms depending on the work tasks taking place in a given system, and each system also has an operational culture built up over time.

Consider the design tasks so that deploying JP1/IM in an existing system improves the efficiency of operational tasks.

- 10.1 Flow of JP1/IM deployment

- 10.2 Design considerations

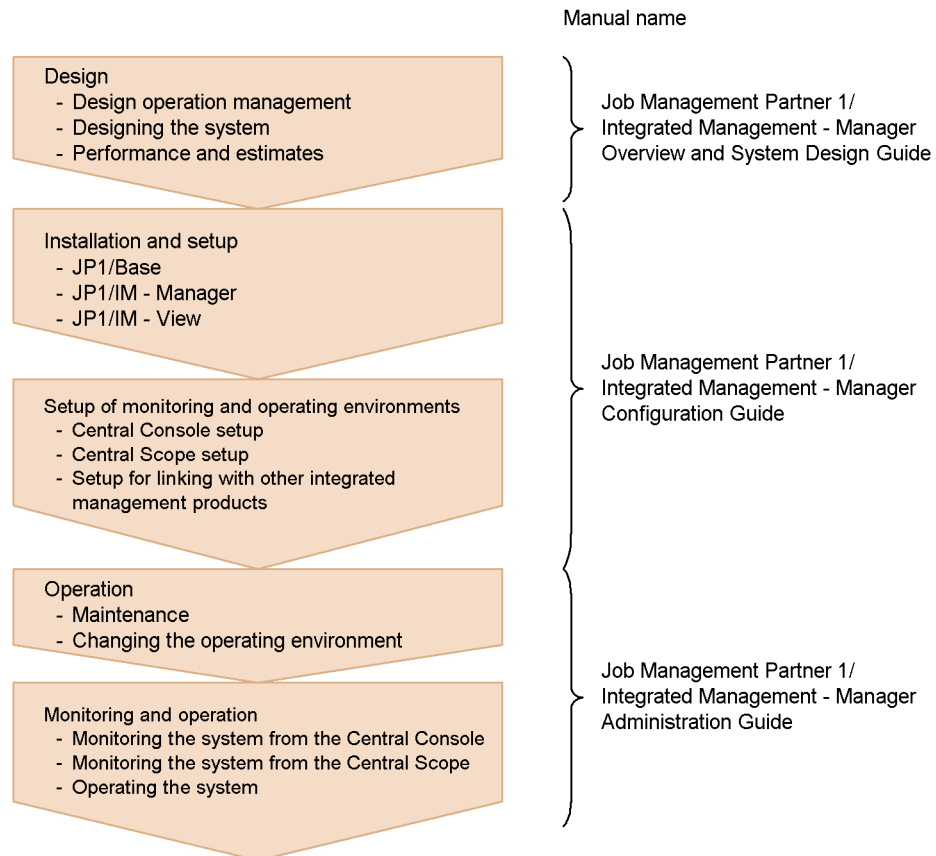
- 10.3 Overview of design for JP1/IM deployment

## 10.1 Flow of JP1/IM deployment

When deploying JP1/IM, follow the tasks set forth in the figure below.

The matters that must be considered and procedures that must be performed in each stage of deployment are described in the corresponding part of the manual.

*Figure 10-1: Flow of JP1/IM deployment*



## 10.2 Design considerations

The following table lists the design items to consider when deploying JP1/IM, and the part of the manual where each item is described.

For details, see the corresponding reference for each item.

*Table 10-1: Design items*

Items to consider at the design stage		Reference
Design related to the JP1/IM integrated monitoring database	Filtering methods	<i>11.1.3 Considerations for filtering JP1 events</i>
	JP1 events to be monitored	<i>11.1.4 Considerations for issuing correlation events</i>
	JP1 events to be modified	<i>11.1.6 Considerations for changing JP1 event levels</i>
	Storage of event information	<i>11.1.9 Considerations for saving event information in the integrated monitoring database (output of event report)</i>
Design related to operation management in JP1/IM	JP1 events to be monitored	<i>11.1 Considerations for system monitoring using JP1 events</i>
	Monitoring objects to be monitored	<i>11.2 Considerations for system monitoring from the Central Scope</i>
	Action taken by JP1/IM at detection of an error	<i>11.3 Considerations for error investigation in JP1/IM</i>
	Automated actions	<i>11.4 Considerations for automated actions</i>
Design related to management of the system hierarchy	How to manage the system hierarchy	<i>11.5 Considerations for managing the system hierarchy</i>

Items to consider at the design stage		Reference
Design related to the JP1/IM system	Operating environment	<i>12.1 Operating environment considerations</i>
	Migrating (upgrading) from a previous version of JP1/IM	<i>12.2 Upgrading from a previous version of JP1/IM</i>
	System configuration	<i>12.3 Designing the system configuration</i>
	Network configuration	<i>12.4 Network considerations</i>
	System configuration definition	<i>12.5 Considerations for the system hierarchy</i>
	User authentication	<i>12.6 Considerations for user authentication</i>
	Designing the environment for JP1/IM and JP1/Base	<i>12.7 Considerations for the JP1/IM and JP1/Base environments</i>
	Linking with other integrated management products	<i>12.8 Considerations for linking with other integrated management products</i>
	Maintenance	<i>12.9 JP1/IM maintenance considerations</i> <i>12.10 Considerations for JP1/IM system-wide maintenance</i>
Design related to JP1/IM performance	Performance and estimates	<i>13. Performance and Estimates</i>

---

## 10.3 Overview of design for JP1/IM deployment

---

This section gives a general idea of the design tasks required when deploying JP1/IM.

When you design for an actual implementation of JP1/IM, you must consider the system configuration and work tasks of the system where JP1/IM is to be deployed. On this basis, plan the deployment in a way that complements the operation of the existing system and improves its efficiency.

### 10.3.1 Overview of design

There are two aspects to designing JP1/IM deployment: System operation management based on JP1/IM, and the JP1/IM system requirements to achieve those objectives.

- Operation management design (designing JP1/IM-based operation management)
  - Monitoring: What will the system monitor?
  - Error detection and reporting: How will you categorize events occurring in the system and report them for rapid operator response?
  - Investigation and resolution: How will you investigate and resolve problems?

Consider how to perform these tasks within the system operating cycle using JP1/IM functions.

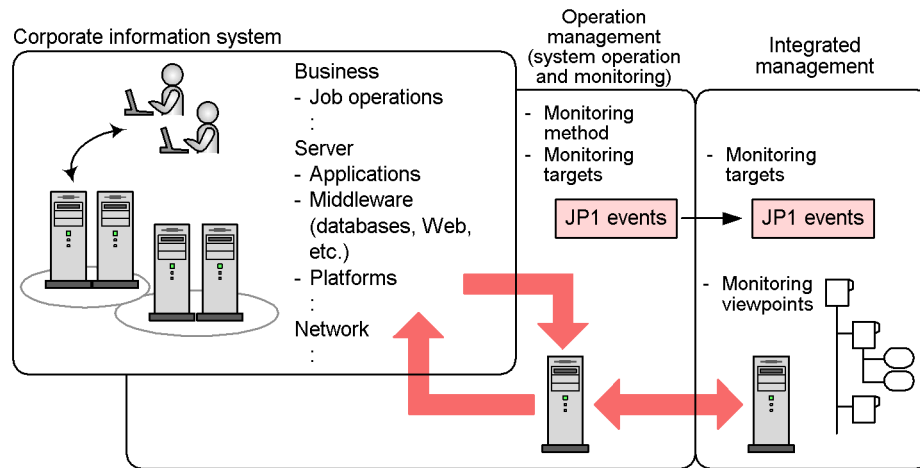
- System design (designing the JP1/IM system)

Reliability is imperative when using JP1/IM to manage the operation of a mission-critical system. Consider the JP1/IM system configuration and setup required to ensure that system operation management can be achieved.

### 10.3.2 Designing monitoring

When designing the system monitoring, consider the elements that must be monitored to ensure reliable operation, the methods to be used, and how monitoring will be managed.

Figure 10-2: Operation management by JP1



### (1) Monitoring methods

Consider what elements in the system require monitoring, and in what way, to ensure that the system operates reliably.

System monitoring method:

In considering how the system is to be monitored, you must first analyze the elements that make up the system. Because a system can contain a broad range of elements, you can simplify the process by breaking down the system into a number of layers, such as those shown below, which can then be considered individually.

- **Business:** The types of jobs executed in the system
- **Servers:** The software and hardware components
- **Network:** The network configuration and the types of devices in the network

Next, consider the methods needed to monitor the various elements in the system. You could use a product designed for system management, for example. You could monitor routine business tasks based on information supplied by a job management server, or use tools designed to monitor applications running on a server, for example.

The products in the JP1 series support system operation from a variety of angles, delivering a total support package from system operation to monitoring.

Monitoring by JP1/IM:

JP1/IM manages the system using *JP1 events*.

Consider collecting the events occurring in the system as JP1 events by linking

JP1/IM with the other programs that manage the various elements in the system. You can collect JP1 events across the system by linking with the products in the JP1 series.

Other events, such as messages in log files, SNMP traps, and entries in the Windows event log can be managed by conversion into JP1 events by the JP1/Base event converters.

## **(2) Monitoring targets**

Consider what aspects or items you would need to monitor to ensure that the system is operating in a stable manner.

Monitoring targets:

Assess what sorts of items can be monitored by each monitoring method you considered earlier. For example, a performance management tool can monitor the utilization and load on the resources it monitors.

Consider whether the items each product monitors are set appropriately for the local system. For example, check whether the threshold values defining the level at which resource usage triggers a JP1 event are at a suitable level.

JP1 events:

When you have settled on what items need to be monitored, consider how these items are recorded as values in JP1 events.

For products that issue JP1 events, ascertain how the item name and value are formatted in the JP1 event.

For log files, SNMP traps, or other events that are converted to JP1 events by a JP1/Base event converter, examine how the content of the original event corresponds to the information in the converted JP1 event.

## **(3) Monitoring viewpoints (when using the Central Scope)**

If you wish to use the Central Scope, consider the viewpoints from which you need to monitor the system operation.

The Central Scope enables objective-oriented system monitoring matched to your monitoring viewpoints, and offers visual representation in a tree view in the Monitoring Tree window or map view in the Visual Monitoring window.

Monitoring tree:

The following monitoring trees can be generated using the auto-generation function:

- Work-oriented tree
- Server-oriented tree

You can then customize the tree to suit your needs by adding or deleting elements.

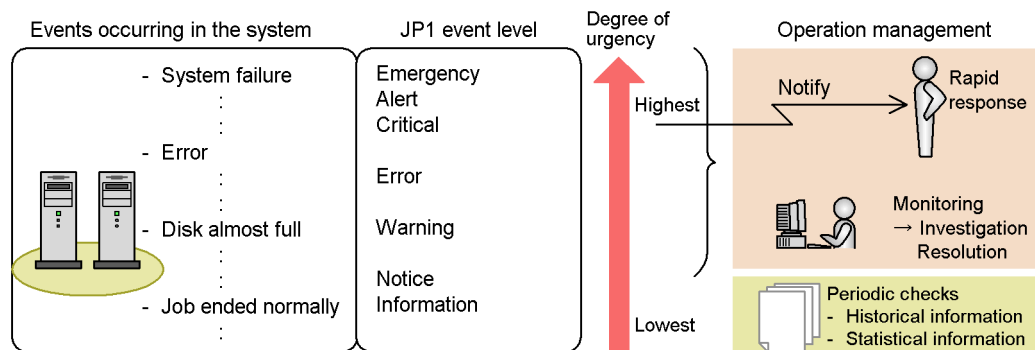
Visual monitoring:

You can arrange the key points that you want to watch closely in a map view using the Visual Monitoring window. Prepare the organizational charts or maps that you want to use as map images.

### 10.3.3 Designing error detection and reporting

After considering the monitoring methods and targets, consider what action to take when a problem is detected.

*Figure 10-3: Considerations for correspondence between event levels and action taken*



#### (1) JP1 events and event levels

JP1/IM uses *JP1 events* to monitor events occurring in the system. JP1 events are assigned an event level that indicates the severity of the occurrence that caused the JP1 event to be issued.

Consider how to detect and deal with problems in the system according to their event level.

Categorizing JP1 events by event level:

Categorize JP1 events based on their event level (attribute name: E.SEVERITY).

JP1 events define an event level associated with a specific event that occurs in the system. Each product that issues JP1 events sets an appropriate event level for the types of events it manages.

When a SNMP trap or entry in the Windows event log is converted to a JP1 event, its severity is associated with a JP1 event level. If you use the integrated monitoring database and change the event level of a JP1 event to one defined by the user, the user-defined event level is associated with a JP1 event level. To monitor these JP1 events, categorize them based on the severity of the source



event. When a message in a log file is converted to a JP1 event, the event level of the resulting JP1 event is determined by the converter settings. Set the converters to assign an appropriate event level.

Checking categorized JP1 events:

Check whether the JP1 events are in the appropriate category for their event level.

The event levels assigned by products in the JP1 series are generally suitable for normal operation. However, check whether reclassifying some events under another event level would suit your system operation better. For example, you might want to exclude some events that are normally classed as severe events.

## **(2) Response based on urgency**

For the categorized JP1 events, consider response procedures based on the urgency of the event.

The following describes an example of response procedures for events with three levels of urgency (*Urgent*, *Severe*, and *Normal*).

Events that require immediate attention:

Consider whether any of the events managed by JP1/IM require an urgent response. A system failure, for example, requires an immediate response because of the far-reaching consequences to work tasks.

Consider reporting such an error to the system administrator.

To avoid placing an undue burden on the system administrator, make sure that only JP1 events requiring a rapid response are reported. Also consider changing the range of events reported to the system administrator according to their content.

In JP1/IM, you can send an emergency notice by executing a command from an automated action. Consider how to identify events that need to be reported to the system administrator, and the command to use for notification (for example a mail sending command), and then define an appropriate automated action.

Severe events that require monitoring:

Consider whether events whose event level indicates a problem should be handled as severe events that require monitoring.

Such events can be forwarded to a JP1/IM manager host where they can be centrally managed.

Use the event level or other attribute to define which JP1 events are to be handled as severe events in JP1/IM. On the Severe Events page of the Event Console window, you can view a list of the events defined as severe events and manage their response status.

Normal events that must be checked periodically:

Events issued in the normal course of operation, such as events indicating that a job has ended normally, can be used in the following ways depending on your system operating requirements:

- Keep for use as an operating history.

Example: JP1 events related to job execution can be saved as a job execution log.

- Use to compile statistical information.

Example: The start and end times reported in JP1 events related to job execution can be used to compile statistical information on job execution times.

Utilize urgent and severe events, by displaying them in JP1/IM - View or outputting them as a CSV snapshot, when you review the system setup, for example.

You can also utilize events that are not monitored by JP1/IM by using the following commands to output the database contents on the hosts in the system in CSV format.

- The JP1/Base `jvexport` command

Outputs the contents of the event databases in CSV format.

- The JP1/IM - Manager `jcoevtreport` command

Outputs the contents of the integrated monitoring database in CSV format.

### **(3) Monitoring from the Central Scope**

You can customize the Central Scope to display events with specific event levels.

Because a monitoring tree shows the layout of the entire system in tree form, you can easily see how the objects being monitored relate to one other. However, depending on the structure of the monitoring tree, a single failure event might cause a large number of monitoring objects to change to a color that indicates an error.

Under the default settings, changes in the status of monitoring objects are triggered by the event levels of JP1 events. However, you can customize the way in which status changes are triggered to suit your system operation.

You can also exclude monitoring objects from monitoring in the Central Scope.

## Chapter

---

# 11. Operation Management Design

---

This chapter describes considerations when monitoring the system operation using JP1/IM.

- 11.1 Considerations for system monitoring using JP1 events
- 11.2 Considerations for system monitoring from the Central Scope
- 11.3 Considerations for error investigation in JP1/IM
- 11.4 Considerations for automated actions
- 11.5 Considerations for managing the system hierarchy

---

## 11.1 Considerations for system monitoring using JP1 events

---

JP1/IM uses *JP1 events* to monitor events occurring in the system.

You must therefore consider the JP1/IM settings so that the events you want to monitor can be managed using JP1 events.

### 11.1.1 Considerations for event management using JP1 events

Consider how to set up JP1/IM to manage system events using JP1 events.

#### (1) *Linkage with programs that issue JP1 events*

A JP1/IM system can use JP1 events issued by products in the JP1 series or by any other program capable of issuing JP1 events.

Some programs require special settings to issue JP1 events. For details, see the documentation for the product concerned.

#### (2) *Using JP1 event-issuing commands*

If you have a program that does not issue JP1 events, consider using the JP1 event-issuing commands (`jevsend` and `jevsendd`) to do so. These two commands differ in whether JP1 event registration is verified. For details, see below.

About JP1 event-issuing commands:

- Registering a JP1 event using a JP1 event-issuing command

See the description of the `jevsend` command and `jevsendd` command in the *Job Management Partner I/Base User's Guide*.

#### (3) *Converting non-JP1 events*

If you want to monitor an event that is output in any of the following forms, you can use an event converter to convert it into a JP1 event that can be managed by JP1/IM:

- Message in a log file
- SNMP trap
- Windows event log entry

Consider the event converter setup required in JP1/Base to use these non-JP1 events

About event conversion:

- Converting log file messages into JP1 events

See the description of converting log files output by an application program in the chapter on setting the event converters in the *Job Management Partner I/Base User's Guide*.

- Converting SNMP traps into JP1 events

See the description of SNMP trap conversion in the chapter on setting the event converters in the *Job Management Partner 1/Base User's Guide*

- Converting Windows event log entries into JP1 events.

See the description of Windows event log conversion in the chapter on setting the event converters in the *Job Management Partner 1/Base User's Guide*.

### 11.1.2 Considerations for forwarding JP1 events to managers

Consider how to set up JP1/IM to forward the JP1 events required for system management to a manager.

JP1 events are managed by the JP1/Base event service and are forwarded according to the target JP1 events and destination hosts defined in the event forwarding settings.

Under the default settings, JP1 events whose event level is *Emergency*, *Alert*, *Critical*, *Error*, or *Warning* are forwarded through the hierarchy of managers and agents set in the system configuration definition.

You will need to customize the default settings in the following cases:

- To manage informational or normal JP1 events using JP1/IM

Add forwarding settings to manage JP1 events of *Notice* or *Information* level in JP1/IM. For example, if you want to manage a JP1 event (*Information* level) that reports normal termination of a jobnet, so that the execution status of the jobs can be checked from JP1/IM, you must set up JP1/IM to forward that event. When customizing the forwarding settings in this way, specify explicit conditions to minimize the number of JP1 events being forwarded to JP1/IM managers.

- To manage JP1/SES events in JP1/IM

Add forwarding settings to manage JP1/SES events in JP1/IM. For example, if you want to manage a JP1/SES event issued by JP1/Open Job Entry (a product for linking with a mainframe computer), you must set up JP1/IM to forward that event. When customizing the forwarding settings in this way, specify explicit conditions to minimize the number of JP1 events being forwarded to JP1/IM managers.

About JP1 event forwarding:

- Setting JP1 event forwarding

See the chapter on setting the event service environment in the *Job Management Partner 1/Base User's Guide*.

- Setting the system configuration definition

See *Configuration definition file (jbs\_route.conf)* in 2. *Definition Files* in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.

*Note:*

Filter the JP1 events issued by agents so that only severe events that need to be managed by a manager will be forwarded. If all JP1 events from agents are sent to managers, there could be delays in event forwarding or in event registration at the manager host.

### **11.1.3 Considerations for filtering JP1 events**

Consider the JP1 event filtering settings so that appropriate JP1 events can be managed by JP1/IM during system monitoring.

The flow of JP1 events in a JP1/IM manager depends on whether the integrated monitoring database is being used. The following figures show in diagrammatic form how filters affect the flow of JP1 events to JP1/IM managers according to whether you are using the integrated monitoring database.

Figure 11-1: Effect of filters (when not using the integrated monitoring database)

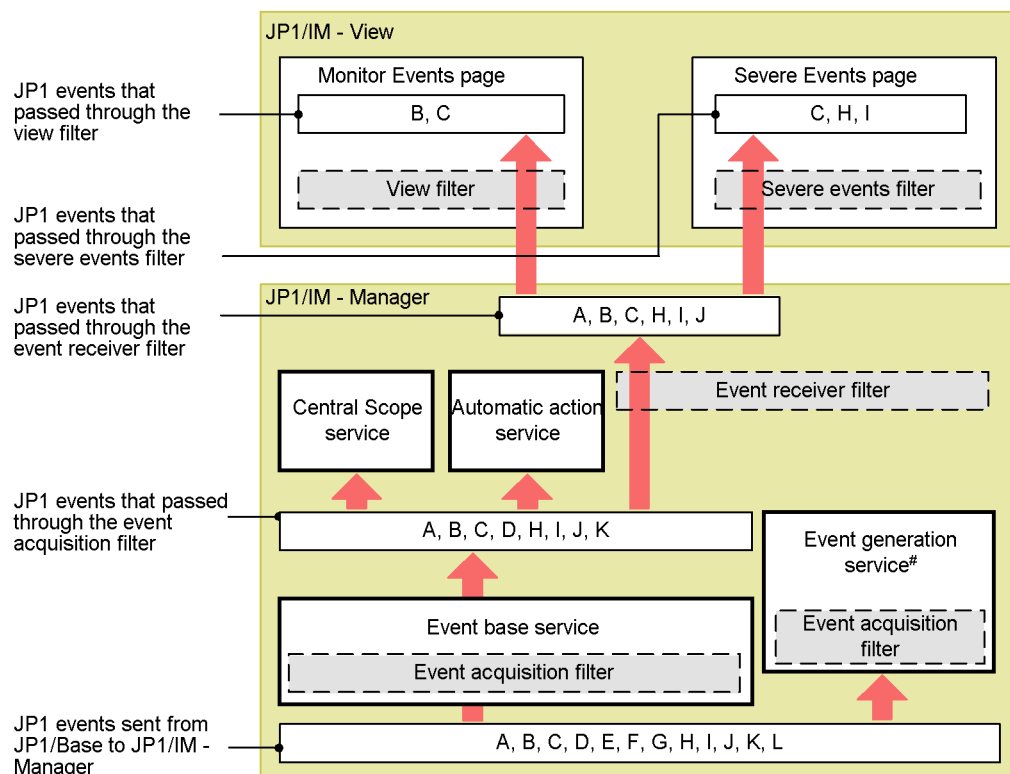
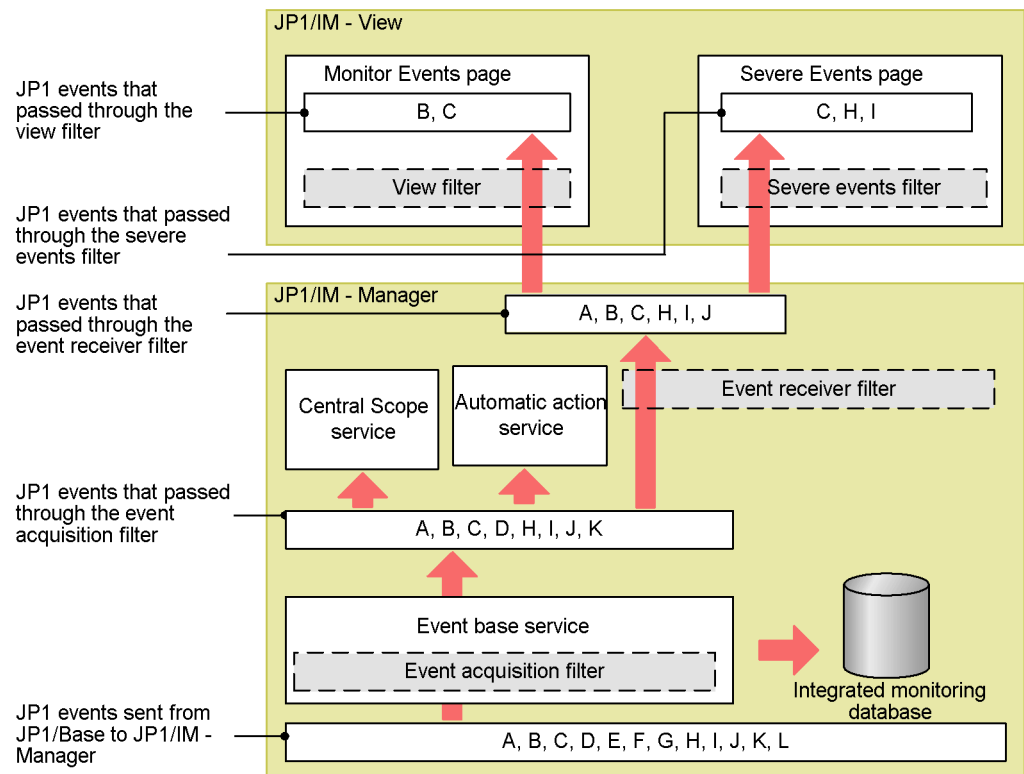


Figure 11-2: Effect of filters (when using the integrated monitoring database)



The event base service and event generation service filter JP1 events according to the conditions set in the event acquisition filter. When you use the integrated monitoring database, the filtered JP1 events are stored in the integrated monitoring database. You can display the filtered JP1 events in JP1/IM - View by applying an event receiver filter.

Each filter is described below, starting from when the JP1 event is first issued.

### (1) Event acquisition filter

An event acquisition filter sets conditions for the JP1 events to be acquired from JP1/Base (event service) by JP1/IM - Manager.

By default, JP1/IM - Manager acquires all JP1 events for which an event level has been



set.

If you use the severity changing feature to change the event level of a JP1 event when using the integrated monitoring database, JP1/IM - Manager acquires JP1 events based on their original event levels.

The following describes how to customize the filter settings and how to set multiple event acquisition filters.

#### (a) Customizing an event acquisition filter

You will need to customize the event acquisition filter settings in the following cases:

- To exclude JP1 events of `Notice` and `Information` level from display on the Monitor Events page of the Event Console window

If the managers encounter a large number of informational or normal JP1 events, set the minimum event level of the JP1 events to be acquired to `Warning` in the event acquisition filter. Numerous job execution events might be generated, for example, if JP1/AJS - Manager runs on the same host as JP1/IM - Manager. To set a minimum event level, in the Event Acquisition Settings window create a separate condition group for that event level.

- To monitor JP1/SES events in JP1/IM

JP1/SES events are not acquired by default because no event level is set. To manage such events in JP1/IM, you must set the event acquisition filter to acquire JP1/SES events. To do so, create a separate condition group with the **Acquire the JP1/SES events** check box selected in the Event Acquisition Settings window.

#### (b) Setting multiple event acquisition filters

Consider whether you need to set a number of different event acquisition filters. For example, you might wish to use different acquisition conditions for JP1 events inside and outside business hours.

#### (c) Setting common exclusion conditions for maintenance purposes

Consider whether you need to add common exclusion conditions to an event acquisition filter used in maintenance mode. For example, during scheduled maintenance of JP1/IM and JP1/Base, you might wish to exclude JP1 events issued by certain hosts from being monitored.

By activating the common exclusion conditions for a host only when the host is under maintenance, you can suppress monitoring of JP1 events issued by that host while leaving the standard filter conditions unchanged.

For details about maintenance by using common exclusion conditions in event acquisition filter settings, see *12.10 Considerations for JP1/IM system-wide maintenance*.

**(d) Notes**

- If you were using the event acquisition filter (for compatibility) in a previous version of JP1/IM, the filter works in a different position and operates differently from a standard event acquisition filter. If you use the integrated monitoring database while the event acquisition filter (for compatibility) is in effect, filtering takes place according to the conditions of the event acquisition filter (for compatibility).

For details, see *12.2.3(2) Upgrading from JP1/IM - Central Console version 7*.

- Event acquisition filters also affect the event generation service. The service is inactive by default. When it is started, however, the filter definitions in effect for the event base service are also applied to the event generation service.

**(2) Event receiver filter**

An event receiver filter is used when the system administrator wants to restrict the JP1 events that can be monitored by JP1 users. An event receiver filter can be set for a specific JP1 user, and administrator permission (JP1\_Console\_Admin) is required to change the settings.

By default, there are no restrictions and all JP1 users can monitor all JP1 events.

You will need to customize this setting in the following cases:

- To restrict the monitoring range of individual JP1 users  
If you want to prevent a certain JP1 user from viewing certain confidential events, set the events that the JP1 user is allowed to view in an event receiver filter.
- To monitor a specific range  
Using event receiver filters, you can limit the range of resources to be monitored if, for example, you want the JP1 user to monitor specific JP1 events only, or if you want multiple JP1 users to monitor different parts of a large-scale system.

**(3) Severe events filter**

Use a severe events filter to specify which JP1 events are important in system monitoring. The JP1 events you define in this filter are regarded as *severe events* and appear on the Severe Events page of the Event Console window. In this window you can also manage the response status of each severe event.

Under the default settings, JP1 events whose event level is Emergency, Alert, Critical, or Error are defined as severe events.

You will need to customize the default settings in the following cases:

- To exclude specific events from being handled as severe events  
If a JP1 event has a severe event level, but does not need to be treated as a severe event in terms of the system operation, specify the event ID and select **Does not**

**match** in the severe events filter conditions.

#### **(4) View filter**

Use a view filter to specify conditions restricting the JP1 events displayed on the Monitor Events page of the Event Console window.

By default, no display conditions are set.

This filter is typically used when you need to temporarily display only certain types of JP1 events during monitoring.

#### **(5) Defining filter conditions**

If you are defining multiple condition groups as filter conditions, make sure that the condition groups do not conflict with one another before you start running the system.

*Example:*

Suppose the following two condition groups are defined:

- Condition group A: Specifies that JP1 events of `Warning` level or higher pass through the filter.
- Condition group B: Specifies that JP1 events from hosts other than host A pass through the filter.

Here, if a `Warning` (or higher level) JP1 event arrives from host A, it will meet the condition in condition group A. Thus, a JP1 event that you actually want to exclude will pass through the filter, regardless of the condition defined in condition group B.

When defining conditions, remember that condition groups are related by an OR condition. In the example above, if you define condition group B as an exclusion condition group that excludes JP1 events arriving from host A, this condition group will take priority over condition group A. In this case, if a `Warning` (or higher level) JP1 event arrives from host A, it will not pass through the filter.

About setting filters:

- Event acquisition filter

Setting a filter in the Event Acquisition Settings window:

See *2.12 Event Acquisition Settings window* in the manual *Job Management Partner 1/Integrated Management - Manager GUI Reference*.

Setting a filter in the Event Acquisition Settings (for compatibility) window:

See *2.13 Event Acquisition Settings (for compatibility) window* in the manual *Job Management Partner 1/Integrated Management - Manager GUI Reference*.

Adding or setting a filter in the Event Acquisition Conditions List window:

See *2.14 Event Acquisition Conditions List window* in the manual *Job Management Partner 1/Integrated Management - Manager GUI Reference*.

Changing the filter location using the `jcochafmode` command:

See `jcochafmode` in *1. Commands* in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.

Switching event acquisition filters using the `jcochfilter` command:

See `jcochfilter` in *1. Commands* in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.

- Event receiver filter

Adding or setting a filter in the Settings for Event Receiver Filter window:

See *2.22 Settings for Event Receiver Filter window* in the manual *Job Management Partner 1/Integrated Management - Manager GUI Reference*.

- Severe events filter

Setting a filter in the Severe Event Definitions window:

See *2.10 Severe Event Definitions window* in the manual *Job Management Partner 1/Integrated Management - Manager GUI Reference*.

- View filter

Setting a filter in the Settings for View Filter window:

See *2.20 Settings for View Filter window* in the manual *Job Management Partner 1/Integrated Management - Manager GUI Reference*.

Adding or setting a filter in the View List of Filters window:

See *2.21 View List of Filters window* in the manual *Job Management Partner 1/Integrated Management - Manager GUI Reference*.

#### 11.1.4 Considerations for issuing correlation events

The JP1 events managed by JP1/IM - Manager can burgeon to huge volumes according to the size of the system. The idea behind JP1 events is that they manage each and every event occurring in the system; they therefore cover a wide range of event types.

By using the various filters provided by JP1/IM - Manager, you can restrict the types of JP1 events displayed in the event console. However, when an error occurs, the system might issue a large number of JP1 events reporting the problem and filling up the event console. It would take the system administrator a great deal of time and trouble to analyze and investigate these JP1 events, to identify the cause and remedy every problem.

In JP1/IM - Manager, you can associate a number of predictable JP1 events in advance, or optionally change the JP1 event attribute values, and thereby issue a new event (correlation event). A correlation event can be issued when a conditions is satisfied, or when a conditions fails to be satisfied. By utilizing correlation event generation, you can lessen your workload and reduce the time you spend troubleshooting problems.

Note that the processing by which correlation events are issued differs depending on whether you are using the integrated monitoring database, specifically in terms of the range of events that the correlation processing inherits. For details, see 3.3 *Issue of correlation events*.

Some points you need to consider when using correlation event generation are discussed below under the following headings:

- Correlation event generation definition
- Operating environment required for correlation event generation
- Notes on correlation event generation

### **(1) Correlation event generation definition**

A correlation event generation definition consists of correlation source events (event conditions), a timeout period, event correlation type, and the correlation event to be issued.

Give proper consideration to the following points when setting a correlation event generation definition:

- Filtering condition for the correlation target range  
Are the JP1 events that match the event conditions issued from specific hosts only?
- Correlation source events (event conditions)
  - Which JP1 events will be correlation source events?
  - Will you need one correlation source event or more than one?
- Timeout period
- Event correlation type (sequence, combination, or threshold)
- Duplicate attribute value condition  
Will you need to manage correlation events by grouping hosts or users?
- Maximum correlation number
- Correlation event to be issued

Six examples are presented below to illustrate the points above. Refer to these examples when you consider how to set a correlation event generation definition:

- Adding an attribute to the JP1 event attribute values
- Changing a JP1 event message to a more manageable message
- Executing an automated action when hosts A, B, and C have all started
- Issuing correlation events for a JP1 event issued from specific hosts
- Managing JP1 events indicating an authentication error by source server
- Monitoring for a situation where an event does not occur within a specified time period

Each of these six examples states the condition that needs to be satisfied, the reason, and the contents that you need to enter in the correlation event generation definition file.

For details about the correlation event generation definition file, see *Correlation event generation definition file* in 2. *Definition Files* in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.

#### (a) Adding an attribute to the JP1 event attribute values

This example shows how to add an attribute value to the fixed attributes of a JP1 event, issued by another JP1 product or other program, to issue a correlation event.

Condition to be satisfied:

Report JP1 event (00004107), which indicates abnormal termination of a JP1/AJS job, as an event of Emergency level.

Set the correlation event for this example as follows:

- Event ID: A01
- Event level: Emergency
- Message: Same message as the correlation source event (00004107).

Reason:

The event levels in this system are defined as in the following table, with Error level currently set for JP1 event (00004107) indicating abnormal termination of a JP1/AJS job.

*Table 11-1: Event level definitions in the system*

Event level	System requirements
Emergency	Problem requiring immediate response
Error	Problem requiring response within one working day

Contents of the correlation event generation definition file:

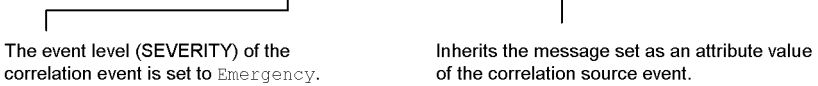
The following figure shows the contents of the correlation event generation definition file.

*Figure 11-3: Contents of the correlation event generation definition file*

```

1 [Emergency_event]
2 CON=CID:1, B.ID==4107
3 SUCCESS_EVENT=B.ID:A01, E.SEVERITY:Emergency, B.MESSAGE:$EV1_B.MESSAGE

```



The event level (SEVERITY) of the correlation event is set to *Emergency*.

Inherits the message set as an attribute value of the correlation source event.

*Note:* In this example, a line number is inserted at the beginning of each line to indicate the individual lines you need to write in the definition file.

To use the correlation event generation definition shown above, copy the following coding:

```

[Emergency_event]
CON=CID:1,B.ID==4107
SUCCESS_EVENT=B.ID:A01,E.SEVERITY:Emergency,B.MESSAGE:$EV1_B.MESSAGE

```

#### (b) Changing a JP1 event message to a more manageable message

This example shows how to change the message of a JP1 event, to issue a correlation event containing the new message.

Condition to be satisfied:

Change the message of a JP1 event to a message appropriate to the system requirements, keeping part of the original message in the new message.

Set the correlation event for this example as follows:

- Event ID: A02
- Event level: Same level as the correlation source event (00004107)
- Message: Partly the same as the correlation source event, as shown in the table below.

*Table 11-2: Message contents*

Event type	Message contents
Correlation source event	KAVS0265-E Job ended abnormally. (name: <i>job-name</i> : <i>execution-ID</i> , status: <i>status</i> , code: <i>code</i> , host: <i>host-name</i> , JOBID: <i>job-number</i> )

Event type	Message contents
Correlation event	Job: <u>job-name</u> ended abnormally with RC= <u>code</u> :Contact job supervisor (ext:xxxx)

Legend:

\_\_\_\_ (underline): Parts whose value is inherited from the correlation source event.

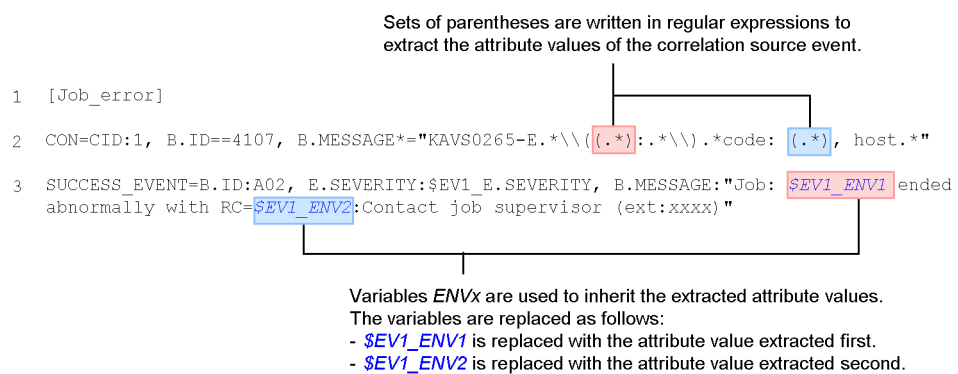
Reason:

When the information needing to be managed comes at the end of a long JP1 event message, you have to scroll to see everything, which increases your workload.

Contents of the correlation event generation definition file:

The following figure shows the contents of the correlation event generation definition file.

Figure 11-4: Contents of the correlation event generation definition file



*Note:* In this example, a line number is inserted at the beginning of each line to indicate the individual lines you need to write in the definition file. Line 3 spans two lines here, but write it as one line in the definition file.

To use the correlation event generation definition shown above, copy the following coding:

```

[Job_error]
CON=CID:1,B.ID==4107,B.MESSAGE*="KAVS0265-E.*\\((.*):.*/\\).*code: (.*),
host.*"
SUCCESS_EVENT=B.ID:A02,E.SEVERITY:$EV1_E.SEVERITY,B.MESSAGE:"Job:$EV1_ENV1
ended abnormally with RC=$EV1_ENV2:Contact job supervisor (ext:xxxx)"

```



**(c) Executing an automated action when hosts A, B, and C have all started**

This example shows how to associate multiple JP1 events to issue a correlation event. The procedure for defining an automated action is not covered here. For details about defining automated actions, see *5.3 Defining an automated action*.

Condition to be satisfied:

Execute an automated action (for system maintenance purposes) when hosts A, B, and C have all started normally.

Assume that the following JP1 event is issued when host A, B, or C starts normally.

- Event ID: 100
- Event level: Information
- Message: *host* started.

The variable value (*host*) in the message is replaced with the host name (A, B, or C).

- Extended attribute (E.HOST): Replaced with the name of the host that has started (A, B, or C).

Set the correlation event for this example as follows:

- Event ID: A03
- Event level: Information
- Message: All hosts started normally. Host names: A B C

A timeout period of 10 minutes is set for a JP1 event indicating normal startup to be issued from each of the three hosts.

Reason:

The definitions would be complex if you tried to set an automated action for the three JP1 events reporting host startup. Setting an automated action for one correlation event is easier.

Contents of the correlation event generation definition file:

The following figure shows the contents of the correlation event generation definition file.

*Figure 11-5: Contents of the correlation event generation definition file*

```

1  [Start_notification]
2  CON=CID:10, B.ID==100, B.MESSAGE==A started.
3  CON=CID:20, B.ID==100, B.MESSAGE==B started.
4  CON=CID:30, B.ID==100, B.MESSAGE==C started.
5  TIMEOUT=600
6  SUCCESS_EVENT=B.ID:A03, E.SEVERITY:Information, B.MESSAGE:
   "All hosts started normally. Host names:$EV10_E.HOST $EV20_E.HOST $EV30_E.HOST"

```

The attribute value of the extended attribute (E.HOST) for the correlation source event is set in the correlation event message.

*Note:* In this example, a line number is inserted at the beginning of each line to indicate the individual lines you need to write in the definition file. Line 6 spans two lines here, but write it as one line in the definition file.

To use the correlation event generation definition shown above, copy the following coding:

```

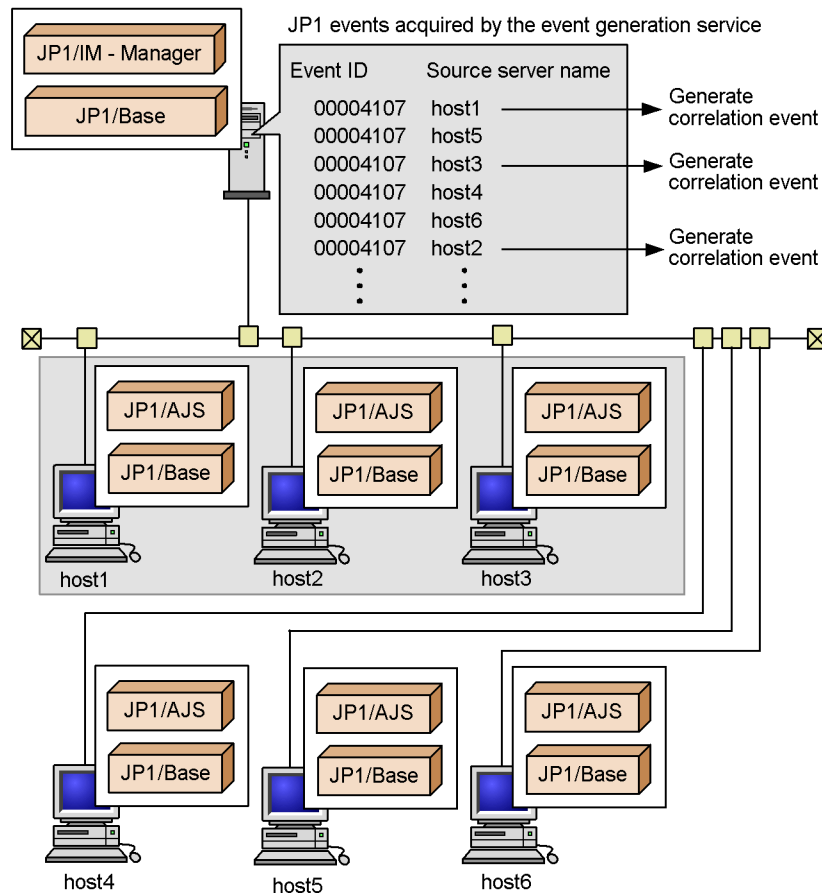
[Start_notification]
CON=CID:10,B.ID==100,B.MESSAGE==A started.
CON=CID:20,B.ID==100,B.MESSAGE==B started.
CON=CID:30,B.ID==100,B.MESSAGE==C started.
TIMEOUT=600
SUCCESS_EVENT=B.ID:A03,E.SEVERITY:Information,B.MESSAGE:"All hosts started
normally. Host names:$EV10_E.HOST $EV20_E.HOST $EV30_E.HOST"

```

#### (d) Issuing correlation events for a JP1 event issued from specific hosts

This example shows how to issue correlation events when a JP1 event is issued from specific hosts in the system configuration shown below.

Figure 11-6: Issuing correlation events targeting specific hosts



Condition to be satisfied:

Apply the following requirement (same as in example (a) above) to host1, host2, and host3 only:

Report JP1 event (00004107), which indicates abnormal termination of a JP1/AJS job, as an event of Emergency level.

Set the correlation event for this example as follows:

- Event ID: A01
- Event level: Emergency
- Message: Same message as the correlation source event (00004107).

Reason:

Several hosts executing JP1/AJS jobs are being monitored, but you want to change the event level of a JP1 event issued only from specific hosts that are executing mission-critical jobs.

Contents of the correlation event generation definition file:

The following figure shows the contents of the correlation event generation definition file.

*Figure 11-7: Contents of the correlation event generation definition file*

```

1  [Emergency_event]
2  TARGET=B.SOURCESERVER==host1;host2;host3
3  CON=CID:1,B.ID==4107
4  SUCCESS_EVENT=B.ID:A01,E.SEVERITY:Emergency,B.MESSAGE:$EV1_B.MESSAGE

```

Specify filter conditions to restrict the correlation target range to host1, host2, and host3 only.

*Note:* In this example, a line number is inserted at the beginning of each line to indicate the individual lines you need to write in the definition file.

To use the correlation event generation definition shown above, copy the following coding:

```

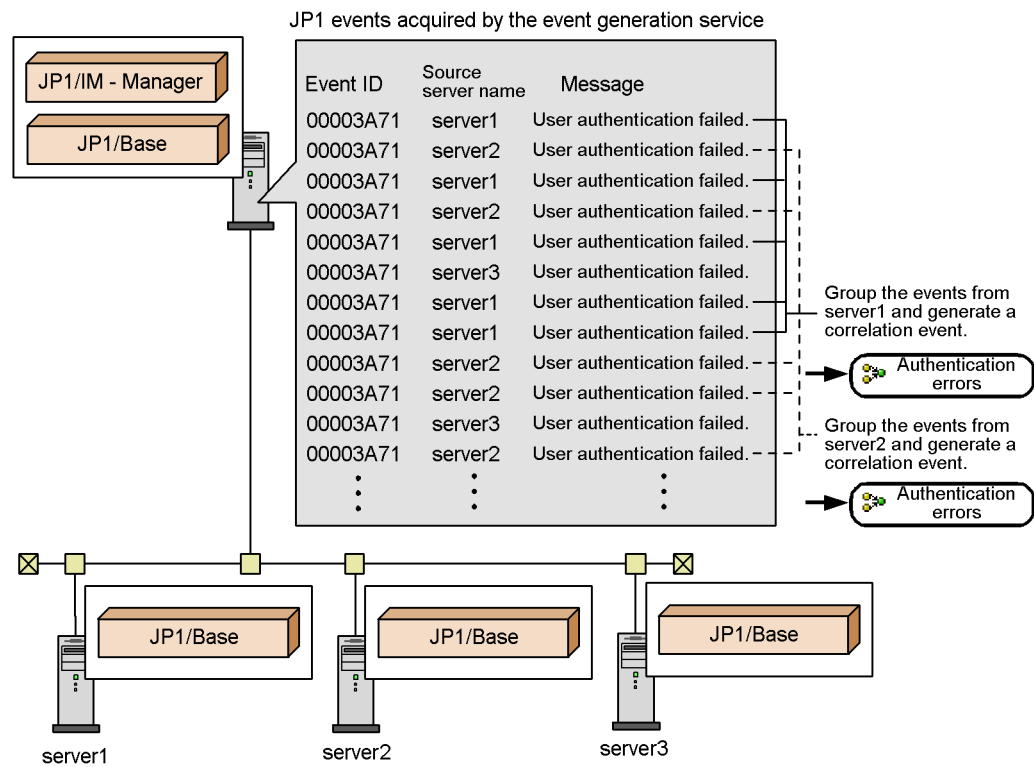
[Emergency_event]
TARGET=B.SOURCESERVER==host1;host2;host3
CON=CID:1,B.ID==4107
SUCCESS_EVENT=B.ID:A01,E.SEVERITY:Emergency,B.MESSAGE:$EV1_B.MESSAGE

```

#### (e) Managing JP1 events indicating an authentication error by source server

This example shows how to issue a correlation event for each server from which a JP1 event (00003A71) indicating an authentication error was issued multiple times, as shown in the figure below.

Figure 11-8: Issuing correlation events by grouping JP1 events by source server



00003A71 is the ID of a JP1 event issued by the Windows event log trapping function of JP1/Base. The procedure for setting this function is not covered here. For details, see the description of converting the Windows event log in the chapter on setting the event converters in the *Job Management Partner 1/Base User's Guide*.

Condition to be satisfied:

Issue a correlation event whenever a JP1 event (00003A71) indicating an authentication error is issued five times from the same server.

Reason:

User authentication is used to restrict connection to specific servers, and a correlation event is issued by associating JP1 events that indicate an authentication error. Authentication is required for a number of hosts, and you want to manage this correlation event for each individual host.

Contents of the correlation event generation definition file:

The following figure shows the contents of the correlation event generation

definition file.

*Figure 11-9: Contents of the correlation event generation definition file*

```

1  [Access_error]
2  CON=CID:1, B.ID==3A71, B.MESSAGE>=User authentication failed.
3  TYPE=threshold:5
4  SAME_ATTRIBUTE=B.SOURCESERVER
5  SUCCESS_EVENT=B.ID:A00,E.SEVERITY:Error,B.MESSAGE:Authentication errors
   occurred on $EV1_B.SOURCESERVER

```

Duplicate attribute value condition specifies an attribute name (B.SOURCESERVER) indicating the server name.

Inherits the host name set as an attribute value of the correlation source event.

*Note:* In this example, a line number is inserted at the beginning of each line to indicate the individual lines you need to write in the definition file.

To use the correlation event generation definition shown above, copy the following coding:

```

[Access_error]
CON=CID:1, B.ID==3A71, B.MESSAGE>=User authentication failed.
TYPE=threshold:5
SAME_ATTRIBUTE=B.SOURCESERVER
SUCCESS_EVENT=B.ID:A00,E.SEVERITY:Error,B.MESSAGE:Authentication errors
occurred on $EV1_B.SOURCESERVER.

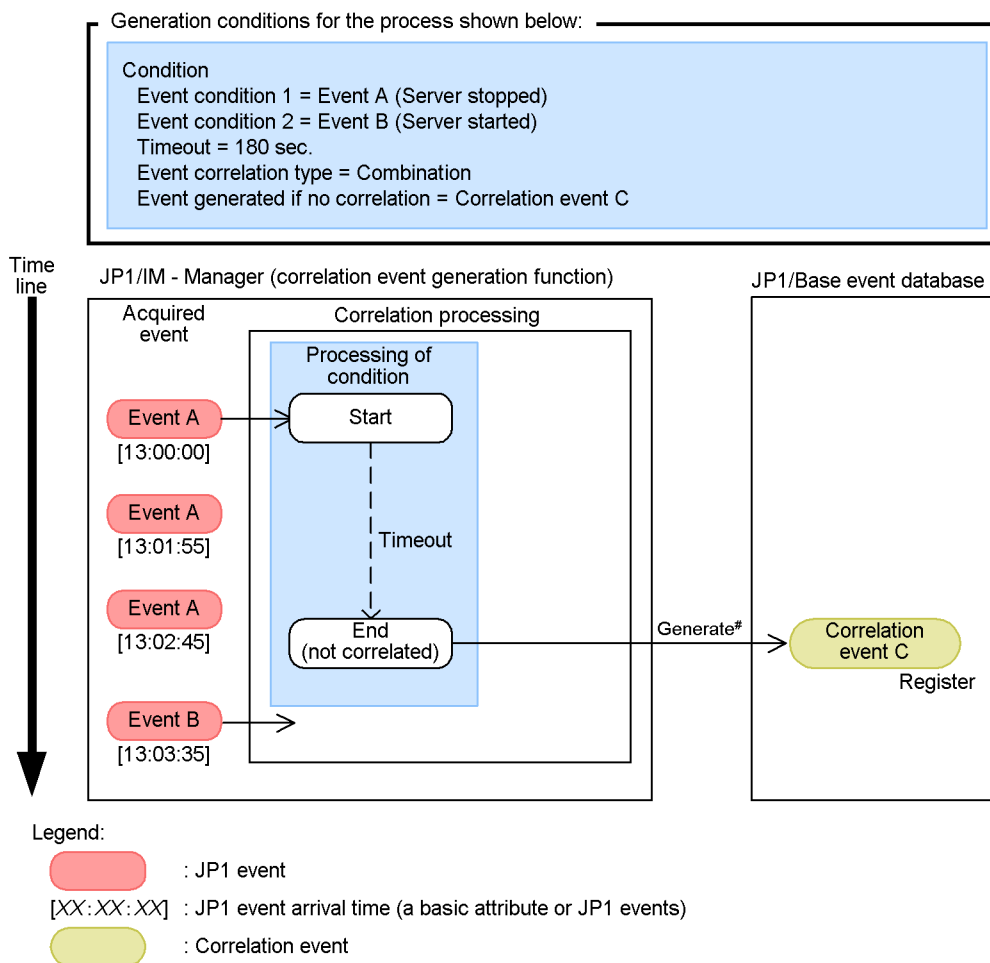
```

**(f) Monitoring for a situation where an event does not occur within a specified time period**

This example shows how to issue a correlation event when a particular event has not occurred within a specified time period, as shown by the figure below.

*Figure 11-10:* Monitoring when an event has not occurred within a specified time period

● Process of correlation event generation



#: When event generation is defined in the correlation event generation definitions for both correlation success and correlation failure for a particular JP1 event, events are generated in both situations.

Condition to be satisfied:

Suppose that a warning event A is issued, indicating that a server has stopped, followed some time later by an information event B indicating that the server has started. If both A and B are not detected within a specified timeout period, a warning event C is to be issued.

Reason:

You want to monitor for a situation where a particular event has not occurred within a specified period of time, so that you can investigate the cause of the problem.

Contents of the correlation event generation definition file:

The following figure shows the contents of the correlation event generation definition file in this example.

*Figure 11-11: Contents of the correlation event generation definition file*

```

1  [sokan1]
   TIMEOUT=180
2  CON=CID:1,B.ID==A
3  CON=CID:2,B.ID==B
4  SAME_ATTRIBUTE=B.SOURCESERVER
5  FAIL_EVENT=B.ID:C,E.SEVERITY:Warning,B.MESSAGE:Server$EV1_B.SOURCESERVER has not
   recovered.
   TYPE=sequence

```

Message is issued when correlation fails.

*Note:* The line number inserted at the beginning of each line indicates the individual lines you need to write in the definition file.

To use the correlation event generation definition shown above, copy the following coding:

```

[sokan1]
TIMEOUT=180
CON=CID:1,B.ID==A
CON=CID:2,B.ID==B
SAME_ATTRIBUTE=B.SOURCESERVER
FAIL_EVENT=B.ID:C,E.SEVERITY:Warning,B.MESSAGE:Server $EV1_B.SOURCESERVER
has not recovered.
TYPE=sequence

```

## (2) Operating environment required for correlation event generation

The following describes the operating environment required for issuing correlation events.

Memory and disk space requirements for correlation event issue

To issue correlation events, the following process of JP1/IM - Manager must be active:

- When not using the integrated monitoring database:  
Event generation service (evgen)
- When using the integrated monitoring database:  
Event base service (evflow)



Estimate in advance the extra memory requirements for starting the relevant process.

Correlation event generation history files are added periodically and make demands on disk space. Allocate sufficient resources for the estimated disk space requirements. You can change the number and size of the correlation event generation history files by adjusting a parameter in the correlation event generation environment definition file. For details, see *Correlation event generation environment definition file* in 2. *Definition Files* in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.

For details on estimating memory and disk space requirements, see the *Release Notes* for JP1/IM - Manager.

### Designing the JP1/IM and JP1/Base filters

Bear in mind the following two points when setting the JP1/IM and JP1/Base filters:

- Filtering of correlation source events

The JP1 events that you want to use as correlation source events must be distributed to the event generation service. To this end, set the JP1/Base forwarding filter and the JP1/IM event acquisition filter so that the source events will pass through.

The JP1/IM severe events filter, event receiver filters, and view filter can be optionally set. Set these filters depending on whether you need to monitor correlation source events.

- Filtering of correlation events

Correlation events must be monitored from JP1/IM - View. As a general rule, set the event acquisition filter and other JP1/IM filters so that correlation events will pass through.

Filtering can be used when you want to issue correlation events for a purpose other than monitoring, such as to trigger an automated action or to effect a status change in a monitoring node. In this case also, make sure that you set the event acquisition filter so as to allow the correlation events to pass through.

For considerations related to setting the JP1/IM filters, see 11.1.3 *Considerations for filtering JP1 events*. For considerations on setting the JP1/Base forwarding filter, see the description of JP1 event forwarding in the chapter on setting the event service in the *Job Management Partner 1/Base User's Guide*.

### **(3) Notes on correlation event generation**

Note the following points regarding correlation event generation:

- You cannot make an issued correlation event subject to any further correlation processing.

If you register a correlation event as a source event in a correlation event generation definition, the setting will be ignored.

- After editing a correlation event generation definition file, always check its contents by executing the `jcoegscheck` command. This will eliminate invalid or redundant conditions as definition errors.

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

The event generation service can still operate when a generation definition contains invalid settings, but any invalid parts in the edited file will be ignored.

- If you specify the same attribute as in an event condition in a filtering condition for the correlation target range, or in a duplicate attribute value condition, you might end up with invalid conditions that can never be satisfied. The `jcoegscheck` command does not catch such problems.

When specifying a filtering condition for the correlation target range or a duplicate attribute value condition, take care that it does not contradict the event conditions.

Two examples of invalid conditions are discussed below. The first is an example of specifying a filtering condition for the correlation target range.

*Figure 11-12: Invalid conditions: Example 1 (filtering condition for the correlation target range)*

```

1  [Wrong_condition1]
2  TARGET=B.SOURCESERVER>=host
3  CON=CID:1,B.ID==999, B.SOURCESERVER==host1;host2;host3
4  CON=CID:2,B.ID==998, B.SOURCESERVER==HOST_A
5  SUCCESS_EVENT=B.ID:A00,E.SEVERITY:Error,B.MESSAGE:$EV1_B.MESSAGE

```

This example is explained below, following the line numbers.

Line 2 declares a filtering condition for the correlation target range, and specifies as correlation targets all JP1 events whose source server name contains `host`. As a result, a JP1 event whose source server name is `HOST_A`, specified in the event condition at line 4, will not be correlated.

Because JP1 events that satisfy the event condition at line 4 are not processed, the correlation event generation condition fails and no correlation event is issued.

The next example is a duplicate attribute value condition.

**Figure 11-13: Invalid conditions: Example 2 (duplicate attribute value condition)**

```

1 [Wrong_condition2]
2 CON=CID:1,B.ID==999, B.MESSAGE*="ERROR= (.*)"
3 CON=CID:2,B.ID==998, B.MESSAGE^="ACCESS ERROR"
4 SAME_ATTRIBUTE=B.MESSAGE
5 SUCCESS_EVENT=B.ID:A00,E.SEVERITY:Error,B.MESSAGE:ErrorCode=$EV1_ENV1

```

This example is explained below, following the line numbers.

The event condition at line 2 correlates messages that begin with `ERROR=`, and the event condition at line 3 correlates messages that begin with `ACCESS ERROR`. The duplicate attribute value condition at line 4 groups JP1 events that have identical messages.

Because the event conditions at line 2 and line 3 target JP1 events that have different messages, the *same message* requirement of the duplicate attribute value condition cannot be satisfied, and correlation events will never be issued.

However, JP1 events that match the event condition in line 2 or line 3 will be processed, starting a correlation processing which can never succeed. Suppose that JP1 events are issued in the following order:

1. JP1 event (event ID: 00000999; message: `ERROR=100`) is issued.

This event satisfies the event condition at line 2, so a correlation processing begins. `ERROR=100` is registered as a potential duplicate attribute value, and the number of sets of JP1 events being correlated is incremented by one.

2. JP1 event (event ID: 00000998; message: `ACCESS ERROR`) is issued.

This event satisfies the event condition at line 3, but its message is not the same as `ERROR=100`, so a new correlation processing begins. `ACCESS ERROR` is registered as a potential duplicate attribute value, and the number of sets of JP1 events being correlated is incremented by one.

### 11.1.5 Considerations for consolidated display of repeated events

Consider whether you want to consolidate a succession of identical events in the Event Console window when a large number of JP1 events are received in a short space of time. By consolidating events of the same nature, thereby reducing the number of displayed JP1 events, you can potentially prevent important events from being overlooked.

Consider whether to use the function for consolidated display of repeated events.

Figure 11-14: Example of consolidating repeated events

(1) Without consolidated display of repeated events

Event level	Registered time	Source event server name	User name
Information	08/18 09:50:18	host	
Error	08/18 09:50:18	host	
Information	08/18 09:50:18	host	
Information	08/18 09:50:18	host	
Notice	08/18 09:50:18	host	
Notice	08/18 09:50:18	host	
Error	08/18 09:50:18	host	
Error	08/18 09:50:18	host	
Error	08/18 09:50:18	host	
Error	08/18 09:50:18	host	
Warning	08/18 09:50:19	host	
Warning	08/18 09:50:19	host	
Warning	08/18 09:50:19	host	
Warning	08/18 09:50:19	host	
Warning	08/18 09:50:19	host	
Alert	08/18 09:50:19	host	
Emergency	08/18 09:50:19	host	
Information	08/18 09:50:19	host	
Information	08/18 09:50:19	host	

(2) With consolidated display of repeated events

Summary status	Event level	Count
Information	Information	2
Error	Error	4
Warning	Warning	5+

Identical events

When this function is used, event consolidation ends when any one of the following conditions is satisfied:

- The contents of the received JP1 event do not match the consolidation start event.
- The difference between the arrival times of the consolidation start event and received JP1 event exceeds the set timeout value.
- The number of repeated events exceeds the maximum repeat count.
- The user clicks the **OK** button in the Preferences window.
- The event being consolidated was not defined as a severe event, but becomes so due to a change in the severe event definition.
- The event being consolidated was defined as a severe event, but is no longer so due to a change in the severe event definition.

You can set a timeout period in the conditions for ending event consolidation. Consider an appropriate timeout period for the type of application.

#### Comparison of event contents

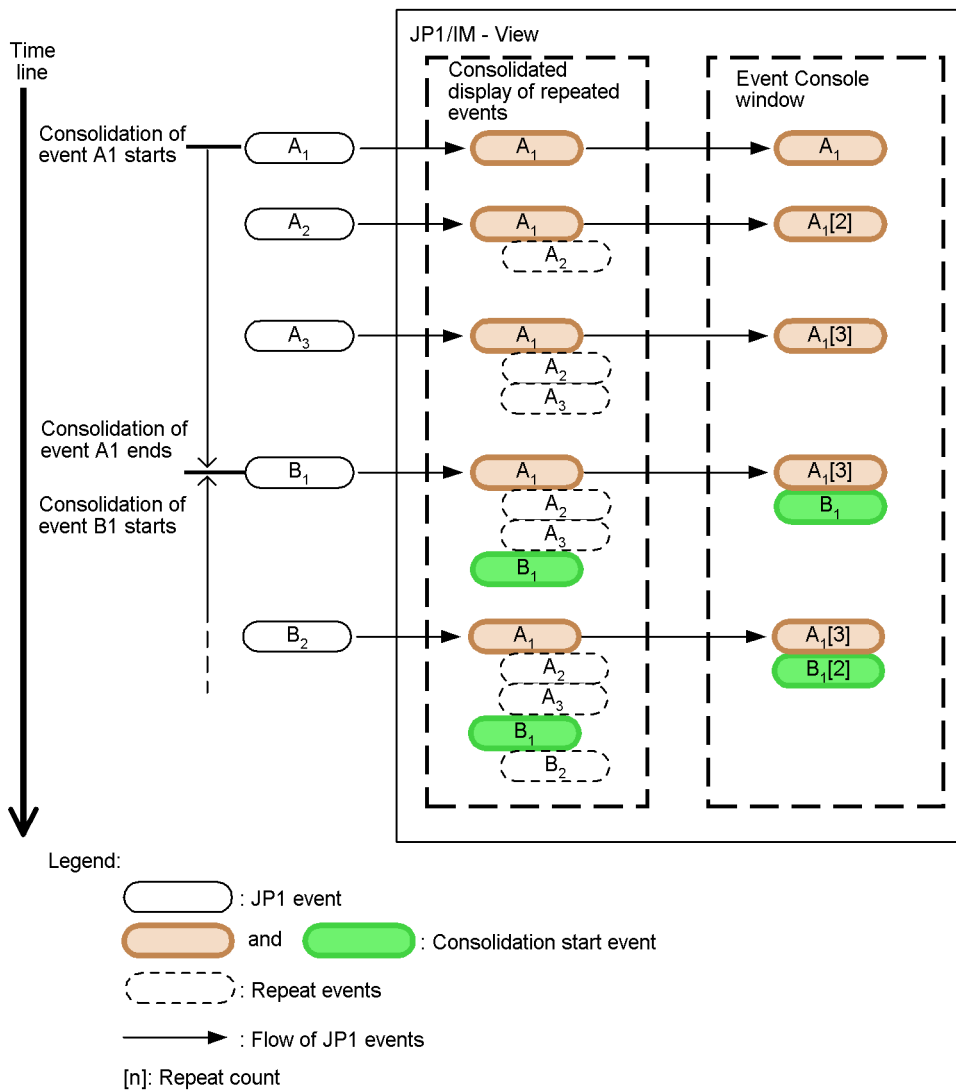
On receipt of a new JP1 event, JP1/IM - View compares its contents with the consolidation start event. If the contents match, the new JP1 event is judged to be a repeated event and the event is consolidated. If the contents do not match, event consolidation ends. The new JP1 event becomes a new consolidation start event,

and a new consolidation cycle begins.

For details about the contents of a JP1 event, see 3.4.1(1) *Event comparison attribute*.

The following figure shows an example of what happens when a received JP1 event does not match the contents of the consolidation start event.

Figure 11-15: Ending event consolidation on receipt of a non-matching JP1 event

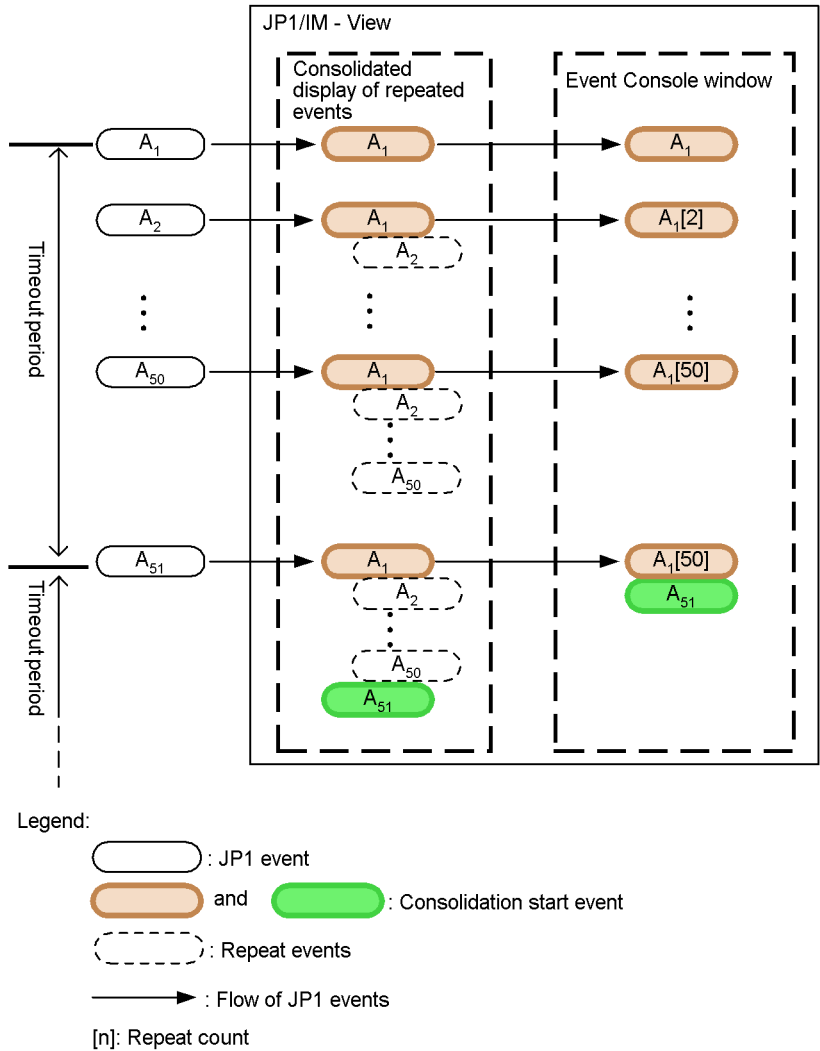


Timeout period

A timeout period must be specified for consolidating repeated events. You can specify from 1 to 3,600 seconds. The default is 60 seconds.

The following figure shows an example of what happens when the difference between the arrival times of the consolidation start event and received JP1 event falls outside the timeout period.

Figure 11-16: Ending event consolidation by timeout



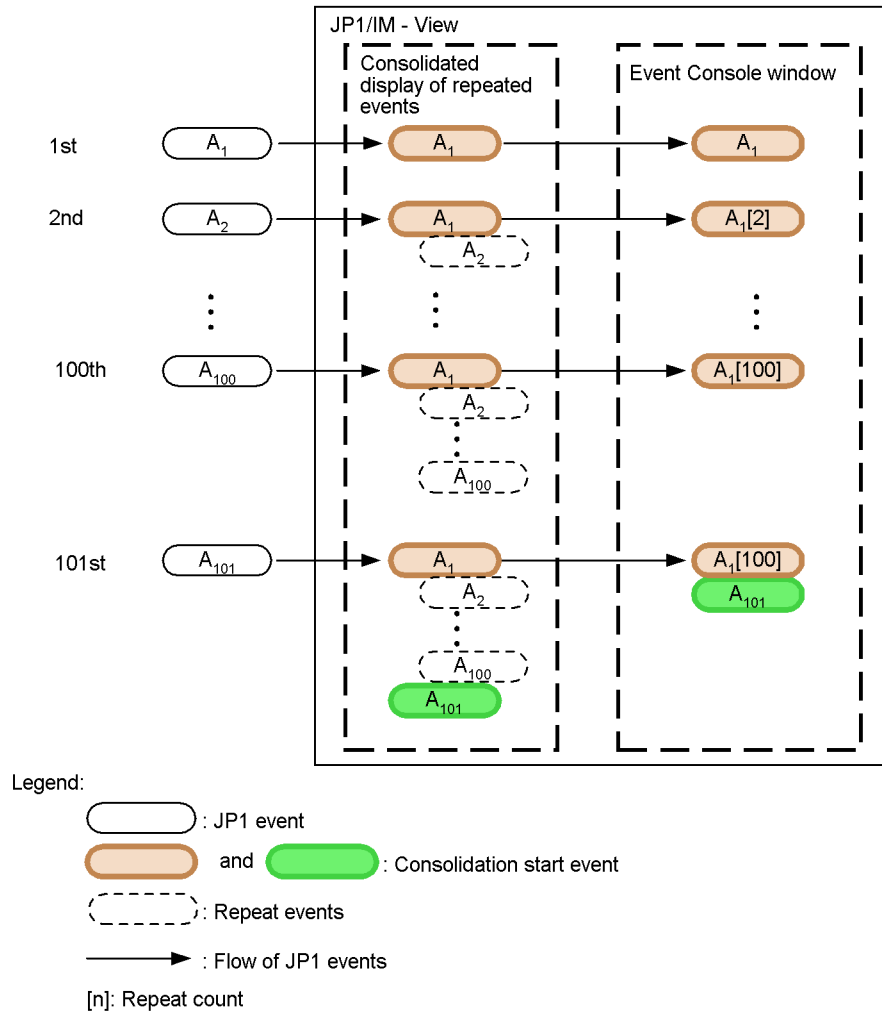
When the difference between the arrival times of the consolidation start event and

received JP1 event exceeds the timeout period, event consolidation ends. If an identical event is subsequently received, it becomes a new consolidation start event in a new cycle.

#### Maximum repeat count

The maximum number of repeated events that can be consolidated in one cycle is 100. You cannot change this limit.

*Figure 11-17: Ending event consolidation by exceeding the maximum repeat count*



Event consolidation ends when the maximum repeat count is exceeded during a

consolidation cycle. If an identical event is subsequently received, it becomes a new consolidation start event in a new cycle.

Setting consolidated display of repeated events

- Setting in the Preferences window

See *2.16 Preferences window* in the manual *Job Management Partner 1/ Integrated Management - Manager GUI Reference*.

### **11.1.6 Considerations for changing JP1 event levels**

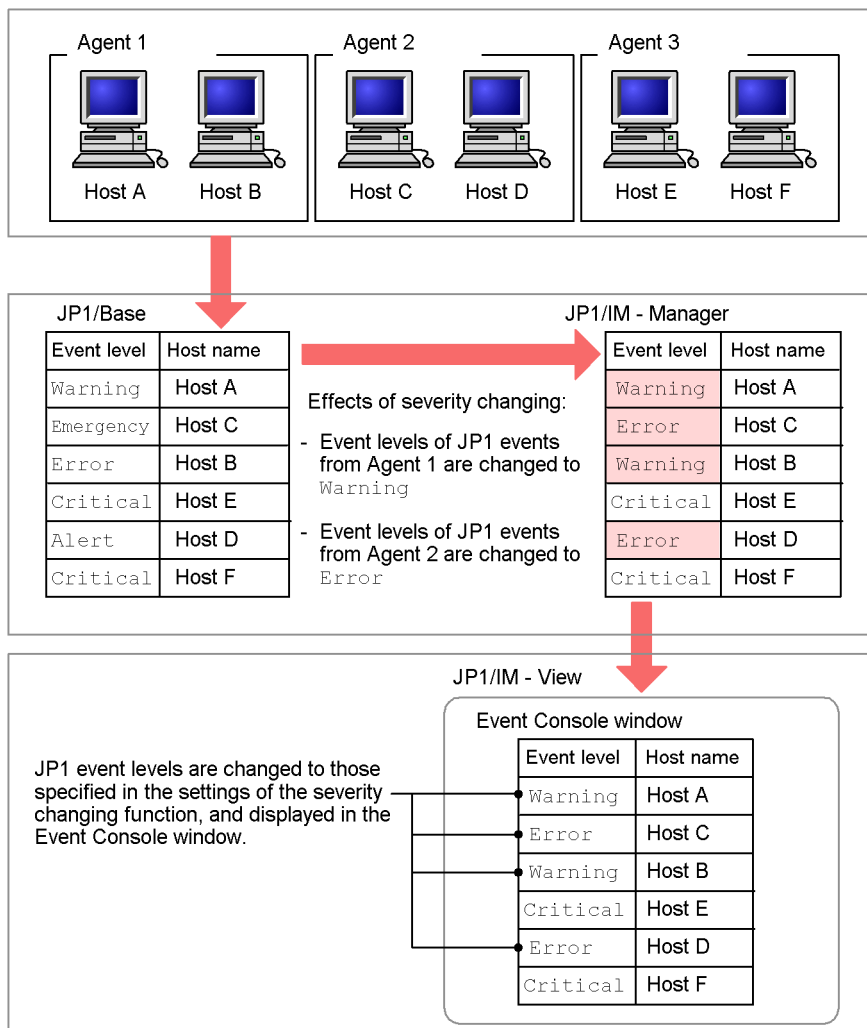
Consider changing the event levels associated with JP1 events so that the events can be appropriately categorized during system monitoring.

A JP1 event issued by a particular host or product and forwarded to the integrated manager might have an event level that does not reflect its importance in terms of system operation.

By using the severity changing function, you can change the event levels of JP1 events to realize event management that takes how you use the system into account. You can also assign a blanket event level to events from a particular agent.



Figure 11-18: Flow of changing event levels of JP1 events

**(1) Event types that support event level changing**

You can change the event level of JP1 events and events in JP1/SES format, except when the severity level is a character string of 256 or more bytes. If JP1/IM is unable to change a severity level as directed, the message KAVB4611-E is output to the integrated trace log file.

**(2) Effect on JP1/IM functions**

The severity changing function has an effect on various JP1/IM functions. The following table lists the definitions affected by changes to event levels, and indicates

which of the event levels you can specify in each function.

*Table 11-3: Effect on JP1/IM functions*

No.	Definition	Event level prior to change	Event level after change
1	Event acquisition filter	Y	N
2	View filter	Y	Y
3	Event receiver filter	N	Y
4	Severe event definition	N	Y
5	Event search conditions	Y	Y
6	Correlation event generation definition	N	Y
7	Automated action definition	N	Y
8	Definition for extended event attributes	N	Y
9	Event guide information	N	Y
10	Definition for opening monitor windows	N	Y

Legend:

Y: Can be specified.

N: Cannot be specified.

### **(3) Effect on linked products**

The severity changing function has an effect on the products linked with JP1/IM.

The following describes the effects of the severity changing function in the Central Scope and JP1/IM - Rule Operation.

#### **■ Effects in Central Scope**

The Central Scope monitors JP1 events based on their new event levels.

In some cases, changing an event level might cause a status change condition already established for a monitoring node not to match the monitoring condition. To avoid a situation in which the status of a monitoring node does not change as intended, you need to review status change conditions set for the following system-monitoring objects:

- Agent Monitoring (PFM) system-monitoring objects
  - Resource error event (PFM)
  - Resource warning event (PFM)

- HiRDB Monitoring system-monitoring objects
  - HiRDB emergency event
  - HiRDB alert event
  - HiRDB critical event
  - HiRDB error event
  - HiRDB warning event
- Physical Host Monitoring (System Manager) system-monitoring objects
  - Physical host emergency event
  - Physical host alert event
  - Physical host critical event
  - Physical host error event
  - Physical host warning event

For details about system-monitoring objects, see 4. *Lists of System-Monitoring Objects (for Central Scope)* in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.

#### ■ Effects in JP1/IM - Rule Operation

In a rule startup condition of JP1/IM - Rule Operation, specify the original event level of the JP1 event.

### 11.1.7 Considerations for setting event guide information

Using the event guide function, you can record your experience and success in resolving problems, and you can reference and accumulate diagnostic case studies, troubleshooting examples, and so on.

The system administrator manages the system through a process of error detection based on JP1 event monitoring, investigation, and remedial action. By recording your experience and results as event guide information after you have resolved a problem, users can respond quickly if the same type of JP1 event occurs again.

Event guide information is displayed as detailed information about a JP1 event in the Event Details window of the Central Console.

One item of event guide information can be displayed for one JP1 event. But the larger the system, the greater the number of JP1 events issued from linked JP1 products and user applications. Consider the following points when setting event guide information.

#### (1) Restricting applicable JP1 events

JP1 events cover a wide range and their number increases according to the size of the

system. It would not be easy to set event guide information for every event. Also, the number of items that can be defined in an event guide information file is limited to 1,000.

For these reasons, you must restrict the JP1 events for which event guide information is set. Decide how to do this from the following perspectives, for example.

**(a) Restricting applicable JP1 events by event level**

The JP1 event levels are Emergency, Alert, Critical, Error, Warning, Notice, Information, and Debug. Depending on the types of JP1 events issued by the managed hosts in your system, register event guide information for the more important JP1 events (Error level or higher, for example).

When you use the integrated monitoring database, the user-defined event level applies for JP1 events.

Under the default settings, JP1 events of Emergency, Alert, Critical, Error, or Warning level are forwarded to a manager from JP1/Base on an agent.

**(b) Restricting applicable JP1 events by frequency and urgency**

Find out what sort of JP1 events are being issued from the managed hosts by performing an event search or by executing the JP1/Base `jevexport` command, and examine the subtotals in the output results. If it appears that some JP1 events of concern are being issued more often than others, you can target those JP1 events according to which host they originate from, or how urgently they need to be identified and dealt with.

If any JP1 events requiring urgent action are being issued at a high frequency, the system administrator and operators will need to discuss and determine troubleshooting procedures. Set event guide information for these sorts of JP1 events.

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

*Note:*

A maximum of 1,000 items of event guide information can be set. Make sure that you prioritize JP1 events to keep them within this limit.

If it is difficult to restrict the applicable JP1 events to no more than 1,000, consider the following strategy:

- Group similar events or related events, and write a list of links (used as an index page) in the event-guide message for the group.

This approach requires the user to search for advice relating to a particular event from the list of links. You should therefore establish clear editing rules and explore other ways of making the list easy to search.

## (2) Setting appropriate event guide information

Because you can set event guide information as you choose, you can set appropriate information for your operational requirements, as in the following examples:

- Event guide information for initial response

State how to respond to a problem detected by a JP1 event, and guide the system administrator on what action to take when the problem occurs. Set this as event guide information.

- Event guide information for error investigation and troubleshooting

State what JP1/IM functions to use when investigating a problem detected by a JP1 event, and write down the action procedure for the problem. Set this as event guide information.

You can also prepare event guide information according to the nature of the JP1 event. For example, for JP1 events of `Error` level or higher that require urgent action, you might describe the initial response procedure, while for JP1 events of `Warning` level indicating a preventable future problem, you might describe how to investigate and preempt the problem.

### (a) Event guide information for initial response (example)

In this example, event guide information is needed for an event indicating that a JP1/AJS job running on a managed host has ended abnormally.

The JP1 event indicating abnormal termination of a JP1/AJS job has an event ID (`B.ID`) of 00004107 and an event level (`E.SEVERITY`) of `Error` level. Set event guide information for this JP1 event as follows.

Example of contents written in the event guide information file (`jco_guide.txt`):

(extract of the condition definition)

```
[EV_GUIDE_001]
EV_COMP=B.ID:00004107:00000000
EV_COMP=E.SEVERITY>Error
EV_GUIDE=The job ended abnormally.\n Contact the system
administrator in charge of host $E.C0 urgently.\n\n List of
system administrator contact details \n
Host-A:TEL(03-xxx-xxx) Mail(xxxx@xxx.co.jp) \n
Host-B:TEL(03-xxx-xxx) Mail(xxxx@xxx.co.jp) \n
Host-C:TEL(03-xxx-xxx) Mail(xxxx@xxx.co.jp)
[END]
```

**(b) Event guide information for error investigation and troubleshooting (example)**

In this example, event guide information is needed for an event indicating that the number of commands queued in JP1/Base running on an agent has reached a set threshold.

The JP1 event indicating that the command queue count threshold has been exceeded has an event ID (`B.ID`) of 00003FA5 and an event level (`E.SEVERITY`) of `Warning` level. Set event guide information for this JP1 event as follows.

Example of contents written in the event guide information file (`jco_guide.txt`):

(extract of the condition definition)

```
[EV_GUIDE_002]
EV_COMP=B.IDBASE:00003FA5
EV_COMP=E.SEVERITY:Warning
EV_FILE=user-specified-folder(path)\jco_guidemes_002.txt
[END]
```

Example of contents written in an event-guide message file (`jco_guidemes_002.txt`)

The number of queued commands has exceeded the threshold (10).

Determine the JP1/Base host from the message text.

Check whether there is insufficient memory or a backlog of automated actions on the host.

Open the List of Action Results window, or execute the `jcashowa` and `jcocmdshow` commands, to check the statuses of the automated actions.

If any urgent automated actions are waiting to be executed, cancel them as a temporary measure.

To cancel an automated action, use the `jcacancel` or `jcocmdel` command.

These two commands display a confirmation message requiring you to type `y` or `n`. When executing either command from the Execute Command window, specify the `-f` option to bypass the confirmation message.

If this event occurs frequently, use the `jcocmddef` command to modify the command execution environment.

**(3) Setting event guide information using variables (placeholder strings)**

A variable (placeholder string) can be used to represent a JP1 event attribute in an event-guide message. For example, if you set the host name of the server where the

problem originated (B.SOURCESERVER) as a variable, the actual host name will be displayed in the event guide information by means of the variable, and the message text will match the actual situation. This reduces the time required to identify the host where the problem occurred.

The following table describes the variables you can use in an event-guide message.

*Table 11-4: Variables that can be used in event-guide messages*

Event attribute		Variable	Format of substituted value
Basic attribute	Serial number	B.SEQNO	Integer character string
	Event ID	Either of the following: 1. B.ID 2. B.IDBASE	String in the format: 1. <i>basic-code:extended-code</i> 2. <i>basic-code</i>
	Source process ID	B.PROCESSID	Integer character string
	Registered time	B.TIME	
	Arrived time	B.ARRIVEDTIME	
	Source user ID	B.USERID	
	Source group ID	B.GROUPID	
	Source user name	B.USERNAME	Character string
	Source group name	B.GROUPNAME	
	Source event server name	B.SOURCESERVER	
	Destination event server name	B.DESTSERVER	
	Source serial number	B.SOURCESEQNO	Integer character string
	Message	B.MESSAGE	Character string
Extended attribute	Event level	E.SEVERITY	
	User name	E.USER_NAME	
	Product name	E.PRODUCT_NAME	
	Object type	E.OBJECT_TYPE	
	Object name	E.OBJECT_NAME	

Event attribute		Variable	Format of substituted value
	Root object type	E.ROOT_OBJECT_TYPE	
	Root object name	E.ROOT_OBJECT_NAME	
	Object ID	E.OBJECT_ID	
	Occurrence	E.OCCURRENCE	
	Start time	E.START_TIME	
	End time	E.END_TIME	
	Return code	E.RESULT_CODE	
	Other extended attribute	E. ....#	

#: Any JP1 product-specific extended attribute can be used. For example, a JP1/AJS job execution host is E.C0. For details about program-specific extended attributes, see the documentation for the particular product that issues JP1 events.

By using these variables, you can write event-guide messages that can be generally applied. For example, if you use the variable for a JP1/AJS job execution host (E.C0), you can write event-guide messages like the following.

Example of an event-guide message using a variable (extract of the EV\_GUIDE segment):

```
EV_GUIDE=The job ended abnormally.\n Check whether an error
occurred on host $E.C0.\n In a previous case, the job failed
due to insufficient memory on host A.\n Check the available
memory using the vmstat command.
```

For details about JP1 event attributes, see *3.1 Attributes of JP1 events* in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.

The character strings that can be substituted in a JP1 event attribute (variable) depend on the product. When using variables in event-guide messages, see also the description of JP1 events in the product documentation.

### 11.1.8 Considerations for saving monitoring information (CSV snapshot)

JP1/IM - View provides functionality for saving the JP1 event information displayed in the Event Console window in CSV format.

Using this function, you can keep a history (CSV snapshots) of problems occurring



from day to day, and of actions taken by the operator.<sup>#</sup> This information can be used, for example, in preparing monitoring reports for the system administrator.

<sup>#</sup>: If you need to keep records of who dealt with a problem, and when the action was taken, consider issuing a JP1 event when the response status of a JP1 event is changed. For details, see *12.7.5 Issuing a JP1 event when a response status changes*.

### **11.1.9 Considerations for saving event information in the integrated monitoring database (output of event report)**

JP1/IM provides functionality for saving the JP1 event information stored in the integrated monitoring database (output of event report).

Using this feature, you can keep a record of problems associated with JP1 events stored in the integrated monitoring database. You can also keep historical JP1 event information by outputting an event report when the integrated monitoring database reaches capacity.

By specifying an option when using the event report output functionality, you can choose the following output modes:

- Maintenance information output  
Outputs all the JP1 events recorded in the integrated monitoring database.
- Backup information output  
Outputs the JP1 events that are at risk of deletion.

For details about outputting event reports, see *3.9.2 Saving event information in the integrated monitoring database (CSV report)*.

---

## 11.2 Considerations for system monitoring from the Central Scope

---

The Central Scope allows you to monitor the system from the viewpoints required by the system administrator.

This section describes points to consider as regards the system monitoring environment required for using the Central Scope and the auto-generation function.

Before you consider system monitoring from the Central Scope, read the following reference and make sure that you understand how the Central Scope works.

About the Central Scope:

- Central Scope functionality

See 4. *Objective-Oriented System Monitoring Using the Central Scope*.

### 11.2.1 Considerations for monitoring trees

Using a monitoring tree, you can monitor the system by grouping resources according to the viewpoints required by the system administrator and displaying them in a tree format.

A monitoring tree can be easily generated using the auto-generation and editing functions.

To generate a monitoring tree, select a purpose-built template in the Auto-generation - Select Configuration window. JP1/IM provides the following monitoring tree models:

- Work-oriented tree
- Server-oriented tree

For details, see the following references.

About monitoring trees:

- Monitoring tree functionality

See 4.2 *Monitoring tree*.

- Auto-generation of a monitoring tree

See 4.3 *Automatically generating a monitoring tree*.

*Reference note:*

By setting JP1 resource groups for specific nodes, you can set up the following controls:

- Restrict the range of resources (monitoring nodes) that individual JP1 users can view and monitor

For example, you can permit a user who has `jp1admin` permission to monitor the entire system, but allow users with `jp1ope` permission to monitor only part of the system.

- Precisely control operations on displayed monitoring nodes to meet your objectives

For example, you can permit response operations (status changes) on specific monitoring nodes, but allow viewing only on particular nodes.

For details about setting JP1 resource groups for monitoring nodes, see 4.4.3 *Setting the monitoring range of a monitoring tree*.

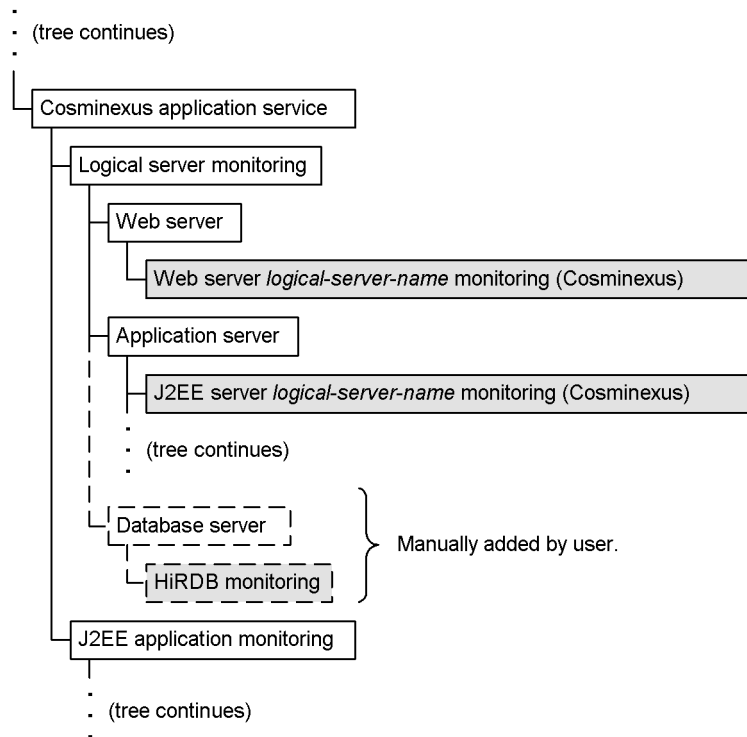
For a JP1 user who is to be registered with JP1/Base (authentication server), the account settings in JP1/Base (JP1 resource group setting) must match the setting in the Central Scope. For details, see the chapter on setting up user management in the *Job Management Partner 1/Base User's Guide*.

**(1) Notes**

- If you automatically generate a work-oriented or server-oriented monitoring tree for monitoring a Cosminexus system environment, the resulting tree will be unable to acquire information from databases that run under Cosminexus such as HiRDB. To monitor a database as a logical server in a Cosminexus environment, you must manually add the database information to the monitoring tree.

The following figure shows how you can add database information to a monitoring tree, using HiRDB as an example.

Figure 11-19: Example of adding database information to a monitoring tree



Legend:

- (Solid lines) : Appears in automatically generated tree.
- - (Dotted lines) : Does not appear in automatically generated tree.
- (White background) : Monitoring group
- (Gray background) : Monitoring object

With HiRDB 07-02 or later, you can use the system-monitoring object provided by the Central Scope to add the database information to the tree. For all other databases, create a general monitoring object and define the monitoring conditions as required.

### 11.2.2 Considerations for visual monitoring

Using the Visual Monitoring window, you arrange the objects and groups that you want to watch closely in a map view. This allows you to easily monitor even a large system from key perspectives.

By customizing the background image and Visual Icon in the Visual Monitoring window with images of your choice, you can create a window that is tailored to your

particular needs. The following figure shows an example of a customized Visual Monitoring window.

*Figure 11-20: Example of Visual Monitoring window customized with background image and Visual Icon*



For details, see the following reference:

About visual monitoring:

- Visual monitoring functionality

See 4.5 *Visual monitoring*.

### 11.2.3 Considerations for setting guide information

Using the guide function, you can display troubleshooting procedures, examples of how various errors have been handled in the past, and other such operating know-how. This guide information can be used as reference material when a problem occurs, lessening the workload of the system administrator at the initial response stage.

The content and display conditions for guide information must be considered and set by the user. Because the data on which guide information is based (operating know-how and so on) is accumulated and changes while the system is being run, make sure that you review it periodically, and amend or augment the information as required.

For details, see the following reference:

About guide information:

- Guide function

See 4.7 *Guide function*.

*Reference note:*

Differences between the two guide functions

Guide functions are provided by both the Central Scope and Central Console. They can be used for different purposes, or you might prefer to use them in combination. They differ as follows.

- Guide function of the Central Scope

Guide information can be set for individual monitoring nodes. A monitoring node is a job or server being monitored in the system. Use the Central Scope's guide function when you are monitoring the system based on a monitoring tree consisting of monitoring nodes.

Use the guide function to write advice about problems in accounting jobs, for example, or about Web server errors.

- Event guide function of the Central Console

Event guide information can be set for individual JP1 events. A JP1 event is an event that occurs in the system, and is also a potential cause when a problem occurs.

Use the Central Console's event guide function to write advice about investigating or handling a specific JP1 event itself. For details, see 3.6 *Event guide function* and 11.1.7 *Considerations for setting event guide information*.

#### **11.2.4 Considerations for defining a status change condition for a monitoring group**

By defining a status change condition for a monitoring group, you can monitor the system more precisely from a monitoring tree.

For example, in a system such as described below, where processing loads are distributed using a load balancer, an error on a lower-level node does not necessarily result in a problem in the higher-level monitoring group. In this type of system with special conditions, you can manage the system status more accurately by defining a status change condition for the monitoring group.

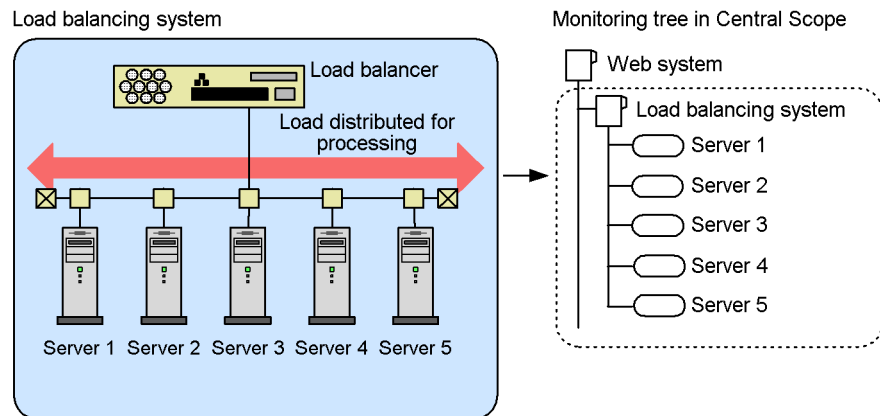
Note that the following restrictions apply when you define a status change condition for a monitoring group.

##### **(1) Examples of defining a status change condition for a monitoring group**

In the following example, the load-balancing system shown below is being monitored

in a monitoring tree. *Load-balancing system* in this context means a system that uses a load balancer to distribute processing loads.

Figure 11-21: Example of monitoring from a tree view



The terms used in the explanation below have the following meaning:

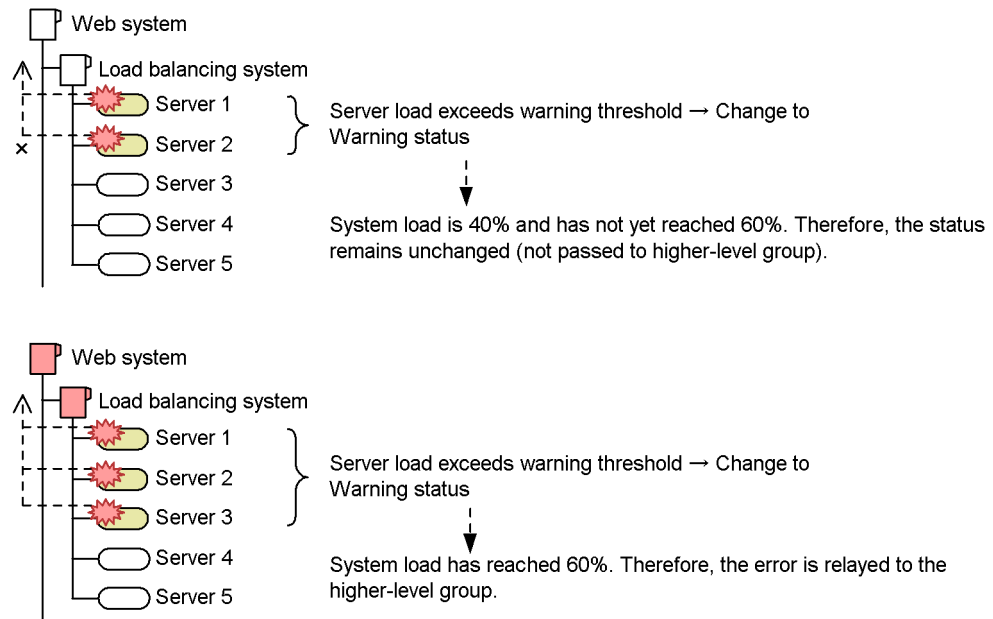
- Web system: Monitoring group (Web system)
- Load-balancing system: Monitoring group (load-balancing system)
- Server *X*: Monitoring object (server *X*)

The following conditions apply:

A Web system problem is assumed when the processing loads of 60% or more (three or more) of the five servers that make up the Web system have reached a **Warning** threshold.

Consider the following approach to relaying the node status when this system is monitored from a tree view.

Figure 11-22: Example of monitoring from a tree view (relaying the node status)



The status change condition in this example is defined as follows:

Table 11-5: Example of defining a status change condition for a monitoring group

Node name	Status change condition for monitoring group		
	Status	Child node status <sup>#</sup>	Comparison condition
Load-balancing system	Error	Warning	Percentage: 60% or more or Count: 3 or more

<sup>#</sup>: The status setting here includes statuses of higher priority. For example, an **Error** setting includes **Emergency**, **Alert**, and **Critical** statuses.

With these settings, as long as less than 60% of the servers (three of the five servers) are in **Warning** status or worse, the status of the load-balancing system and Web system remains unchanged from **Initial** status. Hence, it is not possible to search for status change events from the higher-level load-balancing system or Web system.

If you want to manage status changes in the lower-level monitoring nodes, or to search for status change events in lower-level monitoring nodes from a higher-level



monitoring group, we recommend that you define the condition as shown in the following table, for example.

*Table 11-6:* Example of defining a status change condition for a monitoring group (recommended)

Node name	Status change condition for monitoring group		
	Status	Child node status <sup>#</sup>	Comparison condition
Load-balancing system	Error	Warning	Percentage: 60% or more or Count: 3 or more
	Warning or Normal	Warning	Percentage: 20% or more or Count: 1 or more

<sup>#</sup>: The status setting here includes statuses of higher priority. For example, an `Error` setting includes `Emergency`, `Alert`, and `Critical` statuses.

## (2) Limitations on defining a status change condition for a monitoring group

Bear in mind the following limitations when you define a status change condition for a monitoring group:

- The status of a child node color-coded as being in `Error` status will not necessarily be passed to the higher-level monitoring group.

The higher-level monitoring group might remain in `Initial` status, even if a child node is in `Error` status. Because the child node status is not passed to the top-level monitoring group, the alarm lamp does not flash. (The alarm lamp flashes only when the top-level monitoring node is in `Error` status or higher.)

- When you search for status change events, some that affect lower-level nodes might be missing from the results.

If there is a monitoring group in `Initial` status between the monitoring group from which you are searching and the monitoring object that has `Error` color-coding, status change events below the group in `Initial` status will not be retrieved.

In this case, perform a monitoring node search to find nodes that have `Error` color-coding, and then perform a search for status change events.

If these two limitations are likely to be issues, define the condition so that any one child node in `Error` status will change the higher-level monitoring group to `Warning` status, for example.

- You must review the status change condition if child nodes are added or deleted and their number changes.

You must review the definition if the number of child nodes increases or decreases. For example, if a status change condition is set for a monitoring group of five child nodes, the count (3 or more) and the percentage (60% or more) mean the same. However, they mean different things when the number of child nodes increases, as follows:

- Count: 3 or more. If another five child nodes are added, making a total of 10, the count will be unchanged. (The status of the group changes when three nodes are in the specified status.)
- Percentage: 60% or more. If another five child nodes are added, making a total of 10, the percentage will be 60% of 10; that is, six. (The status of the group changes when six nodes are in the specified status.)

The Central Scope does not automatically redefine status change conditions. You should therefore periodically review the condition definitions.

- When the completed-action linkage function is enabled, the status of the monitoring group changes to `Initial` when you finish actioning all the lower-level monitoring objects (when you change all status change events to **Processed** status). That is, the monitoring group will not be searched when you perform a status-change event search.

If this limitation is likely to be an issue, define the condition so that a status change in any one child node cause a status change in the monitoring group. For example, specify that when a child node shifts to `Normal` status, the monitoring group changes to `Normal` status.

---

## 11.3 Considerations for error investigation in JP1/IM

---

When a problem is detected during system monitoring in JP1/IM, you can verify and identify the source of the error from JP1/IM - View.

Investigation strategies will depend on the applications and programs that make up the system. Consider investigation and troubleshooting methods suitable for the types of applications and programs you are using.

This section describes considerations regarding the system operations you can perform from JP1/IM.

### 11.3.1 Monitor startup

You can select a JP1 event displayed in JP1/IM - View and launch the GUI of the application associated with that event.

To open an application that issued a JP1 event in this way, the application must support the monitor startup function.

For details, see the following reference.

About the monitor startup:

- Monitor startup

See *3.12.1 Launching a linked product by monitor startup*.

### 11.3.2 Tool Launcher

In the Tool Launcher window, you can register and start programs of your choice.

For details, see the following reference.

About the Tool Launcher:

- Tool Launcher

See *3.12.2 Tool Launcher*.

### 11.3.3 Considerations for executing commands from JP1/IM - View

You can remotely execute a command on a JP1/IM agent from JP1/IM - View. The following types of commands can be executed:

- On a UNIX host: UNIX commands and shell scripts
- On a Windows host: Executable files (.com and .exe), batch files (.bat), and JP1/Script script files (.spt)

Commands that require interactive operation or open a window, non-terminating commands, and commands that shut down JP1/Base cannot be executed in this

way.

For details, see the following references:

About command execution from JP1/IM - View:

- Command execution from JP1/IM - View  
See *3.12.3 Executing commands from JP1/IM - View*.
- Overview of the command execution environment  
See *7.4.4 Managing command execution*.
- Overview of the system configuration definition and its effects  
See *7.4.3 Managing the system hierarchy*.

*Reference note:*

Commands that directly shut down the OS cannot be executed from JP1/IM - View. However, you can use JP1/Power Monitor to shut down agents.

### (1) Notes

- The length of the commands that can be executed from JP1/IM - View is restricted by the system in which JP1/IM and JP1/Base are running.

When the command execution path from JP1/IM - View includes a host (including a manager to which JP1/IM - View connects or the target host on which the command is executed) that is running JP1/IM or JP1/Base version 6 or 7, the command must not exceed 1,024 bytes. (When all the hosts on the path are running JP1/IM and JP1/Base version 8 or later, you can specify commands to a maximum length of 4,096 bytes.) When version 6 and version 7 products coexist in the system, command execution fails if the specified command exceeds 1,024 bytes. The command is not executed, and message KAVB2623-E appears in the **Message** field of the **Log** area in the Execute Command window.

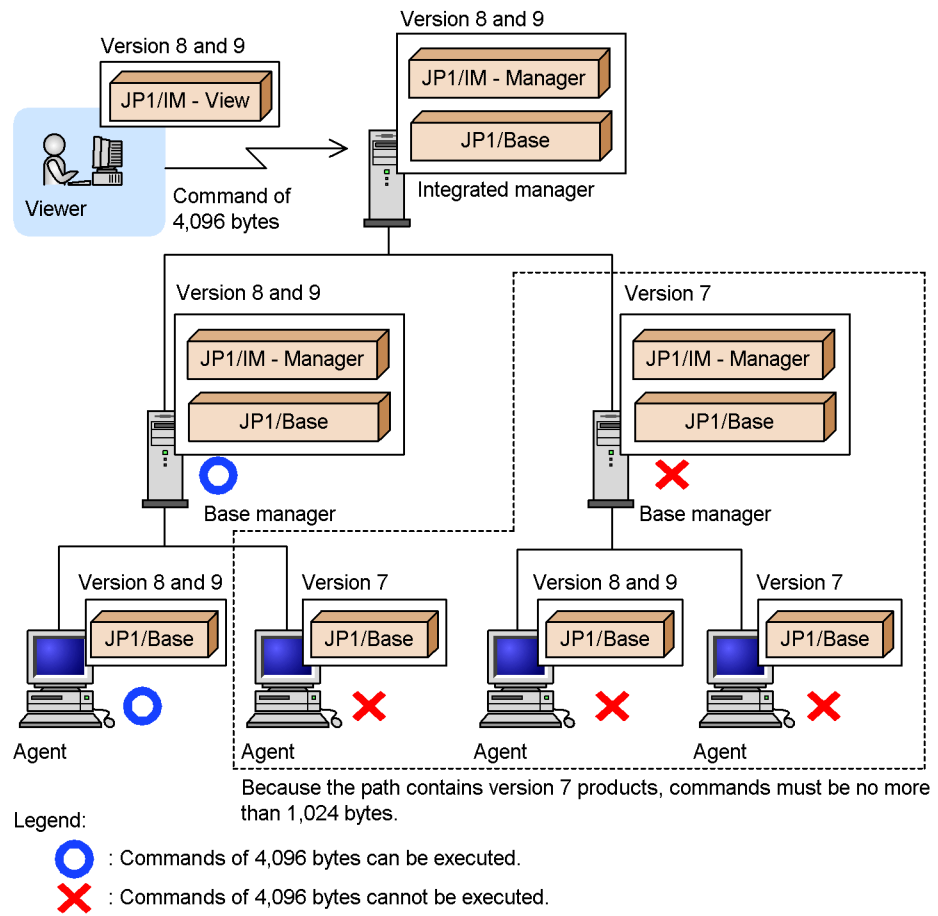
Example 1:

When the managers to which JP1/IM - View connects are running JP1/IM and JP1/Base version 8, but JP1/Base on the target host is version 7, the maximum command length is 1,024 bytes.

Example 2:

When JP1/IM and JP1/Base on the manager and JP1/Base on the target host are all version 8, the maximum command length is 4,096 bytes.

Figure 11-23: Command length restrictions according to the version of JP1/IM and JP1/Base on the execution path



---

## 11.4 Considerations for automated actions

---

Consider both the conditions for executing an automated action, and the resulting action itself (contents of the executed command).

The command execution environment and user authentication functionality are also involved in executing automated actions. Consider these as well.

### **(1) Points to consider when using automated actions**

Consider the following points:

- Before suppressing an automated action, consider carefully whether the action is one that can be safely discarded. Examples are given below.

Examples of actions that need to be executed once only during a set period (actions that can be suppressed):

- An action that flashes a signal light
- A user-notification action that sends an email
- An action that needs to be suppressed during troubleshooting

Examples of actions that should not be suppressed:

- An action that performs recovery without user intervention
- An action that changes depending on the event that triggered it

- When setting delay monitoring of an automated action, consider how long the action should take to complete from the time the JP1 event that triggers the action is received. Also consider the following:

- Number of levels from JP1/IM - Manager to the target host

The processing for sending an action from JP1/IM - Manager to the target host entails transfer processing to send the action request from the higher-level manager host to the lower-level manager hosts, and finally to have the target host receive the action. The greater the depth of the configuration management hierarchy, the greater the transfer processing involved and the longer the action will take to complete.

- Network traffic from JP1/IM - Manager to the target host

If JP1/IM - Manager is on a different server from the target host, the load on the network connecting the two hosts affects how long the action takes to complete. It will take longer when the network is busy than when traffic is light.

- Load on the JP1/IM - Manager server

The load on the server on which JP1/IM - Manager is running affects how long the action takes to complete. The greater the load, the longer it will take for the action to be sent from JP1/IM - Manager to JP1/Base on the same manager host, and the longer the action will take to complete.

- Load on the target host

The load on the target host affects how long the action takes to complete. The greater the load, the longer the action will take to complete.

- Action execution time

When an action takes longer than the delay monitoring time to execute, it will be reported as a delayed action. Make sure that you estimate action execution time accurately and set an appropriate delay monitoring time.

In JP1/IM, you can set a maximum delay monitoring time of 24 hours. If you need to monitor an action that takes longer than 24 hours to execute, link with JP1/AJS as explained below to monitor the action.

Example of monitoring the execution of an automated action by linking with JP1/AJS:

Prepare a batch file or similar as the action to be executed by JP1/IM. The batch file or similar triggers execution of a JP1/AJS job, and then ends.

To check whether a command (executed as a JP1/AJS job) that takes a day or longer to execute is running properly, use JP1/AJS.

- The commands in automated actions execute one by one, in the sequence that the actions are received at the target host. Delays might occur when one of these commands takes a long time to execute. In this case, you can reduce the chance of a delay by using the `jcocmddef` command to increase the number of commands executed concurrently by the JP1/Base on the target host.

However, when commands are executed concurrently, those that take less time to process end more quickly. If you want commands to be processed in sequence, do not change the default (execute commands one by one).

A maximum of 48 commands can be executed concurrently by the JP1/Base on the target host. When automated actions are executed by multiple instances of JP1/IM - Manager, bear the following in mind:

- The total number of commands being executed concurrently by the instances of JP1/IM - Manager must not exceed 48.
- Sufficient resources to execute the commands must be available on the target host of the automated action.
- An event that notifies the user of the status of an automated action references information saved in the action information file when invoked. If you are setting

this type of action, set an adequate file size for the action information file. You can set the size of the action information file in the automated action environment definition file (`action.conf.update`).

For details about automated actions, see the following references:

About automated actions:

- Overview of automated actions  
See 5. *Command Execution by Automated Action*.
- Overview of the command execution environment  
See 7.4.4 *Managing command execution*.
- Setting automated actions (via the GUI)  
See 2.24 *Action Parameter Definitions window* in the manual *Job Management Partner 1/Integrated Management - Manager GUI Reference*.
- Setting automated actions (in a definition file)  
See *Automated action definition file (actdef.conf)* in 2. *Definition Files* in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.
- Setting the automated action environment  
See *Automated action environment definition file (action.conf.update)* in 2. *Definition Files* in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.
- Setting the environment for monitoring the execution of automated actions  
See *Automatic action notification definition file (actnotice.conf)* in 2. *Definition Files* in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.
- Setting the command execution environment for automated actions on the target host  
See the description of the `jcccmddef` command in the *Job Management Partner 1/Base User's Guide*.
- Configuration definition  
See *Configuration definition file (jbs\_route.conf)* in 2. *Definition Files* in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.

## (2) Notes

- When a command execution log (ISAM) file is wrapped, the results of automated



actions can no longer be acquired or displayed.

*Example:*

When you open the Action Log Details window, the message KAVB5150-W appears in the **Message** area.

If this message is displayed, take action as described in 9.5(9) *Actions to take when KAVB5150-W is displayed in the detailed information (message) for the action result in the Job Management Partner 1/Integrated Management - Manager Administration Guide*.

- Delays might occur when a large number of events that trigger actions are generated in a short space of time, leading to a considerable backlog of actions queued on the target hosts.

In this situation, consider changing the number of commands that can be executed concurrently. Use the `jcocmddef` command to change this setting. However, when commands are executed concurrently, those that take less time to process end more quickly. If you want commands to be processed in sequence, do not change the default (execute commands one by one).

- If any of the following events occurs during the execution processing of an automated action, the action ceases to proceed through the usual status transition (this applies only to actions whose status is Wait, Send, Queue, Running, Wait (Canceling), Send (Canceling), Queue (Canceling), or Running (Canceling)):
  - The manager host, action relay host, or action target host is shut down or otherwise stopped.
  - Network error
  - JP1/Base failure

In this situation, check the status of the automated actions as follows.

Using the JP1/Base `jcocmdshow` command (supported in version 07-51):

You can check the action status using this command if the automated action was being processed by JP1/Base (command execution management) on the target host.<sup>#</sup>

<sup>#</sup>: If the processing request has not yet been received or if processing has ended, you cannot use this command to check the action status.

If an automated action ceases to progress and the `jcocmdshow` command cannot be used to check its status, evaluate whether it needs to be re-executed, and do so if necessary from the Execute Command window.

- If you cannot check the execution status or result of an automated action, there

might be inconsistencies in the automated action logs (command execution log file, action information file, and action hosts file).

In this situation, take action as described in *9.5(5) Actions to take when Unknown is displayed as the automated action execution status* in the *Job Management Partner 1/Integrated Management - Manager Administration Guide*.

- Using the `jcocmddef` command, you can disable registration of detailed execution results (message information) to the command execution log file, thereby increasing the processing speed of the underlying JP1/Base components (registration is enabled by default). Disabling registration, by increasing the JP1/Base processing speed, also increases the speed at which automated actions are executed.

However, when you disable registration of detailed information, the **Message** area of the Action Log Details window will show message KAVB2401-I for every action.

Change the setting (disable registration) only if this is not an issue and you definitely need to increase the automated action execution speed.

- Using the `jcocmddef` command, you can restrict the amount of execution log data forwarded to the manager host. This helps control the size of the command execution log file and reduces congestion on the network between the hosts. Note that the default setting for restricting log data transfer differs according to the JP1/Base version, as follows:
  - If you performed a new installation of JP1/Base version 8, the amount of result data logged for an action executed on that host is restricted to a maximum of 1,000 lines.
  - If you are running version 7 or earlier of JP1/Base, or if you upgraded from version 7 to version 8, there is no restriction on the amount of result data logged for an action executed on that host.

When log data transfer is restricted, only the specified amount of execution results will be forwarded. This might mean that the displayed data is truncated. (The fact that the results have been truncated is mentioned at the end of the displayed information.)

Change the setting (restrict log data transfer) only after you have considered whether you will need full data in the execution results.

- Do not use a command that directly shuts down the OS in an automated action. Use JP1/Power Monitor to shut down an agent.
- The length of the commands that can be executed as automated actions is restricted by the system in which JP1/IM and JP1/Base are running.

When the automated action execution path includes a host (including the source

manager or target host) that is running JP1/IM or JP1/Base version 6 or 7, the command must not exceed 1,024 bytes. (When all the hosts on the path are running JP1/IM and JP1/Base version 8 or later, you can specify commands to a maximum length of 4,096 bytes.) When version 6 and version 7 products coexist in the system, the execution status of the automated action will be `ERROR` if the command specified in the action exceeds 1,024 bytes. The command will not be executed, and message KAVB2623-E will appear in the **Message** area of the Action Log Details window.

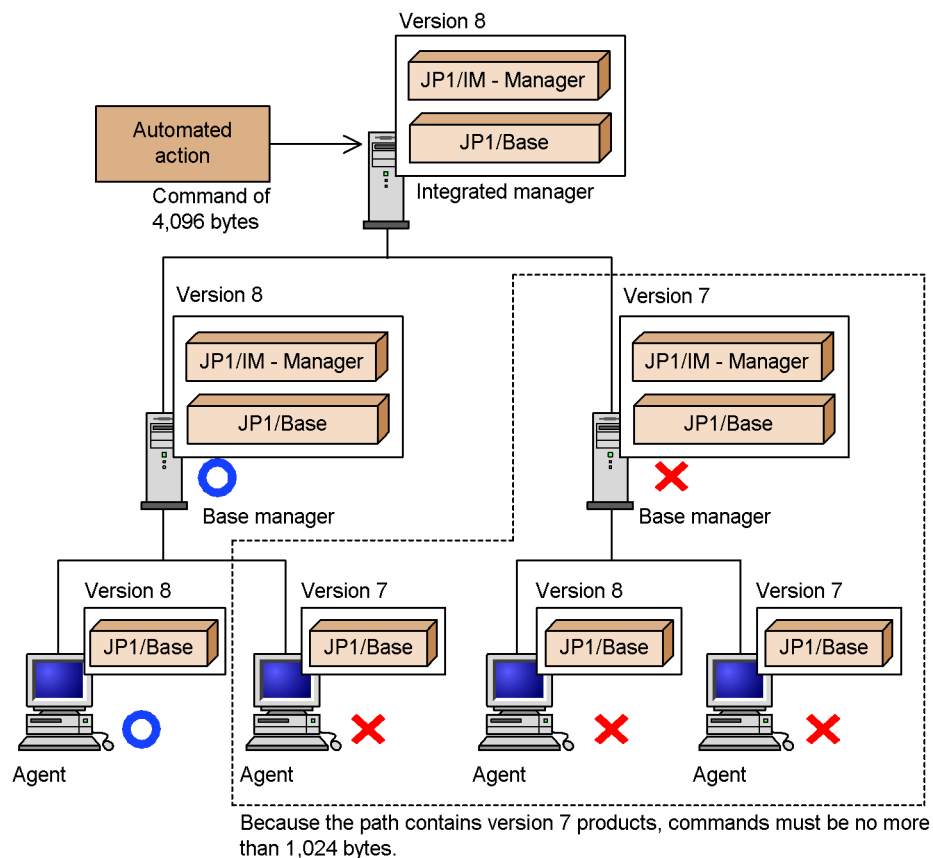
Example 1:

When the manager that generates the automated action is running JP1/IM and JP1/Base version 8, but JP1/Base on the execution target host is version 7, the maximum command length is 1,024 bytes.

Example 2:

When JP1/IM and JP1/Base on the source manager, and JP1/Base on the execution target host, are all version 8, the maximum command length is 4,096 bytes.

*Figure 11-24: Command length restrictions according to the version of JP1/IM and JP1/Base on the execution path*



Legend:



: Commands of 4,096 bytes can be executed.



: Commands of 4,096 bytes cannot be executed.

## 11.5 Considerations for managing the system hierarchy

Consider the method you want to use to configure or change the hierarchy of the system managed by JP1/IM. You can use either of the following methods to manage the system hierarchy:

### *Using IM Configuration Management*

By using IM Configuration Management, you can centrally manage the system hierarchy from IM Configuration Management - View.

To use IM Configuration Management, you must activate the IM Configuration Management database. Make sure that you take into account the IM database space requirements during the system design stage.

When using IM Configuration Management to manage the system hierarchy, do not edit the definition files or execute the commands associated with the configuration management function provided by JP1/Base.

### *Without using IM Configuration Management*

If you do not intend to centrally manage the system hierarchy from a manager, you can use the configuration management function provided by JP1/Base.

With this function, you define the host relationships in the configuration definition file (`jbs_route.conf`) on the manager, and use the associated commands (`jbsrt_distrib`, `jbsrt_sync`, `jbsrt_del`, and `jbsrt_get`) to apply and check the settings.

There is no need to activate the IM Configuration Management database if you do not intend to use IM Configuration Management. Therefore, you do not need to consider the IM database space requirements during the system design stage.

For details about these functions, see the following references:

### *Using IM Configuration Management*

- Managing the system hierarchy using IM Configuration Management  
See 6. *System Hierarchy Management Using IM Configuration Management*.

### *Without using IM Configuration Management*

- Managing the system hierarchy using the configuration definition function provided by JP1/Base  
See 7.4.3 *Managing the system hierarchy* and 7.4.5 *Collecting and distributing definition information*.

Do not change from one method to another after beginning system operation;

otherwise, inconsistencies might arise in the configuration data.

Carefully consider which method of hierarchy management you want to employ before you start using the system.

## Chapter

---

# 12. JP1/IM System Design

---

This chapter describes the system configuration and settings required in a JP1/IM system to achieve integrated system management.

- 12.1 Operating environment considerations
- 12.2 Upgrading from a previous version of JP1/IM
- 12.3 Designing the system configuration
- 12.4 Network considerations
- 12.5 Considerations for the system hierarchy
- 12.6 Considerations for user authentication
- 12.7 Considerations for the JP1/IM and JP1/Base environments
- 12.8 Considerations for linking with other integrated management products
- 12.9 JP1/IM maintenance considerations
- 12.10 Considerations for JP1/IM system-wide maintenance

---

## 12.1 Operating environment considerations

---

This section describes points to consider when planning the operating environment for JP1/IM.

### 12.1.1 Prerequisite operating systems and patches

Check the operating system and OS version required on each server in the JP1/IM system.

Depending on the OS and its version, you may need to apply service packs and patches. Refer to the *Release Notes* accompanying each JP1/IM product, and apply the required service packs and patches.

About prerequisite operating systems and patches:

- Prerequisite OSs  
See *9.3.1 Prerequisite operating systems*.
- Details on prerequisite OSs and patches  
See the *Release Notes*.

### 12.1.2 Estimating memory and disk space requirements

Estimate the amount of memory and disk space required to execute JP1/IM and JP1/Base on each host in the JP1/IM system.

In a cluster system running a number of logical hosts and physical hosts, estimate the total requirements for each individual host.

About estimating memory and disk space requirements:

- JP1/IM estimates (with equations)  
See the JP1/IM - View *Release Notes*.  
See the JP1/IM - Manager *Release Notes*.
- JP1/IM estimates (with general guidelines for a performance evaluation model)  
See *13. Performance and Estimates*.
- JP1/Base estimates  
See the JP1/Base *Release Notes*.

### 12.1.3 Estimating IM database capacity requirements

When using the integrated monitoring database and the IM Configuration Management database, estimate the amount of capacity required for the databases on



the managers where JP1/IM - Manager is running. The following table lists the database sizes available for selection when you set up the system.

*Table 12-1: Database size models*

Size model	Capacity			Example of system scale
	Total	Details		
Small scale (S)	11 GB	Integrated monitoring database	9 GB	Total items of event information: 1,000,000 (approx.) This number is based on the following assumptions: <ul style="list-style-type: none"><li>• Average event size: 1 KB</li><li>• Number of events generated per day: 33,000</li><li>• Storage period for event information: 30 days</li></ul>
		IM Configuration Management database	1 GB	Maximum number of managed hosts: 1,024 hosts
		System database area <sup>#</sup>	1 GB	--
Medium scale (M)	36 GB	Integrated monitoring database	33 GB	Total items of event information: 4,000,000 (approx.) This number is based on the following assumptions: <ul style="list-style-type: none"><li>• Average event size: 1 KB</li><li>• Number of events generated per day: 130,000</li><li>• Storage period for event information: 30 days</li></ul>
		IM Configuration Management database	1 GB	Maximum number of managed hosts: 1,024 hosts
		System database area <sup>#</sup>	2 GB	--

Size model	Capacity			Example of system scale
	Total	Details		
Large scale (L)	114 GB	Integrated monitoring database	96 GB	Total items of event information: 12,000,000 (approx.) This number is based on the following assumptions: <ul style="list-style-type: none"><li>• Average event size: 1 KB</li><li>• Number of events generated per day: 400,000</li><li>• Storage period for event information: 30 days</li></ul>
		IM Configuration Management database	10 GB	Maximum number of managed hosts: 10,000 hosts
		System database area <sup>#</sup>	8 GB	--

Legend:

--: Not applicable.

#

The size of the system database area is estimated from the amount of user data to be managed.

In a cluster system, ensure that sufficient disk space is available on the shared disk and local disk, as specified in the table below.

Table 12-2: Additional disk space requirements in a cluster system

Size model	Total space required	Space required on shared disk			Space required on local disk
		System database area	Integrated monitoring database area	IM Configuration Management database area	System database area
Small scale (S)	11 GB	0.95 GB	9 GB	1 GB	0.05 GB
Medium scale (M)	36 GB	1.9 GB	33 GB	1 GB	0.1 GB
Large scale (L)	114 GB	7.4 GB	96 GB	10 GB	0.6 GB

We recommend that you set a database size that provides sufficient leeway should the number of generated events suddenly increase during system operation.

### 12.1.4 Adjusting kernel parameters (in UNIX)

When using JP1/IM - Manager in a UNIX environment, adjust the OS kernel parameters to allocate the resources required for running JP1/IM - Manager.

Kernel parameters are settings for optimizing the resources used by the UNIX system. They include the maximum number of open files in the UNIX environment and the maximum size of shared memory segments. For details about kernel parameters, see the documentation for your OS.

Estimating kernel parameters (in UNIX):

- JP1/IM - Manager estimates  
See the JP1/IM - Manager *Release Notes*.
- JP1/Base estimates  
See the JP1/Base *Release Notes*.

### 12.1.5 Language environment considerations

Consider the language environments of the various hosts in the JP1/IM system.

Although we recommend that you use one language throughout the system, JP1/IM is capable of operating in a multi-language environment.

However, you cannot use more than one language environment in any one server.

Setting the language environment:

- About the JP1/IM language environment  
See *12.1.6 Operation in a multi-language environment*.
- Setting the JP1/Base language environment  
See the description of the pre-setup tasks in the *Job Management Partner 1/Base User's Guide*.

### 12.1.6 Operation in a multi-language environment

You can deploy JP1/IM in a system set up with multiple languages. For example, JP1/IM - View is able to simultaneously display JP1 events that are registered in JP1/Base under different language codes<sup>#</sup>.

<sup>#</sup>: Some extended characters, special characters, and control codes may not display correctly or be recognized as different characters in JP1/IM - View, regardless of whether JP1/IM is being run in a multi-language environment. For details, see *1.3 Notes on operations in windows* in the manual *Job Management Partner 1/Integrated Management - Manager GUI Reference*.

However, there are several conditions that apply when running JP1/IM in a

multi-language environment. These conditions may influence your system configuration or manner of operation.

### (1) **System conditions**

The following conditions apply to the JP1/IM system itself (the entire JP1/IM system composed of managers and agents).

- Two-byte characters in automated actions will appear garbled.<sup>#</sup> If you specify machine-dependent characters, the automated action may not work correctly.  
#: Level 1 and level 2 Japanese character codes will display normally.
- Note the following when the system contains an agent using a UTF-8 locale:
  - Version 8 or later of JP1/Base must be running in the UTF-8 locale environment. Also, any machines to which that agent forwards events must also be running version 8 or later of JP1/Base.
  - The manager must be running version 8 or later of JP1/IM - Manager and JP1/Base.
  - A system with hosts running version 7 of JP1/IM or JP1/Base will be unable to properly deal with JP1 events issued from the UTF-8 locale environment (the hosts will be unable to display the JP1 events or execute automated actions correctly).

In this case, make sure that the JP1/Base in the UTF-8 environment is version 8 or later, and set up JP1/Base to run in compatibility mode. For details about how to do so, see the description of the pre-setup tasks in the *Job Management Partner 1/Base User's Guide*.

- The following conditions apply when the system contains a combination of hosts running Japanese<sup>#1</sup> and English<sup>#2</sup> language environments:

#1: Hosts running Japanese versions of the operating system and software, in which the `LANG` environment variable is set to Japanese.

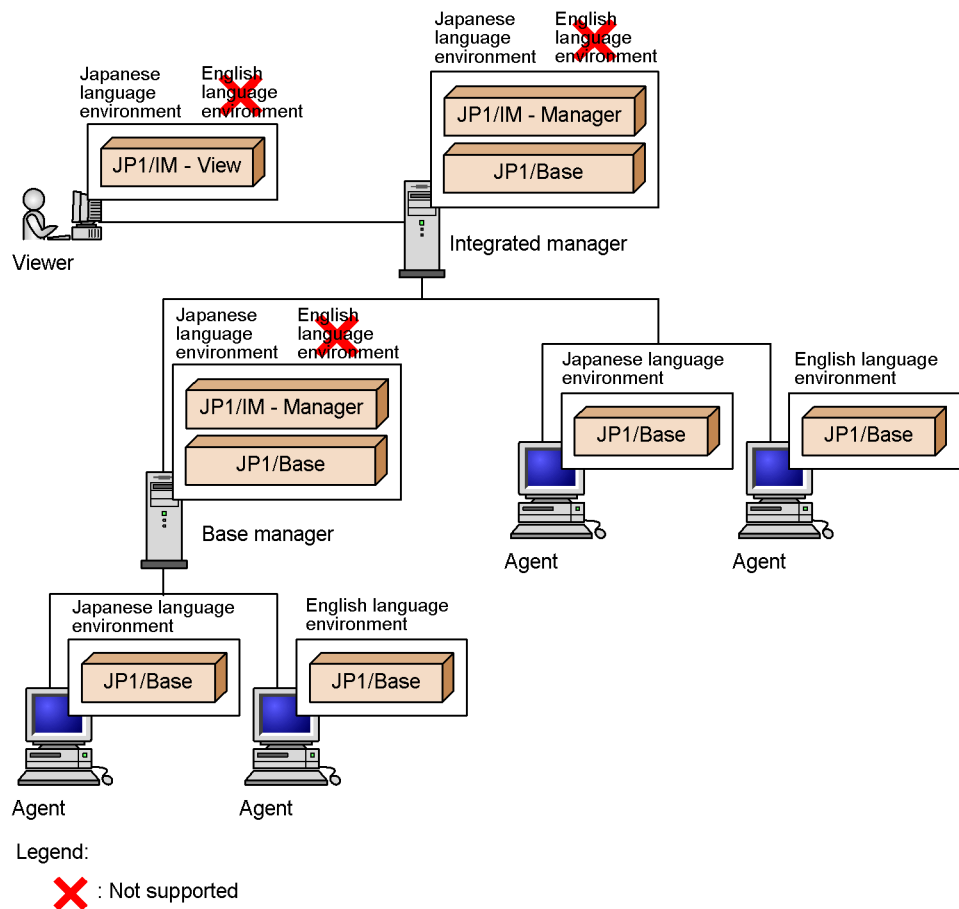
#2: Hosts running English or Japanese versions of the operating system and software, in which the `LANG` environment variable is set to English.

- Hosts configured as an integrated manager or base manager must use a Japanese language environment.
- The manager configured directly above an agent running an English language environment must be running a Japanese language environment.
- On the manager, JP1/IM - Manager and JP1/Base must run in a Japanese language environment. If you also install JP1/IM - View, install the Japanese language version.
- If you intend to monitor the system using the Central Console, when you

connect from JP1/IM - View to JP1/IM - Manager (JP1/IM - Central Console), both must be running Japanese language environments.

- If you intend using the Web-based JP1/IM - View to monitor events, you must use a Japanese Web browser running under a Japanese OS to connect to JP1/IM - Manager (JP1/IM - Central Console) running in a Japanese language environment.
- In a cluster system, both JP1/IM - Manager and JP1/Base must be running in a Japanese language environment.
- The following figure shows an example configuration of a system that combines hosts running Japanese and English language environments:

*Figure 12-1:* Example system configuration comprising hosts with Japanese and English language environments



*Notes:*

Note the following when operating a system comprising hosts running both Japanese and English language environments.

- Definition files and settings files

When you expect definition files and settings files to be used by JP1/Base in an English language environment, make sure that only alphanumeric characters (ASCII) are used for the file names, the characters in the files, and the values of any attributes. If you create and distribute these files from JP1/IM - Manager, avoid distributing files that contain 2-byte characters.

- Automated actions

Note the following when executing an automated action on a target host running an English language environment:

- Do not specify an action that contains 2-byte characters. If you specify such an action, the action results may be garbled and display incorrectly, or the action may fail to execute altogether.
- When defining variables in the automated action definition, do not specify event information that contains 2-byte characters. If you specify such information, the action results may be garbled and display incorrectly, or the action may fail to execute altogether.
- Do not use 2-byte characters in the file name of the environment variable definition file used by the automated action, or in the file itself. If the file or its name contains 2-byte characters, the action results may be garbled and display incorrectly, or the action may fail to execute altogether.
- Do not specify an automated action that outputs execution results containing 2-byte characters. If you specify such an automated action, the action results may be garbled and display incorrectly.
- Command execution from JP1/IM - View

Note the following when executing a command on a target host running an English language environment:

- Do not specify a command that contains 2-byte characters. If you specify such a command, the command execution results may be garbled and display incorrectly, or the command may fail to execute altogether.
- Do not use 2-byte characters in the file name of the environment variable definition file used at command execution, or in the file itself. If the file or its name contains 2-byte characters, the command execution results may be garbled and display incorrectly, or the command may fail to execute altogether.

- Do not specify a command that outputs execution results containing 2-byte characters. If you specify such a command, the command execution results may be garbled and display incorrectly.
- Searching for events  
Do not use 2-byte characters in search conditions when conducting an event search on a JP1/Base in an English language environment. If you specify a 2-byte character, the search will not be conducted correctly.

## **(2) Server conditions**

The following conditions apply to individual servers (all physical and logical hosts within a given machine).

- You must use the same language version (English or Japanese) for JP1/IM and JP1/Base.
- In UNIX systems, the same language code (the locale set for the host by the `LANG` environment variable or similar) must be set for JP1/IM and JP1/Base.

---

## 12.2 Upgrading from a previous version of JP1/IM

---

This section provides some notes on upgrading from a previous version of JP1/IM.

"Upgrading" as used in this manual:

*Upgrading* as used in this manual refers to an upgrade installation from a previous version (including a corrected version or patch version) to the version current in this edition of the manual.

For the JP1/IM version assumed in this manual, see the bottom of the copyright page at the front of this manual.

The product version is stated in the *Release Notes* accompanying the product. If the product version stated there differs from the product version to which this manual applies, read the *Release Notes* first (including any notes on upgrading).

### 12.2.1 Upgrading from version 8 JP1/IM - Manager products

Note the following points if you are upgrading to JP1/IM - Manager version 9 from a version 8 JP1/IM - Manager product.

#### (1) *Upgrading from the Central Console version 8*

Back up the settings information before you upgrade JP1/IM - Manager. For the procedure, see the manual for the previous version.

When you upgrade, the definition information for the Central Console is migrated from JP1/IM - Manager version 8. However, note the following points:

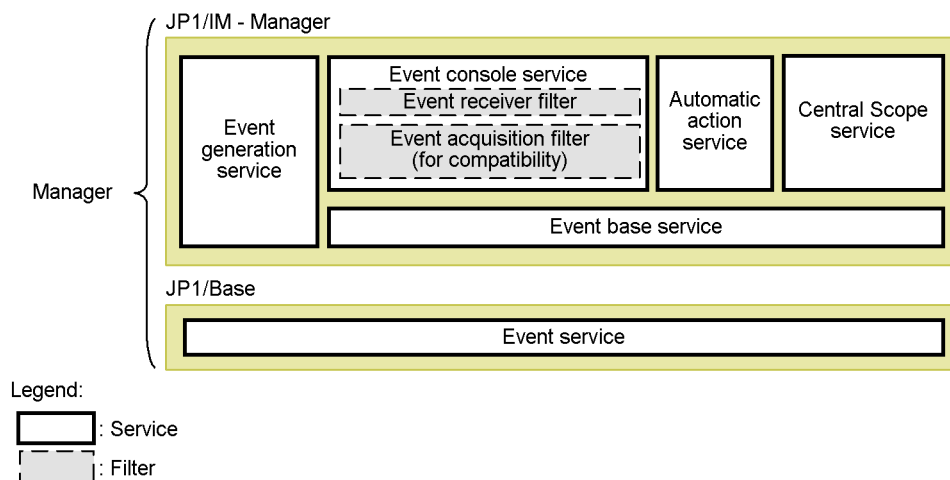
- In a logical host (cluster) environment, you must execute the `jp1cohaverup` command to apply the definition information added in the current version.

See *jp1cohaverup* in 1. *Commands* in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.

- If you were using the event acquisition filter (for compatibility) with the previous versions of JP1/IM - Manager and JP1/IM - Central Console, the event acquisition filter will continue to work in compatibility mode after the upgrade. The event acquisition filter (for compatibility) resides within the event console service and affects JP1 event monitoring only.



Figure 12-2: Position of the event acquisition filter (for compatibility)



With the event acquisition filter (for compatibility), the following functions apply to all JP1 events acquired by JP1/IM - Manager:

- Automated actions (automatic action service)
- Central Scope (central scope service)
- Issue of correlation events (event generation service)

As a result, certain anomalies may occur, depending on the filter settings. For example, an automated action may be executed, but the JP1 event that triggered it may not appear in the Event Console window.

Also, the only contents you can define in an event acquisition filter (for compatibility) are whether to acquire JP1/SES events, and whether to acquire JP1 events that have a particular event level or a particular event ID (you cannot set detailed conditions as with other filters).

To ensure consistency among the types of JP1 events acquired across the system, or to define detailed filter conditions as with other filters, execute the `jcochafmod` command to migrate the event acquisition filter from the event console service to the event base service. For details about migrating the settings in the event acquisition filter (for compatibility), see the table below. Change the settings and condition group names as required.

Table 12-3: Migration of event acquisition filter settings

Settings before <code>jcochafmode</code> command execution	After <code>jcochafmode</code> command execution
No settings	Moved to <b>Existing conditions group</b> without any settings.

Settings before jcochafmode command execution	After jcochafmode command execution
Event ID only	Moved to <b>Existing conditions group</b> .
Event level only	Moved to <b>Existing conditions group</b> .
JP1/SES events only	Moved to <b>Existing conditions group_SES</b>
JP1/SES events and event ID	The JP1/SES event setting and event ID <sup>#</sup> setting are moved to <b>Existing conditions group_SES</b> . The event ID <sup>#</sup> setting is moved to <b>Existing conditions group</b> .
Event level and event ID	Moved to <b>Existing conditions group</b> .
JP1/SES events and event level	The JP1/SES event setting is moved to <b>Existing conditions group_SES</b> . The event level setting is moved to <b>Existing conditions group</b> .
JP1/SES events, event level, and event ID	The JP1/SES event setting and event ID <sup>#</sup> setting are moved to <b>Existing conditions group_SES</b> . The event level setting and event ID <sup>#</sup> setting are moved to <b>Existing conditions group</b> .

#

The event ID setting is inherited by both condition groups.

There is no need to execute the `jcochafmode` command if you want to continue using the event acquisition filter from the previous version.

See `jcochafmode` in 1. *Commands* in the manual *Job Management Partner 1/ Integrated Management - Manager Command and Definition File Reference*.

*Note:*

When you execute the `jcochafmode` command to migrate the event acquisition filter from the event console service to the event base service, you cannot move it back again. Before you execute the `jcochafmode` command, carefully consider the effects of repositioning the filter.

- After you upgrade, the automatic action definition file (for compatibility) of the automated action function takes effect. To use version 9 action definitions, convert them to the automated action definition file for version 9 by executing the `jcdefconv` command.
- After enabling action definitions for version 9, you can:
  - Specify **Match**, **Does not match**, **First characters**, **Is contained**, **Is not contained**, and **Regular expression** as event conditions in an action definition.

- Display the Action Parameter Definitions window in JP1/IM - View version 9. If you are using the automatic action definition file (for compatibility), the Action Parameter Definitions (for compatibility) window is displayed instead.
- The regular expression settings of the automated action function are migrated from the previous version. The Windows version of JP1/IM version 9 uses extended regular expressions instead of JP1-specific regular expressions. Review your use of regular expressions as required.
- The same start option as the previous version is used for the event generation service. However, the default changes from `cold` to `warm`. Review the settings as required.
- In UNIX, if you use the `jco_start` command to start JP1/IM - Manager, copy the following file to the command directory after upgrading:  
Copy from: `/etc/opt/jplcons/jco_start.model`  
Copy to: `/etc/opt/jplcons/jco_start`
- The JP1/IM - Manager will have a different name and adopt a different configuration after the upgrade.

## **(2) Upgrading from the Central Scope version 8**

Back up the settings information and the databases before you upgrade JP1/IM - Manager. For the procedure, see the manual for the previous version.

When you upgrade, the definition information for the Central Scope is migrated from JP1/IM - Manager version 8, regardless of whether the Central Scope is enabled or disabled. However, note the following points:

Immediately after an upgrade, the functionality of the Central Scope is limited to that of the previous version. If you took CSV snapshots of the monitoring tree information and visual monitoring information in the previous version of JP1/IM - View, and you wish to use this information in the new version of JP1/IM - Manager (Central Scope), edit and apply the data now.

When you have applied the data or determined that none of the previous information is needed, execute the `jplcsverup.bat` command (in Windows) or the `jplcsverup` command (in UNIX) to migrate to the version 9 environment of JP1/IM - Manager (JP1/IM - Central Scope).

- In a logical host (cluster) environment, you must execute the `jplcshaverup.bat` command to apply the definition information added in the current version and upgrade the monitoring objects database.

For Windows systems, see *jplcsverup.bat* (Windows only) in *1. Commands* in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.

For UNIX systems, see *jp1csverup* (UNIX only) in *1. Commands* in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.

*Reference note:*

In version 8 of JP1/IM - View, you can view and edit CSV files created using previous versions. The version of the CSV file appears in the title bar. You can also apply the contents of such files to the same version of JP1/IM - Manager and the Central Scope.

The Central Scope operates in the environment of the previous version until you execute the command. This allows you to apply the contents of CSV files created using previous versions of JP1/IM - View.

- Consider enabling automatic backup and recovery of the monitoring objects database if this feature was not enabled in the previous version.

If the OS shuts down or if a failover occurs in a cluster system while the monitoring tree is being updated, the write operation to the monitoring objects database is interrupted and the database may be corrupted. To prevent corruption of the database, we recommend that you enable the automatic backup and recovery function for the monitoring objects database. It is particularly important to enable this function in a cluster system.

To set up the automatic backup and recovery function, execute the `jbssetcnf` command specifying the automatic backup and recovery settings file for the monitoring objects database (`auto_dbbackup_xxx.conf`) as an argument. This applies the contents of the definition file to the JP1 common definition information.

See *Automatic backup and recovery settings file for the monitoring object database (auto\_dbbackup\_xxx.conf)* in *2. Definition Files* in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.

- If the following functions were disabled in the previous version, consider enabling them:
  - Completed-action linkage function
  - Monitoring the maximum number of status change events

To enable these functions, edit the relevant definition files and then execute the `jbssetcnf` command.

See *Settings file for the maximum number of status change events (evhist\_warn\_event\_xxx.conf)* in *2. Definition Files* in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.

*Definition File Reference.*

Also see *Settings file for the completed-action linkage function (action\_complete\_xxx.conf)* in 2. *Definition Files* in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.

### **(3) Using IM Configuration Management with version 9 products**

In version 8, the configuration management functionality provided by JP1/Base was used to manage the hierarchical configuration of the system managed by JP1/IM - Manager. From version 9, you can use IM Configuration Management to manage the system hierarchy.

If you intend to use IM Configuration Management to manage the system hierarchy in version 9, when you migrate the system you can convert the configuration definition information defined in JP1/Base, using the IM Configuration Management functionality.

When using IM Configuration Management to manage the system hierarchy after migrating the system, do not edit the configuration definition files used by the JP1/Base configuration management functionality or execute the associated commands.

### **12.2.2 Upgrading from JP1/IM - View version 8**

Back up the settings information before you upgrade from version 8 to version 9 of JP1/IM - View. For the procedure, see the manual for the previous version.

When you upgrade, the definition information is migrated from the previous version. However, note the following points:

- A Specify Program Folder window appears during the installation. The program folder name in the existing version appears as the initial value. Change the name as required.

For a new installation, the folder name appears as **JP1\_Integrated Management - View**.

- The display names in the Tool Launcher window are not updated for version 8. If you want to use the updated contents provided in version 8, copy the following files:

- Definition file for executing applications

Copy from:

`view-path\conf\appexecute\en\!JP1_CC_APP0.conf.model`

Copy to: `view-path\conf\appexecute\en\!JP1_CC_APP0.conf`

- Definition file for the Tool Launcher window

Copy from:

```
view-path\conf\function\en\!JP1_CC_FTREE0.conf.model
```

Copy to: *view-path\conf\function\en\!JP1\_CC\_FTREE0.conf*

For details about the contents displayed in the version 8 Tool Launcher window, see 7.3.2 *Functions that can be operated from the Tool Launcher window* in the *Job Management Partner 1/Integrated Management - Manager Administration Guide*.

- In Windows Server 2008 and Windows Vista, if you attempt to perform an upgrade while JP1/IM - View is running, a dialog box appears informing you that JP1/IM - View is in use.

In this case, click the **Cancel** button to cancel the installation processing, and shut down all instances of JP1/IM - View that are active in the system. Then proceed with JP1/IM - View installation.

- If there is not enough disk space in a Windows Server 2008 or Windows Vista system, a dialog box appears informing you that there is insufficient disk space.

In this case, click the **Cancel** button to cancel the installation processing, and check the available disk space. Then proceed with JP1/IM - View installation.

### 12.2.3 Upgrading from version 7 JP1/IM - Manager products

Note the following points if you are upgrading to JP1/IM - Manager version 9 from a version 7 JP1/IM - Manager product.

#### (1) *Installation directories*

As described in the table below, JP1/IM - Manager consists of three broad categories of information, each of which is stored in a separate directory at JP1/IM - Manager installation.

Table 12-4: Categories of JP1/IM - Manager information

Category	Description
JP1/IM - Manager information	Information about JP1/IM - Manager as a whole (including JP1/IM - Central Console and JP1/IM - Central Scope)
Central Console information	Information about Central Console functionality (corresponds to JP1/IM - Central Console in previous versions)
Central Scope information	Information about Central Scope functionality (corresponds to JP1/IM - Central Scope in previous versions)

When you upgrade in Windows, the information is sorted into folders as follows:

```
Manager-path <- JP1/IM - Manager information
Console-path <- Central Console information#
Scope-path   <- Central Scope information#
```

#: If you installed a previous version of JP1/IM - Central Console or JP1/IM - Central Scope in a different folder, that folder is used and the folder shown above is not created.

When you upgrade in UNIX, the information is sorted into directories as follows:

```
/etc/opt/jplimm/      <- JP1/IM - Manager information
/opt/jplimm/          <- As above
/var/opt/jplimm/      <- As above
/etc/opt/jplcons/     <- Central Console information
/opt/jplcons/         <- As above
/var/opt/jplcons/     <- As above
/etc/opt/jplscope/    <- Central Scope information
/opt/jplscope/        <- As above
/var/opt/jplscope/    <- As above
```

## (2) Upgrading from JP1/IM - Central Console version 7

Back up the settings information before you upgrade JP1/IM - Manager. For the procedure, see the manual for the previous version.

When you upgrade, the definition information is migrated from JP1/IM - Central Console version 7. However, note the following points:

- When you upgrade from JP1/IM - Central Console version 07-00, the information defined as conditions for event receiver filters, severe events filter, view filters, and event searches is migrated as follows. Change the condition group names as required.
  - Event receiver filter
 

The filter name and user name remain as set; the filter conditions are moved to **Existing conditions group**.
  - Severe events filter
 

The filter conditions are moved to **Existing conditions group**.
  - View filter
 

The filter name becomes **Existing filter condition**, and the filter conditions are moved to **Existing conditions group**.
  - Event search conditions
 

The event search conditions are moved to **Existing conditions group**.
- When you upgrade from JP1/IM - Central Console version 07-00 or 07-10, the following message may appear in a dialog box: KAVB9032-E An attempt to switch the action information file has failed. (code = *maintenance-code*). In this case, take action according to the maintenance codes

listed in the table below.

*Table 12-5: KAVB9032-E maintenance codes*

Maintenance code	Action
2	When the installation has finished, collect information using a data collection tool and contact the system administrator. Report the maintenance code also.
3	When the installation has finished, collect information using a data collection tool and contact the system administrator. Report the maintenance code also.
4	When the installation has finished, stop all applications not in use. Then re-install the program by performing an overwrite installation.

- The Web-based operation definition file used in version 7 is renamed as described in the table below, and a new file is created for version 9. The definition information is not migrated.

*Table 12-6: Renaming of the Web-based operation definition file*

OS	Before renaming	After renaming
Windows	<code>console-path\www\console.html</code>	<code>console-path\www\console.html.jp1_im_console_v7_backup</code>
UNIX	<code>/opt/jplcons/www/console.html</code>	<code>/opt/jplcons/www/console.html.jp1_im_console_v7_backup</code>

If you want to continue using the previous definition information in version 9, access the renamed file and copy its contents to a new file for version 9. For details about the Web-based operation definition file, see *Web-based operation definition file (console.html)* in 2. *Definition Files* in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.

- The same cautionary notes apply as when upgrading the Central Console from JP1/IM - Manager version 8. For details, see 12.2.1(1) *Upgrading from the Central Console version 8*.

#### 12.2.4 Upgrading from JP1/IM - View version 7

Back up the settings information before you upgrade JP1/IM - View from version 7 to version 9. For the procedure, see the manual for version 7.

When you upgrade, the definition information is migrated from the previous version.

The same cautionary notes apply as when upgrading from JP1/IM - View version 8. For details, see 12.2.2 *Upgrading from JP1/IM - View version 8*.



### 12.2.5 Upgrading from JP1/Base version 8

To use JP1/IM - Manager, you must install JP1/Base version 9 on the same host. Note the following points when you upgrade JP1/Base on a manager:

- If there are any command execution log files from version 7 or version 6, make sure that you execute the `jccmdconv` command after you upgrade JP1/Base and before you begin running JP1/IM.

This command migrates command execution logs from the previous version to version 9. (If this is not done, the command execution logs cannot be accessed.)

If you are using JP1/IM in a cluster environment, execute the `jccmdconv` command once only on the logical host from either the primary node or secondary node with the shared disk online.

See the section describing the `jccmdconv` command in the *Job Management Partner 1/Base User's Guide*.

- The start sequence definition file is not updated when you upgrade. The definitions related to JP1/IM - Manager and the Central Console will need to be changed manually to the definitions of JP1/IM - Manager version 9.

For other cautionary notes that apply when upgrading JP1/Base, see the notes on installation and uninstallation in the *Job Management Partner 1/Base User's Guide*.

### 12.2.6 Upgrading from JP1/Base version 7

To use JP1/IM - Manager, you must install JP1/Base version 9 on the same host. When you upgrade JP1/Base on a manager, the same cautionary notes apply as when upgrading from JP1/Base version 8. For details, see *12.2.5 Upgrading from JP1/Base version 8*.

### 12.2.7 Upgrading from JP1/Base version 6

To use JP1/IM - Manager, you must install JP1/Base version 9 on the same host. When you upgrade JP1/Base on a manager, the same cautionary notes apply as when upgrading from JP1/Base version 8. For details, see *12.2.5 Upgrading from JP1/Base version 8*.

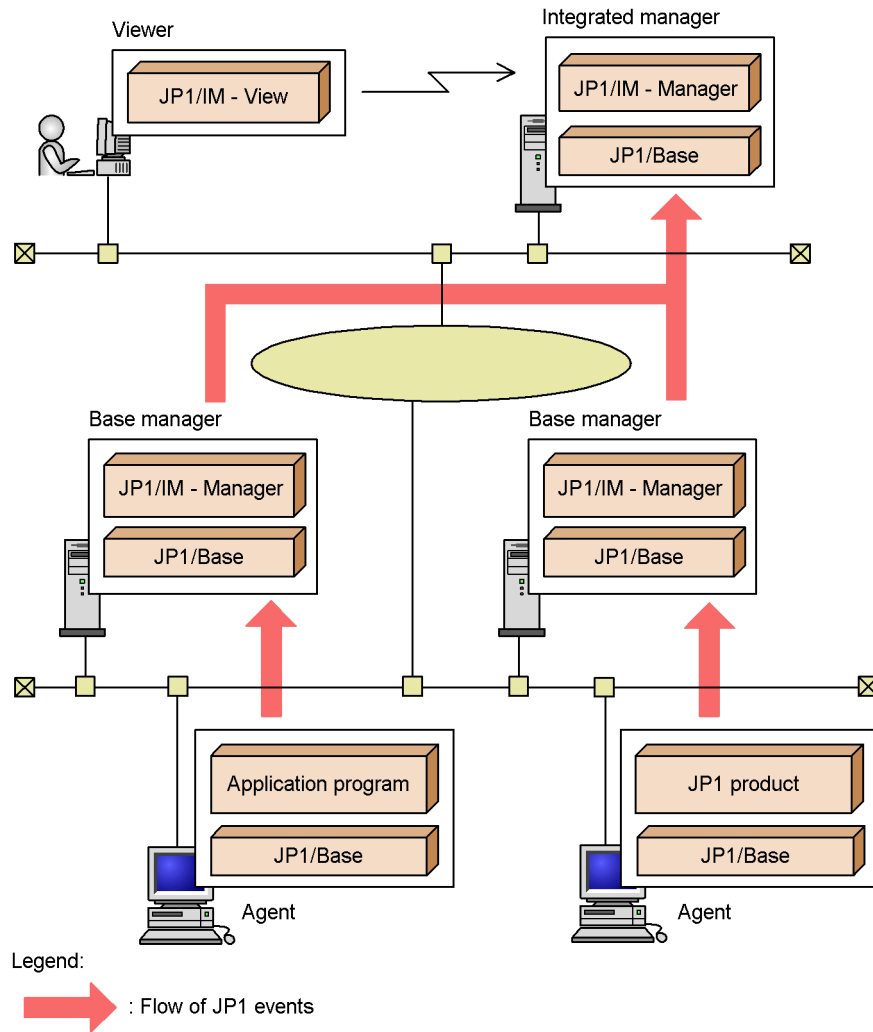
## 12.3 Designing the system configuration

This section provides some examples of configuring JP1/IM with a variety of programs.

### 12.3.1 Basic configuration

An example of a basic JP1/IM configuration is shown below.

Figure 12-3: Example of a basic configuration



This example shows a system configuration that manages job execution in a two-tier structure.

The following products are required on each host:

Integrated manager (top-level manager)

- JP1/IM - Manager  
Runs the Central Console, Central Scope, and IM Configuration Management. The Central Scope is required to monitor the system by associating jobs and JP1 events. It is not required to monitor job execution simply by monitoring JP1 events. The IM Configuration Management feature is available when the IM Configuration Management database is activated.
- JP1/Base

Base manager

- JP1/IM - Manager
- JP1/Base

Base manager

- JP1/IM - Manager
- JP1/Base

Agents (job execution hosts)

- JP1/Base  
JP1/Base is required on every agent. JP1/Base performs processing such as sending and receiving JP1 events and executing commands.
- Job execution programs (user application programs, JP1 products, and so on)

Viewers (for monitoring the system)

- JP1/IM - View

In the system shown in this example, JP1 events related to the status of jobs executing on the agents are forwarded to the base manager by JP1/Base. Then, if necessary, each JP1 event is forwarded from the base manager to the integrated manager.

The administrator can manage the whole system by logging into the integrated manager from JP1/IM - View on a viewer.

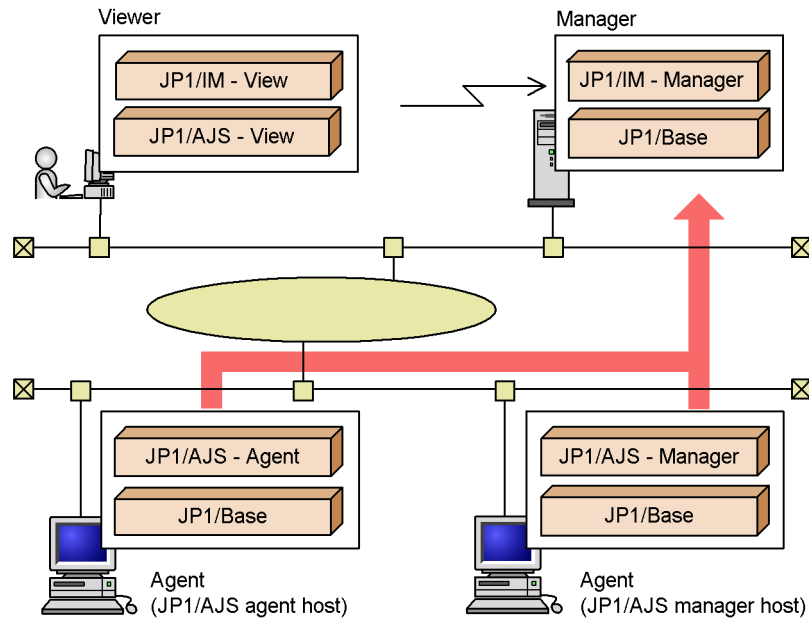
JP1/IM supports multi-level system configurations. JP1/IM - Manager is required on the top-level manager and on each intermediate-level manager. The Central Scope can also be used on the intermediate-level managers.

### 12.3.2 Configuration with JP1/AJS for monitoring job execution

By linking JP1/IM with JP1/AJS, you can view information about jobs being executed by JP1/AJS from JP1/IM - View. Also, you can open JP1/AJS windows from JP1/IM - View, and then define or operate on jobs.

The figure below shows an example of a system configuration that links JP1/IM with JP1/AJS.

Figure 12-4: Example of linkage with JP1/AJS



Legend:



: Flow of JP1 events

(host name) : Host name as defined in the linked product

The following products are required on each host:

#### Managers

- JP1/IM - Manager

Runs the Central Console and Central Scope. The Central Scope is required to monitor the system by associating jobs and JP1 events. It is not required to monitor job execution simply by monitoring JP1 events.

- JP1/Base

#### Agents (JP1/AJS manager hosts)

- JP1/AJS - Manager
- JP1/Base

Agents (JP1/AJS agent hosts)

- JP1/AJS - Agent
- JP1/Base

Viewer

- JP1/IM - View
- JP1/AJS - View

JP1/AJS - View is required on the viewer to open and work with JP1/AJS windows from JP1/IM - View.

In this example, JP1 events related to the execution status of JP1/AJS jobs are forwarded to the manager, and the status of each job is monitored from JP1/IM - View.

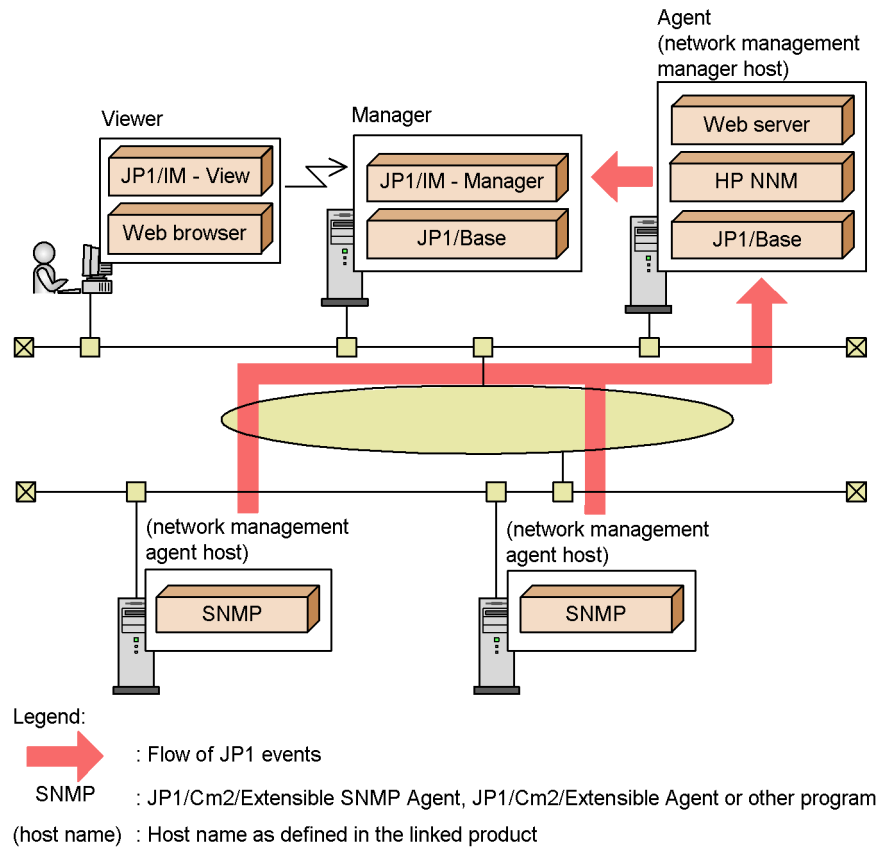
On the viewer, the user accesses JP1/AJS - View from JP1/IM - View. JP1/AJS - View connects to JP1/AJS - Manager for performing operations in JP1/AJS.

### 12.3.3 Configuration with HP NNM for monitoring the network

You can monitor the system network by linking JP1/IM with HP NNM version 7.5 or earlier.

The user opens the windows of HP NNM version 7.5 or earlier from JP1/IM - View. Also, in the Event Console window of JP1/IM - View, you can monitor SNMP traps managed by HP NNM version 7.5 or earlier and converted into JP1 events by JP1/Base.

Figure 12-5: Example of linkage with HP NNM version 7.5 or earlier



The following products are required on each host:

#### Managers

- JP1/IM - Manager

Runs the Central Console and Central Scope. The Central Scope is required to monitor the system by associating jobs and JP1 events. It is not required to monitor job execution simply by monitoring JP1 events.

- JP1/Base

#### Agents (network management manager host)

- Version 7.5 or earlier of HP NNM
- HTTP server

Required for displaying HP NNM Web pages.

- JP1/Base

(Network management agent hosts)

- JP1/Cm2/Extensible SNMP Agent, JP1/Cm2/Extensible Agent, and so on

Viewer

- JP1/IM - View
- Web browser

Required for displaying HP OpenView NNM Web pages.

Event levels of SNMP traps after conversion to JP1 events

- When a SNMP trap is converted into a JP1 event, the trap severity level is converted into an event level, as listed in the table below.

*Table 12-7: Event level when a SNMP trap is converted into a JP1 event*

Severity level of SNMP trap	Display (event level) after conversion into a JP1 event
Normal	Information
Warning	Warning
Minor	Error
Major	Critical
Critical	Alert

SNMP trap conversion and precautions are described in the *Job Management Partner 1/Base User's Guide*. See the chapter on setting the event converters for details about converting SNMP traps.

- If your system monitors JP1 events converted by JP1/Base from SNMP traps issued by version 7.5 or earlier of HP NNM, the IP address of the host at which the problem occurred may not be received correctly. This is because, when JP1/Base converts a SNMP trap into a JP1 event, the value set in the *source IP address* attribute of the JP1 event is the IP address of the host on which JP1/Base resides, not the IP address of the host that issued the SNMP trap. To acquire the name of the issuing host, specify the *SNMP trap source* extended attribute. To define the attribute value, specify the `$EV"SNMP_SOURCE"` variable.

*Reference note:*

For details about system configurations with HP NNMi, see the manual *Job Management Partner 1/Integrated Management - Event Gateway for Network Node Manager i Description, User's Guide and Reference*.

### 12.3.4 Configuration for monitoring JP1 events from a Web browser

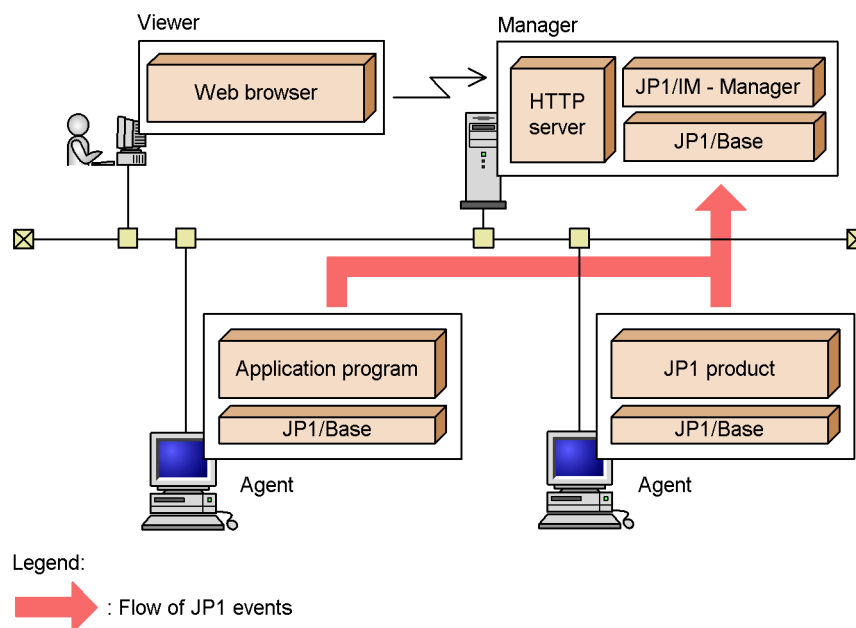
JP1 events can be monitored in JP1/IM using a Web browser. In this case, JP1/IM - View is not required on the viewer.

However, the following limitations apply when you use a Web browser:

- You cannot connect to JP1/IM - Manager (JP1/IM - Central Scope).
- You cannot access windows such as the Execute Command window and Tool Launcher window. There are also operational limitations: You cannot invoke the monitor startup to launch linked applications, and you cannot save event list information (as CSV snapshots). For details about browser limitations, see *1. Window Transitions and Login Window* in the manual *Job Management Partner 1/Integrated Management - Manager GUI Reference*.
- Some limits are different. See *D. Limits* for details.

A system configuration example is shown below.

*Figure 12-6: Example of configuration for monitoring JP1 events from a Web browser*





The following products are required on each host:

Manager

- JP1/IM - Manager
- JP1/Base
- HTTP server

Agents

- JP1/Base
- JP1-series products, application program, and so on

Viewer

- Web browser

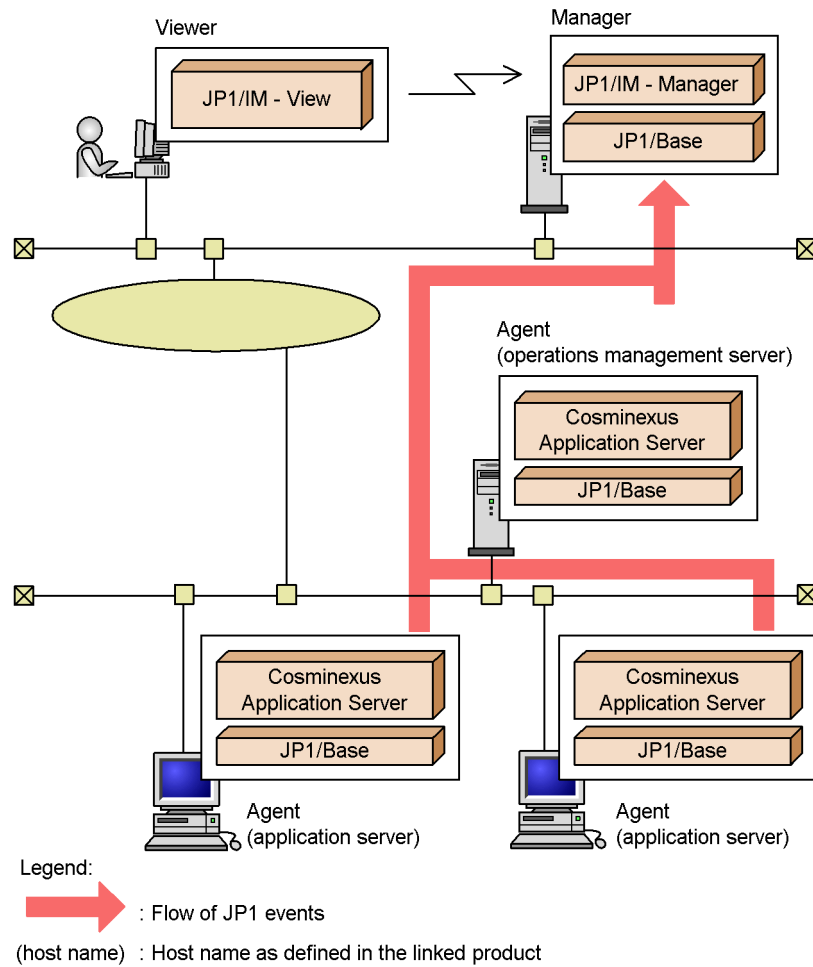
The Java Runtime Environment (JRE) and bundled plug-ins are required in the Web browser to monitor JP1 events. For details, see the JP1/IM - Manager *Release Notes*.

### **12.3.5 Configuration for monitoring the status of a Cosminexus system environment**

You can monitor the status of a Cosminexus system environment (an execution and management environment for a Web system) by linking JP1/IM with Cosminexus. This streamlines the process of error investigation by allowing you to open the Cosminexus windows from JP1/IM - View, in the same manner as with other linked products.

An example system configuration is shown below.

Figure 12-7: Example of linkage with Cosminexus



The following products are required on each host:

#### Manager

- JP1/IM - Manager

Runs the Central Console and Central Scope. The Central Scope is required to monitor the system by associating jobs and JP1 events. It is not required to monitor job execution simply by monitoring JP1 events.

- JP1/Base

#### Agent (Cosminexus operations management server host)

- Cosminexus Application Server

Required to run and manage the applications on the application servers.

This host requires the Cosminexus Management Server and its prerequisite processes, provided with the application server.

- JP1/Base

Agents (application server hosts)

- Cosminexus Application Server

On an application server host, install Cosminexus Application Server and use the configuration software according to your needs. Operation and management of Cosminexus Application Server is performed by Cosminexus Manager (Cosminexus Management Server) on the operations management server.

- JP1/Base

Viewer

- JP1/IM - View

*Reference note:*

Cosminexus is an application server that allows you to consolidate information from distributed systems accessed via a network (Internet or intranet).

Cosminexus can be used to manage environments such as the execution environment of a Web system.

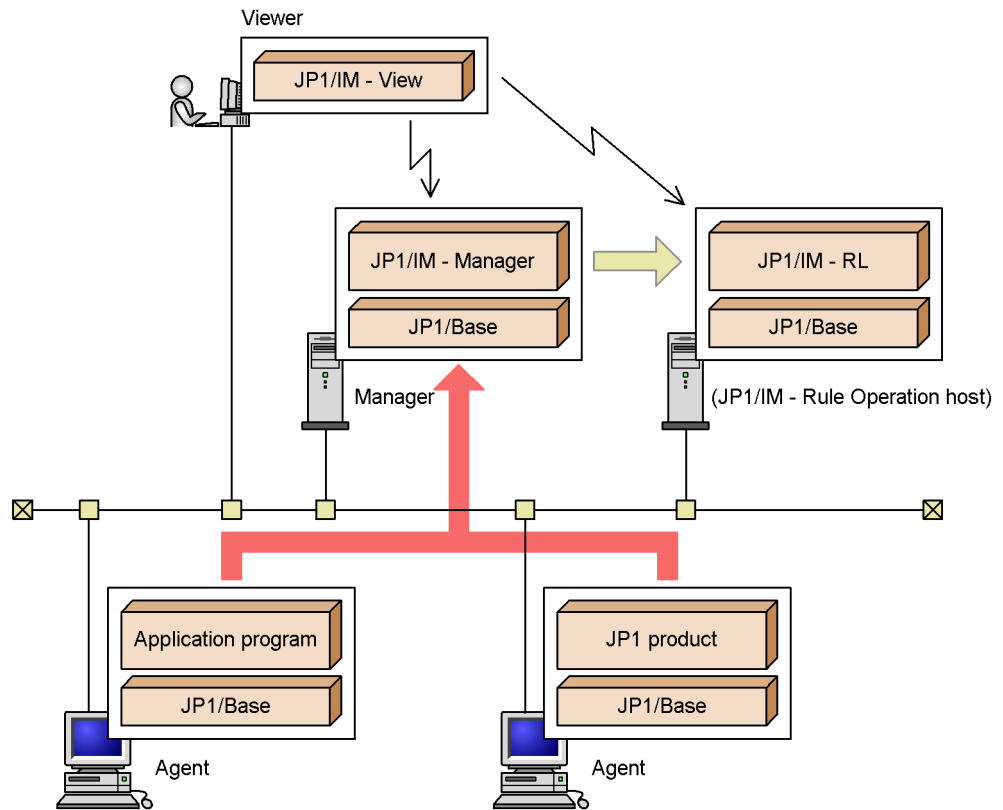
Errors that occur at startup or shutdown or during execution of a logical server managed by Cosminexus (J2EE servers, Web servers, naming services, CTM and so on) are converted into JP1 events and initially registered with JP1/Base on the Cosminexus operations management server host. These events are later forwarded to the JP1/IM - Manager host by the JP1 event forwarding function of JP1/Base. In this manner, JP1/IM can monitor JP1 events that occur on the Cosminexus operations management server host by monitoring the associated JP1 events registered on the JP1/IM - Manager host.

### 12.3.6 Configuration with JP1/IM - Rule Operation

By linking JP1/IM - Manager with JP1/IM - Rule Operation, you can automatically notify JP1/IM - Rule Operation when a rule startup event (JP1 event) is issued in the system.

An example of a system configuration for this purpose is shown below.

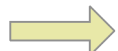
Figure 12-8: Example of configuration with JP1/IM - Rule Operation



Legend:



: Flow of JP1 events



: Reporting to JP1/IM - Rule Operation

(host name) : Host name as defined in the linked product

The following products are required on each host:

Viewer

- JP1/IM - View

Manager

- JP1/IM - Manager

The JP1/IM - Rule Operation linkage function must be enabled.

- JP1/Base

(JP1/IM - RL host)

- JP1/IM - Rule Operation
- JP1/Base

Agents

- Application program, JP1-series products, and so on
- JP1/Base

In this example, JP1 events related to the status of application programs and JP1 products executing on the agents are forwarded to the manager and are monitored from JP1/IM - View.

When a rule startup request event is received among the forwarded JP1 events, JP1/IM - Manager on the manager sends the request to JP1/IM - Rule Operation automatically.

JP1/IM - Rule Operation invokes the rule specified in the rule startup request. The user can check whether it was executed by accessing JP1/IM - Rule Operation from JP1/IM - View. The JP1/IM - Rule Operation host and manager can be the same server.

*Note:*

As with automated actions, JP1/IM - Manager performs the processing to notify JP1/IM - Rule Operation according to the system hierarchy.

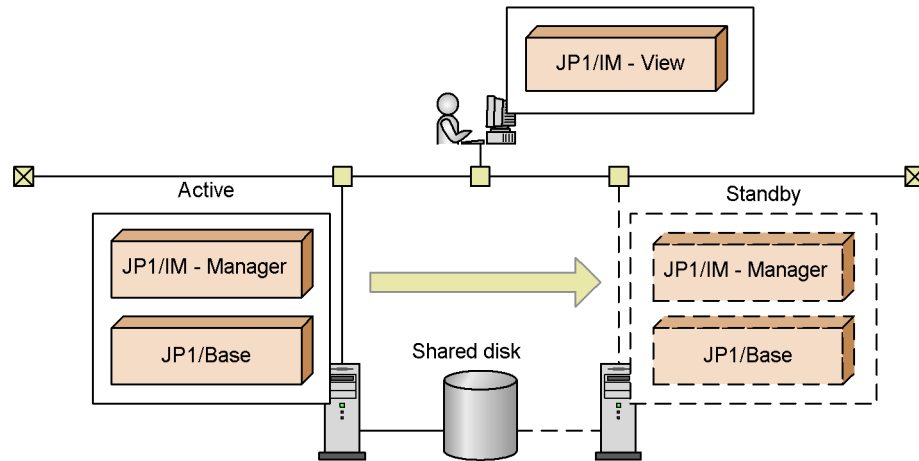
For this reason, if you want to run JP1/IM - Manager and JP1/IM - Rule Operation on different hosts, you must configure the JP1/IM - Rule Operation host at a level below the JP1/IM - Manager host.

### 12.3.7 Configuration for operation in a cluster system

JP1/IM supports cluster systems. When used in a cluster system, JP1/IM - Manager is failed over to the secondary node when a problem occurs on the primary node, and system monitoring continues without interruption.

An example of a system configuration for using JP1/IM - Manager in a cluster system is shown below.

Figure 12-9: Example of configuration for operation in a cluster system (active-standby configuration)



In this configuration, there is a primary server and a secondary server.

JP1/IM - Manager executes on the primary server. The secondary server stands by in case a failure occurs on the primary server. In normal circumstances, JP1/IM - Manager on this server is in stopped state.

For details, see 6. *Operation and Environment Configuration in a Cluster System* in the *Job Management Partner 1/Integrated Management - Manager Configuration Guide*.

#### (1) Notes

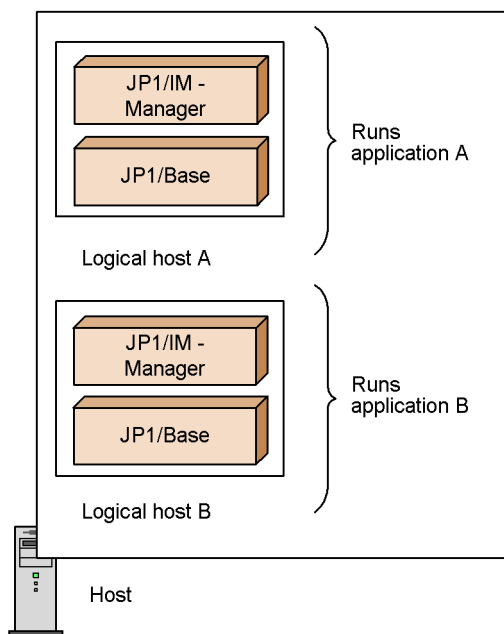
- When using JP1/IM in a cluster system, do not set up JP1/IM - Manager to restart after abnormal termination. If you need to restart JP1/IM - Manager, do so under the control of the cluster software.
- When a process management process is activated on a logical host in a cluster configuration, if the logical host's `conf` folder does not contain an extended startup process definition file, the extended startup process definition file on the physical host is copied.

### 12.3.8 Configuration for operation on a logical host in a non-cluster environment

JP1/IM - Manager can be run on a logical host in a non-cluster environment. By using a logical host that is not subject to failover, you can run multiple instances of JP1/IM - Manager, each dedicated to a particular application.

You can monitor more than one system from a single machine by running an instance of JP1/IM - Manager on a logical host corresponding to each system. The following figure shows an example of using JP1/IM - Manager to perform integrated monitoring of two systems from a single machine.

*Figure 12-10: Performing integrated monitoring of two systems from one machine*

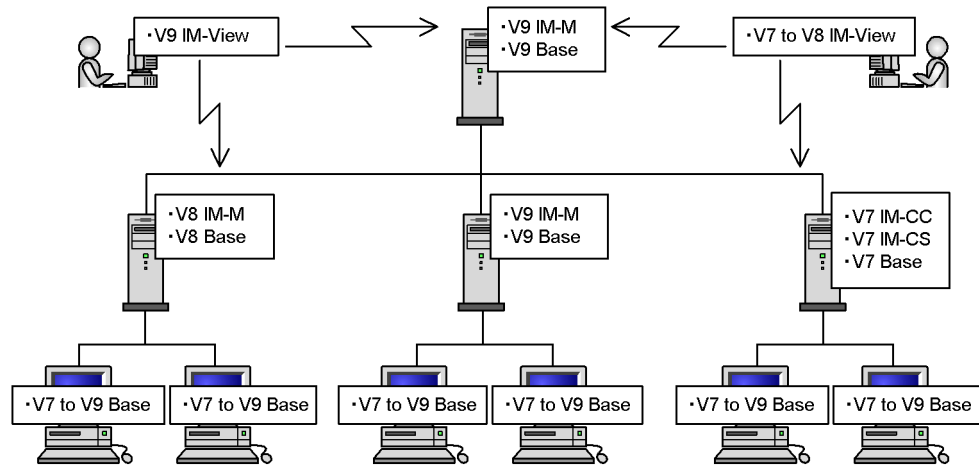


For details, see *6.5 Logical host operation and environment configuration in a non-cluster system* in the *Job Management Partner 1/Integrated Management - Manager Configuration Guide*.

### 12.3.9 Configuration for differing product versions

An example of a system configuration in which differing versions of JP1 products coexist is shown below.

Figure 12-11: Example of configuration for differing product versions



## Legend:

V9 IM-View	: JP1/IM - View V9
V9 IM-M	: JP1/IM - Manager V9
V9 Base	: JP1/IM - Base V9
V8 IM-M	: JP1/IM - Manager V8
V8 Base	: JP1/IM - Base V8
V7 IM-CC	: JP1/IM - Central Console V7
V7 IM-CS	: JP1/IM - Central Scope V7
V7 Base	: JP1/IM - Base V7
V7 to V8 IM-View	: JP1/IM - View V7 or V8
V7 to V9 Base	: JP1/IM - Base V7 to V9

Note the following points when monitoring operations in a JP1/IM system with differing product versions:

- Versions 9, 8, and 7 cannot coexist on the same machine.  
For example, you cannot run JP1/Base version 8 and JP1/IM - Central Console version 7 on the same machine.
- When products of different versions are linked, only the functions provided by the oldest of the versions can be used.  
For example, if JP1/IM - View version 7 connects to JP1/IM - Manager version 8, the operations you can perform are limited to those supported in JP1/IM - View version 7.



For details about the restrictions that apply when different product versions coexist, see *H. Connectivity with Previous Versions*.

---

## 12.4 Network considerations

---

Consider the configuration of the network in which JP1/IM will be used.

There are several aspects to consider, from the network settings on each host through to the network as a whole.

JP1/IM communication is controlled by the JP1/Base core functionality. This section discusses JP1/IM, but you should also consider JP1/Base network requirements.

### 12.4.1 Host names and IP addresses

JP1/IM operates using the host name displayed by the `hostname` command or, in a cluster system, the specified logical host name.

When specifying a host name in a JP1/IM function, set the host name displayed by the `hostname` command or the logical host name.

Set the host names to be used by JP1/IM in the `hosts` file or similar so that they can be converted into IP addresses.

If you are using the DNS, do not specify the host name in FQDN format. For example, specify `jp1v6.soft.hitachi.co.jp` as `jp1v6`.

When specifying a logical host name, comply with the following conventions:

*Number of specifiable characters when not using the IM database:*

- In Windows: 1 to 196 bytes (recommended: 63 bytes or less)
- In UNIX: 1 to 255 bytes (recommended: 63 bytes or less)

*Number of specifiable characters when using the IM database:*

- 1 to 32 bytes

If you are using any other host names, see *12.4.3 Operation in a configuration connected to multiple networks*.

- When a host has multiple IP addresses, and a local host name is defined for each IP address in the `hosts` file, you can only specify the host name output by the `hostname` command as the **Target host** setting for an automated action.

An example is shown below.

Suppose that the following is defined in the `hosts` file:

```
100.0.0.10  hostA
200.0.0.10  hostB
```

If the host name displayed by the `hostname` command is `hostA`, you can only specify `hostA` as the target host name.

- When `jp1hosts` information is set, the definitions in the `hosts` file are not referenced for those host names and IP addresses defined in the `jp1hosts` information.

An example is shown below.

Suppose that the following is defined in the `jp1hosts` information:

```
hostA 100.0.0.10 200.0.0.10
```

Suppose also that the following is defined in the `hosts` file:

```
100.0.0.10 hostA hostB
200.0.0.10 hostC
```

In this case, the `hosts` file is not referenced for `hostA`, IP address `100.0.0.10`, or IP address `200.0.0.10`. For this reason, you cannot specify `hostB` and `hostC`, which are not defined in the `jp1hosts` information, as target host names for command execution.

Note the following points:

- Using DHCP

If the IP addresses used by JP1/IM and JP1/Base are managed using DHCP, set an unlimited duration for the IP address lease so that the IP address does not change.

JP1/IM and JP1/Base will not work properly if the IP address changes during JP1/IM and JP1/Base operation.

- Using a DNS server

Set the DNS server so that host names can be converted to IP addresses, and IP addresses can be converted to host names (reverse lookup). Note that when a DNS server (including Active Directory) is used for name resolution, you must purposely set JP1/IM to allow address lookup in both directions.

## 12.4.2 Server network configuration

Check the following points regarding the server network configuration in which JP1/IM is to be used:

- Media sense (in Windows)

We recommend that you disable the Windows media sense functionality that

detects LAN cable disconnection and inactivates IP addresses. If the media sense functionality is enabled, a temporary network error will cause IP addresses to be lost, disabling JP1 communication.

- Duplicate NIC

Some OSs provide duplicate NIC functionality (for example, Windows NIC teaming, Solaris network multipath, or AIX Ethernet channel) for switching to a standby NIC if the primary NIC fails. A server running JP1 that uses the duplicate NIC functionality must be completely compatible with non-duplicate NIC operations and must not affect JP1 operations.

### 12.4.3 Operation in a configuration connected to multiple networks

When the JP1/IM hosts are configured in an environment connected to multiple networks, requirements like the following may apply to the JP1/IM system:

- Example: The host name should not be the host name displayed by the `hostname` command or a host name specified as a logical host name.
- Example: JP1 needs to communicate over a designated LAN dedicated for operation management, separate from other products.

If your system has such requirements, use the special setting called *multiple LAN connection* in JP1/IM and JP1/Base. For example, set `jp1hosts` information to associate host names with IP addresses uniquely in JP1.

See the following references when considering setup and operation.

About multiple networks:

- Operation in a multi-network environment

See *7. Operation and Environment Configuration Depending on the Network Configuration* in the *Job Management Partner 1/Integrated Management - Manager Configuration Guide*.

Also see the description of JP1/Base communication settings according to network configuration in the *Job Management Partner 1/Base User's Guide*.

Notes:

When `jp1hosts` information is set, the definitions in the `hosts` file are not referenced for those host names and IP addresses defined in the `jp1hosts` information.

### 12.4.4 Operation behind a firewall

JP1/IM supports operation in a network configuration through a firewall. JP1/IM supports the firewall packet filtering method and the NAT static conversion method.

See the following references when considering setup and operation.

About operation behind a firewall:

- Use in a firewall environment

See 7. *Operation and Environment Configuration Depending on the Network Configuration* in the *Job Management Partner 1/Integrated Management - Manager Configuration Guide*.

Also see the description of JP1/Base communication settings according to network configuration in the *Job Management Partner 1/Base User's Guide*.

### (1) Notes

- There are two types of communication between a manager and agent: Communication according to the JP1/IM system hierarchy, and direct communication with the target host (see 7.3 *Communication performed in the JP1/IM system environment*). The firewall settings must support the type of communication being used.
- JP1/IM and JP1/Base use ports even for communication within the local host. If you are using JP1/IM and JP1/Base on the host set up as a firewall, the firewall settings must permit local traffic through all the ports used by JP1/IM and JP1/Base.

## 12.4.5 WAN connection

JP1/IM can be used over a WAN, but note the following precautions.

- Due to the periodic traffic between JP1/IM - View and JP1/IM - Manager, we do not recommend use of a WAN (INS-P or INS-C) network that charges by time or traffic.
- Communication timeouts may tend to occur between JP1/IM - View and JP1/IM - Manager. If this is the case, review the timeout periods set for communication between JP1/IM - View and JP1/IM - Manager.

About JP1/IM - View and JP1/IM - Manager timeout periods:

See *Communication environment definition file (console.conf.update)* in 2. *Definition Files* in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.

See *Communication environment definition file (view.conf.update)* in 2. *Definition Files* in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.

See *Communication environment definition file (tree\_view.conf.update)* in 2. *Definition Files* in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.

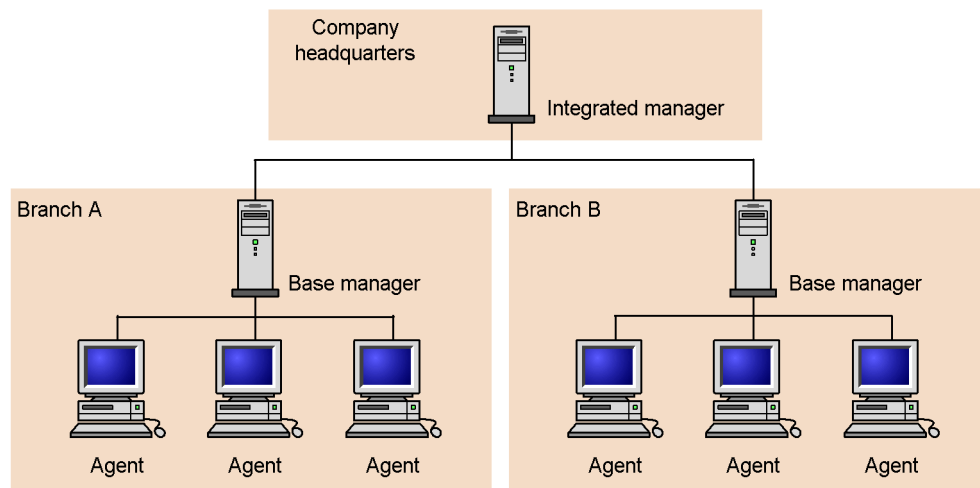
## 12.5 Considerations for the system hierarchy

Consider the hosts to be managed by JP1/IM and their hierarchical relationships.

In JP1/IM, the configuration management functionality is used to determine the range of the systems to be monitored by JP1/IM. You can also configure a hierarchy with base managers or relay managers arranged below the integrated manager, and agents placed below the base managers or relay managers.

The following figure shows a potential configuration in which a machine at the head office serves as the integrated manager, main machines at each branch office serve as base managers, and the other machines at the branch offices serve as agents.

Figure 12-12: Example system hierarchy



Using the configuration management functions, you can define the configuration of the system to be managed by JP1/IM as *configuration definition* information. This allows you to perform the following tasks:

- Forward JP1 events to higher-level hosts
- Execute commands remotely from JP1/IM - View
- Execute automated actions from JP1/IM
- Collect and distribute definition information

When using IM Configuration Management, you define the system hierarchy through IM Configuration Management - View. If you are not using IM Configuration Management, you define the system hierarchy using the JP1/Base configuration management functionality.

For details about these functions, see the following references:

When using IM Configuration Management:

- Hierarchical configurations that can be set with IM Configuration Management

See *6.2.1 Hierarchical configurations managed by IM Configuration Management*.

When not using IM Configuration Management:

- Hierarchical configurations that can be set with the JP1/Base configuration management functions

See *7.4.3 Managing the system hierarchy*.

Due to the risk of introducing inconsistencies in the data describing the system hierarchy, you cannot change the management mode after you begin managing the system hierarchy.

Carefully consider which mode you want to use to manage the system hierarchy before you begin running JP1/IM.

## 12.6 Considerations for user authentication

Consider the authentication servers used to manage JP1 users.

To monitor the system operation in JP1/IM, the user logs in to JP1/IM - Manager on the manager from JP1/IM - View. The authentication server authenticates the user at login, and the user's operating permissions are returned to JP1/IM - View. In JP1/IM, this processing flow is called *user authentication*.

In JP1/IM, user authentication setup is required on the managers and on the host on which JP1/Base serves as the authentication server. (For details about setting up user authentication, see the description of setting up the user management functionality in the *Job Management Partner 1/Base User's Guide*.)

### 12.6.1 User authentication blocks

On a manager, you must specify the authentication server that is accessed by the manager. If multiple managers access the same authentication server, the management range of the authentication server will cover all those managers. This management range is called a *user authentication block*.

You can construct one or more user authentication blocks within a system by specifying settings in JP1/Base. The table below describes the relative advantages and disadvantages of having one or multiple user authentication blocks. Determine how many to construct by referring to this table and *(1) Recommended number of user authentication blocks*.

*Table 12-8: Number of user authentication blocks and advantages/disadvantages*

Number of user authentication blocks	Advantages/disadvantages
Only one user authentication block in the system	The system administrator can centrally manage the JP1 users. However, if the authentication server goes down, JP1/IM will be inoperable because the entire system will be affected and its reliability impaired.
Multiple user authentication blocks in the system	The system administrator must manage every block of JP1 users. However, because the authentication servers are independent, the system is more robust.

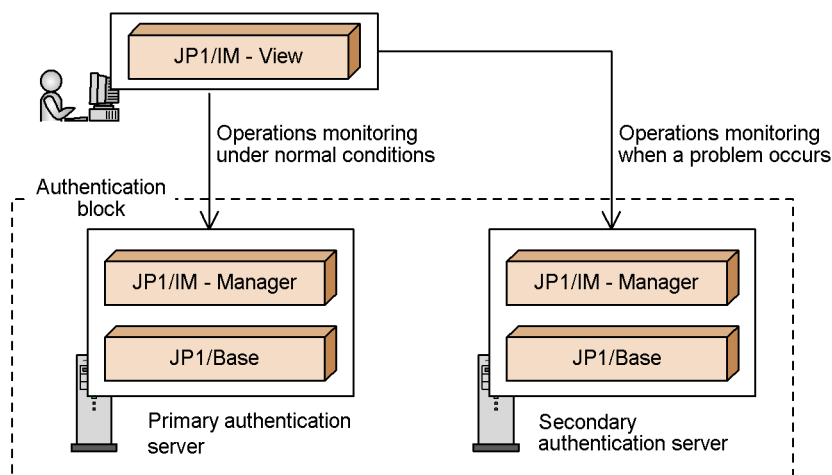
#### **(1) Recommended number of user authentication blocks**

Management of multiple user authentication blocks in a system can be complex. We recommend that you construct one or only a few blocks, and take measures to make the system more robust.



One way of making the system more robust is to install two authentication servers (primary and secondary authentication servers) in one user authentication block.

Figure 12-13: Authentication servers



By having two authentication servers, the secondary authentication server can be swapped in automatically and you can perform uninterrupted system operation monitoring if a problem occurs on the primary authentication server. You can also enhance the robustness of the system by running the authentication server hosts in a cluster system, or by setting automatic restart if an authentication server terminates abnormally.

About authentication servers:

- JP1 user management and authentication servers

See 7.4.1 *Managing JP1 users*.

Also see the description of setting up the user management functionality in the *Job Management Partner 1/Base User's Guide*.

- Authentication servers to be used by JP1/IM

Specification via the JP1/Base Environment Settings window or the `jbssetusrsv` command

See the description of setting up the user management functionality in the *Job Management Partner 1/Base User's Guide*.

## 12.6.2 Access permissions of JP1 users

When registering a JP1 user on an authentication server, you must assign the most appropriate JP1 resource group and JP1 permission level for the JP1 user's scope of operation.

To enable use of the Central Console, assign the JP1 resource group JP1\_Console and the JP1 permission level JP1\_Console\_Admin, JP1\_Console\_Operator, or JP1\_Console\_User (according to the JP1 user's scope of operation).

For the Central Scope, assign the JP1 resource group JP1\_Console and the JP1 permission level JP1\_Console\_Admin to allow the JP1 user to edit monitoring trees and save tree data to the server. To allow the JP1 user to perform monitoring from the Central Scope, assign the JP1 resource group JP1\_Console<sup>#</sup> and the JP1 permission JP1\_Console\_Admin, JP1\_Console\_Operator, or JP1\_Console\_User (according to the JP1 user's scope of operation).

<sup>#</sup>: If you want to set a different monitoring range within a monitoring tree for each JP1 user, you must set JP1 resource groups for specific nodes, and then allocate the appropriate JP1 resource group to each of the JP1 users you are registering on the authentication server. For details about setting a resource group for selected nodes, see *4.4.3 Setting the monitoring range of a monitoring tree*.

When using IM Configuration Management, assign the JP1 resource group JP1\_Console and the JP1 permission level JP1\_CF\_Admin, JP1\_CF\_Manager, or JP1\_CF\_User to the JP1 user (according to the JP1 user's scope of operation).

For details about JP1/IM user operation control based on JP1/IM permission levels, see *E. Operating Permissions*.

### **(1) Notes**

- To implement user operation control based on JP1 permission level in JP1/IM - View, use JP1/Base version 7 or later as the authentication server.
- When two authentication servers are used, they must be running the same version of JP1/Base.
- The JP1 user information registered on each authentication server must be identical. For details about the setting procedure, see the description of setting up the user management functionality in the *Job Management Partner 1/Base User's Guide*.

---

## 12.7 Considerations for the JP1/IM and JP1/Base environments

---

Consider the JP1/IM and JP1/Base environments.

### 12.7.1 Selecting regular expressions

In JP1/IM and JP1/Base, you can use regular expressions when specifying items such as filter conditions and search conditions. The default values of the available regular expressions depend on the OS and the function in which the regular expression is interpreted.

When using the default values, you need to be aware of how each function and operating system interprets regular expressions differently. If you prefer to use regular expressions transparently, you can change a setting in JP1/IM - Manager or JP1/Base to standardize regular expressions.

Use the default setting for the type of regular expressions only if a large number of filter conditions with regular expressions are already set, for example, and compatibility is your primary concern.

Set the type of regular expressions to be used in JP1/Base and in the "REGEXP" parameter of the automated action environment definition file.

About regular expressions:

- Description of regular expression types

See *G. Regular Expressions*.

- Setting the regular expressions to be used

See *Automated action environment definition file (action.conf.update)* in 2. *Definition Files* in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.

See the description of available regular expressions in the chapter on installation and setup in the *Job Management Partner 1/Base User's Guide*.

### 12.7.2 Troubleshooting in JP1/IM and JP1/Base

System operation management is affected by any failure that causes JP1/IM or JP1/Base to stop. JP1/IM and JP1/Base therefore provides the following functionality to enhance failure tolerance:

- Automatic restart if a process ends abnormally (process management)
- Issuing of a JP1 event when an error is detected during process start or stop processing (process management)
- Issuing of a JP1 event and execution of a notification command when a hangup is

detected in a process (health check function)

Consider enabling these functions. They are disabled by default.

About process error troubleshooting and reporting:

- Process management  
See *7.1 JP1/IM - Manager process management*.
- Setting to enable process restart after an error  
See *Extended startup process definition file (jp1co\_service.conf)* in 2. *Definition Files* in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.
- Setting to enable issuing of a JP1 event when a process error occurs  
See *IM parameter definition file (jp1co\_param\_V7.conf)* in 2. *Definition Files* in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.
- Health check function  
See *7.2 JP1/IM - Manager health check function*.
- Setting to enable issuing of a JP1 event and execution of a notification command on detection of a process hangup  
See *Health check definition file (jcohc.conf)* in 2. *Definition Files* in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.
- JP1/Base troubleshooting and error reporting  
See the description of setup for troubleshooting JP1/Base errors in the *Job Management Partner 1/Base User's Guide*.

To enable prompt retrieval of relevant information in the event of a failure, JP1/IM provides dump output commands and data collection tools. These are normally used to collect data when a problem occurs in JP1/IM. However, they cannot be used with the Web-based JP1/IM - View; instead, you must use the debugging tools provided by Java™ Plug-in to collect error information.

Dump output commands

JP1/IM - View and JP1/IM - Manager each have their own dump output command.

Table 12-9: Dump output commands

Command	Description
jcothreaddmp	Dump output command for JP1/IM - View. Outputs the following dump as diagnostic data when a hangup occurs in JP1/IM - View: <ul style="list-style-type: none"> <li>Java thread dump</li> </ul>

#### Data collection tools

The data collection tools are provided as a batch files (in Windows) or scripts (in UNIX).

Table 12-10: Data collection tools provided by JP1/IM

OS	Data collection tool	Description
Windows	jcoview_log.bat	Tool for collecting in a batch all data required for error investigation in JP1/IM - View
	jim_log.bat	Tool for collecting in a batch all data required for error investigation in JP1/IM - Manager <sup>#</sup>
UNIX	jim_log.sh	Tool for collecting in a batch all data required for error investigation in JP1/IM - Manager <sup>#</sup>

<sup>#</sup>: To collect data for investigating an error in JP1/Base, you must execute the data collection tool provided by JP1/Base. (The JP1/Base data collected by the tools in the above table relates to JP1/IM operation only.)

For details about the collected data, see 9.3 *Data that needs to be collected when a problem occurs* in the *Job Management Partner 1/Integrated Management - Manager Administration Guide*. In Windows, a memory dump or crash dump may be required if a problem occurs. We recommend that you set Windows to output these dump files in case they are needed.

However, note the following points:

- The size of the memory dump depends on the real memory size. The larger the installed physical memory, the larger the memory dump. Allocate sufficient disk space to collect a memory dump. For details, see *STOP errors* in the Windows help.
- Not only JP1 event information but also error data for other application programs is output in a crash dump. Output of a crash dump reduces the amount of available disk space by the volume of output data. Allocate sufficient disk space if you have set Windows to output a crash dump.

Java™ Plug-in debugging tool

If a hangup occurs while you are using the Web-based JP1/IM - View, collect a Java stack trace log using the debugging tool provided by Java™ Plug-in. You must first set up the Java™ Plug-in Control Panel window so that the tool will be accessible when the Web-based JP1/IM - View is running. 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*.

### 12.7.3 JP1/IM - Manager system environment

You can change the JP1/IM - Manager system environment via the GUI or by using a profile (system profile). The changes are managed by JP1/IM - Manager on the manager.

The following describes settings related to the JP1/IM - Manager system environment that can be changed by the user. Consider changing the settings as required.

#### (1) **Considerations for the JP1/IM - Manager system environment**

Consider the event buffer and permission for connection from the `jcochstat` command.

##### (a) **Event buffer**

The event buffer is an area of memory used by JP1/IM - Manager (JP1/IM - Central Console) to store JP1 events extracted from the event service of JP1/Base.

Set the maximum number of events that can be extracted from the event service and buffered on the manager. You can set the number in the range from 10 to 2,000 (events).

The default is 500 (events).

If the event buffer size is too small, some JP1 events may be missing from the **Monitor Events** page and **Severe Events** page of the Event Console window.

On the other hand, if the event buffer size is too large, the Event Console window may take a long time to display when you start JP1/IM - View.

When setting the event buffer size, estimate the memory requirements of the Central Console viewer and make sure that sufficient resources are available on the machine. For the equations you can use to estimate memory requirements, see the JP1/IM - Manager *Release Notes*.

##### (b) **Connection permission from the jcochstat command**

Using the `jcochstat` command, you can change the response status of JP1 events in the event database or integrated monitoring database. This allows you to change the response status of JP1 events from other applications, but it may impair JP1/IM operation management.

For this reason, you can set JP1/IM - Manager to prohibit response status changes by

the `jcochstat` command to the event database or integrated monitoring database on the manager. (Changes are permitted by default.) We recommend that you prohibit changes by the `jcochstat` command if there is no need for other applications to change the response status of JP1 events.

About customizing the JP1/IM - Manager system environment:

- Customizing the JP1/IM - Manager system environment via the GUI (recommended procedure)

See *2.11 System Environment Settings window* in the manual *Job Management Partner 1/Integrated Management - Manager GUI Reference*.

- Customizing the JP1/IM - Manager system environment in a definition file

In normal circumstances, customize the settings in the System Environment Settings window rather than in a definition file.

See *System profile (.system)* in *2. Definition Files* in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.

## (2) Notes

If the system profile contains any errors, such as an attribute value that is out of range, JP1/IM - Manager may not work properly.

### 12.7.4 JP1 user environment

You can change the JP1/IM user environment (contents displayed in the Event Console window, for example, for an individual JP1 user) via the GUI or by using a profile (user profile). The changes are managed by JP1/IM - Manager.

The following discusses some points and precautions you should consider in regard to the JP1 user environment settings.

#### (1) Scroll buffer

The *scroll buffer* is an area of memory used by JP1/IM - View to store JP1 events extracted from the event buffer of JP1/IM - Manager.

A scroll buffer is kept for each of the **Monitor Events** page, **Severe Events** page, and **Search Events** page.

The JP1 events that JP1/IM - View displays on each page is determined by the contents of the scroll buffer for that page.

You can change the scroll buffer size (maximum number of JP1 events that can be buffered) in the Preferences window. You can set the number in the range from 10 to 2,000 (events). For the Web-based JP1/IM - View, the range is 10 to 1,000 (events).

The default is 500 events, or 100 in the Web-based JP1/IM - View. The recommended

value is 500, or from 10 to 100 in the Web-based JP1/IM - View.

If the scroll buffer size is too large, the Event Console window may take a long time to display when you start JP1/IM - View.

When setting the scroll buffer size, estimate the memory requirements of the Central Console viewer and make sure that sufficient resources are available on the machine. For the equations you can use to estimate memory requirements, see the JP1/IM - View *Release Notes*.

About customizing the user environment:

- Customizing the user environment via the GUI

See 2.16 *Preferences window* in the manual *Job Management Partner 1/Integrated Management - Manager GUI Reference*.

## (2) Notes

- When a user is deleted from the JP1 user management, the associated user profile is not deleted.
- When a user name is changed in the JP1 user management, the associated user profile is not updated.
- The definition of the JP1 user environment is included in the user profile. However, do not directly modify an attribute or attribute value in the user profile that is not mentioned in the sections *User profile (defaultUser | profile\_user-name)* and Information that is specified in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*. If you modify such an attribute or attribute value, JP1/IM - View may not work properly.
- If a user profile contains any errors, such as an attribute value that is out of range, JP1/IM - View may not work properly.

### 12.7.5 Issuing a JP1 event when a response status changes

By setting JP1/IM to issue a JP1 event (3F11) when the response status of a JP1 event changes, you can achieve the following control. Hereafter, the JP1 event issued when a response status changes is referred to as a *status event*.

- Keeping a history of response operations

When a number of operators perform response operations, you can utilize the issued status events to see who changed the response status, when it was changed, and to what status.

You can also obtain a historic record of operator responses for auditing purposes by outputting the event information (including status events) displayed in the Event Console window as a CSV snapshot.

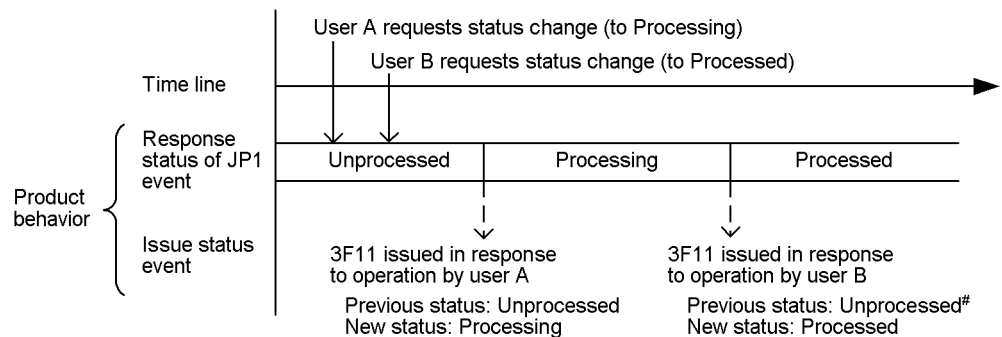


**(1) Notes**

- When JP1/IM is set to issue JP1 events for response status changes, one status event (3F11) is issued for one JP1 event that has been resolved. When the operator changes the response status of a number of JP1 events in a single operation, either in the **Severe Events** page of the Event Console window or by the `jcochstat` command, a status event (3F11) will be issued for every one of those JP1 events. Bear this in mind when using status event issue.
- A status event (3F11) is triggered when a JP1 user changes the response status of a JP1 event in JP1/IM, and the status event is then registered in JP1/Base. If another JP1 user changes the response status of the same JP1 event before the preceding status event (3F11) is registered, the pre-response status stored in the new status event (3F11) may not be the actual status.

For example, if user A changes an *Unprocessed* JP1 event to *Processing*, and user B changes it to *Processed* at roughly the same time (slightly later than user A), the product will behave as follows.

Figure 12-14: Product behavior when a response status is changed by multiple users



#: Previous status other than Processing.

The actual status transition follows the order in which the change requests are received (in this case, *Unprocessed* -> *Processing* -> *Processed*), but the pre-response status stored in the triggered status events (3F11) is the response status that applied when each user issued the change request (in this case, *Unprocessed*).

## 12.7.6 Command execution environment

Consider the environment for the command execution functionality.

The command execution environment comes into play when the user executes a command from JP1/IM - View or when a command is executed in an automated action.

The command execution environment also relates to the system configuration management and user authentication functionality.

### (1) *Considerations for the command execution environment*

#### ■ Setting the number of commands to be executed concurrently

The commands that are executed in automated actions are normally set to execute one by one on the host concerned. However, concurrent execution is supported if you want the next command to start executing sooner when it follows a command that takes a long time to complete.

To enable commands to be executed concurrently on a host, set the *command-concurrent-execution-count* parameter by specifying the `-execnum` option in the `jcccmddef` command. You can specify a value from 1 to 48. The default is 1.

Commands are executed in parallel up to the number defined as *command-concurrent-execution-count*. Although the number of commands being executed at any one time depends on how long each command takes to execute and on the command execution environment, it never exceeds the specified count. Delays may occur when a command executed by an automated action takes a long time to execute and commands are set to be executed serially (the default setting). In this case, you can reduce delays by setting the command execution control to execute commands in parallel.

When you specify a value greater than 1 in this option, commands will be executed concurrently, which means that the command executed first will not necessarily end first. For this reason, do not specify this option if you want the automated actions to end in execution order.

For details, see the following reference:

About the command execution environment:

- Overview of the command execution environment

See 7.4.4 *Managing command execution*.

### (2) *Notes*

- If the number of queued commands is exceeded when an automated action is executed, the action returns an error. Wait until the queued actions have executed, and then retry the failed action. To do so, in the Execute Command window, type the contents displayed in the **Action** field of the Action Log Details window.

Setting of the command queue count differs according to the JP1/Base version.

JP1/Base 06-51 or earlier:

Set the command queue count by editing the automated action environment definition file. You can specify a value from 1 to 64. The default is 10. For details

about setting the environment, see *4.3.1 Setting up an execution environment for the automated action function* in the *Job Management Partner 1/Integrated Management - Manager Configuration Guide*.

JP1/Base 06-71 or later:

Set the *command-queue-count* parameter by specifying the *-queueenum* option in the *jcocmddef* command. You can specify a value from 0 to 65,535. The default is 1,024. For details about the *jcocmddef* command, see the chapter on commands in the *Job Management Partner 1/Base User's Guide*.

- If JP1/Base stops while an automated action is being executed, the action will result in an error.

## 12.7.7 System design for using the Central Scope

Consider the following points in regard to using the Central Scope.

### (1) Host information managed by JP1/IM - Manager (JP1/IM - Central Scope)

JP1/IM - Manager (JP1/IM - Central Scope) compares host names to determine the monitoring tree structure, or to change the status of monitoring objects, when a monitoring tree is generated automatically or when the status of a monitoring object is changed.

When comparing host names, JP1/IM - Manager (JP1/IM - Central Scope) uses the JP1/Base *jp1hosts* information, the OS *hosts* file, and the DNS or NIS settings. Where there are discrepancies between the host names defined in these settings and those recognized by the products to be represented in an automatically generated tree, or by products that issue JP1 events, information may not be acquired correctly or the status of a monitoring object may not be changed correctly.

Examples:

- The monitoring objects collected by the auto-generation function relating to the same host appear as monitoring objects of different hosts.
- The status of a monitoring object fails to change because the name of the host it is monitoring differs from the name of the host that issued the JP1 event.

To avoid these sorts of problems, JP1/IM - Manager (JP1/IM - Central Scope) can manage host information using a database of its own. You can preempt any problems by registering the host names recognized by other programs in the JP1/IM - Manager (JP1/IM - Central Scope)-specific host information.

To utilize host information in JP1/IM - Manager, prepare a *jcs\_hosts* file, and register the information in the host information database. In the *jcs\_hosts* file, write the real host name, alias, and IP address of the hosts to be monitored in the Monitoring Tree window, using the same format as the OS *hosts* file. You can specify a maximum of eight host names for one IP address.

Make sure that you prepare the host information file and register the information in the host information database before you configure the monitoring object environment.

#### (a) Notes

- If referencing of the host information is unsuccessful, JP1 event processing and monitoring tree auto-generation by JP1/IM - Manager (JP1/IM - Central Scope) may take a long time.

So that the information can be referenced, set the following host names in the host information database of JP1/IM - Manager (JP1/IM - Central Scope), the JP1/Base jp1hosts information, the hosts file of the host running JP1/IM - Manager (JP1/IM - Central Scope), and the DNS or NIS:

1. Any host name set in the status change condition for a monitoring object as an individual attribute value in an individual condition for which **Host name comparison** is selected.
2. Any host name included in the attribute values of a JP1 event monitored by JP1/IM that may be set as the event attribute specified in an individual condition for which **Host name comparison** is selected (as in 1 above).
3. All host names defined in the JP1/IM configuration management.
4. All host names included in the configuration information of a linked product set up to support auto-generation of monitoring trees.

### 12.7.8 Communication timeout period

If the network uses low-speed lines or if the viewer is heavily loaded, a timeout during server communication processing may result in a communication error. You can correct such errors by changing the JP1/IM settings.

By default, the timeout period is 2,500 milliseconds. Increase this value if JP1/IM is used in a low-speed network or in an environment that generates considerable event traffic.

About adjusting the communication timeout value:

- Modifying the communication timeout value of JP1/IM - Manager (JP1/IM - Central Console)

See *Communication environment definition file (console.conf.update)* in 2. *Definition Files* in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.

- Modifying the communication timeout value of JP1/IM - View

See *Communication environment definition file (view.conf.update)* in 2. *Definition Files* in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.

See *Communication environment definition file (tree\_view.conf.update)* in 2. *Definition Files* in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.

There is no need to adjust the communication timeout value of JP1/IM - Manager (JP1/IM - Central Scope).

## 12.7.9 JP1/IM - View environment

### (1) Customizing JP1/IM - View

You can customize aspects of JP1/IM - View operation, such as the number of connection hosts displayed in the Login dialog box and the startup behavior of the Tool Launcher window.

About customizing JP1/IM - View:

- Customizing JP1/IM - View operation

See *IM-View settings file (tuning.conf)* in 2. *Definition Files* in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.

### (2) Setting up linkage with JP1/IM - Rule Operation

To use the JP1/IM - Rule Operation linkage component of JP1/IM - View, you must execute the set command `jcovrmsetup`.

For details about window operations after setup is completed, see the JP1/IM - Rule Operation manuals.

JP1/IM - Rule Operation manuals:

- *Job Management Partner 1/Integrated Management - Rule Operation System Configuration and User's Guide*
- *Job Management Partner 1/Integrated Management - Rule Operation GUI Reference*

## 12.7.10 Event monitoring from the Web-based JP1/IM - View

JP1/IM - Manager provides a Web-based JP1/IM - View. By using this program, users can log in to a manager from a host that does not have JP1/IM - View, and perform event monitoring. However, there are some limitations: The Execute Command window and Tool Launcher window are not available.

Before using the Web-based JP1/IM - View, make sure that you are aware of the limitations described in 1. *Window Transitions and Login Window* in the manual *Job Management Partner 1/Integrated Management - Manager GUI Reference*.

To use the Web-based JP1/IM - View, an HTTP server must be installed and set up on the host on which JP1/IM - Manager is installed, and the Java Runtime Environment

(JRE) and bundled plug-ins are required in the Web browser. For details, see the JP1/IM - Manager *Release Notes*.

About event monitoring from the Web-based JP1/IM - View:

- Using the Web-based JP1/IM - View

See *4.14 Settings for using a Web-based JP1/IM - View* in the *Job Management Partner 1/Integrated Management - Manager Configuration Guide*.

### 12.7.11 Setting the event acquisition start location

The event acquisition start location is set by the `-b` option of the `jcoimdef` command. The location is determined as shown in the table below, according to the value specified in the `-b` option.

*Table 12-11: Relationship between -b option value and acquisition start location*

Value specified in <code>-b</code> option	Acquisition start location
-1	The event following the last event processed by JP1/IM - Manager
0	Events registered since JP1/IM - Manager started
1 to 144	Events registered within a specified period of time before JP1/IM - Manager started

The effect of each setting is as follows:

#### **(1) Acquisition start location when -1 is specified**

If you start JP1/IM - Manager with -1 specified in the `-b` option of the `jcoimdef` command, the event base service sends the event with the oldest serial number (the event at the location where processing stopped) to JP1/IM - Manager.

#### **(2) Acquisition start location when 0 is specified**

If you start JP1/IM - Manager with 0 specified in the `-b` option of the `jcoimdef` command, the event base service sends events registered after JP1/IM - Manager startup to JP1/IM - Manager in the order in which they were registered.

If no such events exist, the event base service remains in standby mode until a new event is registered.

#### **(3) Acquisition start location when 1 to 144 is specified**

If you start JP1/IM - Manager with any of 1 to 144 specified in the `-b` option of the `jcoimdef` command, the event base service sends events to JP1/IM - Manager that were registered within the length of time specified by the `-b` option before JP1/IM - Manager started.

In this case, the acquisition start location is the time at which JP1/IM - Manager started, less the time specified by the `-b` option of the `jcoimdef` command.

---

## 12.8 Considerations for linking with other integrated management products

---

Consider the environment settings required for linking with the following integrated management product:

- JP1/IM - Rule Operation

### 12.8.1 System design for linking with JP1/IM - Rule Operation

To link with JP1/IM - Rule Operation, the following setup is required on the JP1/IM side. For details about JP1/IM - Rule Operation, see the *Job Management Partner 1/ Integrated Management - Rule Operation System Configuration and User's Guide*.

#### (1) Settings for JP1/IM - Rule Operation linkage

The following settings are required for linking with JP1/IM - Rule Operation:

Settings for JP1/IM - Rule Operation linkage (`jcoimdef` command)<sup>#</sup>

- Enable or disable JP1/IM - Rule Operation linkage (`-rule` option)
- Specify the JP1/IM - Rule Operation host (`-rulehost` option)
- Specify the execution user (`-ruleuser` option)

<sup>#</sup>: Enabling the linkage function enables the notification condition settings to be exported from JP1/IM - View to JP1/IM - Rule Operation.

Condition for notifying JP1/IM - Rule Operation

Set in either of the following:

- Action Parameter Detailed Definitions window
- Automated action definition file (`actdef.conf`)

Display settings

- Preferences window
- Settings for View Filter window
- Severe Event Definitions window
- Detailed Settings for Event Receiver Filter window

Registration in the Start menu of JP1/IM - View (rule operation viewer)

- `jcovrmsetup` command



**(2) Notes**

- In the JP1/IM - Rule Operation notification conditions, specify all the JP1 events that could potentially match a rule startup condition. (Rule startup judgments for notifications from JP1/IM - Manager are performed on the JP1/IM - Rule Operation side.)
- Processing of notifications to JP1/IM - Rule Operation is executed according to the system hierarchy, in the same way as for normal automated actions.

For this reason, if you want to run JP1/IM - Manager and JP1/IM - Rule Operation on different hosts, you must configure the JP1/IM - Rule Operation host at a level below the JP1/IM - Manager host.

- The following problems occur if you enable JP1/IM - Rule Operation linkage and set a notification condition, and then disable the function without first deleting the condition settings:
  - Automated actions cannot be set from JP1/IM - View.
  - Because the notification conditions in JP1/IM - Manager are still in effect, JP1/IM - Manager will send a rule startup request to JP1/IM - Rule Operation whenever a JP1 event matching a notification condition occurs.

To prevent such problems, before you disable the linkage function, delete the condition settings for notifying JP1/IM - Rule Operation from JP1/IM - View, or open the automated action definition file (`actdef.conf`) and delete the automated action definition parameter for JP1/IM - Rule Operation linkage. For details about the automated action definition file (`actdef.conf`), see *Automated action definition file (actdef.conf)* in 2. *Definition Files* in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.

- JP1/IM - Rule Operation issues a JP1 event whenever a rule starts, finishes, or ends abnormally, for example. If you want to monitor such JP1 events in JP1/IM, change the filter settings so that they can be forwarded and displayed in JP1/IM - View.

---

## 12.9 JP1/IM maintenance considerations

---

Not only when running JP1/IM but for any IT system generally, establishing and implementing a maintenance plan is necessary to guard against problems and to be prepared in case of an emergency.

The following discusses some points you should consider when carrying out maintenance tasks in a system that uses JP1/IM.

### 12.9.1 Backup requirements

Consider how to back up the JP1/IM and JP1/Base settings information and the databases so that if the system crashes, it can be rebuilt and restarted in the same environment. Take backup at the following times:

- When you set up JP1/IM or otherwise reconfigure the system
- Before you perform an upgrade installation

For details about the settings information to back up in JP1/IM, and on backup and recovery procedures, see *1.1 Managing the configuration information* in the *Job Management Partner 1/Integrated Management - Manager Administration Guide*. For details about database reorganization, backup and recovery, and recreation, see *1.2 Managing the databases* in the *Job Management Partner 1/Integrated Management - Manager Administration Guide*. For details about JP1/Base, see the description of backup and recovery in the chapter on installation and setup in the *Job Management Partner 1/Base User's Guide*.

### 12.9.2 Database maintenance considerations

Invalid areas may build up in the IM database over time as data is added and deleted. In this case, you may be unable to register new hosts or properties even within system limits. You may also experience delays when attempting to add, update, or delete data. To avoid these problems, we recommend that you periodically re-organize the database.

For details about when and how to re-organize the IM database, see *1.2.1 Database reorganization* in the *Job Management Partner 1/Integrated Management - Manager Administration Guide*.

The other databases used by JP1/IM are designed so that there is no increase in invalid areas when the system is run continuously. Therefore, there is no need to check the databases if enough disk space is available.

### 12.9.3 Checking disk space

To ensure that JP1/IM operates reliably during continuous operation, you must ensure that sufficient disk space is available.

For example, when an error occurs during JP1/IM operation, a dump file may be required for troubleshooting. Because a dump file temporarily occupies a large amount of disk space, estimate the disk space required and ensure that sufficient disk space is available.

#### 12.9.4 Use of failure reports

JP1/IM - View provides functionality for saving the JP1 event information listed in the Event Console window in CSV format. By using this functionality in conjunction with an event search (see 3.5 *Searching for events*), you can view a listing of JP1 events that occurred around the same time as an error in the system, and output the list as a CSV snapshot for use in analyzing the error.

Consider saving monitoring information (CSV snapshots) as a task within your system management program. If applicable, also consider saving the event information stored in the integrated monitoring database (output of event report).

##### *Reference note:*

##### Producing JP1/Base failure reports (jevexport command)

Various events are recorded in a standard format as JP1 events in the JP1/Base event databases used by JP1/IM. By periodically reviewing the database contents, you can use the JP1 event records as failure reports, to find out which hosts or products are experiencing frequent problems, for example. Use the JP1/Base `jevexport` command to review the event database contents. The `jevexport` command outputs the contents to a CSV file.

Because the event databases have a fixed size (by default, 10 MB per database; total capacity 20 MB), you should output the contents using the `jevexport` command before the database is full. Consider doing so at regular intervals.

---

## 12.10 Considerations for JP1/IM system-wide maintenance

---

Among the hosts monitored by JP1/IM, some may be running processing that cannot be halted even when the server requires maintenance. For example, if a host runs 24 hours a day, 365 days a year, you will need to schedule maintenance work so as to minimize its impact, by migrating job processing to another server or by suspending some processing for a short time, for example.

During maintenance work, you may need to stop and start the server several times, or halt job processing temporarily, potentially issuing a large volume of events that detected these start/stop operations as errors.

To enable continuous operation monitoring by JP1/IM, you must filter out redundant events and keep only those that are required. You should therefore consider the order in which maintenance tasks will be carried out, and perform settings in advance to filter out unwanted JP1 events.

This section describes some points to consider in maintaining the entire system including JP1/IM, and discusses how to implement a maintenance schedule that allows for uninterrupted system monitoring. It also provides an example of carrying out urgent maintenance when a problem occurs on an agent.

### 12.10.1 Preparatory tasks

The following describes some precautions and points to consider at the planning stage before you implement maintenance.

#### **(1) Maintenance planning for the entire system**

- Decide the order in which maintenance will be implemented throughout the system.

Always implement maintenance from the higher-level hosts to the lower-level hosts, following the definition order in the JP1/IM system configuration definition.

You should also consider the following points when planning the order in which maintenance is implemented:

- When grouping the agents, make sure that maintenance of one host will not affect job processing on another host.
- If a system operates around the clock, prepare a server that can take over processing while the system is being maintained.
- Estimate how long maintenance will take for the JP1/IM servers and agents.

*Note:*

When maintaining the entire system, use the `jcoimdef` command to adjust the event acquisition start location, and switch between event acquisition filters prepared in advance.

The event acquisition start location and event acquisition filter are inter-related. That is, one setting affects the other. In brief, the relationship is as follows:

- Event acquisition start location

At startup, JP1/IM - Manager acquires events from the JP1/Base event database, according to the start location setting, and stores them in its event buffer.

- Event acquisition filter

When the events acquired from JP1/Base are stored in the JP1/IM - Manager event buffer, the event acquisition filter processes them according to the set conditions.

In other words, if the event acquisition filter is switched (hence, different filter conditions apply when JP1/IM - Manager stops and when it restarts), and if the event acquisition start location is set so that events will be acquired from before JP1/IM - Manager restarts, the events stored in the event buffer after JP1/IM - Manager restarts may differ from those when it stopped (that is, the events you can see in JP1/IM - View may be different). To avoid this problem, always schedule maintenance starting with the top-level host and proceeding down the hierarchy.

## **(2) Maintenance planning for managers(JP1/IM - Manager)**

The following points should be considered in regard to performing maintenance on the managers (JP1/IM - Manager):

- Backup requirements
- Database maintenance
- Disk space checks
- Use of failure reports

For details about these aspects, see *12.9 JP1/IM maintenance considerations*. You should also consider the following points from a monitoring perspective:

- Acquire JP1 events generated while the manager (JP1/IM - Manager) is in stopped state.

To manage JP1 events generated while JP1/IM - Manager is being maintained, you must set up JP1/IM - Manager to acquire JP1 events from before it restarts.

During maintenance of the whole JP1/IM system, JP1/IM - Manager on the

manager will be stopped at some stage. To enable management of all generated events, set up JP1/IM - Manager so that events generated while it is stopped will be acquired.

Use the `jcoimdef` command to acquire events from before JP1/IM - Manager is restarted.

The parameter settings are described below, based on an example.

Events generated while JP1/Base is stopped on the manager cannot be acquired. This is because JP1 events cannot be registered in the event database while JP1/Base is in stopped state. For details, see *12.10.1(3) Maintenance planning for agents (JP1/Base)*.

- Disable monitoring of error events generated during agent maintenance.

Maintenance work will involve restarting the server at some point, which could generate a large number of unwanted error events. As this may disrupt ongoing monitoring operations, set up filtering to eliminate unwanted events.

To filter out unwanted events, you can define an event acquisition filter in which common exclusion conditions exclude JP1 events issued by hosts that are under maintenance. You can then activate this filter during maintenance. The parameter settings are described below, based on an example.

If JP1/Base is in stopped state on the agent throughout the maintenance work, there is no need for filtering because events will not be registered in the event database.

### **(3) Maintenance planning for agents (JP1/Base)**

- Forward JP1 events generated while JP1/Base is stopped on the manager.

Set JP1/Base on the agents to retry event forwarding, bearing in mind how long JP1/Base will be stopped on the manager. You can set JP1/Base to retry at set intervals for a set length of time if event transfer fails due to an error or because JP1/Base is stopped on the destination host.

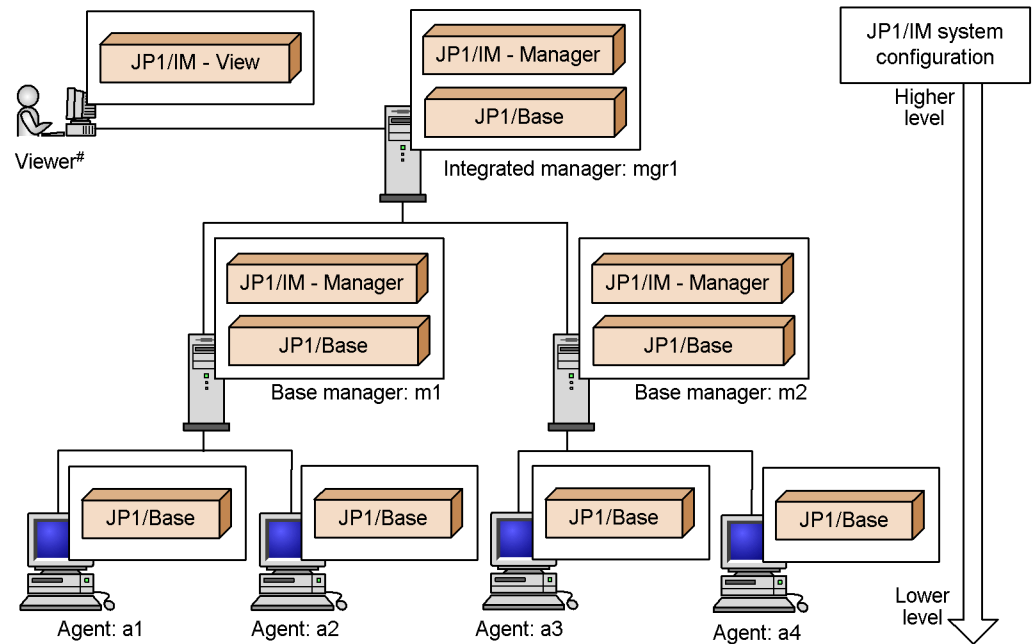
For details, see the description of setting the event service in the *Job Management Partner 1/Base User's Guide*.

## **12.10.2 Example of JP1/IM system-wide maintenance**

The following describes an example of implementing maintenance throughout the JP1/IM system.

In this example, maintenance is to be carried out in a monitored system configured as shown in the figure below (integrated manager x 1; base managers x 2; agents x 4).

Figure 12-15: Hierarchical structure of a system monitored by JP1/IM



#: As viewers can be subjected to maintenance at any time and in any order, they are omitted from the following description.

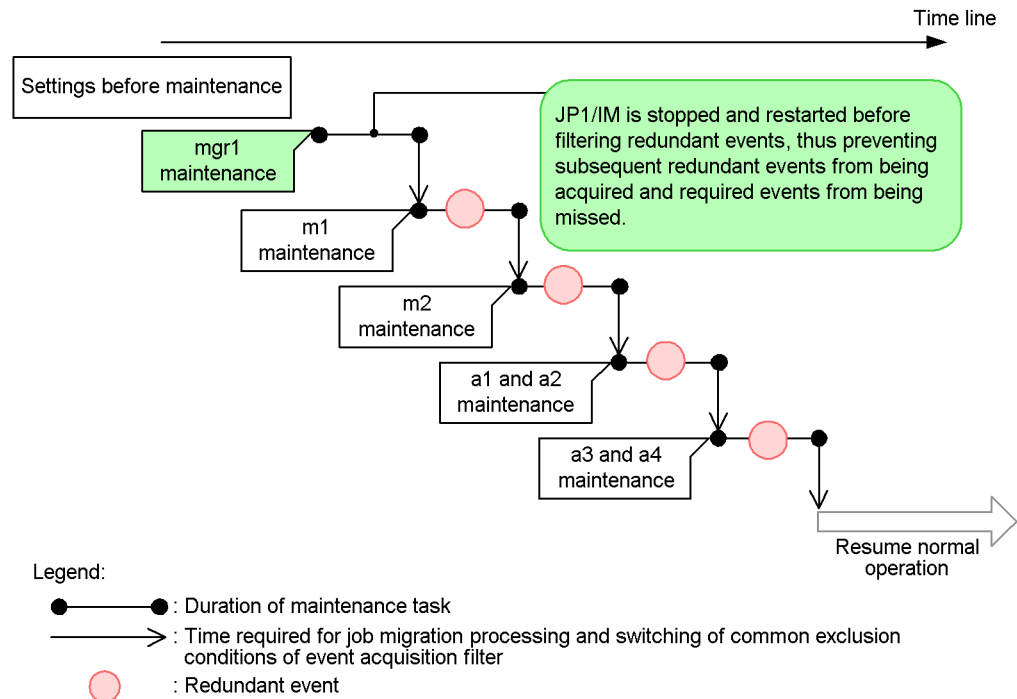
This system monitored by JP1/IM is configured as defined by the JP1/Base configuration management. For details about defining a system hierarchy, see 7.4.3 *Managing the system hierarchy*.

### (1) Order of maintenance

Maintenance is carried out in order, from the higher-level hosts to the lower-level hosts, following the definition of the system hierarchy. In this example, the order of maintenance is as follows:

1. Integrated manager (mgr1)
2. Base manager (m1)
3. Base manager (m2)
4. Agents (a1 and a2)
5. Agents (a3 and a4)

Figure 12-16: Order of maintenance



Maintenance is carried out on the integrated manager (mgr1), base manager (m1 or m2), and agent (a1, a2, a3, or a4), in that order. This prevents redundant events from being acquired and required events from being overlooked.

*Note:*

Always schedule maintenance work on the manager (in this case, mgr1) first of all. Determine the order for the other hosts according to the system hierarchy.

**(2) Settings on the integrated manager (JP1/IM - Manager) side**

Using the JP1/IM - Manager functionality, set up filtering of redundant events and specify JP1 event acquisition while JP1/IM - Manager is in stopped state.

**(a) Setting the event acquisition start location**

Use the `jcoimdef` command to set the event acquisition start location. There are two settings for acquiring events from before JP1/IM - Manager restarts:

- `jcoimdef -b -l`

Acquires JP1 events going back to the status when JP1/IM - Manager was last stopped.



- `jcoimdef -b xxx` (xxx: length of time; from 1 to 144 (hours))

Acquires JP1 events going back the specified length of time before JP1/IM - Manager restarts.

There is also a setting for starting event acquisition from the JP1 events issued after JP1/IM - Manager starts, but the setting does not apply in this example because the starting point needs to be specified explicitly.

For details about setting the event acquisition start location, see *12.7.11 Setting the event acquisition start location*. For details about the `jcoimdef` command, see `jcoimdef` in *1. Commands* in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.

#### (b) Setting common exclusion conditions in an event acquisition filter

You can define common exclusion conditions in an event acquisition filter to temporarily exclude some JP1 events from being monitored. You can add and edit common exclusion conditions from the Event Acquisition Conditions List window, leaving the standard filter conditions unchanged.

Maintenance is to be carried out in the order shown in *Figure 12-15 Hierarchy of a system monitored by JP1/IM*, starting with the integrated manager (mgr1), then the base managers (m1 -> m2), and lastly the agents (a1, a2 -> a3, a4). Four common exclusion conditions separate from the event acquisition filter normally used, that is one for each setting, will be required for maintenance purposes. These common exclusion conditions are described in the table below. Here it is assumed that the settings to prevent acquisition of redundant events generated by a host undergoing maintenance will be performed on the integrated manager (mgr1) only.

*Table 12-12: Common exclusion condition set in the event acquisition filter*

Common exclusion condition ID	Host undergoing maintenance	Common exclusion condition
1	Base manager (m1)	Include source host m1
2	Base manager (m2)	Include source host m2
3	Agents (a1 and a2)	Include source hosts a1 and a2
4	Agents (a3 and a4)	Include source hosts a3 and a4

*Source host* in the event acquisition conditions means a host from which events are issued.

If you want to set up the same type of filtering for the base managers, set common exclusion conditions in event acquisition filters, referring to the settings given above. For details about setting common exclusion conditions, see *2.15 Common Exclusion-Conditions Settings window* in the manual *Job Management Partner 1/*

*Integrated Management - Manager GUI Reference.*

### **(3) Settings in JP1/Base on the base managers and agents**

Set the event forwarding retry parameters, bearing in mind how long the destination host will be in stopped state. Set the parameters on the base managers (m1 and m2) and agents (a1, a2, a3, and a4). By default, the retry time limit is 3,600 seconds (that is, JP1/Base retries at set intervals for 60 minutes). Adjust this value if JP1/Base on the destination host will be stopped for longer than 60 minutes.

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

### **(4) Maintenance procedures**

The following describes the maintenance procedure on each host.

#### **(a) Maintenance procedure on the integrated manager**

Follow these steps to carry out maintenance on the integrated manager (mgr1):

1. Stop JP1/IM - Manager.
2. Stop JP1/Base.
3. Perform maintenance of JP1/IM - Manager and JP1/Base.

For details about backup and recovery of JP1/IM - Manager settings information and disk space management, see *1. JP1/IM System Maintenance* in the *Job Management Partner 1/Integrated Management - Manager Administration Guide*. For details about JP1/Base maintenance, see the description of maintenance in the *Job Management Partner 1/Base User's Guide*.

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

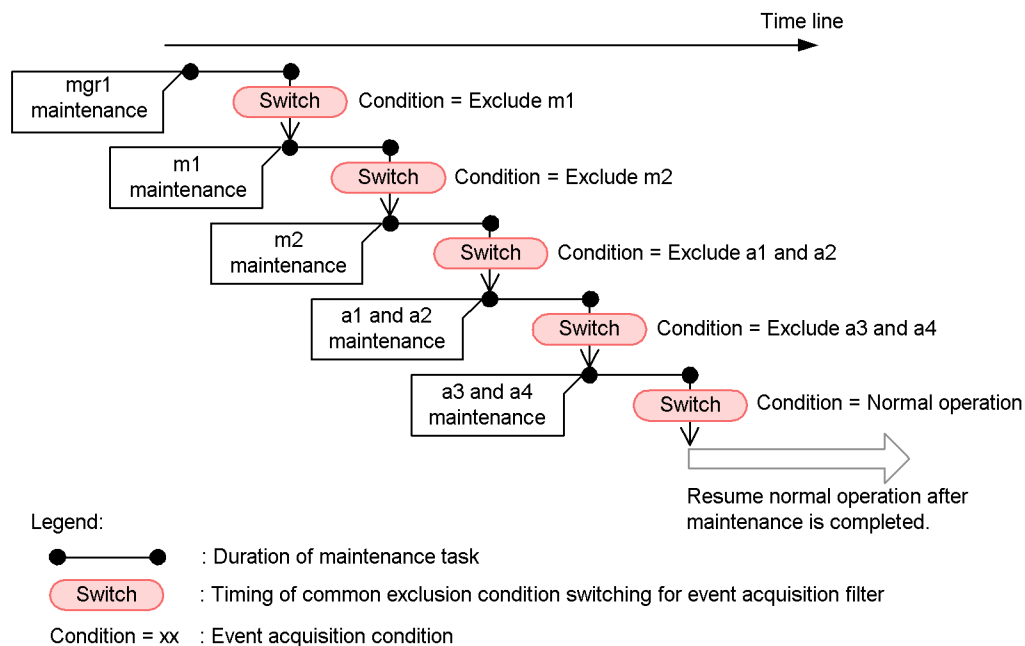
The same procedure applies for maintenance of JP1/IM - Manager on the base managers.

#### **(b) Maintenance procedure on the base managers and agents**

To carry out maintenance on the base managers (m1 and m2) and agents (a1, a2, a3, and a4), switch the common exclusion conditions associated with the event acquisition filter on the integrated manager (mgr1) to eliminate redundant events.

The figure below shows the order of the maintenance tasks and when to switch the common exclusion conditions defined for the event acquisition filter.

Figure 12-17: Maintenance task order and timing of common exclusion condition switching



You can switch the common exclusion conditions of the event acquisition filter using the `jcochfilter` command, the System Environment Settings window, or the Event Acquisition Conditions List window.

Procedure for switching the common exclusion conditions of the event acquisition filter

See 5.8 *Switching the event acquisition filter* in the *Job Management Partner 1/Integrated Management - Manager Administration Guide*.

Details on the `jcochfilter` command

See `jcochfilter` in 1. *Commands* in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.

Details on the System Environment Settings window

See 2.11 *System Environment Settings window* in the manual *Job Management Partner 1/Integrated Management - Manager GUI Reference*.

Details on the Event Acquisition Conditions List window

See 2.14 *Event Acquisition Conditions List window* in the manual *Job Management Partner 1/Integrated Management - Manager GUI Reference*.

The maintenance procedure and files needing to be backed up will depend on the products installed on the base managers and agents. When carrying out maintenance, see the manual *Job Management Partner 1/Base User's Guide* or the documentation for the particular products that issue JP1 events.

*Reference note:*

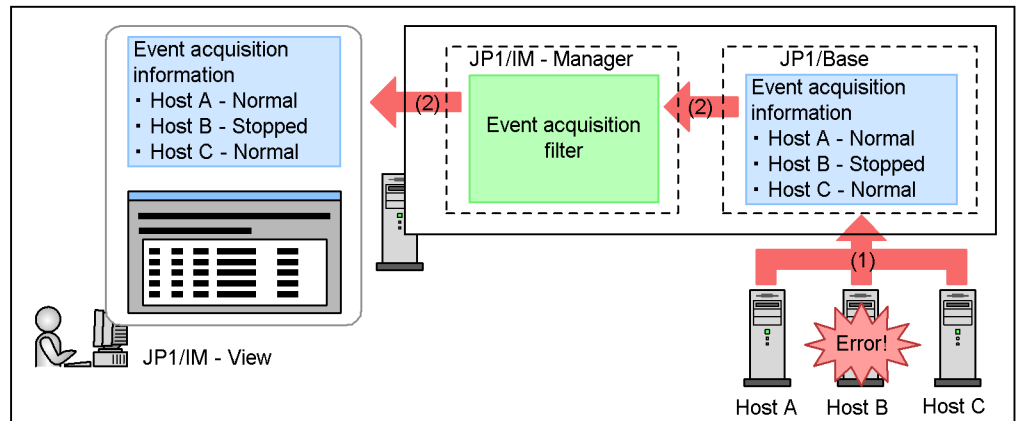
When you use the `jcochfilter` command, you can switch the event acquisition filter automatically at a specified time, based on the JP1/AJS scheduling and calendar functionality. This also lets you change the monitoring status of the host automatically.

### **12.10.3 Example of agent maintenance**

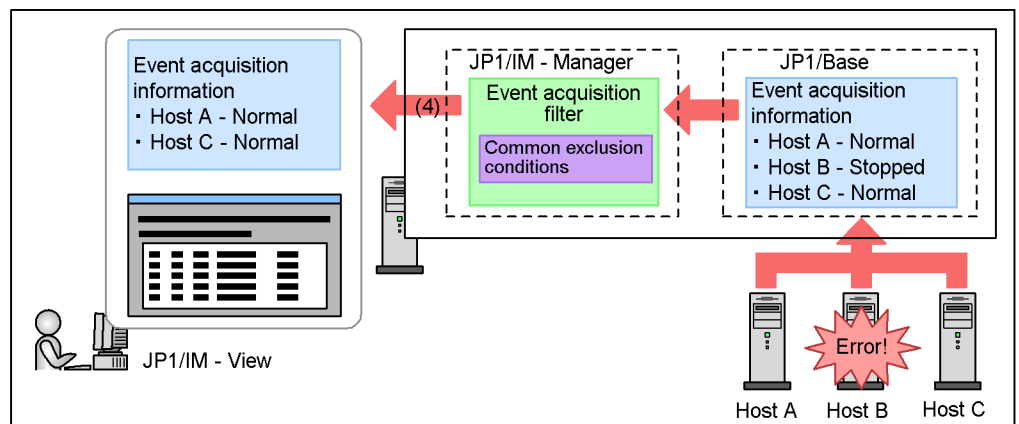
The following describes an example of implementing maintenance on a specific agent.

When a problem needing urgent attention occurs on an agent, events related to the issue should be monitored, but events occurring after maintenance is underway will not be required. Before maintenance work starts, set common exclusion conditions in an event acquisition filter that eliminate redundant events, so that JP1/IM - Manager can continue monitoring the other hosts. The figure below shows an example of implementing maintenance on a specific agent.

Figure 12-18: Example of agent maintenance



- (3) To carry out maintenance work on host B, common exclusion conditions are enabled to stop acquisition of JP1 events from host B.



- (5) Carry out host B maintenance.

- (6) Restart normal monitoring by disabling common exclusion conditions.

Legend:

➡ : Flow of events

The workflow is described below, following the numbers in the figure:

1. An error occurs on agent B being monitored by JP1/IM, and a JP1 event is issued.
2. The JP1 event is relayed through JP1/Base and through the event acquisition filter

in JP1/IM - Manager on the manager, and is displayed in JP1/IM - View.

3. To carry out maintenance tasks on host B, enable the predefined common exclusion conditions for host B maintenance (a set of common exclusion conditions which exclude JP1 events issued from host B from acquisition by JP1/IM - Manager).

The common exclusion conditions can be switched from the JP1/IM - View System Environment Settings window or Event Acquisition Conditions List window, or by using the `jcochfilter` command.

4. Because the common exclusion conditions for host B maintenance are now in effect, JP1 events issued from host B are not acquired by JP1/IM - Manager (they do not appear in the JP1/IM - View windows).
5. Carry out host B maintenance.
6. After maintenance is completed, disable the common exclusion conditions from the JP1/IM - View System Environment Settings window or Event Acquisition Conditions List window, or by using the `jcochfilter` command.

For the procedure for enabling or disabling common exclusion conditions, see 5.8 *Switching the event acquisition filter* in the *Job Management Partner 1/Integrated Management - Manager Administration Guide*.

## Chapter

---

# 13. Performance and Estimates

---

This chapter gives an overview of JP1/IM processing performance, and provides a model case that illustrates the memory and disk space requirements for a particular implementation of JP1/IM. Use this information as a reference when reviewing the JP1/IM settings for your system requirements.

Equations for calculating the memory and disk space requirements of JP1/IM can be found in the *Release Notes* for JP1/IM - Manager and JP1/IM - View. Use these references when estimating system requirements.

13.1 JP1/IM processing performance

13.2 Model for performance evaluation

---

## 13.1 JP1/IM processing performance

---

The performance of the integrated monitoring system depends on the performance of:

- Event display in JP1/IM - View, event reception by JP1/IM - Manager, and automated actions
- The machines on which JP1/IM - Manager and JP1/IM - View are installed
- The network environment

For this reason, you must actually build the integrated monitoring system first, and use it to perform the integrated monitoring tasks for which it is intended. By running the system with a peak load, you can find out if JP1/IM - Manager and JP1/IM - View can execute automated actions and display events in that configuration without delays occurring.

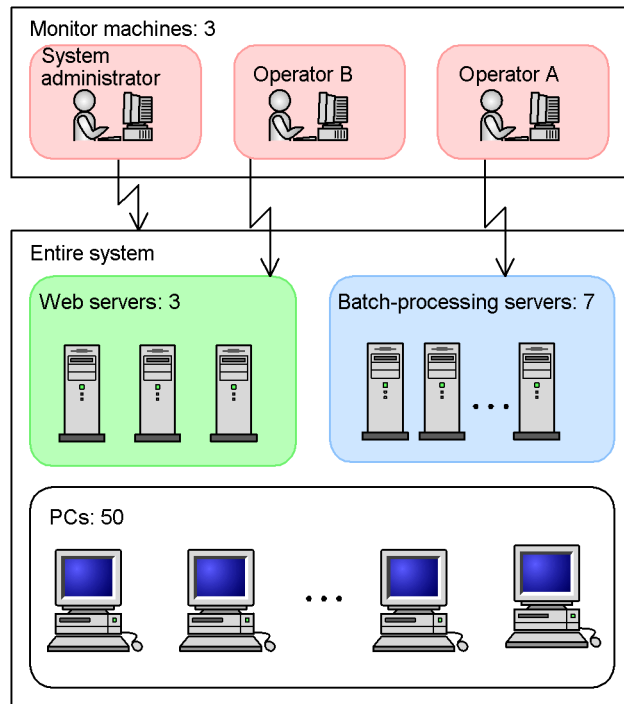
If the processing capacity of the Central Console cannot cope with the peak load, take action to reduce the load. This may entail reducing the number of JP1 events in the system by changing the filter conditions, eliminating redundant automated actions by changing the automated action settings, or increasing the number of base managers.



## 13.2 Model for performance evaluation

This section uses the example of the business system shown below to give a rough estimate of the increase in memory and disk space requirements incurred when JP1/IM is deployed.

*Figure 13-1:* Example of business system operation (before JP1/IM deployment)



This system operates as follows:

- Batch processing of work tasks is handled by seven servers.
- Web server functionality is handled by three servers.
- There are 50 user PCs.

Monitoring tasks are divided among three operators (three monitor machines) as follows:

- Operator A monitors the status of batch processing.
- Operator B monitors the status of the Web servers.

- A system administrator monitors the entire system (including end-user PCs).

### 13.2.1 User requirements

Suppose that JP1/IM is to be deployed in the business system described in *13.2 Model for performance evaluation*, based on the following user requirements (italics indicate JP1/IM keywords).

- A new monitoring server is installed to centrally monitor the business system, and investigate machines where failures occur as necessary.  
-> *JP1/IM system configuration*, centralized monitoring using the *Central Console*, and *event searches*
- The style of monitoring involves three operators, each assigned a specific role as in the existing system.  
-> Applying *event receiver filters*
- Monitoring targets are grouped according to the purpose of the business system.  
-> Using the *Central Scope* (implementing *monitoring range settings*)
- The operator is to be notified automatically when an error requiring immediate attention occurs, even if after hours.  
-> Using *automated actions*
- A history of day-to-day monitoring is kept.  
-> *Saving event list information (CSV snapshot)*

To satisfy these user requirements, the appropriate settings must be made in JP1/IM. For the purposes of this model, the requirements are satisfied by completing the following settings:

#### *System hierarchy*

- A new monitoring server is installed to centrally monitor the business system.  
-> A system configuration consisting of one manager and 60 agents

#### Centralized monitoring using the *Central Console*

Events forwarded from agents to the monitoring server are suppressed under the following conditions:

- Events forwarded from a batch-processing server: High priority; forwarded when *warning* or higher  
-> Assume 20 to 30 such events per server per day
- Events forwarded from a Web server: High priority; forwarded when *warning* or higher

-> Assume 10 to 20 such events per server per day

- Events forwarded from a PC: Low priority; forwarded when `Error` or higher

-> Assume 1 or 2 such events per PC per day

Taking the higher of the two values, you can expect approximately 370 events to be forwarded each day, or 400 when you include the events that occur on the monitoring server (approximately 20 to 30 events with the event level `Warning` or higher). Add a further allowance of 100 to the total, and set the resulting value as the number of events to be stored by JP1/IM - Manager at any one time (the *event buffer size*).

However, supposing that you want to check past events at the same time as recent ones, set the event buffer to 1,000 so that JP1/IM - Manager stores two days' events.

Also, on the assumption that event searches will be carried out as needed from the three monitor machines, set the number of events acquired from machines where errors occurred (the *number of events to acquire in one search*) to 100.

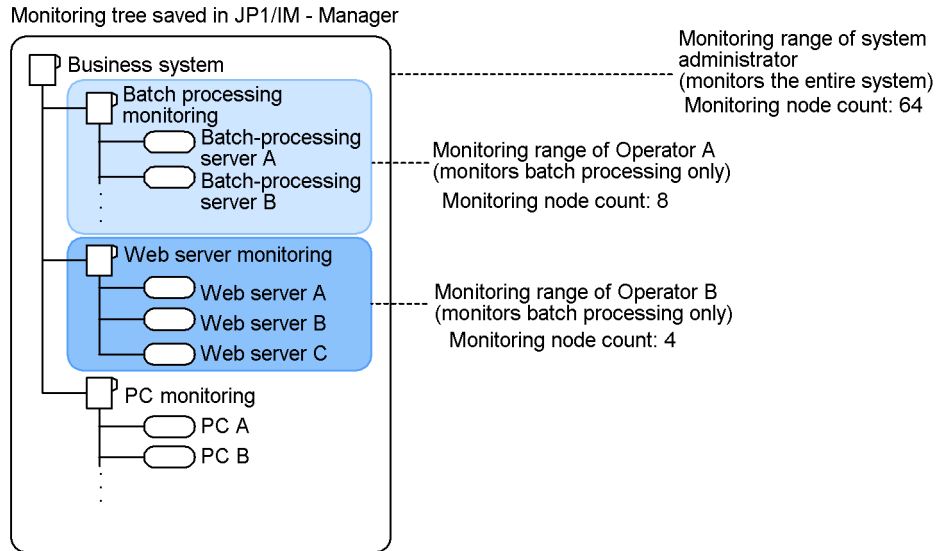
#### Utilizing *event receiver filters*

Filter the monitored events according to your requirements. Then, calculate the number of events to be saved (the *scroll buffer size*) in the JP1/IM - View for each operator as follows:

- Operator A: Monitors batch-processing servers. Set the scroll buffer size to 500 events ((30 events x 7 servers + 40 event allowance) x 2 days).
- Operator B: Monitors Web servers. Set the scroll buffer size to 200 events ((20 events x 3 servers + 40 event allowance) x 2 days).
- System administrator: Monitors the entire system. Set the scroll buffer size to 1,000, the same as the event buffer size.

Using the *Central Scope* (implementing *monitoring range settings*)

Create the following monitoring tree:



The total number of monitoring nodes in the tree (the total number of monitoring nodes managed in JP1/IM - Manager) is 64, made up of four monitoring groups and 60 monitoring objects.

Implement *monitoring range settings* to restrict the number of monitoring nodes appearing in JP1/IM - View as follows:

- Operator A: One monitoring group, seven monitoring objects
- Operator B: One monitoring group, three monitoring objects
- System administrator: Four monitoring groups, 60 monitoring objects

#### *Automated actions*

To enable smooth error detection and basic troubleshooting, 20 automated actions are defined to suit the operating requirements. Of these, five are triggered by multiple conditions joined by an AND condition<sup>#</sup>.

<sup>#</sup>: An event in an AND condition is kept in memory for the specified keep limit (60 minutes by default) or until the AND condition is satisfied. Depending on the situation, assume that in a 60-minute period approximately 30 events will be kept (an estimate obtained by dividing the number of events in a day (500) by 24 hours, and adding 10).

#### *Saving event list information (CSV snapshot)*

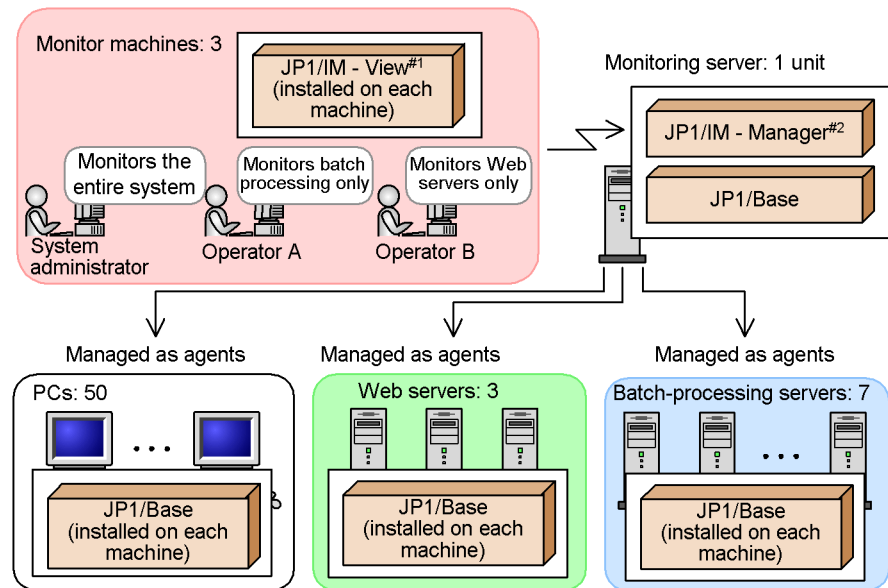
When monitoring is interrupted for some reason, such as at the end of the working day, a CSV snapshot is taken of the event information displayed in JP1/IM - View.

## Other

Do not modify settings, such as the log file size, that increase the amount of disk space used. Continue to use the default settings.

The following figure shows the system operation after JP1/IM is deployed.

*Figure 13-2: Example of business system operation (after JP1/IM deployment)*



#1: Important keywords

Scroll buffer size, number of monitoring nodes, saving event list information (CSV snapshot)

#2: Important keywords

Event buffer size, number of monitoring nodes, number of events acquired in one search, number of AND events

*Reference note:*

The memory required by JP1/IM to monitor the system takes two forms:

1. Memory required by JP1/IM on a constant basis
2. Memory allocated and released for specific purposes during JP1/IM operation

In the above figure, the relevant keywords for the first type of memory are the *event buffer size* and *number of monitoring nodes* for JP1/IM - Manager, and the *scroll buffer size* and *number of (displayed) monitoring nodes* for JP1/IM - View.

The relevant keywords for the second type are *Number of events to acquire in one search* and *Number of AND events* for JP1/IM - Manager, and *Saving event list information (CSV snapshot)* for JP1/IM - View.

When estimating the amount of memory required by JP1/IM, use the sum of the maximum amount of both types of memory.

Estimate your system requirements in terms of this framework. Based on this information, estimate the memory usage and disk space requirements of JP1/IM from the equations in the *Release Notes* for JP1/IM - Manager and JP1/IM - View.

From the results of the equations, make sure that JP1/IM deployment will leave some leeway in the resources of each machine. If you discover that a machine has insufficient memory or disk space, you must consider adding more memory or upgrading the disk. If this cannot be done, you may need to revise your requirements for the system in a way that accommodates your existing hardware.

Also, make sure that a sudden increase in the number of events acquired and processed by JP1/IM due to an unexpected error will not significantly impair performance in terms of displaying events and executing automated actions.

### **13.2.2 Memory, disk capacity, and database capacity required on a monitoring server**

JP1/IM - Manager on a monitoring server has different memory and disk space requirements depending on how JP1/IM is set up. The settings that have the most significant effect on memory and disk usage by JP1/IM - Manager are as follows. For details on the other settings, see the *Release Notes* for JP1/IM - Manager and JP1/IM - View.

- Settings that significantly affect memory usage:
  - Number of event buffers
  - Number of events to acquire in one search
  - Number of monitoring nodes

- Settings that significantly affect disk space usage:
  - Automated action trace log
  - Number of monitoring nodes
  - Number of registered hosts
  - Number of files defined for log trapping

JP1/Base is a prerequisite product when you monitor a system using JP1/IM. For the pertinent information relating to JP1/Base, see the JP1/IM - Base *Release Notes*.

### 13.2.3 Memory and disk capacity required on a monitor machine

The memory and disk space requirements differ between monitor machines, due to the different monitoring ranges and settings of each operator.

These values vary widely depending on how JP1/IM is set up. The settings that have the most significant effect on memory and disk usage by JP1/IM - View are as follows. For details on the other settings, see the JP1/IM - View *Release Notes*.

- Settings that significantly affect memory usage:
  - Scroll buffer size
  - Number of monitoring nodes
- Settings that significantly affect disk space usage:
  - Number of monitoring nodes
  - Saving event list information (CSV snapshot)<sup>#</sup>

<sup>#</sup>: The amount of disk space used increases with each additional monitoring log saved.





---

# Appendixes

---

- A. Files and Directories
- B. List of Processes
- C. Port Numbers
- D. Limits
- E. Operating Permissions
- F. Support for Changing Communication Settings
- G. Regular Expressions
- H. Connectivity with Previous Versions
- I. Performance and Estimation
- J. Kernel Parameters
- K. Version Changes
- L. Glossary

## A. Files and Directories

This appendix lists the names of the files and directories used by JP1/IM.

This appendix does not cover the JP1/IM files that you need to back up when changing system settings, or the log files output by JP1/IM. For details on these files, see the following:

- Information about files to back up: See *1.1 Managing the configuration information* in the *Job Management Partner 1/Integrated Management - Manager Administration Guide*.
- Information about log files: See *9.2.4 Log files and directory list* in the *Job Management Partner 1/Integrated Management - Manager Administration Guide*.

In the case of a logical host, the path notation used in the following tables is described in the table below.

*Table A-1: Files and folders (or directories) on the shared disk*

OS	Internal component	Path notation in the following tables	File or folder (directory) on the shared disk
Windows	JP1/IM - Central Console	<i>console-path</i> \conf\	<i>shared-folder</i> \JP1Cons\conf\
		<i>console-path</i> \log\	<i>shared-folder</i> \JP1Cons\log\
		<i>console-path</i> \tmp\	<i>shared-folder</i> \JP1Cons\tmp\
		<i>console-path</i> \operation\	<i>shared-folder</i> \JP1Cons\operation\
	JP1/IM - Central Scope	<i>scope-path</i> \conf\	<i>shared-folder</i> \JP1Scope\conf\
		<i>scope-path</i> \log\	<i>shared-folder</i> \JP1Scope\log\
		<i>scope-path</i> \tmp\	<i>shared-folder</i> \JP1Scope\tmp\
		<i>scope-path</i> \database\	<i>shared-folder</i> \JP1Scope\database\
	JP1/IM - IM Configuration Management	<i>IM-path</i> \conf\	<i>shared-folder</i> \JP1IMM\conf\imcf\
		<i>IM-path</i> \log\	<i>shared-folder</i> \JP1IMM\log\imcf\
		<i>IM-path</i> \tmp\	<i>shared-folder</i> \JP1IMM\tmp\

OS	Internal component	Path notation in the following tables	File or folder (directory) on the shared disk
UNIX	JP1/IM - Central Console	/etc/opt/jplcons/conf/	shared-directory/jplcons/conf/
		/var/opt/jplcons/log/	shared-directory/jplcons/log/
		/var/opt/jplcons/tmp/	shared-directory/jplcons/tmp/
		/var/opt/jplcons/operation/	shared-directory/jplcons/operation/
	JP1/IM - Central Scope	/etc/opt/jplscope/conf/	shared-directory/jplscope/conf/
		/var/opt/jplscope/log/	shared-directory/jplscope/log/
		/var/opt/jplscope/tmp/	shared-directory/jplscope/tmp/
		/var/opt/jplscope/database/	shared-directory/jplscope/database/
	JP1/IM - IM Configuration Management	/etc/opt/jplimm/conf/	shared-directory/jplimm/conf/imcf/
		/var/opt/jplimm/log/	shared-directory/jplimm/log/imcf/
		/var/opt/jplimm/tmp/	shared-directory/jplimm/tmp/

For a logical host, read *console-path*\conf\ as *shared-folder*\JP1Cons\conf. For example, *console-path*\conf\action\actdef.conf will be *shared-folder*\JP1Cons\conf\action\actdef.conf.

For details on the files and directories used by JP1/IM - EG for NNMi, see the manual *Job Management Partner 1/Integrated Management - Event Gateway for Network Node Manager i Description, User's Guide and Reference*.

## A.1 Files and folders of JP1/IM - Manager (for Windows)

This appendix lists the names of the files and folders used by JP1/IM - Manager (for Windows).

### (1) JP1/IM - Manager (common to all components)

The tables below show the names of the files and folders used by JP1/IM - Manager (all components). *Ref.* in the tables has the following meaning:

- *Ref.* for a folder: The act of checking what the folder contains
- *Ref.* for a file: The act of opening the file and checking its contents

*Table A-2: Files and folders that can be referenced and edited by the user  
(Windows version of JP1/IM - Manager (all components))*

File or folder name	Description	Ref.	Edit
<i>manager-path</i> \Readme.txt	Readme file	Y	N
<i>manager-path</i> \tools\jim_log.bat	Data collection tool	Y	N

Legend:

Y: Can be performed.

N: Cannot be performed.

*Table A-3: Files and folders that do not need to be referenced or edited  
(Windows version of JP1/IM - Manager (all components))*

Folder name	Description
<i>manager-path</i> \bin\	Folder for commands
<i>manager-path</i> \conf\	Folder for environment settings files
<i>manager-path</i> \log\	Log folder
<i>manager-path</i> \tools\	Files and folders in the tools folder other than those in the list of files and folders that can be referenced and edited by the user
<i>manager-path</i> \PATCHLOG.txt	Patch log file
<i>manager-path</i> \patch_backup_dir\	Files and folders in the patch backup folder other than patch utilities mentioned in the patch RELEASE.TXT. (This folder is created only when applying a patch.)
<i>system-drive</i> :\Program Files\jplcommon\	Folder for program information

## (2) JP1/IM - Manager (JP1/IM - Central Console)

The tables below describe the names of the files and folders used by the Windows version of JP1/IM - Manager (JP1/IM - Central Console). *Ref.* in the tables has the following meaning:

- *Ref.* for a folder: The act of checking what the folder contains
- *Ref.* for a file: The act of opening the file and checking its contents

*Table A-4:* Files and folders that can be referenced and edited by the user  
(Windows version of JP1/IM - Manager (JP1/IM - Central Console))

File or folder name	Description	Ref.	Edit
<i>console-path\bin\</i>	Folder for commands	Y	N
<i>console-path\conf\</i>	Folder for environment settings files	Y	N
<i>console-path\conf\jplco_param_v7.conf</i>	IM parameter definition file	Y	Y
<i>console-path\conf\jplco_param_v7.conf.model</i>	Model IM parameter definition file	Y	N
<i>console-path\conf\jplco_service.conf</i>	Extended startup process definition file	Y	Δ
<i>console-path\conf\action\actdef.conf</i>	Automated action definition file	Y	Y
<i>console-path\conf\action\actnotice.conf</i>	Automatic action notification definition file	Y	Y
<i>console-path\conf\action\actnotice.conf.model</i>	Model automatic action notification definition file	Y	N
<i>console-path\conf\action\event_info_replace.conf</i>	Configuration file for converting information	Y	Y <sup>#2</sup>
<i>console-path\conf\action\attr_list\attr_list.conf</i>	File that defines which items are displayed for event conditions	Y	Y
<i>console-path\conf\action\attr_list\attr_list.conf.model</i>	Model file that defines which items are displayed for event conditions	Y	Y
<i>console-path\conf\action\actdef.conf.model</i>	Model automated action definition file	Y	N <sup>#1</sup>
<i>console-path\conf\console\attribute\company-name_product-name_attr_en.conf</i>	Definition file for extended event attributes	Y	Y <sup>#2</sup>
<i>console-path\conf\console\monitor\company-name_product-name_mon_en.conf</i>	Definition file for opening monitor windows	Y	Y <sup>#2</sup>
<i>console-path\conf\console\object_type\company-name_product-name_obj.en</i>	Definition file for object types	Y	Y <sup>#2</sup>
<i>console-path\conf\console\profile\.system</i>	System profile	Y	Δ
<i>console-path\conf\console\profile\.system.model</i>	Model file for the system profile	Y	N

# A. Files and Directories

File or folder name	Description	Ref.	Edit
<i>console-path</i> \conf\console\profile\defaultUser	Default user profile	Y	Δ
<i>console-path</i> \conf\console\profile\defaultUser.model	Model file for the default user profile	Y	N
<i>console-path</i> \conf\console\profile\profile_user-name	User profile for a specific JP1 user	Y	Δ
<i>user-specified-folder</i> \file-name.conf	Correlation event generation definition file	Y	Y <sup>#2</sup>
<i>console-path</i> \conf\evgen\profile\egs_system.conf	Correlation event generation system profile	Y	Y
<i>console-path</i> \conf\evgen\profile\egs_system.conf.model	Model file for the correlation event generation system profile	Y	N <sup>#1</sup>
<i>console-path</i> \conf\guide\jco_guide.txt	Event guide information file	Y	Y <sup>#1</sup>
<i>console-path</i> \conf\guide\sample_jco_guide.txt	Sample event guide information file	Y	N
<i>console-path</i> \conf\guide\sample_jco_guide.txt.model	Model file for an event guide information sample	Y	N
<i>console-path</i> \conf\health\jcohc.conf	Health check definition file	Y	Y
<i>console-path</i> \conf\health\jcohc.conf.model	Model health check definition file	Y	N
<i>console-path</i> \conf\processupdate\processupdate.conf	Status event definition file	Y	Y
<i>console-path</i> \conf\processupdate\processupdate.conf.model	Model status event definition file	Y	N
<i>console-path</i> \default	Common definitions folder	Y	N
<i>console-path</i> \default\action.conf.update	Model automated action environment definition file	Y	N <sup>#1</sup>
<i>console-path</i> \default\console.conf.update	Model communication environment definition file	Y	N <sup>#1</sup>
<i>user-specified-folder</i> \file-name	Correlation event generation environment definition file	Y	Y <sup>#2</sup>
<i>console-path</i> \operation\	Folder for the operation log	Y	N
<i>console-path</i> \operation\evgen\egs_discrim{1 2 3}.log	Correlation event generation history files	Y	N

File or folder name	Description	Ref.	Edit
<i>console-path\www\</i>	Web-based folder	Y	N
<i>console-path\www\console.html</i>	Web-based operation definition file	Y	Δ
<i>console-path\www\console.html.model</i>	Model Web-based operation definition file	Y	N

**Legend:**

Y: Can be performed.

Δ : Can be partially edited.

N: Cannot be performed.

#1: Use a copy of this file

#2: The following files must be added by the user after JP1/IM - Manager is installed: Configuration file for converting information, definition file for extended event attributes, definition file for objects types, definition file for opening monitor windows, correlation event generation definition file, and correlation event generation environment definition file. For details about the definition file for extended event attributes, definition file for objects types, and definition file for opening monitor windows, see *Definition file for opening monitor windows* in 2. *Definition Files* in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*. For details about the last two files, see the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.

*Table A-5: Files and folders that do not need to be referenced or edited (Windows version of JP1/IM - Manager (JP1/IM - Central Console))*

Folder name	Description
<i>console-path\conf\</i>	Files and folders in the folder for environment settings files other than those in the list of files and folders that can be referenced and edited by the user
<i>console-path\classes\</i>	Folder for class files
<i>console-path\default\</i>	Files and folders in the common definitions folder other than those in the list of files and folders that can be referenced and edited by the user
<i>console-path\lib\</i>	Libraries folder
<i>console-path\log\</i>	Logs folder
<i>console-path\operation\</i>	Files and folders in the folder for the operation log other than those in the list of files and folders that can be referenced and edited by the user

Folder name	Description
<i>console-path</i> \system\	Folder for Windows initialization files
<i>console-path</i> \tmp\	Work folder
<i>console-path</i> \tools\	Tools folder
<i>console-path</i> \www\	Files and folders in the Web-based folder other than those in the list of files and folders that can be referenced and edited by the user

### (3) JP1/IM - Manager (JP1/IM - Central Scope)

The tables below describe the names of the files and folders used by the Windows version of JP1/IM - Manager (JP1/IM - Central Scope). *Ref.* in the tables has the following meaning:

- *Ref.* for a folder: The act of checking what the folder contains
- *Ref.* for a file: The act of opening the file and checking its contents

*Table A-6:* Files and folders that can be referenced and edited by the user (Windows version of JP1/IM - Manager (JP1/IM - Central Scope))

File or folder name	Description	Ref.	Edit
<i>scope-path</i> \bin\	Folder for commands	Y	N
<i>scope-path</i> \conf\action_complete_on.conf	Settings files for the completed-action linkage function	Y	Y
<i>scope-path</i> \conf\action_complete_off.conf			
<i>scope-path</i> \conf\action_complete_on.conf.model	Model settings files for the completed-action linkage function	Y	N
<i>scope-path</i> \conf\action_complete_off.conf.model			
<i>scope-path</i> \conf\auto_dbbackup_on.conf	Settings files for automatic backup and recovery of the monitoring object database	Y	Y
<i>scope-path</i> \conf\auto_dbbackup_off.conf			



File or folder name	Description	Re f.	Ed it
<i>scope-path</i> \conf\auto_dbbackup_on.conf.model	Model settings files for automatic backup and recovery of the monitoring object database	Y	N
<i>scope-path</i> \conf\auto_dbbackup_off.conf.model			
<i>scope-path</i> \conf\evhist_warn_event_on.conf	Settings files for the maximum number of status change events	Y	Y
<i>scope-path</i> \conf\evhist_warn_event_off.conf			
<i>scope-path</i> \conf\evhist_warn_event_on.conf.model	Model settings files for the maximum number of status change events	Y	N
<i>scope-path</i> \conf\evhist_warn_event_off.conf.model			
<i>scope-path</i> \conf\guide\	Folder for guide-message files	Y	N
<i>scope-path</i> \conf\jcs_guide.txt	Guide information file	Y	Y
<i>scope-path</i> \conf\jcs_guide.txt.model	Model guide information file	Y	N
<i>scope-path</i> \conf\jcs_hosts	Host information file	Y	Y
<i>scope-path</i> \conf\jcs_hosts.model	Model host information file	Y	N
<i>scope-path</i> \database\	Folder for ISAM files	Y	N
<i>scope-path</i> \database\jcldb\	Folder for the monitoring object database	Y	N
<i>scope-path</i> \database\jcshosts\	Folder for the host information database	Y	N
<i>scope-path</i> \sample\	Sample folder	Y	N
<i>scope-path</i> \sample\guide\jcs_guide_html_sample.txt	Samples of HTML guide information	Y	N
<i>scope-path</i> \sample\guide\exfile\jcs_guide_html_sample001.txt			

**Legend:**

Y: Can be performed.

N: Cannot be performed.

*Table A-7: Files and folders that do not need to be referenced or edited (Windows version of JP1/IM - Manager (JP1/IM - Central Scope))*

File or folder name	Description
<i>scope-path</i> \conf\	Files and folders in the folder for environment settings files other than those in the list of files and folders that can be referenced and edited by the user
<i>scope-path</i> \database\event\	Work folder for event collation processing
<i>scope-path</i> \default\	Common definitions folder
<i>scope-path</i> \log\	Logs folder
<i>scope-path</i> \system\	Folder for Windows initialization files
<i>scope-path</i> \tmp\	Work folder
<i>scope-path</i> \tools\	Tools folder

**(4) JP1/IM - Manager (JP1/IM - IM Configuration Management)**

The tables below describe the names of the files and folders used by the Windows version of JP1/IM - Manager (JP1/IM - IM Configuration Management). *Ref.* in the tables has the following meaning:

- *Ref.* for a folder: The act of checking what the folder contains
- *Ref.* for a file: The act of opening the file and checking its contents

*Table A-8: Files and folders that can be referenced and edited by the user (Windows version of JP1/IM - Manager (JP1/IM - IM Configuration Management))*

File or folder name	Description	Ref.	Edit
<i>IM-path</i> \bin\	Folder for commands	Y	N
<i>IM-path</i> \conf\imcf\const\ppinfotemplate.conf	Product information template file	Y	Y

File or folder name	Description	Re f.	Ed it
<i>IM-path</i> \conf\imcf\const\ppinfotemplate.conf.model	Model product information template file	Y	N
<i>IM-path</i> \conf\imcf\const\profile_list0708.csv	Profile list template file	Y	N
<i>IM-path</i> \conf\imcf\const\profile_listEuropa.csv			
<i>IM-path</i> \conf\imcf\const\jplbase_profile_type_en.csv	Profile type file	Y	N
<i>IM-path</i> \conf\imcf\const\jplbase_profile_type_jp.csv			
<i>IM-path</i> \conf\imcf\const\jplbase_opiTagList_en.csv	Profile tag list file	Y	N
<i>IM-path</i> \conf\imcf\const\jplbase_opiTagList_jp.csv			

Legend:

Y: Can be performed.

N: Cannot be performed.

*Table A-9:* Files and folders that do not need to be referenced or edited (Windows version of JP1/IM - Manager (JP1/IM - IM Configuration Management))

File or folder name	Description
<i>IM-path</i> \conf\	Files and folders in the folder for environment settings files other than those in the list of files and folders that can be referenced and edited by the user
<i>IM-path</i> \system\default\	Common definitions folder
<i>IM-path</i> \data\	Profile data
<i>IM-path</i> \log\	Logs folder
<i>IM-path</i> \tmp\	Work folder
<i>IM-path</i> \lib\	Libraries folder

## A.2 Files and directories of JP1/IM - Manager (for UNIX)

This appendix lists the names of the files and directories used by JP1/IM - Manager (for UNIX).

### (1) JP1/IM - Manager (common to all components)

The tables below describe the names of the files and directories used by JP1/IM -

Manager (all components). *Ref.* in the tables has the following meaning:

- *Ref.* for a directory: The act of checking what the directory contains
- *Ref.* for a file: The act of opening the file and checking its contents

*Table A-10:* Files and directories that can be referenced and edited by the user (UNIX version of JP1/IM - Manager (all components))

File or directory name	Description	Ref.	Edit
/opt/jplimm/tools/jim_log.sh	Data collection tool	Y	N

Legend:

Y: Can be performed.

N: Cannot be performed.

*Table A-11:* Files and directories that do not need to be referenced or edited (UNIX version of JP1/IM - Manager (all components))

Directory name	Description
/opt/jplimm/tools/	Files and directories in the tools directory other than those in the list of files and directories that can be referenced and edited by the user
/opt/jplimm/patch_backup_dir/	Files and directories in the patch backup directory other than patch utilities mentioned in the patch RELEASE.TXT. (This directory is created only when applying a patch.)
/opt/jplimm/update.log	Update log file
/opt/jplimm/patch_history	Patch history file
/var/opt/jplimm/log/	Logs directory

## (2) JP1/IM - Manager (JP1/IM - Central Console)

The tables below describe the names of the files and directories used by the UNIX version of JP1/IM - Manager (JP1/IM - Central Console). *Ref.* in the tables has the following meaning:

- *Ref.* for a directory: The act of checking what the directory contains
- *Ref.* for a file: The act of opening the file and checking its contents

*Table A-12:* Files and directories that can be referenced and edited by the user (UNIX version of JP1/IM - Manager (JP1/IM - Central Console))

File or directory name	Description	Ref.	Edit
/etc/opt/jplcons/jco_start	Script for starting JP1/IM - Manager automatically	Y	N <sup>#1</sup>
/etc/opt/jplcons/jco_start.model	Model script file for starting JP1/IM - Manager automatically	Y	N
/etc/opt/jplcons/jco_stop	Script for stopping JP1/IM - Manager automatically	Y	N <sup>#1</sup>
/etc/opt/jplcons/jco_stop.model	Model script file for stopping JP1/IM - Manager automatically	Y	N
/etc/opt/jplcons/jco_start.cluster	Script for starting JP1/IM - Manager on a logical host	Y	N
/etc/opt/jplcons/jco_stop.cluster	Script for stopping JP1/IM - Manager on a logical host	Y	N
/etc/opt/jplcons/jco_killall.cluster	Script for forcibly ending JP1/IM - Manager processes in a cluster system	Y	N
/etc/opt/jplcons/conf/	Directory for environment settings files	Y	N
/etc/opt/jplcons/conf/jplco_env.conf	IM environment definition file	Y	Y
/etc/opt/jplcons/conf/jplco_service.conf	Extended startup process definition file	Y	Δ
/etc/opt/jplcons/conf/jplco_service_0700_cc.conf	Model file for JP1/IM - Central Console	Y	Δ
/etc/opt/jplcons/conf/jplco_service_0700_cc_cs.conf	Model file for JP1/IM - Central Console and JP1/IM - Central Scope	Y	Δ
/etc/opt/jplcons/conf/jplco_param_V7.conf	IM parameter definition file	Y	Y
/etc/opt/jplcons/conf/jplco_param_V7.conf.model	Model IM parameter definition file	Y	N
/etc/opt/jplcons/conf/action/actdef.conf	Automated action definition file	Y	Y

## A. Files and Directories

File or directory name	Description	Ref.	Edit
/etc/opt/jplcons/conf/action/actnotice.conf	Automatic action notification definition file	Y	Y
/etc/opt/jplcons/conf/action/actnotice.conf.model	Model automatic action notification definition file	Y	N
/etc/opt/jplcons/conf/action/event_info_replace.conf	Configuration file for converting information	Y	Y <sup>#2</sup>
/etc/opt/jplcons/conf/action/attr_list/attr_list.conf	File that defines which items are displayed for event conditions	Y	Y
/etc/opt/jplcons/conf/action/attr_list/attr_list.conf.model	Model of file that defines which items are displayed for event conditions	Y	Y
/etc/opt/jplcons/conf/action/actdef.conf.model	Model automated action definition file	Y	N <sup>#1</sup>
/etc/opt/jplcons/conf/console/attribute/company-name_product-name_attr_en.conf	Definition file for extended event attributes	Y	Y <sup>#2</sup>
/etc/opt/jplcons/conf/console/monitor/company-name_product-name_attr_mon.conf	Definition file for opening monitor windows	Y	Y <sup>#2</sup>
/etc/opt/jplcons/conf/console/object_type/company-name_product-name_obj.en	Definition file for object types	Y	Y <sup>#2</sup>
/etc/opt/jplcons/conf/console/profile/.system	System profile	Y	Δ
/etc/opt/jplcons/conf/console/profile/.system.model	Model file for the system profile	Y	N
/etc/opt/jplcons/conf/console/profile/defaultUser	Default user profile	Y	Δ
/etc/opt/jplcons/conf/console/profile/defaultUser.model	Model file for the default user profile	Y	N
/etc/opt/jplcons/conf/console/profile/profile_user-name	User profile for a specific JP1 user	Y	Δ
user-specified-directory/file-name.conf	Correlation event generation definition file	Y	Y <sup>#2</sup>
/etc/opt/jplcons/conf/evgen/profile/egs_system.conf	Correlation event generation system profile	Y	Y
/etc/opt/jplcons/conf/evgen/profile/egs_system.conf.model	Model file for the correlation event generation system profile	Y	N <sup>#1</sup>

File or directory name	Description	Ref.	Edit
/etc/opt/jplcons/conf/guide/jco_guide.txt	Event guide information file	Y	Y <sup>#1</sup>
/etc/opt/jplcons/conf/guide/sample_jco_guide.txt	Sample event guide information file	Y	N
/etc/opt/jplcons/conf/guide/sample_jco_guide.txt.model	Model file for event guide information sample	Y	N
/etc/opt/jplcons/conf/processupdate/processupdate.conf	Status event definition file	Y	Y
/etc/opt/jplcons/conf/processupdate/processupdate.conf.model	Model status event definition file	Y	N
/etc/opt/jplcons/default/	Common definitions directory	Y	N
/etc/opt/jplcons/default/action.conf.update	Model automated action environment definition file	Y	N <sup>#1</sup>
/etc/opt/jplcons/default/console.conf.update	Model communication environment definition file	Y	N <sup>#1</sup>
<i>user-specified-directory/file-name</i>	Correlation event generation environment definition file	Y	Y <sup>#2</sup>
/etc/opt/jplcons/conf/health/jcohc.conf	Health check definition file	Y	Y
/etc/opt/jplcons/conf/health/jcohc.conf.model	Model health check definition file	Y	N
/opt/jplcons/bin/	Commands directory	Y	N
/opt/jplcons/tools/	Tools directory	Y	N
/opt/jplcons/www/	Web-based directory	Y	N
/opt/jplcons/www/console.html	Web-based operation definition file	Y	Δ
/opt/jplcons/www/console.html.model	Model file for a Web-based operation definition file	Y	N
/var/opt/jplcons/operation	Operation log directory	Y	N
/var/opt/jplcons/operation/evgen/egs_discrim{1 2 3}.log	Correlation event generation history files	Y	N

Legend:

Y: Can be performed.

Δ : Can be partially edited.

N: Cannot be performed.

#1: Use a copy of this file.

#2: The following files must be added by the user after JP1/IM - Manager is installed: Definition file for the extended event attributes, definition file for objects types, definition file for opening monitor windows, correlation event generation definition file, and correlation event generation environment definition file. For details about the first three files, see *Definition file for opening monitor windows* in 2. *Definition Files* in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*. For details about the last two files, see the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.

Table A-13: Files and directories that do not need to be referenced or edited (UNIX version of JP1/IM - Manager (JP1/IM - Central Console))

Directory name	Description
/etc/opt/jplcons/conf/	Files and directories in the directory for environment settings files other than those in the list of files and directories that can be referenced and edited by the user
/etc/opt/jplcons/default/	Files and directories in the common definitions directory other than those in the list of files and directories that can be referenced and edited by the user
/opt/jplcons/tools/	Tools directory
/opt/jplcons/classes/	Directory for class files
/opt/jplcons/www/	Files and directories in the Web-based directory other than those in the list of files and directories that can be referenced and edited by the user
/opt/jplcons/lib/	Directory of library files
/var/opt/jplcons/log/	Logs directory
/var/opt/jplcons/operation/	Files and directories in the directory for the operation log other than those in the list of files and directories that can be referenced and edited by the user
/var/opt/jplcons/tmp/	Work directory

### (3) JP1/IM - Manager (JP1/IM - Central Scope)

The tables below describe the names of the files and directories used by the UNIX version of JP1/IM - Manager (JP1/IM - Central Scope). *Ref.* in the tables has the



following meaning:

- *Ref.* for a directory: The act of checking what the directory contains
- *Ref.* for a file: The act of opening the file and checking its contents

*Table A-14:* Files and directories that can be referenced and edited by the user (UNIX version of JP1/IM - Manager (JP1/IM - Central Scope))

File or directory name	Description	Re f.	Ed it
/etc/opt/jplscope/conf/action_complete_on.conf	Settings files for completed-action linkage function	Y	Y
/etc/opt/jplscope/conf/action_complete_off.conf			
/etc/opt/jplscope/conf/action_complete_on.conf.model	Model settings files for completed-action linkage function	Y	N
/etc/opt/jplscope/conf/action_complete_off.conf.model			
/etc/opt/jplscope/conf/auto_dbbackup_on.conf	Settings files for automatic backup and recovery of the monitoring object database	Y	Y
/etc/opt/jplscope/conf/auto_dbbackup_off.conf			
/etc/opt/jplscope/conf/auto_dbbackup_on.conf.model	Model settings files for automatic backup and recovery of the monitoring object database	Y	N
/etc/opt/jplscope/conf/auto_dbbackup_off.conf.model			
/etc/opt/jplscope/conf/evhist_warn_event_on.conf	Settings files for the maximum number of status change events	Y	Y
/etc/opt/jplscope/conf/evhist_warn_event_off.conf			
/etc/opt/jplscope/conf/evhist_warn_event_on.conf.model	Model settings files for the maximum number of status change events	Y	N
/etc/opt/jplscope/conf/evhist_warn_event_off.conf.model			
/etc/opt/jplscope/conf/jcs_guide.txt	Guide information file	Y	Y
/etc/opt/jplscope/conf/jcs_guide.txt.model	Model guide information file	Y	N
/etc/opt/jplscope/conf/jcs_hosts	Host information file	Y	Y

## A. Files and Directories

File or directory name	Description	Re f.	Ed it
/etc/opt/jplscope/conf/jcs_hosts.model	Model host information file	Y	N
/etc/opt/jplscope/sample/	Sample directory	Y	N
/etc/opt/jplscope/sample/guide/jcs_guide_html_sample.txt	Samples of HTML guide information	Y	N
/etc/opt/jplscope/sample/guide/exfile/ jcs_guide_html_sample001.txt			
/opt/jplscope/bin/	Commands directory	Y	N
/opt/jplscope/lib/	Directory of library files	Y	N
/opt/jplscope/lib/\$LANG	Message catalog	Y	N
/var/opt/jplscope/log/JCS_SETUP/jcs_setup.log	Installation log file	Y	N

### Legend:

Y: Can be performed.

N: Cannot be performed.

*Table A-15:* Files and directories that do not need to be referenced or edited (UNIX version of JP1/IM - Manager (JP1/IM - Central Scope))

File or directory name	Description
/etc/opt/jplscope/conf/	Files and directories in the directory for environment settings files other than those in the list of files and directories that can be referenced and edited by the user
/etc/opt/jplscope/default/	Common definitions directory
/opt/jplscope/tools/	Tools directory
/var/opt/jplscope/database/event/	Work directory for event collation processing
/var/opt/jplscope/log/	Files and directories in the logs directory other than those in the list of files and directories that can be referenced and edited by the user
/var/opt/jplscope/tmp/	Work directory

**(4) JP1/IM - Manager (JP1/IM - IM Configuration Management)**

The tables below describe the names of the files and directories used by the UNIX version of JP1/IM - Manager (JP1/IM - IM Configuration Management). *Ref.* in the tables has the following meaning:

- *Ref.* for a directory: The act of checking what the directory contains
- *Ref.* for a file: The act of opening the file and checking its contents

*Table A-16:* Files and directories that can be referenced and edited by the user (UNIX version of JP1/IM - Manager (JP1/IM - IM Configuration Management))

File or directory name	Description	Ref.	Edit
/opt/jplimm/bin/	Commands directory	Y	N
/etc/opt/jplimm/conf/imcf/const/ppinfotemplate.conf	Product information template file	Y	Y
/etc/opt/jplimm/conf/imcf/const/ppinfotemplate.conf.model	Model product information template file	Y	N
/etc/opt/jplimm/conf/imcf/const/profile_list0708.csv	Profile list template file	Y	N
/etc/opt/jplimm/conf/imcf/const/profile_listEuropa.csv			
/etc/opt/jplimm/conf/imcf/const/jplbase_profile_type_en.csv	Profile list type file	Y	N
/etc/opt/jplimm/conf/imcf/const/jplbase_profile_type_jp.csv			
/etc/opt/jplimm/conf/imcf/const/jplbase_opiTagList_en.csv	Profile tag list file	Y	N
/etc/opt/jplimm/conf/imcf/const/jplbase_opiTagList_jp.csv			

Legend:

Y: Can be performed.

N: Cannot be performed.

*Table A-17:* Files and folders that do not need to be referenced or edited (UNIX version of JP1/IM - Manager (JP1/IM - IM Configuration Management))

File or directory name	Description
/etc/opt/jplimm/conf/	Files and folders in the folder for environment settings files other than those in the list of files and folders that can be referenced and edited by the user
/etc/opt/jplimm/default/	Common definitions directory
/var/opt/jplimm/data/	Profile data
/var/opt/jplimm/log/	Logs directory
/var/opt/jplimm/tmp/	Work directory
/opt/jplimm/lib/	Libraries directory

### A.3 JP1/IM - View

This appendix lists the names of the files and folders used by JP1/IM - View.

The tables below describe the names of the files and folders used by JP1/IM - View. *Ref.* in the tables has the following meaning:

- *Ref.* for a folder: The act of checking what the folder contains
- *Ref.* for a file: The act of opening the file and checking its contents

*Table A-18:* Files and folders that can be referenced and edited by the user (JP1/IM - View)

File or folder name	Description	Ref.	Edit
<i>view-path</i> \Readme.txt	Readme file	Y	N
<i>view-path</i> \bin\	Folder for commands	Y	N
<i>view-path</i> \conf\	Folder for definition files	Y	N
<i>view-path</i> \conf\appexecute\en\company-name_product-name_app.conf	Definition file for executing applications	Y	Y <sup>#1</sup> , #2
<i>view-path</i> \conf\appexecute\en\!JP1_CC_APP0.conf.model	Model definition file for executing applications	Y	N
<i>view-path</i> \conf\function\en\company-name_product-name_tree.conf	Definition file for the Tool Launcher window	Y	Y <sup>#1</sup> , #2

File or folder name	Description	Ref.	Edit
<i>view-path</i> \conf\function\en\!JP1_CC_FTREE0.conf.model	Model definition file for the Tool Launcher window	Y	N
<i>view-path</i> \conf\tuning.conf	IM-View settings file	Y	Y
<i>view-path</i> \conf\tuning.conf.model	Model IM-View settings file	Y	N
<i>view-path</i> \conf\jcfview\jcfview.conf	Operation definition file of the IM configuration management viewer	Y	Y
<i>view-path</i> \conf\jcfview\jcfview.conf.model	Model operation definition file of the IM configuration management viewer	Y	N
<i>view-path</i> \conf\sovtoolexec\en\!JP1_CS_APP0.conf	Start program definition file	Y	Y
<i>view-path</i> \conf\sovtoolexec\en\!JP1_CS_APP0.conf.model	Model start program definition file	Y	N
<i>view-path</i> \conf\sovtoolitem\en\!JP1_CS_FTOOL0.conf	Toolbar definition file	Y	Y
<i>view-path</i> \conf\sovtoolitem\en\!JP1_CS_FTOOL0.conf.model	Model toolbar definition file	Y	N
<i>view-path</i> \conf\sovtoolitem\en\!JP1_CS_FTREE0.conf	Icon operation definition file	Y	Y
<i>view-path</i> \conf\sovtoolitem\en\!JP1_CS_FTREE0.conf.model	Model icon operation definition file	Y	N
<i>view-path</i> \conf\webdata\en\hitachi_jp1_product-name.html	Web page call definition file	Y	Y
<i>view-path</i> \conf\webdata\en\hitachi_jp1_product-name.html.model	Model Web page call definition file	Y	N
<i>view-path</i> \default\	Common definitions folder	Y	N
<i>view-path</i> \default\view.conf.update	Model communication environment definition file	Y	N <sup>#1</sup>
<i>view-path</i> \default\tree_view.conf.update	Model communication environment definition file	Y	N <sup>#1</sup>
<i>view-path</i> \image\icon\	Icons folder	Y	Y
<i>view-path</i> \image\visual\#3	Visual icons folder	Y	Y
<i>view-path</i> \image\map\	Background images folder	Y	Y
<i>view-path</i> \tools\	Tools folder	Y	N

File or folder name	Description	Ref.	Edit
<i>view-path</i> \tools\jcoview_log.bat	Data collection tool	Y	N

Legend:

Y: Can be performed.

N: Cannot be performed.

#1: Use a copy of this file.

#2: The definition file for executing applications and definition file for the Tool Launcher window must be added by the user after JP1/IM - View is installed. For details, see 2. *Definition Files* in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.

#3: This folder is created by the user after JP1/IM - View is installed.

*Table A-19:* Files and folders that do not need to be referenced or edited (JP1/IM - View)

Folder name	Description
<i>view-path</i> \conf\	Files and folders in the folder for environment settings files other than those in the list of files and folders that can be referenced and edited by the user
<i>system-drive</i> :\ProgramData\HITACHI\JP1\JP1_DEFAULT\JP1 CoView\conf\ #1	
<i>view-path</i> \classes\	Folder for class files
<i>view-path</i> \default\	Files and folders in the common definitions folder other than those in the list of files and folders that can be referenced and edited by the user
<i>view-path</i> \doc\	Help folder
<i>view-path</i> \image\	Files and folders in the folder for image data other than those in the list of files and folders that can be referenced and edited by the user
<i>view-path</i> \log\ #2	Logs folder
<i>view-path</i> \patch_backup_dir\	Files and folders in the patch backup folder other than patch utilities mentioned in the patch RELEASE.TXT. (This folder is created only when applying a patch.)

Folder name	Description
<i>view-path</i> \tools\	Files and folders in the tools folder other than those in the list of files and folders that can be referenced and edited by the user
<i>system-drive</i> :\Program Files\jplcommon\	Folder for program information

#1: This folder is present only in Windows Vista and Windows Server 2008. In Windows Vista and Windows Server 2008, environment settings files are stored in this folder as well as in *view-path*\conf\.

#2: In Windows Vista and Windows Server 2008, the applicable folder is *system-drive*:\ProgramData\HITACHI\JP1\JP1\_DEFAULT\JP1CoView\log\.

## B. List of Processes

This appendix describes JP1/IM processes.

### B.1 JP1/IM processes (Windows)

The following shows the process names displayed in the **Processes** page of the Windows Task Manager.

#### (1) JP1/IM - Manager

The table below describes the JP1/IM - Manager processes. The numbers in parentheses are the number of processes that can be executed concurrently.

Table B-1: JP1/IM - Manager processes (Windows)

Parent process	Functionality	Child process	Functionality
jco_spmc.exe (1)	JP1/IM - Manager process management	jcamain.exe (1)	Automatic Action Service (displayed process name: jcamain)
		evtcon.exe (1)	Event console service (displayed process name: evtcon)
		evflow.exe (1)	Event base service (displayed process name: evflow)
		jcsmain.exe (1)	Central Scope service (displayed process name: jcsmain)
		evgen.exe (2) <sup>#1</sup>	Correlation event generation service <sup>#2</sup> (displayed process name: evgen)
		jcfmain.exe(1)	IM Configuration Management service (displayed process name: jcfmain)
jco_service.exe (1)	Windows service control in JP1/IM - Manager	--	--
pdservice.exe	IM database	--	Windows service control
		pdprcd.exe	Process server process
pdprcd.exe(1)	IM database	--	Process server process
		pdrsvre.exe(3)	Post-processing process. Performs recovery processing when a process terminates abnormally.
		pdmlogd.exe(1)	Message log server process. Controls message output.



Parent process	Functionality	Child process	Functionality
		pdrdmd.exe(1)	System manager process. Controls unit starting and stopping and manages connected users.
		pdstd.exe(1)	Status server process. Controls I/O operations to unit status files.
		pdsd.exe(1)	Scheduler process. Distributes transactions among single server processes.
		pdtrnd.exe(1)	Transaction server process. Controls transactions.
		pdtrnrvd.exe(1 to 128) <sup>#3</sup>	Transaction recovery process. Controls transaction determination and recovery.
		pdlod.exe(1)	Log server process. Controls acquisition of system logs and log-related processes.
		pd_buf_dfw.exe(1)	Deferred write process. Controls background writing to disks where the database is kept.
		pdlodswd.exe(1)	Log swapper process. Allocates and de-allocates system log-related files, manages I/O operations for system log-related files, and acquires syncpoint dumps.
		pdsds.exe(10 to 128) <sup>#4</sup>	Single server process. Performs SQL processing.
pdsha.exe (1)	IM database	--	Service for embedded HiRDB in a cluster environment

Legend:

--: None

#1: Maximum 2; normally 1. Breakdown as follows:

- Main processes of the event generation service
- Temporary process issued when the event service is connected. The process is generated when the event generation service starts and when an event acquisition filter is updated.

#2: Functionality for correlation event issue (inactive by default). The correlation event generation service is used in systems that do not use the integrated monitoring

database.

#3: Only one process runs when the system starts, but this number increases temporarily with each abnormal termination of the `pdsds.exe` process.

#4: 10 instances of this process run at startup, and this number increases with the number of access requests to the IM database. The maximum number of concurrent processes is 32.

When JP1/IM - Manager is used in a cluster system, the above processes are executed on each physical host and logical host. The number of processes that can be executed concurrently is the number of processes in the table multiplied by the number of physical and logical hosts on which the processes are running.

Processes in the above table whose parent process is `jco_spmd.exe` are controlled by the process management. You can check their status using the `jco_spmd_status` command.

An example of the display when the processes are running normally is shown below.

```
c:\>jco_spmd_status
KAVB3690-I Processing to report the status of JP1_CONS has
started.
Display the running processes
Process name Process ID
      evflow      3672
      jcamain      4088
      evtcon       4236
      jcsmain      4668
      evgen        5624
KAVB3691-I All the processes have started.
```

`jcsmain` is listed only when the Central Scope functionality is enabled, `evgen` is listed only when correlation event generation is enabled, and `jcfmain` is listed only when the IM Configuration Management functionality is enabled.

## (2) JP1/IM - View

The table below describes JP1/IM - View processes. The numbers in parentheses are the number of processes that can be executed concurrently.

Table B-2: JP1/IM - View processes

Parent process	Functionality	Child process	Functionality
jcoview.exe (3 + 3 <sup>#</sup> )	JP1/IM - View process management	jcoview_evt.exe (3)	Sends thread dump output events
		java.exe (3 + 3 <sup>#</sup> )	JP1/IM - View window control

Parent process	Functionality	Child process	Functionality
jcfview.exe (3)	JP1/IM - IM Configuration Management - View process management	jcfview_evt.exe (3)	Sends thread dump output events
		java.exe (3 + 3 <sup>#</sup> )	JP1/IM - IM Configuration Management - View window control

#: Add when the JP1/IM - View (JP1/IM - Rule Operation linkage function) is active.

## B.2 JP1/IM processes (UNIX)

The following shows the process names displayed by the `ps` command.

### (1) JP1/IM - Manager

The table below describes the JP1/IM - Manager processes. The numbers in parentheses are the number of processes that can be executed concurrently.

Table B-3: JP1/IM - Manager processes (UNIX)

Parent process	Functionality	Child process	Functionality
jco_spmc (1) <sup>#1</sup>	Process management	jcmain (1)	Automatic action service (displayed process name: jcmain)
		evtcon (1) <sup>#1</sup>	Event console service (displayed process name: evtcon)
		evflow (1)	Event base service (displayed process name: evflow)
		jcsmain (1)	Central Scope service (displayed process name: jcsmain)
		evgen (2) <sup>#2</sup>	Event generation service <sup>#3</sup> (displayed process name: evgen)
		jcfmain(1)	IM Configuration Management service (displayed process name: jcfmain)
pdprcd(1)	IM database	--	Process server process
		pdrsvre(3)	Post-processing process. Performs recovery processing when a process terminates abnormally.

Parent process	Functionality	Child process	Functionality
		pdmlgd(1)	Message log server process. Controls message output.
		pdrdmd(1)	System manager process. Controls unit starting and stopping and manages connected users.
		pdstd(1)	Status server process. Controls I/O operations to unit status files.
		pdscdd(1)	Scheduler process. Distributes transactions among single server processes.
		pdtrnd(1)	Transaction server process. Controls transactions.
		pdtrnrvd(1 to 128) <sup>#4</sup>	Transaction recovery process. Controls transaction determination and recovery.
		pdlogd(1)	Log server process. Controls acquisition of system logs and log-related processes.
		pd_buf_dfw(1)	Deferred write process. Controls background writing to disks where the database is kept.
		pdlogswd(1)	Log swapper process. Allocates and de-allocates system log-related files, manages I/O operations for system log-related files, and acquires synpoint dumps.
		pdsds(10 to 32) <sup>#5</sup>	Single server process. Performs SQL processing.
pdsha(1)	IM database	--	Service for embedded HiRDB in a cluster environment

## Legend:

--: None

#1: The number of processes may increase temporarily.

#2: Maximum 2; normally 1. Breakdown as follows:

- Main processes of the event generation service
- Temporary process generated when the event service is connected. The process is generated when the event generation service starts and when an event acquisition filter is updated.

#3: Functionality for correlation event generation (inactive by default). The event generation service is used in systems that do not use the integrated monitoring database.

#4: Only one process runs when the system starts, but this number increases temporarily with each abnormal termination of the `pdsds` process.

#5: 10 instances of this process run at startup, and this number increases with the number of access requests to the IM database. The maximum number of concurrent processes is 32.

When JP1/IM - Manager is used in a cluster system, the above processes are executed on each physical host and logical host. The number of processes that can be executed concurrently is the number of processes in the table multiplied by the number of physical and logical hosts on which the processes are running. Processes running in a cluster system are displayed by the `ps` command as follows:

```
jco_spmd logical-host-name
evflow logical-host-name
jcamain logical-host-name
evtcon logical-host-name
jcdmain logical-host-name
evgen logical-host-name
jcfmain logical-host-name
jcsmain logical-host-name
```

Processes in the above table whose parent process is `jco_spmd` are controlled by the process management. You can check their status using the `jco_spmd_status` command.

An example of the display when the processes are running normally is shown below.

```
# jco_spmd_status
KAVB3690-I Processing to report the status of JP1_CONS has
started.
Display the running processes
Process name Process ID
      evflow      3672
      jcamain      4088
      evtcon       4236
      jcsmain      4846
      jcdmain      5423
      evgen        5624
KAVB3691-I All the processes have started.
```

`jcsmain` is listed only when the Central Scope functionality is enabled, `evgen` is listed only when correlation event generation is enabled, and `jcfmain` is listed only when the IM Configuration Management functionality is enabled.

## C. Port Numbers

This appendix lists the port numbers used by JP1/IM. The protocol is TCP/IP.

These port numbers are set when the product is installed.

### C.1 Port numbers for JP1/IM

*Table C-1: List of port numbers*

Service name	Port number	IM-V	IM-M	Description
jplimevtcon	20115/tcp	Y	Y	Used to connect to JP1/IM - Manager (event console service) from JP1/IM - View
jplimcmda	20238/tcp	Y	--	Used to execute commands from JP1/IM - View
jplimcss	20305/tcp	Y	Y	Used to connect to JP1/IM - Manager (Central Scope service) from JP1/IM - View
JP1/IM-Manager DB Server	20700/tcp <sup>#</sup>	--	Y	Used for internal processing by JP1/IM - Manager (IM database)
jplimcf	20702/tcp	Y	Y	Used to connect to JP1/IM - Manager (IM Configuration Management service) from JP1/IM - View
jplimfcs	20701/tcp	--	Y	Used for internal processing by JP1/IM - Manager (event base service)
jplimegs	20383/tcp	--	Y	Used for internal processing by JP1/IM - Manager (event generation service)
jplrmregistry	20380/tcp	Y	--	Used to connect to JP1/IM - Rule Operation from JP1/IM - View
jplrmobject	20381/tcp	Y	--	

Legend:

IM-V: JP1/IM - View

IM-M: JP1/IM - Manager

Y: Registered in the `services` file at installation.

--: Not registered in the `services` file at installation (and does not need to be set).

<sup>#</sup>: The port number used by the JP1/IM-Manager DB Server is not registered in the `services` file. The port number increases with each logical host configured in the

system. The default is 20700/tcp. The port number of the IM database is set in the setup information file. For details, see *Setup information file (jimdbsetupinfo.conf)* in 2. *Definition Files* in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.

The Web-based JP1/IM - View uses the port numbers shown in the following table.

Service name	Port number	Description
http	80/tcp <sup>#</sup>	Used to connect to the Web server (to download <code>console.html</code> from JP1/IM - Manager)
jplimevtcon	20115/tcp	Used to connect to JP1/IM - Manager (event console service) from the Web-based JP1/IM - View (through a Web browser)

<sup>#</sup>: The port number may differ depending on the Web server settings.

## C.2 Direction of communication through a firewall

The table below describes the direction in which hosts communicate through a firewall. JP1/IM supports both packet filtering and NAT (static mode).

Table C-2: Direction of communication through a firewall

Service name	Port number	Direction of communication
jplimevtcon	20115/tcp	JP1/IM - View -> JP1/IM - Manager (JP1/IM - Central Console)
jplimcmda	20238/tcp	JP1/IM - View -> JP1/IM - Manager (JP1/IM - Central Console) JP1/IM - Manager (JP1/IM - Central Console) -> JP1/Base <sup>#1</sup>
jplimcss	20305/tcp	JP1/IM - View -> JP1/IM - Manager (JP1/IM - Central Scope)
jplrmregistry	20380/tcp	JP1/IM - View -> JP1/IM - Rule Operation
jplrmobject	20381/tcp	
jplimegs	20383/tcp	Firewall setup is unnecessary because all communication takes place on the machine on which JP1/IM - Manager is installed.
JP1/IM-Manager DB Server	20700/tcp	JP1/IM - Manager -> JP1/IM-Manager DB Server
jplimcf	20702/tcp	JP1/IM - View -> JP1/IM - Manager (IM Configuration Management)

Service name	Port number	Direction of communication
jplimfcs	20701/tcp	Firewall setup is unnecessary because all communication takes place on the machine on which JP1/IM - Manager is installed.
jplimeds	23045/tcp	Firewall setup is unnecessary because all communication takes place on the machine on which JP1/IM - Manager is installed.
http	80/tcp <sup>#2</sup>	Web-based JP1/IM - View (Web browser) -> Web server

Legend:

->: Direction of the connection when established

#1: Refers to JP1/Base on the manager.

#2: The port number may differ depending on the Web server settings.

When a connection is established, the port number in the table is used by the side being connected (the side the arrow points at). The connecting side uses an available port number assigned by the OS. The range of port numbers that can be used is OS-dependent.

When JP1/IM is installed on a firewall server host, communications within that machine may also be subject to the firewall restrictions. In this case, set up the firewall so that services can use the port numbers in the table even for communications within the firewall server host.

For details on operation with a firewall, see *7.3 Operating in a firewall environment* in the *Job Management Partner 1/Integrated Management - Manager Configuration Guide*.

### C.3 Connection status

The following table describes the connection status at each JP1/IM port number.



Table C-3: Connection status

Service name	Port number	Connection status
jp1imevtcon	20115/tcp	<p>A connection is established when you log in to the Event Console window from the Login window, and is maintained until you log out.</p> <p>If a communication error occurs or if you forcibly terminate the connection, message KAVB1200-E appears. Click the <b>OK</b> button in the message box to re-establish the connection (only if <b>Automatic refresh</b> is set to <b>Apply</b> in the Preferences window).</p> <p>If <b>Do not apply</b> is set for <b>Automatic refresh</b> in the Preferences window, you can re-establish the connection by clicking the <b>Refresh</b> button in the Event Console window.</p>
jp1imcnda	20238/tcp	<p>A connection is established when you launch the Execute Command window and is maintained until you close the window.</p> <p>If a communication error occurs or if you forcibly terminate the connection, message KAVB0414-E appears. To re-establish the connection, re-execute the command in the Execute Command window.</p>
jp1imcss	20305/tcp	<p>A connection is established when you log in to the Monitoring Tree window from the Login window, and is maintained until you log out.</p> <p>If a communication error occurs or if you forcibly terminate the connection, message KAVB6241-E or KAVB6251-E appears. Click the <b>OK</b> button in the message box to re-establish the connection.</p>
jp1imegs	20383/tcp	<p>A connection is established when any of the following commands related to the event generation service or any of the following processes is executed, and is maintained until the command or process completes:</p> <ul style="list-style-type: none"> <li>• jcoegschange command</li> <li>• jcoegsstatus command</li> <li>• jcoegsstart command</li> <li>• jcoegsstop command</li> <li>• Update of an event acquisition filter (using the System Environment Settings window of JP1/IM - View or the jcochfilter command)</li> </ul> <p>When an event acquisition filter is updated, a connection is established between the event console service and event generation service, and is terminated when the update processing ends.</p>
jp1rmregistry	20380/tcp	<p>A connection is established when you log in to JP1/IM - Rule Operation from JP1/IM - View, and is maintained until you log out from JP1/IM Operation from JP1/IM - View.</p>

## C. Port Numbers

Service name	Port number	Connection status
jplrmobject	20381/tcp	A connection is established when you log in to JP1/IM - Rule Operation from JP1/IM - View, and is maintained until you log out from JP1/IM - Rule Operation from JP1/IM - View.
JP1/IM-Manager DB Server	20700/tcp	A connection is established when you start the JP1/IM-Manager service while JP1/IM-Manager DB Server is running, and is maintained until you shut down JP1/IM-Manager.
jplimcf	20702/tcp	<p>A connection is established with the IM Configuration Management service when any of the following services related to JP1/IM - Manager is executed or you log in or execute a command from JP1/IM - View. The connection is maintained until the service, operation, or command is finished.</p> <ul style="list-style-type: none"> <li>• IM Configuration Management service</li> <li>• A connection is established when you log in to the IM Configuration Management window from the Login window in JP1/IM - View, and is maintained until you log out.</li> <li>• jcfimport command</li> <li>• jcfexport command</li> </ul> <p>If a communication error occurs in a connection to JP1/IM - View or if you forcibly terminate the connection, message KNAN20101-E appears. If this occurs, make sure that the IM Configuration Management service is operating correctly, and click the <b>OK</b> button in the message box to re-establish the connection.</p>
jplimfcs	20701/tcp	<p>A connection is established with the event base service when any of the following services or commands related to JP1/IM - Manager is executed, and is maintained until the service or command finishes executing:</p> <ul style="list-style-type: none"> <li>• Event console service</li> <li>• Automatic action service</li> <li>• Central Scope service</li> <li>• Event generation service</li> <li>• jcoevtreport command</li> <li>• jcohtest command</li> <li>• jcoimdef command</li> <li>• jcastatus command</li> <li>• jcachechange command</li> <li>• jcoegschange command</li> <li>• jcoegsstart command</li> <li>• jcoegsstatus command</li> <li>• jcoegsstop command</li> </ul>

## D. Limits

This appendix shows the limits of JP1/IM.

### (1) Limits when using the Central Console

The tables below describe the limits that apply to JP1/IM - Manager and JP1/IM - View when using the Central Console. The Web-based JP1/IM - View, as a feature of JP1/IM - Manager (JP1/IM - Central Console), is subject to the JP1/IM - Manager limits.

#### (a) JP1/IM - Manager limits

The following table describes the limits that apply to JP1/IM - Manager and the Web-based JP1/IM - View.

*Table D-1: Limits for JP1/IM - Manager*

Item	Limit
Number of instances of JP1/IM - View that can connect to one JP1/IM - Manager	64
Number of instances of the Web-based JP1/IM - View that can run on one machine	1
Number of hosts that can be managed by one instance of JP1/IM - Manager (the number of JP1/Base hosts that can be configured directly under JP1/IM - Manager)	1,024 When <code>close</code> is specified as the communication type in the event server settings file ( <code>conf</code> ) of JP1/Base on the manager 100 (UNIX); 62 (Windows) When a value other than <code>close</code> is specified as the communication type in the event server settings file ( <code>conf</code> ) of JP1/Base on the manager This value is for a maximum configuration. The number of managed hosts is restricted by the system configuration and network traffic.
Number of hosts that can execute commands from one instance of JP1/IM - Manager	1,024 When the managed hosts include a host running JP1/Base 06-51 or earlier, a maximum of 60 such hosts can be configured directly under JP1/IM - Manager. In this case, the maximum number of hosts that can execute commands concurrently from one JP1/IM - Manager is 60 (in Windows) or equal to the number of file descriptors <sup>#1</sup> that can be used in one process minus 10 (in UNIX). The calculation here assumes that a host running JP1/Base 06-51 or earlier under JP1/IM - Manager is executing commands even if it is not doing so in reality.

# D. Limits

Item	Limit
Event buffer size (number of extracted events that can be buffered from the event database)	2,000
Scroll buffer size (number of events that can be displayed in a window) in the Web-based JP1/IM - View	1,000
Number of events that can be acquired when a window is refreshed in the Web-based JP1/IM - View	200
Number of events that can be acquired in a search in the Web-based JP1/IM - View	1,000
Maximum length of an event acquisition filter	60 KB When an exclusion condition group or a valid common exclusion condition group is not set. 64 KB When an exclusion condition group or a valid common exclusion condition group is set.
Maximum length of an event receiver filter	1 MB (total size when more than one event receiver filter is set)
Maximum length of a severe events filter	64 KB
Maximum length of a view filter	1 MB per JP1 user (total size when more than one view filter is set) <sup>#2</sup>
Maximum length of an event search	64 KB (when connected to JP1/Base 06-51 or later; 4 KB when connected to JP1/Base 06-00) <sup>#2</sup>
Number of event receiver filters	128
Number of conditions that can be set in a filter (applies to passing conditions and exclusion conditions)	<ul style="list-style-type: none"> <li>• Event acquisition filter: 30 per filter</li> <li>• Event receiver filter: 30 per filter</li> <li>• Severe events filter: 30</li> <li>• View filter: 5 per filter</li> <li>• Event search: 5</li> </ul>
Maximum length that can be entered in the input field of an item for which multiple attribute values can be specified in a filter window <sup>#3</sup> of the Web-based JP1/IM - View	30,000 bytes
Number of filters that can be defined in the list of event acquisition filters	50
Maximum length of a filter name specified in the list of event acquisition filters	50 bytes

Item	Limit
Number of common exclusion conditions that can be defined in the list of event acquisition filters	30
Maximum size of the file containing the list of event acquisition filters	1 MB
Number of queued commands executed by automated actions	65,535 When the target host on which the automated actions are to be executed is running JP1/Base 06-71 or later 64 When the target host on which the automated actions are to be executed is running JP1/Base 06-51 or earlier
Length of an action definition parameter	5,706 bytes The following limits apply to the individual items specified in the action definition parameter: <ul style="list-style-type: none"> <li>Length of an event monitoring condition: 1,040 bytes</li> <li>Length of an action: 4,096 bytes</li> <li>Length of the user name for executing an action: 31 bytes</li> <li>Length of an environment variable file name: 255 bytes</li> <li>Length of a target host name: 255 bytes</li> </ul>
Length of a target group name	30 bytes
File size of an event guide information file	1 MB
File size of an event-guide message file	1 MB
Total number of items that can be defined in an event guide information file	1,000
Length of an event-guide message after processing of placeholders (variables) and HTML encoding	196,608 characters <sup>#4</sup>
Length of an event guide-message file name that can be specified in an event guide information file	1,024 characters <sup>#4</sup>
Number of comparison conditions that can be defined in event guide information	100
Number of correlation event generation conditions that can be defined in a correlation event generation definition file	1,000
Number of filtering conditions for the correlation target range that can be defined in one correlation event generation condition	1

#### D. Limits

Item	Limit
Number of event conditions that can be defined in one correlation event generation condition	10
Timeout period for a correlation event generation condition	1 second to 86,400 seconds (24 hours)
Maximum value that can be specified in the threshold event correlation type	100 events
Number of duplicate attribute value conditions that can be defined in one correlation event generation condition	3
Number of maximum correlation numbers that can be defined in one correlation event generation condition	1
Maximum length of the attribute value used in defining a correlation approval event	1,023 bytes
Number of sets of JP1 events that can be correlated simultaneously by one correlation event generation condition	1,024 sets
Number of sets of JP1 events that can be correlated simultaneously by all correlation event generation conditions	20,000 sets
Health check timeout period	216,000 seconds (60 hours)

#1: The number of file descriptors available to one process is system-dependent.

#2: This limit applies to the Web-based JP1/IM - View.

#3: Filter windows are the Severe Event Definitions window, Event Search Conditions window, Settings for View Filter window, and Detailed Settings for Event Receiver Filter window.

#4: Each one-byte character counts as one character. For example, *AAA* counts as three characters.

#### (b) JP1/IM - View limits

The following table describes the limits that apply to JP1/IM - View.

*Table D-2: Limits for JP1/IM - View*

Item	Limit
Number of concurrent logins from one instance of JP1/IM - View	3 <sup>#1</sup>

Item	Limit
Scroll buffer size (number of events that can be displayed in a window)	2,000
Number of events that can be acquired when a window is refreshed	200
Number of events that can be acquired in a search	2,000
Maximum length of a filter	<ul style="list-style-type: none"> <li>View filter: 1 MB per JP1 user (total size when more than one view filter is set)</li> <li>Event search: 64 KB (when connected to JP1/Base 06-51 or later; 4 KB when connected to JP1/Base 06-00)</li> </ul>
Number of view filters	50
Maximum length of a name of a view filter	50 bytes
Number of condition groups that can be set in a filter (applies to passing conditions and exclusion conditions)	<ul style="list-style-type: none"> <li>Event acquisition filter: 30 per filter</li> <li>Event receiver filter: 30 per filter</li> <li>Severe events filter: 30</li> <li>View filter: 5 per filter</li> <li>Event search: 5</li> </ul>
Maximum length that can be entered in the input field of an item for which multiple attribute values can be specified in a filter window <sup>#2</sup>	30,000 bytes
Number of filters that can be defined in the list of event acquisition filters	50 (When connected to JP1/IM - Central Console 07-00 or later)
Number of common exclusion condition groups that can be defined in the list of event acquisition filters	30
Longest environment variable file name that can be specified in the Execute Command window	255 bytes
Longest target host name that can be specified in the Execute Command window	255 bytes

Item	Limit
Length of an action definition parameter	<p>When connected to JP1/IM - Manager 08-01 or later: 5,706 bytes</p> <p>The following limits apply to the individual items specified in the action definition parameter:</p> <ul style="list-style-type: none"> <li>Length of an event monitoring condition: 1,040 bytes</li> <li>Length of an action: 4,096 bytes</li> <li>Length of the user name for executing an action: 31 bytes</li> <li>Length of an environment variable file name: 255 bytes</li> <li>Length of a target host name: 255 bytes</li> </ul> <p>When connected to JP1/IM - Central Console 07-01 or earlier: 1,023 bytes</p> <p>The following limits apply to the individual items specified in the action definition parameter:</p> <ul style="list-style-type: none"> <li>Length of an event monitoring condition: 1,023 bytes</li> <li>Length of an action: 1,023 bytes</li> <li>Length of the user name for executing an action: 31 bytes</li> <li>Length of an environment variable file name: 255 bytes</li> <li>Length of a target host name: 255 bytes</li> </ul>
Number of lines of execution results to display in the Execute Command window that can be specified in the Preferences window	100 to 10,000 lines
Column width for display of messages in the Execute Command window that can be specified in the Preferences window	50,000 pixels
Size of text data that can be copied to the clipboard	6 MB

#1: The larger the number of concurrent logins, the greater the memory and disk space requirements.

#2: Filter windows are the Severe Event Definitions window, Event Search Conditions window, Settings for View Filter window, and Detailed Settings for Event Receiver Filter window.

## **(2) Limits when using the Central Scope**

The following tables describe the limits that apply to JP1/IM - Manager and JP1/IM - View when using the Central Scope.

### **(a) JP1/IM - Manager limits**

The following table describes the limits that apply to JP1/IM - Manager.



Table D-3: Limits for JP1/IM - Manager

Item	Limit
Number of instances of JP1/IM - View that can connect to one JP1/IM - Manager	64
Number of hosts that can be monitored by one instance of the Central Scope	5,000 This value includes all hosts being monitored from the Central Scope, such as JP1/AJS - Agent hosts and hosts being monitored using the SNMP trap converter of JP1/Base, in addition to hosts configured under JP1/IM - Manager.
Number of Monitoring Tree windows that can be managed by JP1/IM - Manager	1
Longest monitoring node name that can be set in a configuration file for a monitoring tree	255 bytes
Longest basic information for a monitoring node that can be set in a configuration file for a monitoring tree	Attribute value: 1,023 bytes <sup>#</sup>
Longest status change condition name that can be set in a configuration file for a monitoring tree	63 bytes
Longest value specifiable for individual conditions in a configuration file for a monitoring tree	Attribute value: 1,023 bytes <sup>#</sup>
File size of a guide information file	1 MB
File size of a guide-message file	1 MB

<sup>#</sup>: The total for all fields is a maximum of 1,280 bytes. (For example, if five conditions are set, the total size of the five attribute values must not exceed 1,280 bytes.)

#### (b) JP1/IM - View limits

The following table describes the limits that apply to JP1/IM - View.

Table D-4: Limits for JP1/IM - View

Item	Limit
Number of concurrent logins from one viewer host	3 <sup>#1</sup>
Number of monitoring nodes that can be monitored in a Monitoring Tree window	50,000
Length of a monitoring node name	255 bytes
Number of basic information items that can be set for one monitoring node	5

#### D. Limits

Item	Limit
Number of characters that can be entered in a basic information field	Attribute name: 32 bytes Attribute value: 1,023 bytes <sup>#2</sup>
Number of status change conditions that can be set for one monitoring node	8
Length of a status change condition name	63 bytes
Number of individual conditions that can be set in one status change condition for monitoring objects	5
Percentage value that can be set as a comparison condition in one status change condition for monitoring groups	100
Maximum count that can be set as a comparison condition in one status change condition for monitoring groups	50,000
Number of characters that can be entered in an individual condition field	Attribute name: 32 bytes Attribute value: 1,023 bytes <sup>#2</sup>
Number of JP1 events that can be issued by one monitoring node	7
Number of status change event logs that can be kept by each monitoring node	100
File name length of a background image that can be set in a monitoring group	260 bytes
File name length of an image file used as an icon for a monitoring node (for the normal and expanded status, and Visual Icon)	260 bytes
Number of common conditions that can be added by the user	191
Length of the common condition name set in the Common Condition Detailed Settings window	63 bytes
Number of characters that can be entered in a <b>Common condition details</b> field (other than the <b>Extended attribute</b> area) of the Common Condition Detailed Settings window	1,023 bytes
Number of characters that can be entered in a <b>Common condition details</b> field ( <b>Extended attribute</b> area) of the Common Condition Detailed Settings window	Attribute name: 32 bytes Attribute value: 1,023 bytes <sup>#2</sup>

Item	Limit
Length of the file name of the background image in a Visual Monitoring window	260 bytes
Number of monitoring nodes that can be placed in one Visual Monitoring window	128
Number of Visual Monitoring windows that users can create	64
Length of the name set for a Visual Monitoring window	63 bytes
Length of a comment about a Visual Monitoring window	80 bytes

#1: The larger the number of concurrent logins, the greater the memory and disk space requirements.

#2: The total for all fields is a maximum of 1,280 bytes. (For example, if five conditions are set, the total size of the five attribute values must not exceed 1,280 bytes.)

### **(3) Limits when using IM Configuration Management**

The tables below describe the limits that apply to JP1/IM - Manager and JP1/IM - IM Configuration Management - View when using IM Configuration Management.

#### **(a) JP1/IM - Manager limits**

The following table describes the limits that apply to JP1/IM - Manager.

*Table D-5: Limits for JP1/IM - Manager*

Item	Limit
Number of instances of JP1/IM - IM Configuration Management - View that can connect to one JP1/IM - Manager	64
Number of hosts that can be monitored from one instance of IM Configuration Management	10,000 1,024 agents can be configured directly under IM Configuration Management
Number of hierarchical levels that can be monitored from one instance of IM Configuration Management	3 levels
Maximum number of log file traps that can be managed	100 <sup>#</sup>
Number of standby hosts that can be set up on one logical host	4
Number of IP addresses that can be displayed for one host	4

D. Limits

Item	Limit
Number of alias host names that can be displayed for one host	4

#: If 101 or more log trap files are active, the message KNAN22450-W is output and the first 100 are collected.

**(b) JP1/IM - View limits**

The following table describes the limits that apply to JP1/IM - View.

*Table D-6: Limits for JP1/IM - View*

Item	Limit
Number of concurrent logins from one instance of JP1/IM - View	3 <sup>#</sup>

#: The larger the number of concurrent logins, the greater the memory and disk space requirements.

---

## E. Operating Permissions

---

Operating permissions are assigned to each JP1 user. There are six JP1 permission levels, as follows:

- `JP1_Console_Admin`  
Allows the JP1 user to perform all operations (system settings, system operations, viewing operations, setting the user environment, and starting linked products) in the Central Console and Central Scope.
- `JP1_Console_Operator`  
Allows the JP1 user to perform system operations, viewing operations, set the user environment, and start linked products in the Central Console and Central Scope.
- `JP1_Console_User`  
Allows the JP1 user to perform viewing operations, set the user environment, and start linked products in the Central Console and Central Scope.
- `JP1_CF_Admin`  
Allows the JP1 user to perform all IM Configuration Management operations (change and apply the system hierarchy, change and apply profiles).
- `JP1_CF_Manager`  
Allows the JP1 user to perform the following IM Configuration Management operations: Register host information, change and apply profiles, view configuration information and host settings, and collect information.
- `JP1_CF_User`  
Allows the JP1 user to perform the following IM Configuration Management operations: View configuration information and host information.

*Note 1:* JP1/IM - Manager (JP1/IM - Central Console)

- `JP1_Console_Operator` permission is assumed if no JP1 permission level has been set.
- `JP1_Console_Operator` and `JP1_Console_User` permissions cannot be set if the authentication server is running JP1/Base version 6.  
`JP1_Console_Admin` permission is assumed if `JP1_Console_Operator` or `JP1_Console_User` permission is set.

*Note 2:* JP1/IM - Manager (JP1/IM - Central Scope)

- `JP1_Console_User` permission is assumed if no JP1 permission level has

been set.

## E.1 Operating permissions required for system monitoring using the Central Console

The following table describes the operating permissions required to perform operations while monitoring the system using the Central Console.

*Table E-1: Operating permissions required for Central Console operations*

Type of operation			JP1 permission level			
Category	Operation	Description	Admin	Operator	User	None
System settings	Set the system environment	Set the JP1/IM - Manager environment in the following windows: <ul style="list-style-type: none"> <li>System Environment Settings window</li> <li>Event Acquisition Settings window</li> </ul>	Y	--	--	--
	Define severe events	Define severe events in the Severe Event Definitions window.	Y	--	--	--
	Set an event receiver filter	Set an event receiver filter in the following windows: <ul style="list-style-type: none"> <li>Settings for Event Receiver Filter window</li> <li>Detailed Settings for Event Receiver Filter window</li> </ul>	Y	--	--	--
	Set automated actions	Set automated actions in the following windows: <ul style="list-style-type: none"> <li>Action Parameter Definitions window</li> <li>Action Parameter Detailed Definitions window</li> <li>Action Parameter Detailed Definitions (Extended Event Information) window</li> </ul>	Y	--	--	--

Type of operation			JP1 permission level			
Category	Operation	Description	Admin	Operator	User	None
	Set event information mapping	Set event information mapping in the following windows: <ul style="list-style-type: none"> <li>Event-Information Mapping Definitions window</li> <li>Event-Information Mapping Detailed Definitions window</li> </ul>	Y	--	--	--
System operations	Change the response status of severe events	Change the response status of JP1 events.	Y	Y	--	Y
	Release a severe event	Change a JP1 event displayed on the Severe Events page to a non-severe event.	Y	--	--	--
	Clear status notification suppression	Re-enable notification of automated action errors when the notification function is suppressed during delay monitoring or status monitoring.	Y	Y	--	Y
	Cancel an automated action	Request the cancellation of an automated action in <i>Wait</i> , <i>Queue</i> , or <i>Running</i> status (by clicking the <b>Cancel Action</b> button in the Action Log window, Action Log Details window, or List of Action Results window).	Y	Y	--	Y
	Re-execute an automated action	Re-execute an automated action in <i>Error</i> or <i>Ended</i> status (by clicking the <b>Re-execute</b> button in the Action Log window, Action Log Details window, or List of Action Results window).	Y	Y	--	Y
	Execute commands	Execute commands on managed hosts in the Execute Command window.	Y	Y	--	Y

Type of operation			JP1 permission level			
Category	Operation	Description	Admin	Operator	User	Non e
	Edit memo entries	Set memo entries in the following window: <ul style="list-style-type: none"> <li>Edit Event Details window</li> </ul>	Y	Y	--	Y
Viewing operations	View JP1 events	View JP1 events on the <b>Monitor Events</b> page and <b>Severe Events</b> page of the Event Console window.	Y	Y	Y	Y
		View JP1 event details in the Event Details window				
		View related events in the Related Events window.				
	View the results of automated actions	View the results of automated actions in the following windows: <ul style="list-style-type: none"> <li>Action Log window</li> <li>Action Log Details window</li> <li>List of Action Results window</li> <li>Conditions for Updating List of Action Results window</li> </ul>	Y	Y	Y	Y
	Search for events	Search for events in the following windows and display the results on the <b>Search Events</b> page of the Event Console window: <ul style="list-style-type: none"> <li>Event Search Conditions window</li> <li>Event Search Conditions (Program-Specific Information in Extended Attribute) window</li> <li>Event Search Detailed Conditions (Program-Specific Information in Extended Attribute) window</li> </ul>	Y	Y	Y	Y



Type of operation			JP1 permission level			
Category	Operation	Description	Admin	Operator	User	None
	Use a view filter	Set conditions for the JP1 events displayed on the <b>Monitor Events</b> page of the Event Console window.	Y	Y	Y	Y
		Switch between view filters.				
	Display event guide information	Check guide information in the Event Details window.	Y	Y	Y	Y
Set the user environment	Set the user environment	Open the Preferences window and set the user environment.	Y	Y	Y	Y
Start linked products	Launch the GUI of another application	Launch the application that reported a JP1 event, and view or manipulate information.	Y	Y	Y	Y
	Open the Tool Launcher window	Use the Tool Launcher window to start linked products.	Y	Y	Y	Y
	Launch the Rule Operation viewer GUI	Launch the Rule Log Details window of JP1/IM - Rule Operation from the Action Log window, Action Log Details window, or List of Action Results window.	Y	Y	Y	Y

**Legend:**

Admin: JP1\_Console\_Admin

Operator: JP1\_Console\_Operator

User: JP1\_Console\_User

Y: Can perform the operation.

--: Cannot perform the operation.

**Notes:**

- When a JP1 user is granted two or more JP1 permission levels, and a particular operation is permitted by one level but prohibited by another, the operation is permitted.

- Menus and buttons for functions that are not permitted under the various permission levels are unavailable in the JP1/IM - View windows.
- Functions that cannot be performed in the Web-based Event Console window are unavailable regardless of the JP1 permission level.
- The assigned JP1 permission level is checked only when the JP1 user logs in. If the JP1 permission level is subsequently changed on the authentication server, the new permission level takes effect the next time the JP1 user logs in.

## E.2 Operating permissions required for system monitoring using the Central Scope

User operations related to system monitoring using the Central Scope can be broadly classified into two types:

- **Monitoring:** Operations performed while monitoring the system using the Monitoring Tree window or Visual Monitoring window
- **Editing:** Operations for creating or editing the system monitoring environment using the Monitoring Tree (Editing) window or Visual Monitoring (Editing) window

The operating permissions required for each type of operation are described below.

### (1) Monitoring permissions (Monitoring Tree window and Visual Monitoring window)

Tables E-2 and E-3 describe the operating permissions required for monitoring-related operations.

*Table E-2:* Operating permissions required for Central Scope operations (in the Monitoring Tree window)

Type of operation			JP1 resource group	JP1 permission level			
Category	Operation	Description		Admin	Operator	User	None
System settings	Add, change, and delete common conditions	Add, change, and delete common conditions in JP1/IM - Manager.	JP1_Console	Y	--	--	--

Type of operation			JP1 resource group	JP1 permission level			
Category	Operation	Description		Admin	Operator	User	None
System operations and viewing (when the monitoring range settings are enabled)	Change monitoring node attributes	Change the following attributes of a monitoring node: <ul style="list-style-type: none"> <li>• Monitoring node name</li> <li>• Icon</li> <li>• Visual Icon</li> <li>• Status</li> <li>• Monitoring status</li> <li>• Basic information</li> <li>• Status change condition<sup>#</sup></li> <li>• Event generation condition</li> </ul> <sup>#</sup> : Excluding adding or changing a common condition in JP1/IM - Manager.	JP1 resource group for the particular node	Y	Y	--	--
			JP1_Console	Y	--	--	--
	View monitoring nodes	View monitoring nodes in the Monitoring Tree window.	JP1 resource group for the particular node	Y	Y	Y	--
			JP1_Console	Y	--	--	--
	Search for monitoring nodes	Search for monitoring nodes in the Search window.	JP1 resource group for the particular node	Y	Y	Y	--
			JP1_Console	Y	--	--	--

Type of operation			JP1 resource group	JP1 permission level			
Category	Operation	Description		Admin	Operator	User	None
	Display monitoring node attributes	Check the attributes of a monitoring node in the Properties window.	JP1 resource group for the particular node	Y	Y	Y	--
			JP1_Console	Y	--	--	--
	Perform visual monitoring	Monitor nodes in the Visual Monitoring window.	JP1 resource group for the particular node	Y	Y	Y	--
			JP1_Console	Y	--	--	--
	Display guide information	Check guide information in the Guide window.	JP1 resource group for the particular node	Y	Y	Y	--
			JP1_Console	Y	--	--	--
	Search for status change events	Search for JP1 events that triggered a status change.	JP1 resource group for the particular node	Y	Y	Y	--
			JP1_Console	Y	--	--	--

Type of operation			JP1 resource group	JP1 permission level			
Category	Operation	Description		Admin	Operator	User	None
System operations and viewing (when the monitoring range settings are disabled)	Changing monitoring node attributes	Change the following attributes of a monitoring node: <ul style="list-style-type: none"> <li>Monitoring node name</li> <li>Icon</li> <li>Visual Icon</li> <li>Status</li> <li>Monitoring status</li> <li>Basic information</li> <li>Status change condition<sup>#</sup></li> <li>Event generation condition</li> </ul> <sup>#</sup> : Excluding adding or changing a common condition in JP1/IM - Manager.	JP1_Console	Y	Y	--	--
	View monitoring nodes	View monitoring nodes in the Monitoring Tree window.	JP1_Console	Y	Y	Y	Y
	Search for monitoring nodes	Search for monitoring nodes in the Search window.	JP1_Console	Y	Y	Y	Y
	Display monitoring node attributes	Check the attributes of a monitoring node in the Properties window.	JP1_Console	Y	Y	Y	Y
	Perform visual monitoring	Monitor nodes in the Visual Monitoring window.	JP1_Console	Y	Y	Y	Y
	Display guide information	Check guide information in the Guide window.	JP1_Console	Y	Y	Y	Y
	Search for status change events	Search for JP1 events that triggered a status change.	JP1_Console	Y	Y	Y	Y

Type of operation			JP1 resource group	JP1 permission level			
Category	Operation	Description		Admin	Operator	User	None
Toggle between <b>Detailed view</b> and <b>Icon view</b>		Toggle between <b>Detailed view</b> and <b>Icon view</b> in the detailed view area of the Monitoring Tree window. In <b>Icon view</b> , draw a selection rectangle and arrange icons evenly.	JP1_Console	Y	Y	Y	Y
View tree editing		View the Monitoring Tree (Editing) window.	JP1_Console	Y	Y	Y	Y
List login users		View the Login User List window.	JP1_Console	Y	Y	Y	Y
Display the event console		View the Event Console window.	JP1_Console	Y	Y	Y	Y
Open the Tool Launcher window		View the Tool Launcher window.	JP1_Console	Y	Y	Y	Y
Save monitoring trees locally		Save monitoring trees to the local host.	JP1_Console	Y	Y	Y	Y

**Legend:**

Admin: JP1\_Console\_Admin

Operator: JP1\_Console\_Operator

User: JP1\_Console\_User

Y: Can perform the operation.

--: Cannot perform the operation.

**Notes:**

- When a JP1 user is granted two or more JP1 permission levels, and a particular operation is permitted by one level but prohibited by another, the operation is permitted.
- Menus and buttons for functions that are not permitted under the various permission levels are unavailable in the JP1/IM - View windows.
- The assigned JP1 permission level is checked only when the JP1 user logs in. If the JP1 permission level is subsequently changed on the authentication

server, the new permission level takes effect the next time the JP1 user logs in.

*Table E-3: Operating permissions required for Central Scope (Visual Monitoring window)*

Type of operation			JP1 resource group	JP1 permission level			
Category	Operation	Description		Admin	Operator	User	None
System settings	Add, change, and delete common conditions	Add, change, and delete common conditions in JP1/IM - Manager.	JP1_Console	Y	--	--	--
System operations and viewing (when the monitoring range settings are enabled)	Change monitoring node attributes	Change the following attributes of a monitoring node: <ul style="list-style-type: none"> <li>Monitoring node name</li> <li>Icon</li> <li>Visual Icon</li> <li>Status</li> <li>Monitoring status</li> <li>Basic information</li> <li>Status change condition<sup>#</sup></li> <li>Event generation condition</li> </ul> <sup>#</sup> : Excluding adding or changing a common condition in JP1/IM - Manager.	JP1 resource group for the particular node	Y	Y	--	--
			JP1_Console	Y	--	--	--
	Display a monitoring tree	Select nodes in a Visual Monitoring window and display them in the Monitoring Tree window.	JP1 resource group for the particular node	Y	Y	Y	--
			JP1_Console	Y	--	--	--

Type of operation			JP1 resource group	JP1 permission level			
Category	Operation	Description		Admin	Operator	User	None
	Search for monitoring nodes	Search for monitoring nodes in the Search window.	JP1 resource group for the particular node	Y	Y	Y	--
			JP1_Console	Y	--	--	--
	Display monitoring node attributes	Check the attributes of a monitoring node in the Properties window.	JP1 resource group for the particular node	Y	Y	Y	--
			JP1_Console	Y	--	--	--
	Display guide information	Check guide information in the Guide window.	JP1 resource group for the particular node	Y	Y	Y	--
			JP1_Console	Y	--	--	--
	Search for status change events	Search for JP1 events that triggered a status change.	JP1 resource group for the particular node	Y	Y	Y	--
			JP1_Console	Y	--	--	--



Type of operation			JP1 resource group	JP1 permission level			
Category	Operation	Description		Admin	Operator	User	None
System operations and viewing (when the monitoring range settings are disabled)	Changing monitoring node attributes	Change the following attributes of a monitoring node: <ul style="list-style-type: none"> <li>Monitoring node name</li> <li>Icon</li> <li>Visual Icon</li> <li>Status</li> <li>Monitoring status</li> <li>Basic information</li> <li>Status change condition<sup>#</sup></li> <li>Event generation condition</li> </ul> <sup>#</sup> : Excluding adding or changing a common condition in JP1/IM - Manager.	JP1_Console	Y	Y	--	--
	Display a monitoring tree	Select nodes in a Visual Monitoring window and display them in the Monitoring Tree window.	JP1_Console	Y	Y	Y	Y
	Search for monitoring nodes	Search for monitoring nodes in the Search window.	JP1_Console	Y	Y	Y	Y
	Display monitoring node attributes	Check the attributes of a monitoring node in the Properties window.	JP1_Console	Y	Y	Y	Y
	Display guide information	Check guide information in the Guide window.	JP1_Console	Y	Y	Y	Y
	Search for status change events	Search for JP1 events that triggered a status change.	JP1_Console	Y	Y	Y	Y

Legend:

Admin: JP1\_Console\_Admin

Operator: JP1\_Console\_Operator

User: JP1\_Console\_User

Y: Can perform the operation.

--: Cannot perform the operation.

**(2) Editing operations (Monitoring Tree (Editing) window and Visual Monitoring (Editing) window)**

No special JP1 user operations are involved in editing the Monitoring Tree window or Visual Monitoring window of the Central Scope. Any user who can log in to the OS can perform editing.

However, operations such as automatically generating a monitoring tree or saving edited information to JP1/IM - Manager require connection to JP1/IM - Manager.

To log in to JP1/IM - Manager in such cases, you must have JP1 user permissions.

Tables E-4 and E-5 describe the operating permissions required for editing operations.

*Table E-4: Operating permissions required for Central Scope operations (in the Monitoring Tree (Editing) window)*

Type of operation			JP1 resource group	JP1 permission level			
Category	Operation	Description		Admin	Operator	User	None
Operations that include login processing	Automatically generate a tree	Collect monitoring tree information from the system through JP1/IM - Manager.	JP1_Console	Y	--	--	--
	Acquire a tree from the server	Acquire monitoring tree data from JP1/IM - Manager.	JP1_Console	Y	--	--	--
	Update server data	Export edited data to JP1/IM - Manager.	JP1_Console	Y	--	--	--
	Acquire the latest definitions	Acquire a list of common conditions managed by JP1/IM - Manager.	JP1_Console	Y	--	--	--
	Rearrange or delete listed Visual Monitoring windows	Change the display order of the Visual Monitoring windows managed by JP1/IM - Manager, or delete a Visual Monitoring window from the list.	JP1_Console	Y	--	--	--

Type of operation			JP1 resource group	JP1 permission level			
Category	Operation	Description		Admin	Operator	User	None
Operations without login processing	Move monitoring nodes	Move monitoring nodes.	Not required	Not required	Not required	Not required	Not required
	Add and delete monitoring nodes, and change node attributes	Add and delete monitoring nodes, and change node attributes. #: Defining a status change condition involves setting a common condition, which requires login to JP1/IM - Manager (JP1_Console_Admin permission required).	Not required	Not required	Not required	Not required	Not required
	Add, change, and delete common conditions	Add, change, and delete common conditions.	Not required	Not required	Not required	Not required	Not required
	Save monitoring trees locally	Save monitoring trees to the local host.	Not required	Not required	Not required	Not required	Not required
	Acquire local monitoring trees	Acquire monitoring tree data saved to the local host.	Not required	Not required	Not required	Not required	Not required
	Search for monitoring nodes	Search for monitoring nodes in the Search window.	Not required	Not required	Not required	Not required	Not required
	Display visual monitoring (editing)	Display the Visual Monitoring (Editing) window.	Not required	Not required	Not required	Not required	Not required

Legend:

Admin: JP1\_Console\_Admin

Operator: JP1\_Console\_Operator

User: JP1\_Console\_User

Y: Can perform the operation.

--: Cannot perform the operation.

Not required: Any user who can log in to the OS can perform the operation.

*Table E-5: Operating permissions required for Central Scope operations (in the Visual Monitoring (Editing) window)*

Type of operation			JP1 resource group	JP1 permission level			
Category	Type of operation	Description		Admin	Operator	User	None
Operations that include login processing	Acquire data from the server	Acquire information about the Visual Monitoring windows managed by JP1/IM - Manager.	JP1_Console	Y	--	--	--
	Update server data	Export edited data to JP1/IM - Manager.	JP1_Console	Y	--	--	--
Operations without login processing	Arrange monitoring nodes	Drag-and-drop monitoring nodes from the Monitoring Tree (Editing) window.	Not required	Not required	Not required	Not required	Not required
	Delete monitoring nodes	Delete monitoring nodes placed in the Monitoring Tree (Editing) window.	Not required	Not required	Not required	Not required	Not required
	Change the background image	Change the background image.	Not required	Not required	Not required	Not required	Not required
	Save data locally	Save data to the local host.	Not required	Not required	Not required	Not required	Not required
	Acquire local data	Acquire data from the local host.	Not required	Not required	Not required	Not required	Not required

Legend:

Admin: JP1\_Console\_Admin

Operator: JP1\_Console\_Operator

User: JP1\_Console\_User

Y: Can perform the operation.

--: Cannot perform the operation.

Not required: Any user who can log in to the OS can perform the operation.

### E.3 Operating permissions required for IM Configuration Management

The following table describes the operating permissions required for IM Configuration Management.

*Table E-6: Operating permissions required for IM Configuration Management*

Type of operation			JP1 permission level		
Category	Operation	Description	Admin	Manager	User
Host management	Register hosts	Register managed hosts (JP1/Base hosts or VMM hosts) with IM Configuration Management.	Y	Y	--
	Collect host information	Collect and store host and product information from managed hosts.	Y	Y	--
	Edit host information	Edit host and product information in a host list	Y	Y	--
	Delete hosts	Delete hosts from a host list.	Y	Y	--
	View hosts	View a list of registered hosts.	Y	Y	Y
IM configuration	Collect	Collect IM configuration information.	Y	Y	--
	Display	Display IM configuration information.	Y	Y	Y
	Edit information and acquire exclusive rights	Edit IM configuration information and acquire exclusive rights.	Y	--	--
	Apply	Apply edited IM configuration information to the system.	Y	--	--

Type of operation			JP1 permission level		
Category	Operation	Description	Admin	Manager	User
Profiles	Collect	Collect valid configuration information and configuration file contents from agents (JP1/Base).	Y	Y	--
	Display	Display valid configuration information and configuration file contents for each host in the profile list.	Y	Y	Y
	Edit information and acquire exclusive rights	Edit configuration files for each host in the profile list and acquire exclusive rights.	Y	Y	--
	Apply	Apply edited configuration file contents to the system.	Y	Y	--
	List	View a list of information about registered profiles.	Y	Y	Y
Services	Status display	View the activity status of services on an agent (JP1/Base).	Y	Y	Y
Release of exclusive rights	IM configuration	Clear update rights set for an IM configuration.	Y	--	--
	Profiles	Clear exclusive rights set for a profile.	Y	Y	--

## Legend:

Admin: JP1\_CF\_Admin

Manager: JP1\_CF\_Manager

User: JP1\_CF\_User

Y: Can perform the operation.

--: Cannot perform the operation.

## F. Support for Changing Communication Settings

In JP1/Base, which is the prerequisite program for JP1/IM - Manager, the communication settings can be changed to support a variety of network configurations. This allows you to use JP1/IM - Manager even in network configurations that have special requirements, such as the following:

- Specific communication network

The JP1/IM - Manager and JP1/Base hosts are connected to multiple LANs, but you require them to communicate over a specific LAN only (using IP addresses other than those associated with the host names).

- Separate network

The JP1/IM - Manager and JP1/Base hosts are connected to multiple LANs, but you do not want them to communicate across LANs (they cannot communicate using the IP address associated with the destination host name).

To change the communication settings, use the JP1/Base `jp1hosts` definition file and communication protocol settings file. For details on communication settings, see the description of JP1/Base communication settings for various network configurations in the *Job Management Partner 1/Base User's Guide*.

The following table describes the communication settings that can be entered in these two files for the functionality provided by JP1/IM - Manager and JP1/Base.

*Table F-1: JP1/IM functions and support for communication settings (for viewer-manager communication)*

Function	Communication setting	
	jp1hosts definition file	Communication protocol settings file
Command execution (JP1/IM - View -> JP1/Base)	Y	Y
Event monitoring (JP1/IM - View -> JP1/IM - Manager (JP1/IM - Central Console))	Y	Y
Object status monitoring (JP1/IM - View -> JP1/IM - Manager (JP1/IM - Central Scope))	Y	Y
IM Configuration Management (JP1/IM - View -> JP1/IM - Manager (IM Configuration Management))	Y	Y

Function	Communication setting	
	jp1hosts definition file	Communication protocol settings file
Rule management (JP1/IM - View -> JP1/IM - Rule Operation)	Y	Y

Legend:

Y: The communication setting can be changed, allowing JP1/IM - Manager to be used in a network configuration with special requirements.

(*product* -> *product*): Required product-to-product connection.

Table F-2: JP1/IM functions and support for communication settings (for manager-agent communication)

Function	Communication setting	
	jp1hosts definition file	Communication protocol settings file
Configuration management (JP1/Base -> JP1/Base)	Y	Y
Command execution (JP1/Base -> JP1/Base)	Y	Y
Event search (JP1/IM - Manager -> JP1/Base)	N	N
Definition collection and distribution (JP1/Base -> JP1/Base)	Y	Y
IM Configuration Management (JP1/IM - Manager -> JP1/Base)	Y	Y

Legend:

Y: The communication setting can be changed, allowing JP1/IM - Manager to be used in a network configuration with special requirements.

N: It may not be possible to use JP1/IM - Manager in a network configuration with special requirements even if the communication settings are changed.

(*product* -> *product*): Required product-to-product connection.



---

## G. Regular Expressions

---

In JP1/IM, regular expressions can be used in various conditional expressions, such as an execution condition for an automated action or a search condition for finding JP1 events or monitoring nodes. (A *regular expression* is a means of representing a particular character string by the use of a special character when performing a search or replacing text.) Care is required, however, as the regular expressions you can use in JP1/IM depend on your operating system and the particular JP1/IM function in which the regular expression is used.

This appendix describes regular expressions under the following headings:

- Types of regular expressions
- Syntax of regular expressions
- Comparison between types of regular expressions
- Tips on using regular expressions
- Examples of using regular expressions

### G.1 Types of regular expressions

The regular expressions available in JP1/IM differ according to the operating system and the function in which the regular expression is interpreted. This is because the various JP1/IM functions and operating systems support different types of regular expressions. These differences mean differences in the syntax of the available regular expressions. For details, see *G.2 Syntax of regular expressions*.

The types of regular expressions are as follows:

#### JP1-specific regular expressions (Windows)

Special characters that can be used as regular expressions, defined specifically in JP1.

You can change the JP1/IM and JP1/Base settings to operate with XPG4-compliant extended regular expressions, but this may result in unintended behavior. You should therefore review the defined conditional expressions and redefine them to comply with the extended regular expressions.

#### XPG4-compliant extended regular expressions (Windows)

Regular expressions (special characters) additional to the preset JP1-specific regular expressions.

Functions in which the use of regular expressions is supported from version 7 operate according to the syntax of these regular expressions.

## XPG4 basic regular expressions (HP-UX, Solaris, AIX)

XPG4 basic regular expressions provided by UNIX (for details, see the OS *regex(5)*).

Care is required as the range of basic regular expressions you can use is dependent on the computer model and OS.

You can change the JP1/Base settings to operate with XPG4-compliant extended regular expressions, but this may result in unintended behavior. You should therefore review the existing settings and redefine them to comply with the extended regular expressions.

## XPG4 extended regular expressions (HP-UX, Solaris, AIX)

XPG4 extended regular expressions provided by UNIX (for details, see the OS *regex(5)*). These are basically XPG4 basic regular expressions plus a number of additional regular expressions (special characters), but with some XPG4 basic regular expressions deleted.

Care is required as the range of extended regular expressions you can use is dependent on the computer model and OS.

The table below describes the functions in which regular expressions can be used and the types of regular expressions that each function supports.

*Table G-1:* Regular expressions that can be used in JP1/IM functions

Function	Description	Windows		HP-UX, Solaris, AIX	
		Default	Can be set	Default	Can be set
Search for events from JP1/IM - View	Regular expressions can be used in JP1 event search conditions. The types of regular expressions that can be used depend on the JP1/Base settings on the target host.	JP1-specific regular expressions	Extended regular expressions (XPG4-compliant)	Basic regular expressions (XPG4)	Extended regular expressions (XPG4)
Search for monitoring nodes from JP1/IM - View	Regular expressions can be used in monitoring node search conditions. The types of regular expressions are fixed.	Extended regular expressions (XPG4-compliant)	--	Extended regular expressions (XPG4-compliant)	--
Display event guide information	Regular expressions can be used in conditions for displaying event guide information. The types of regular expressions are fixed.	Extended regular expressions (XPG4-compliant)	--	Extended regular expressions (XPG4-compliant)	--

Function	Description	Windows		HP-UX, Solaris, AIX	
		Default	Can be set	Default	Can be set
Change monitoring node status and display guide information	Regular expressions can be used in the common conditions and individual conditions of monitoring node status change conditions, and in conditions for displaying guide information. The types of regular expressions are fixed.	Extended regular expressions (XPG4-compliant)	--	Extended regular expressions (XPG4-compliant)	--
Automated actions	Regular expressions can be used in conditions for executing automated actions. In Windows, the types of regular expressions that can be used depend on the settings in the JP1/IM - Manager that executes the automated action. (Fixed in UNIX.)	Extended regular expressions (XPG4-compliant)	JP1-specific regular expressions	Extended regular expressions (XPG4)	--
Issue correlation events	Regular expressions can be used in the event attribute specified in a correlation event generation condition. The types of regular expressions are fixed.	Extended regular expressions (XPG4-compliant)	--	Extended regular expressions (XPG4-compliant)	--
Filtering <ul style="list-style-type: none"> <li>Event receiver filter</li> <li>Severe events filter</li> <li>View filter</li> </ul>	Regular expressions can be used in conditions for displaying JP1 events in the Event Console window. The types of regular expressions are fixed in both Windows and UNIX.	Extended regular expressions (XPG4-compliant)	--	Basic regular expressions (XPG4)	--
<ul style="list-style-type: none"> <li>Event acquisition filter</li> </ul>	Regular expressions can be used in conditions for JP1 event acquisition by JP1/IM - Manager from JP1/Base on the manager. The types of regular expressions that can be used depend on the settings in JP1/Base on the manager.	JP1-specific regular expressions	Extended regular expressions (XPG4-compliant)	Basic regular expressions (XPG4)	Extended regular expressions (XPG4)

Legend:

--: Cannot be changed because extended regular expressions are used by default.

As shown above, under the default settings, the types of regular expressions used in JP1/IM differ according to the function and operating system used. You need to be

aware of these differences when using regular expressions.

If you prefer to use regular expressions transparently, you can change the settings and use extended regular expressions compliant with the XPG4 standard in Windows, or extended regular expressions according to XPG4 in UNIX. We recommend changing the settings because you can then use regular expressions without regard to OS-based or function-based differences in usage.

For details on JP1/IM settings, see *Automated action environment definition file (action.conf.update)* in 2. *Definition Files* in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.

For details on the JP1/Base functions that can use regular expressions, and the types of regular expressions used in JP1/Base, see the chapter on JP1/Base installation and setup in the *Job Management Partner 1/Base User's Guide*.

## G.2 Syntax of regular expressions

The following regular expressions can be used in JP1/IM. Use them in accordance with the coding conventions explained below.

*Note:*

We advise against using regular expressions other than those described here because the specifications differ according to the computer model and operating system. Use only the regular expressions described below.

### (1) Ordinary characters

An *ordinary character* is one that requires a complete match with itself when specified as the search target in a regular expression. The only characters not handled as ordinary characters are control codes and special characters.

### (2) Special characters

*Special characters* are the following: ^ \$ . \* + ? | ( ) { } [ ] \. These special characters are explained below.

^

The caret (^) means the first characters (match the start). The caret is a special character only when used as the first character in a regular expression. When used elsewhere, the caret is handled as an ordinary character.

When a caret is specified as a special character, lines beginning with the specified string make a match.

\$

The dollar sign (\$) means the last characters (match the end). It is a special character only when used as the last character in a regular expression. When used

elsewhere, the dollar sign is handled as an ordinary character.

When a dollar sign is specified as a special character, lines ending with the specified string make a match. When \$ and ^ are used together, lines containing only the specified string make a match.

. (period)

The period (.) means any single character.

When a period is specified as a special character, any single character makes a match.

\*

The asterisk (\*) means zero or more occurrences of the preceding character.

+

In JP1-specific regular expressions and basic regular expressions, the plus sign (+) is handled as an ordinary character.

As a special character, + means one or more occurrences of the preceding character.

?

In JP1-specific regular expressions and basic regular expressions, the question mark (?) is handled as an ordinary character.

As a special character, ? means zero or one occurrence of the preceding character.

|

In JP1-specific regular expressions and basic regular expressions, the vertical bar (|) is handled as an ordinary character.

As a special character, | means an OR condition between the regular expressions on either side. It is used in combination with the special characters ( ).

( )

In JP1-specific regular expressions and basic regular expressions, left and right parentheses are handled as ordinary characters.

As special characters, ( ) group the enclosed regular expression.

Parentheses are used to explicitly indicate to the program that the enclosed characters are a regular expression. They are mainly used with a vertical bar (|). (See *G.4 Tips on using regular expressions*.)

{ }

In JP1-specific regular expressions and basic regular expressions, curly brackets are handled as ordinary characters.

As special characters, { } mean that the preceding character occurs repeatedly for the number of times specified inside the curly brackets.

[ ]

In JP1-specific regular expressions and basic XPG4 regular expressions, square brackets are handled as ordinary characters.

As special characters, [ ] mean a match with any of the characters enclosed in the square brackets (or with any character *not* enclosed if a caret (^) is the first character).

\

The backslash (\) cancels a special character (^ \$ . \* + ? | ( ) { } [ ] \).<sup>#</sup>

A special character preceded by a backslash is handled as an ordinary character. Use the backslash only to cancel a special character. You can sometimes use an alphanumeric character as a regular expression indicating a control code (linefeed code or tab character, for example) by prefixing it with a backslash. However, this can lead to unintended behavior as the regular expression will be handled differently according to the operating system and product.

#

In JP1-specific regular expressions and basic XPG4 regular expressions, the following are handled as ordinary characters: + ? | ( ) { } [ ]

### G.3 Comparison between types of regular expressions

The table below describes the differences in the types of regular expressions that can be used in Windows and other operating systems.

Table G-2: Comparison between types of regular expressions

Expression	Meaning	Windows		HP-UX, Solaris, AIX	
		JP1	Extd XPG4	Basic	Extd
<i>String</i>	Matches lines containing the specified string.	Y	Y	Y	Y
<i>^string</i>	Matches the specified string at the beginning of a line.	Y	Y	Y	Y
<i>string\$</i>	Matches the specified string at the end of a line.	Y	Y	Y	Y
<i>^string\$</i>	Combination of ^ and \$. Matches lines containing only the specified string.	Y	Y	Y	Y
<i>^\$</i>	Combination of ^ and \$. Matches empty lines.	Y	Y	Y	Y

Expression	Meaning	Windows		HP-UX, Solaris, AIX	
		JP1	Extd XPG4	Basic	Extd
<code>.</code> (period)	Matches any single character.	Y	Y	Y	Y
<code>char*</code>	Matches strings of zero or more occurrences of the preceding character.	Y	Y	Y	Y
<code>.*</code>	Combination of a period ( <code>.</code> ) and asterisk ( <code>*</code> ). Matches any character string.	Y	Y	Y	Y
<code>char+</code>	Matches strings of one or more occurrences of the preceding character.	N	Y	N	Y
<code>char?</code>	Matches strings of zero or one occurrence of the preceding character.	N	Y	N	Y
<code>regex regex</code>	Matches either regular expression.	N	Y	N	Y
<code>(regex)</code>	Groups a regular expression. Used to explicitly indicate to the program that the specified characters are a regular expression. Used mainly with a vertical bar ( <code> </code> ). (See <i>G.4 Tips on using regular expressions.</i> )	N	Y	N	Y
<code>char{n}</code>	Matches strings in which the preceding character occurs <i>n</i> times.	N	Y	N	Y
<code>char{n, }</code>	Matches strings in which the preceding character occurs at least <i>n</i> times.	N	Y	N	Y
<code>char{n, m}</code>	Matches strings in which the preceding character occurs at least <i>n</i> times but no more than <i>m</i> times.	N	Y	N	Y
<code>[string]</code>	Matches any character specified in the string enclosed in square brackets.	N	Y	N	Y
<code>[^string]</code>	Matches any character not specified in the string enclosed in square brackets.	N	Y	N	Y
<code>[char-char]</code>	Matches any character in the range, in ascending order of the character codes.	N	Y	N	Y
<code>[^char-char]</code>	Matches any character not in the specified range, in ascending order of the character codes.	N	Y	N	Y
<code>\special-char</code>	Handles the special character as an ordinary character.	N	Y	N	Y

**Legend:**

JP1: JP1-specific regular expression

Extd XPG4: XPG4-compliant extended regular expression

Basic: XPG4 basic regular expression

Extd: XPG4 extended regular expression

Y: Can be used.

N: Cannot be used.

**G.4 Tips on using regular expressions**

- To prevent unintended behavior when switching to extended regular expressions from JP1-specific regular expressions (Windows) or XPG4 basic regular expressions (HP-UX, Solaris, and AIX), you should review the existing settings and redefine them to comply with extended regular expressions.
- Control codes (linefeed codes, tab characters, and so on) may be handled differently depending on the product and operating system. For this reason, you should not include control codes in a regular expression used to specify a condition for a message.
- A period followed by an asterisk ( . \* ) matches any character. If you make frequent use of this regular expression, it may take a long time to find matches. When defining a condition to match a long message, for example, use the period-and-asterisk combination only where required in the search string.

In an environment that supports extended regular expressions, you can use the combination [ ^ ] \* instead of the period-and-asterisk combination to match non-null characters. This reduces the search time.

- The vertical bar ( | ) represents an OR condition. Note the following when using this OR condition in a regular expression:  
Because a vertical bar ( | ) has low precedence in a regular expression, you must specify the range of the OR condition explicitly; otherwise, it may work erroneously or not at all. You can specify the range of an OR condition by enclosing it in parentheses. An example of specifying the conditions for a source event server name as an OR condition is shown below.

*Example:* JP1 events issued by work or host

```
^.* .* .* .* .* (work|host) .*$
```

- Spaces before or after the vertical bar ( | ) special character are treated as characters. Do not enter a space unless you want it to be included in the OR condition.



## G.5 Examples of using regular expressions

The table below describes examples of using regular expressions.

Table G-3: Examples of using regular expressions

Expression	Meaning	String specified as a regular expression	Example pattern	Match (Y) or No match (N)
<i>string</i>	Matches lines containing the specified string.	spring	<b>spring</b> has come.	Y
			winter-summer-autumn- <b>spring</b>	Y
			----- <b>spring</b> -----	Y
^ <i>string</i>	Matches the specified string at the beginning of a line.	^spring	<b>spring</b> has come.	Y
			winter-summer-autumn-spring	N
			-----spring-----	N
<i>string</i> \$	Matches the specified string at the end of a line.	spring\$	spring has come.	N
			winter-summer-autumn- <b>spring</b>	Y
			-----spring-----	N
^ <i>string</i> \$	Matches lines containing only the specified string.	^spring\$	spring has come.	N
			winter-summer-autumn-spring	N
			<b>spring</b>	Y
			spring	N
^\$	Matches empty lines.	^\$		Y
			spring	N
. (period)	Matches any single character.	in.e	<b>winter</b> has come.	Y
			mother of <b>in</b> vention	Y
			life is <b>in</b> everything	Y
			eight nine ten	N

Expression	Meaning	String specified as a regular expression	Example pattern	Match (Y) or No match (N)
			increasing population	N
		s..ing	picnic in <b>spring</b>	Y
			<b>skiing</b> in winter	Y
[ <i>string</i> ] <sup>#1,#2</sup>	Matches any character specified in the string enclosed in square brackets.	[pr]	<b>spring</b> has come.	Y
			today is monday.	N
[ <i>char-char</i> ] <sup>#1,#2</sup>	Matches any character in the range, in ascending order of the character codes.	[a-i]	<b>spring has</b> come.	Y
[ <i>^char-char</i> ] <sup>#1,#2</sup>	Matches any character not in the specified range, in ascending order of the character codes.	[^a-i]	<b>spring</b> has come.	Y
<i>char</i> *	Matches strings of zero or more occurrences of the preceding character.	ro*m	<b>terminal</b>	Y
			cd- <b>rom</b>	Y
			living <b>room</b>	Y
		h.*n	<b>This is a pen.</b>	Y
			<b>That is an</b> apple.	Y
<i>regex regex</i> <sup>#1,#2</sup>	Matches either regular expression.	[0-9]+ apple	That is an <b>apple</b> .	Y
			spring in <b>2003</b>	Y
\special-char <sup>#1,#2</sup>	Handles the special character as an ordinary character.	o\.h	<stdio. <b>h</b> >	Y
			another man	N

Expression	Meaning	String specified as a regular expression	Example pattern	Match (Y) or No match (N)
(regex) <sup>#1,#2</sup>	Groups a regular expression. Used to explicitly indicate to the program that the specified characters are a regular expression. Used mainly with a vertical bar ( ). (See <i>G.4 Tips on using regular expressions</i> .)	i (n . e   ng)	winter has come.	Y
			interesting book	Y

## Legend:

Bold type: String matching the specified regular expression.

Y: The example pattern is a match.

N: The example pattern is not a match.

#1: Cannot be specified as a JP1-specific regular expression.

#2: Cannot be specified as a basic XPG4 regular expression.

## H. Connectivity with Previous Versions

This appendix describes restrictions when connecting different versions of JP1/IM products or different versions of JP1/Base on agents.

### H.1 Connectivity with version 8 products

#### (1) Restrictions on connecting to JP1/IM - Manager 08-01 from JP1/IM - View 09-00 (when using the Central Console)

*Table H-1:* Restrictions on connecting to JP1/IM - Manager 08-01 from JP1/IM - View 09-00 (when using the Central Console)

JP1/IM - Manager version	Restrictions <sup>#</sup>
	1 to 8
08-01	Y

Legend:

Y: Applicable

#: The restriction numbers correspond to the numbers in the following table.

*Table H-2:* List of restrictions

No.	Details
1	<p>You cannot specify exclusion conditions in the following windows (the <b>Exclusion-conditions group</b> area is unavailable):</p> <ul style="list-style-type: none"> <li>• Settings for View Filter window</li> <li>• Severe Event Definitions window</li> <li>• Detailed Settings for Event Receiver Filter window</li> <li>• Event Search Conditions window</li> <li>• Event Acquisition Settings window</li> </ul> <p>You cannot specify common exclusion conditions in the following windows (the <b>Common exclusion-conditions groups</b> area is unavailable):</p> <ul style="list-style-type: none"> <li>• System Environment Settings window</li> <li>• Event Acquisition Conditions List window</li> </ul>
2	The <b>event display start-time specification</b> area does not appear on the <b>Monitor Events</b> and <b>Severe Events</b> pages.
3	The <b>Display range:</b> area does not appear on the <b>Monitor Events</b> and <b>Severe Events</b> pages.

No.	Details
4	The following items related to the specified display event period feature do not appear: <ul style="list-style-type: none"> <li>• <b>Use specified display event period</b> check box on the <b>Monitor Events</b> page</li> <li>• <b>Use specified display event period</b> check box on the <b>Severe Events</b> page</li> <li>• <b>Use specified display event period</b> menu in the Event Console window</li> <li>• <b>Specified display event period</b> area in the Preferences window</li> </ul>
5	<ul style="list-style-type: none"> <li>• The Action Parameter Detailed Definitions window (for compatibility) is displayed instead of the Action Parameter Detailed Definitions window.</li> <li>• Action names are not displayed in the Action Parameter Definition window.</li> </ul>
6	<ul style="list-style-type: none"> <li>• You cannot view or set memo entries.</li> <li>• <b>Memo</b> does not appear in the <b>Display items &amp; order</b> area of the Preferences window.</li> <li>• The <b>Memo</b> area does not appear in the Event Details window.</li> <li>• You cannot set memo entries in the Settings for View Filter window.</li> <li>• You cannot set memo entries in the Event Search Conditions window.</li> </ul>
7	You cannot specify a response status in the following windows: <ul style="list-style-type: none"> <li>• Settings for View Filter window</li> <li>• Event Search Conditions window</li> </ul>
8	Correlation failure events are displayed as correlation approval events in the following windows: <ul style="list-style-type: none"> <li>• Event Console window</li> <li>• Related Events window</li> </ul>

**(2) Restrictions on connecting to JP1/IM - Manager 08-01 from JP1/IM - View 09-00 (when using the Central Scope)**

*Table H-3:* Restrictions on connecting to JP1/IM - Manager 08-01 from JP1/IM - View 09-00 (when using the Central Scope)

JP1/IM - Manager version	Restrictions <sup>#</sup>
	1 to 2
08-01	Y

Legend:

Y: Applicable

<sup>#</sup>: The restriction numbers correspond to the numbers in the following table.

Table H-4: List of restrictions

No.	Details
1	<ul style="list-style-type: none"> <li>The <b>Visual Icon display</b> option is unavailable in the <b>View</b> menu of the Monitoring Tree window.</li> <li>The <b>Visual Icon display</b> option is unavailable in the <b>Options</b> menu of the Monitoring Tree (editing) window.</li> <li>You cannot set Visual Icon on the <b>General</b> page of the Properties window.</li> </ul>
2	<p>The following restrictions apply:</p> <ul style="list-style-type: none"> <li>When creating a monitoring object, you cannot select the system-monitoring objects <i>Node Monitoring (NNMi)</i> and <i>NNMi Monitoring</i> added in version 09-00. These system-monitoring objects will not appear in the <b>Monitoring node type</b> drop-down list in the Create New Monitoring Node window.</li> <li>You cannot use common conditions associated with system-monitoring objects (NNMi) added in version 09-00. These common conditions will not appear in the <b>Common Condition Settings</b> area in the Common Condition Settings window.</li> <li>You cannot use the <i>Agent Monitoring (PFM)</i> system-monitoring object or associated common conditions to monitor JP1/PFM system events.</li> </ul>

**(3) Restrictions on connecting to JP1/IM - Manager 08-01 from JP1/IM - View 09-00 (when using IM Configuration Management)**

Table H-5: Restrictions on connecting to JP1/IM - Manager 08-01 from JP1/IM - View 09-00 (when using IM Configuration Management)

JP1/IM - Manager version	Restrictions <sup>#</sup>
	<b>1</b>
08-01	Y

Legend:

Y: Applicable

<sup>#</sup>: The restriction numbers correspond to the numbers in the following table.

Table H-6: List of restrictions

No.	Details
1	You cannot connect to JP1/IM - Manager from IM Configuration Management - View.

**(4) Restrictions on connecting to JP1/IM - Manager 09-00 from JP1/IM - View 08-01 (when using the Central Console)**

*Table H-7: Restrictions on connecting to JP1/IM - Manager 09-00 from JP1/IM - View 08-01 (when using the Central Console)*

JP1/IM - View version	Restrictions <sup>#</sup>
	1 to 10
08-01	Y

Legend:

Y: Applicable

<sup>#</sup>: The restriction number corresponds to the number in the following table.

*Table H-8: List of restrictions*

No.	Details
1	The <b>Edit</b> menu does not appear in the Event Console window.
2	<ul style="list-style-type: none"> <li>You cannot display or modify the following filters if exclusion conditions are set for the filter: <ul style="list-style-type: none"> <li>- Event acquisition filter</li> <li>- Event receiver filter</li> <li>- Severe event filter</li> </ul> </li> <li>You cannot display or modify an event acquisition filter if common exclusion conditions are set for the filter.</li> </ul>
3	The <b>event display start-time specification</b> area does not appear on the <b>Monitor Events</b> and <b>Severe Events</b> pages.
4	The <b>Display range:</b> area does not appear on the <b>Monitor Events</b> and <b>Severe Events</b> pages.
5	The following items related to the specified display event period feature do not appear: <ul style="list-style-type: none"> <li><b>Use specified display event period</b> check box on the <b>Monitor Events</b> page</li> <li><b>Use specified display event period</b> check box on the <b>Severe Events</b> page</li> <li><b>Use specified display event period</b> menu in the Event Console window</li> <li><b>Specified display event period</b> area in the Preferences window</li> </ul>
6	The following restrictions apply when using an action definition file from version 08-01 or earlier of JP1/IM - Manager: <ul style="list-style-type: none"> <li>The Action Parameter Detailed Definitions window from version 08-01 is displayed.</li> <li>Action names are not displayed in the Action Parameter Definition window.</li> </ul>
7	The following restriction applies when using an action definition file from version 09-00 of JP1/IM - Manager: <ul style="list-style-type: none"> <li>You cannot display the Action Parameter Detailed Definitions window.</li> </ul>

No.	Details
8	<ul style="list-style-type: none"> <li>You cannot view or set memo entries.</li> <li><b>Memo</b> does not appear in the <b>Display items &amp; order</b> area of the Preferences window.</li> <li>The <b>Memo</b> area does not appear in the Event Details window.</li> <li>You cannot set memo entries in the Settings for View Filter window.</li> <li>You cannot set memo entries in the Event Search Conditions window.</li> </ul>
9	You cannot specify a response status in the following windows: <ul style="list-style-type: none"> <li>Settings for View Filter window</li> <li>Event Search Conditions window</li> </ul>
10	Correlation failure events are displayed as correlation approval events in the following windows: <ul style="list-style-type: none"> <li>Event Console window</li> <li>Related Events window</li> </ul>

**(5) Restrictions on connecting to JP1/IM - Manager 09-00 from JP1/IM - View 08-01 (when using the Central Scope)**

*Table H-9:* Restrictions on connecting to JP1/IM - Manager 09-00 from JP1/IM - View 08-01 (when using the Central Scope)

JP1/IM - View version	Restrictions <sup>#</sup>
	1 to 3
08-01	Y

Legend:

Y: Applicable

<sup>#</sup>: The restriction numbers correspond to the numbers in the following table.

*Table H-10:* List of restrictions

No.	Details
1	The following restriction applies to the Monitoring Tree window: <ul style="list-style-type: none"> <li>All login users operate under the JP1_Console_User permission (for details on the range of operations available to users with JP1_Console_User permission, see <i>E.2 Operating permissions required for system monitoring using the Central Scope</i>).</li> </ul>



No.	Details
2	<p>Restrictions apply when using the Monitoring Tree (Editing) window and the Visual Monitoring (Editing) window<sup>#</sup>.</p> <p>Because you cannot log in to the server, the following operations are unavailable:</p> <ul style="list-style-type: none"> <li>• Auto-generate a monitoring tree.</li> <li>• Acquire existing monitoring tree settings from the server.</li> <li>• Apply the edited monitoring tree settings to the server.</li> <li>• Acquire the existing settings of the Visual Monitoring window from the server.</li> <li>• Apply the settings edited in the Visual Monitoring window to the server.</li> <li>• Acquire the latest data for the common condition of a status change condition.</li> </ul>
3	<p>The following restriction applies to the Monitoring Tree window:</p> <ul style="list-style-type: none"> <li>• The icon and monitoring node type are not displayed for the system-monitoring object (NNMi).</li> </ul>

<sup>#</sup>: For details on dealing with these restrictions, see 9.5(10) *Actions to take when an earlier version of JP1/IM - Central Scope or JP1/IM - View is being used in the Job Management Partner 1/Integrated Management - Manager Administration Guide.*

**(6) Restrictions on connecting to JP1/IM - Manager 09-00 from JP1/IM - View 08-01 (when using IM Configuration Management)**

*Table H-11: Restrictions on connecting to JP1/IM - Manager 09-00 from JP1/IM - View 08-01 (when using IM Configuration Management)*

JP1/IM - Manager version	Restrictions <sup>#</sup>
	1
08-01	Y

Legend:

Y: Applicable

<sup>#</sup>: The restriction number corresponds to the number in the following table.

*Table H-12: List of restrictions*

No.	Details
1	You cannot connect to IM Configuration Management.

## H.2 Connectivity with version 7 products

### (1) Restrictions on connecting to JP1/IM - Central Console 07-00 or 07-01 from JP1/IM - View 09-00

Table H-13: Restrictions on connecting to JP1/IM - Central Console 07-00 or 07-01 from JP1/IM - View 09-00

JP1/IM-CC version	Restrictions <sup>#</sup>			
	1 to 5	6 to 17	18	19 to 36
07-00	Y	Y	--	Y
07-01	--	Y	--	Y

Legend:

JP1/IM-CC: JP1/IM - Central Console




Y: Applicable

--: Not applicable

<sup>#</sup>: The restriction numbers correspond to the numbers in the following table.

Table H-14: List of restrictions

No.	Details
1	A condition group cannot be specified when defining a filter.
2	You cannot set multiple view filters or use the <b>Filter name</b> list box on the <b>Monitor Events</b> page of the Event Console window.
3	The following command is unavailable in the <b>View</b> menu of the Event Console window: <ul style="list-style-type: none"> <li>• <b>View List of Filters</b></li> </ul>
4	The following window cannot be accessed: <ul style="list-style-type: none"> <li>• Event Acquisition Conditions List window</li> </ul>
5	You cannot set multiple conditions separated by commas in the <b>Source host</b> , <b>User name</b> , or <b>Object name</b> box in the Event Acquisition Settings window.
6	The following commands are unavailable in the <b>View</b> menu or <b>Options</b> menu of the Event Console window: <ul style="list-style-type: none"> <li>• <b>Function-Status Notification Return</b></li> <li>• <b>Display Related Event List</b></li> </ul>
7	The <b>Summary status</b> column does not appear in the Event Console window.
8	You cannot set <b>Display most significant status</b> in the Preferences window.
9	You cannot set <b>Status monitoring</b> in the Action Parameter Definitions window.

No.	Details
10	You cannot set <b>Suppress</b> or <b>Delay monitoring</b> in the Action Parameter Detailed Definitions window.
11	You cannot perform the following operations in the Action Log window: <ul style="list-style-type: none"> <li>• View the <b>Action serial number</b> or <b>Delay</b> fields.</li> <li>• Click the <b>Cancel Action</b>, <b>Re-execute</b>, or <b>Suppress Trigger Details</b> buttons.</li> </ul>
12	You cannot perform the following operations in the Action Log Details window when opened from the Action Log window: <ul style="list-style-type: none"> <li>• View the <b>Action serial number</b>, <b>Delay</b>, <b>Starting time</b>, or <b>Inserted time</b> fields.</li> <li>• Click the <b>Cancel Action</b> or <b>Re-execute</b> button.</li> </ul>
13	You cannot perform the following operations on the <b>General</b> page of the System Environment Settings window: <ul style="list-style-type: none"> <li>• Click the <b>Editing list</b> button.</li> <li>• Select an item in the <b>Event acquisition conditions</b> drop-down list.</li> </ul>
14	You cannot set <b>Filter name</b> or <b>Filter ID</b> in the Event Acquisition Settings window.
15	You cannot perform the following operations in the Action Log Details window when opened from the List of Action Results window: <ul style="list-style-type: none"> <li>• View the <b>Action serial number</b>, <b>Event arrival time</b>, <b>Delay</b>, <b>Starting time</b>, or <b>Inserted time</b> fields.</li> <li>• Click the <b>Cancel Action</b> button.</li> </ul>
16	You cannot perform the following operations in the List of Action Results window: <ul style="list-style-type: none"> <li>• View the <b>Action serial number</b>, <b>Event arrival time</b>, or <b>Delay</b> fields.</li> <li>• Click the <b>Cancel Action</b>, <b>Suppress Trigger Details</b>, , , , or <b>Target Event Search</b> buttons.</li> </ul>
17	You cannot set an action whose parameters exceed 1,023 bytes in length in the Action Parameter Detailed Definitions window.
18	You cannot set an action whose parameters exceed 1,040 bytes in length in the Action Parameter Detailed Definitions window.
19	You cannot change the response status on the <b>Search Events</b> page of the Event Console window.
20	You cannot perform the following operations during an event search: <ul style="list-style-type: none"> <li>• Access another window.</li> <li>• Cancel the event search.</li> </ul> Search results are not listed sequentially.
21	<b>Type</b> and <b>Action type</b> do not appear in the <b>Display items &amp; order</b> area of the Preferences window.
22	You cannot set <b>Lines of execution results to display</b> in the Preferences window.

No.	Details
23	The <b>Rule Log Details</b> button does not appear in the List of Action Results window.
24	The <b>Type</b> column does not appear in the Action Log window. Also, <b>Type</b> is not shown in the <b>Log</b> area of the Action Log Details window.
25	The <b>Type</b> column does not appear in the Action Parameter Definitions window. Also, <b>Type</b> is not shown in the <b>Action Definition</b> area of the Action Parameter Detailed Definitions window.
26	The <b>Type</b> column does not appear in event listings in the Event Console window.
27	You cannot execute commands exceeding 1,024 bytes in length in the Execute Command window.
28	The <b>Rule Log Details</b> button does not appear in the following windows: <ul style="list-style-type: none"> <li>• Action Log window</li> <li>• Action Log Details window</li> </ul>
29	The <b>Type</b> column does not appear in the List of Action Results window.
30	You cannot specify exclusion conditions in the following windows (the <b>Exclusion-conditions group</b> area is unavailable): <ul style="list-style-type: none"> <li>• Settings for View Filter window</li> <li>• Severe Event Definitions window</li> <li>• Detailed Settings for Event Receiver Filter window</li> <li>• Event Search Conditions window</li> <li>• Event Acquisition Settings window</li> </ul> You cannot specify common exclusion conditions in the following windows (the <b>Common exclusion-conditions groups</b> area is unavailable): <ul style="list-style-type: none"> <li>• System Environment Settings window</li> <li>• Event Acquisition Conditions List window</li> </ul>
31	The <b>event display start-time specification</b> area does not appear on the <b>Monitor Events</b> and <b>Severe Events</b> pages.
32	The <b>Display range</b> area does not appear on the <b>Monitor Events</b> and <b>Severe Events</b> pages.
33	The following items related to the specified display event period feature do not appear: <ul style="list-style-type: none"> <li>• <b>Use specified display event period</b> check box on the <b>Monitor Events</b> page</li> <li>• <b>Use specified display event period</b> check box on the <b>Severe Events</b> page</li> <li>• <b>Use specified display event period</b> menu in the Event Console window</li> <li>• <b>Specified display event period</b> area in the Preferences window</li> </ul>
34	<ul style="list-style-type: none"> <li>• The Action Parameter Detailed Definitions window (for compatibility) is displayed instead of the Action Parameter Detailed Definitions window.</li> <li>• Action names are not displayed in the Action Parameter Definition window.</li> </ul>

No.	Details
35	<ul style="list-style-type: none"> <li>You cannot view or set memo entries.</li> <li><b>Memo</b> does not appear in the <b>Display items &amp; order</b> area of the Preferences window.</li> <li>The <b>Memo</b> area does not appear in the Event Details window.</li> <li>You cannot set memo entries in the Settings for View Filter window.</li> <li>You cannot set memo entries in the Event Search Conditions window.</li> </ul>
36	You cannot specify a response status in the following windows: <ul style="list-style-type: none"> <li>Settings for View Filter window</li> <li>Event Search Conditions window</li> </ul>

**(2) Restrictions on connecting to JP1/IM - Manager 09-00 from JP1/IM - View 07-00 or 07-01 (when using the Central Console)**

*Table H-15: Restrictions on connecting to JP1/IM - Manager 09-00 from JP1/IM - View 07-00 or 07-01 (when using the Central Console)*

JP1/IM - View versions	Restrictions <sup>#</sup>			
	1 to 6	7 to 19	20 to 22	23 to 44
07-00, 07-01	Y	Y	Y	Y




Legend:

Y: Applicable

<sup>#</sup>: The restriction numbers correspond to the numbers in the following table.

*Table H-16: List of restrictions*

No.	Details
1	You cannot select the <b>Read From Selected Event</b> option in the Event Acquisition Settings window.
2	View filters set in JP1/IM - View 08-01 or later cannot be used. <ol style="list-style-type: none"> <li>View filters View filters set in JP1/IM - View 08-01 or later cannot be used.</li> <li>Severe events filter and event receiver filter Defined filters cannot be applied to the manager.</li> <li>Event search conditions Event search conditions set in JP1/IM - View 08-01 or later cannot be used.</li> </ol>
3	You cannot set multiple view filters or use the <b>Filter name</b> list box on the <b>Monitor Events</b> page of the Event Console window.
4	You cannot set <b>Search direction</b> in the Event Search Conditions window. Also, you cannot click <b>Current Time</b> for <b>Start timeframe</b> , <b>End timeframe</b> , <b>Registered timeframe</b> , or <b>Arrived timeframe</b> .

No.	Details
5	You cannot set multiple conditions separated by commas in the <b>Source host</b> , <b>User name</b> , or <b>Object name</b> box in the Event Acquisition Settings window.
6	You cannot select <b>Regular expression</b> in the Event Acquisition Settings window.
7	The following commands are unavailable in the <b>View</b> menu and <b>Options</b> menu of the Event Console window: <ul style="list-style-type: none"> <li>• <b>Function-Status Notification Return</b></li> <li>• <b>Display Related Event List</b></li> </ul>
8	The <b>Summary status</b> column does not appear in the Event Console window.
9	You cannot open the Event Acquisition Conditions List window.
10	You cannot set <b>Display most significant status</b> in the Preferences window.
11	You cannot open the Related Events window.
12	You cannot set <b>Status monitoring</b> in the Action Parameter Definitions window.
13	You cannot set <b>Suppress</b> or <b>Delay monitoring</b> in the Action Parameter Detailed Definitions window.
14	You cannot perform the following operations in the Action Log window: <ul style="list-style-type: none"> <li>• View the <b>Action serial number</b> or <b>Delay</b> fields.</li> <li>• Click the <b>Update</b>, <b>Cancel Action</b>, <b>Suppress Trigger Details</b>, or <b>Re-execute</b> buttons.</li> </ul>
15	You cannot perform the following operations in the Action Log Details window: <ul style="list-style-type: none"> <li>• View the <b>Action serial number</b>, <b>Event arrival time</b>, <b>Delay</b>, <b>Starting time</b>, or <b>Inserted time</b> fields.</li> <li>• Click the <b>Cancel Action</b> or <b>Re-execute</b> button.</li> </ul>
16	You cannot set <b>Filter name</b> or <b>Filter ID</b> in the Event Acquisition Settings window.
17	You cannot perform the following operations on the <b>General</b> page of the System Environment Settings window: <ul style="list-style-type: none"> <li>• Click <b>Editing list</b>.</li> <li>• Select an item in the <b>Event acquisition conditions</b> drop-down list.</li> </ul>
18	You cannot define and switch between multiple event acquisition filters.
19	You cannot perform the following operations in the List of Action Results window: <ul style="list-style-type: none"> <li>• View the <b>Action serial number</b>, <b>Event arrival time</b>, or <b>Delay</b> fields.</li> <li>• Click the <b>Cancel Action</b>, <b>Suppress Trigger Details</b>, , , , or <b>Target Event Search</b> buttons.</li> </ul>
20	You cannot change the response status on the <b>Search Events</b> page of the Event Console window.

No.	Details
21	You cannot view event guide information in the Event Details window.
22	You cannot perform the following operations during an event search: <ul style="list-style-type: none"> <li>• Access another window.</li> <li>• Cancel the event search.</li> </ul> Search results are not listed sequentially.
23	You cannot display icons in the <b>Action</b> column of the Event Console window.
24	The <b>Type</b> and <b>Action type</b> columns do not appear in event listings in the Event Console window.
25	Correlation source events cannot be displayed because no window is provided for displaying them.
26	<b>Type</b> and <b>Action type</b> do not appear in the <b>Display items &amp; order</b> area of the Preferences window.
27	You cannot set <b>Lines of execution results to display</b> in the Preferences window.
28	You cannot sort the execution results displayed in the Execute Command window.
29	You cannot execute commands exceeding 1,024 bytes in length in the Execute Command window.
30	The <b>Rule Log Details</b> button does not appear in the following windows: <ul style="list-style-type: none"> <li>• Action Log window</li> <li>• Action Log Details window</li> </ul>
31	The <b>Type</b> column does not appear in the Action Log window. Also, <b>Type</b> is not shown in the <b>Log</b> area of the Action Log Details window.
32	The <b>Type</b> column does not appear in the Action Parameter Definitions window. Also, <b>Type</b> is not shown in the <b>Action Definition</b> area of the Action Parameter Detailed Definitions window.
33	You cannot specify <RULE> in the <b>Action</b> field of the Action Parameter Definitions window.
34	You cannot open the Action Parameter Definitions window when a rule startup request to JPI/IM - Rule Operation is defined in the automated action definition file (actdef.conf).
35	The <b>Rule Log Details</b> button does not appear in the List of Action Results window.
36	The <b>Type</b> column does not appear in the List of Action Results window.
37	The <b>Edit</b> menu does not appear in the Event Console window.

No.	Details
38	<p>You cannot display or modify the following filters if exclusion conditions are set for the filter:</p> <ul style="list-style-type: none"> <li>• Event acquisition filter</li> <li>• Event receiver filter</li> <li>• Severe event filter</li> </ul> <p>You cannot display or modify an event acquisition filter if common exclusion conditions are set for the filter.</p> <p>You cannot display or modify the following filters if a conditions group with an <b>Action type</b> specified is defined for the filter:</p> <ul style="list-style-type: none"> <li>• Event receiver filter</li> <li>• Severe event filter</li> </ul>
39	The <b>event display start-time specification</b> area does not appear on the <b>Monitor Events</b> and <b>Severe Events</b> pages.
40	The <b>Display range:</b> area does not appear on the <b>Monitor Events</b> and <b>Severe Events</b> pages.
41	<p>The following items related to the specified display event period feature do not appear:</p> <ul style="list-style-type: none"> <li>• <b>Use specified display event period</b> check box on the <b>Monitor Events</b> page</li> <li>• <b>Use specified display event period</b> check box on the <b>Severe Events</b> page</li> <li>• <b>Use specified display event period</b> menu in the Event Console window</li> <li>• <b>Specified display event period</b> area in the Preferences window</li> </ul>
42	<ul style="list-style-type: none"> <li>• The Action Parameter Detailed Definitions window (for compatibility) is displayed instead of the Action Parameter Detailed Definitions window.</li> <li>• Action names are not displayed in the Action Parameter Definition window.</li> </ul>
43	<ul style="list-style-type: none"> <li>• You cannot view or set memo entries.</li> <li>• <b>Memo</b> does not appear in the <b>Display items &amp; order</b> area of the Preferences window.</li> <li>• The <b>Memo</b> area does not appear in the Event Details window.</li> <li>• You cannot set memo entries in the Settings for View Filter window.</li> <li>• You cannot set memo entries in the Event Search Conditions window.</li> </ul>
44	<p>You cannot specify a response status in the following windows:</p> <ul style="list-style-type: none"> <li>• Settings for View Filter window</li> <li>• Event Search Conditions window</li> </ul>



**(3) Restrictions on connecting to JP1/IM - Manager 09-00 from JP1/IM - View 07-00 or 07-01 (when using the Central Scope)**

*Table H-17: Restrictions on connecting to JP1/IM - Manager 09-00 from JP1/IM - View 07-00 or 07-01 (when using the Central Scope)*

JP1/IM - View versions	Restrictions <sup>#</sup>
	1 to 11
07-00, 07-01	Y

Legend:

Y: Applicable

<sup>#</sup>: The restriction numbers correspond to the numbers in the following table.

*Table H-18: List of restrictions*

No.	Details
1	The following restrictions apply when using the Monitoring Tree window: <ul style="list-style-type: none"> <li>JP1/IM - View functionality is limited to that provided by version 07-00 (you cannot use map view, for example).</li> <li>When five or more status change conditions are set, only the first four are displayed.</li> <li>The <b>Condition</b> list box does not appear in the <b>Individual conditions</b> area of the Status-Change Condition Settings window.</li> </ul>
2	The following restriction applies when using the Monitoring Tree window: <ul style="list-style-type: none"> <li>All login users operate under the JP1_Console_User permission (for details on the range of operations available to users with JP1_Console_User permission, see <i>E.2 Operating permissions required for system monitoring using the Central Scope</i>).</li> </ul>
3	Restrictions apply when using the Monitoring Tree (Editing) window and the Visual Monitoring (Editing) window <sup>#</sup> . Because you cannot log in to the server, the following operations are unavailable: <ul style="list-style-type: none"> <li>Auto-generate a monitoring tree.</li> <li>Acquire existing monitoring tree settings from the server.</li> <li>Apply edited monitoring tree settings to the server.</li> <li>Acquire the existing settings of the Visual Monitoring window from the server.</li> <li>Apply the settings edited in the Visual Monitoring window to the server.</li> <li>Acquire the latest data for the common condition of a status change condition.</li> </ul>
4	The following restriction applies when using the Monitoring Tree window: <ul style="list-style-type: none"> <li>The icon and monitoring node type are not displayed for the system-monitoring object (Cosminexus) added in version 08-01.</li> </ul>
5	The following restriction applies when using the Monitoring Tree window: <ul style="list-style-type: none"> <li>The icon and monitoring node type are not displayed for the system-monitoring objects (HiRDB and System Manager) added in version 08-01.</li> </ul>

No.	Details
6	The following restrictions apply when using the Monitoring Tree window: <ul style="list-style-type: none"> <li>You cannot view or modify a status change condition set for a monitoring group. However, monitoring of the status change condition will take place.</li> <li>The icon indicating that a status change condition is set for a monitoring group is not displayed in the Monitoring Tree window.</li> </ul>
7	Monitoring range settings for monitoring trees have no effect (the JP1 resource group does not appear in the Properties window).
8	You cannot use the same event attribute name for more than one individual condition.
9	The following restrictions apply when using the same event attribute name for more than one individual condition: <ul style="list-style-type: none"> <li>When the same event attribute name is shared by more than one individual condition in a status change condition, only the first individual condition is displayed in the Monitoring Tree window.</li> <li>Access to the Monitoring Tree window is subject to view permission only. You cannot edit individual conditions or other settings.</li> <li>In the Monitoring Tree (Editing) window, you cannot specify the same event attribute name in more than one individual condition.</li> </ul>
10	The following restriction applies to the Monitoring Tree window: <ul style="list-style-type: none"> <li>Visual Icon are not displayed in the Monitoring Tree window (normal icons are displayed instead).</li> </ul>
11	The following restriction applies to the Monitoring Tree window: The icon and monitoring node type are not displayed for the system-monitoring object (NNMi).

#: For details on dealing with these restrictions, see *9.5(10) Actions to take when an earlier version of JP1/IM - Central Scope or JP1/IM - View is being used in the Job Management Partner 1/Integrated Management - Manager Administration Guide.*

### H.3 Connectivity with previous versions of JP1/Base

#### (1) Restrictions on event searches in JP1/Base 06-00 to 08-00 from JP1/IM - View 09-00

Table H-19: Restrictions on event searches in JP1/Base 06-00 to 08-00 from JP1/IM - View 09-00

JP1/Base version <sup>#1</sup>	JP1/IM-M or JP1/IM-CC version	Restrictions <sup>#2</sup>										
		1	2	3	4	5	6	7	8	9	10	11
06-00	07-00, 07-10	--	Y	--	Y	Y	Y	--	Y	Y	Y	--
	08-01 or later	--	Y	--	Y	Y	Y	--	--	--	Y	--

JP1/Base version <sup>#1</sup>	JP1/IM-M or JP1/IM-CC version	Restrictions <sup>#2</sup>										
		1	2	3	4	5	6	7	8	9	10	11
06-51	07-00, 07-01	--	--	--	Y	--	--	--	Y	Y	Y	--
	08-01 or later	--	--	--	Y	--	--	--	--	--	Y	--
06-71	07-00, 07-01	--	--	--	--	--	--	--	Y	Y	Y	--
	08-01 or later	--	--	--	--	--	--	--	--	--	Y	--
07-00 to 08-00	07-00, 07-01	--	--	--	--	--	--	--	Y	Y	Y	--
	08-01 or later	--	--	--	--	--	--	--	--	--	Y	--

Legend:

JP1/IM-M: JP1/IM - Manager (version 08-00 or later)

JP1/IM-CC: JP1/IM - Central Console

Y: Applicable

--: Not applicable

#1: Refers to the version of JP1/Base on the search target host.

#2: The restriction numbers correspond to the numbers in the following table.

Table H-20: List of restrictions

No.	Details
1	The maximum length of the conditional statements in the Event Search Conditions window and Detailed Settings for Event Receiver Filter window combined is 4 KB.
2	The maximum length of a conditional statement in the Event Search Conditions window is 4 KB.
3	The maximum length of the conditional statements in the Event Search Conditions window and Detailed Settings for Event Receiver Filter window combined is 64 KB.
4	<p><b>Regular expression</b> cannot be specified for a search.</p> <ul style="list-style-type: none"> <li>If the manager is running JP1/IM - Central Console version 06-00 to 06-51: You cannot specify <b>Regular expression</b>.</li> <li>If the manager is running JP1/IM - Central Console version 06-71 or later: If you specify <b>Regular expression</b>, message KAVB0248-E is displayed.</li> </ul>

No.	Details
5	<b>Is contained</b> or <b>Is not contained</b> cannot be specified for a search. <ul style="list-style-type: none"> <li>If the manager is running JP1/IM - Central Console version 06-00: You cannot specify <b>Is contained</b> or <b>Is not contained</b>.</li> <li>If the manager is running JP1/IM - Central Console version 06-51 or later: If you specify <b>Is contained</b> or <b>Is not contained</b>, message KAVB1527-E is displayed.</li> </ul>
6	Multiple response statuses cannot be specified in a search for <b>Severe events</b> . <ul style="list-style-type: none"> <li>If the manager is running JP1/IM - Central Console version 06-00: You cannot specify multiple response statuses in a search for <b>Severe events</b>.</li> <li>If the manager is running JP1/IM - Central Console version 06-51 or later: If you specify multiple response statuses in a search for <b>Severe events</b>, message KAVB1527-E is displayed.</li> </ul>
7	<b>Extended attribute</b> cannot be specified as a search condition.
8	A condition group cannot be specified for an event search.
9	You cannot cancel an event search while the search is in progress. Search results are not listed sequentially.
10	<b>Exclusion condition</b> cannot be specified for a search.
11	<b>Exclusion condition</b> cannot be specified for a search. <ul style="list-style-type: none"> <li>If the manager is running JP1/Base version 08-00: You cannot specify <b>Exclusion condition</b>.</li> <li>If the manager is running JP1/Base version 09-00 or later: If you specify <b>Exclusion condition</b>, message KAVB0251-E is displayed.</li> </ul>

**(2) Restrictions on managing JP1/Base 06-00 to 08-00 from JP1/IM - Manager 09-00**

Table H-21: Restrictions on managing JP1/Base 06-00 to 08-00 from JP1/IM - Manager 09-00

JP1/Base version <sup>#1</sup>	Restrictions <sup>#2</sup>			
	1	2	3	4
06-00 to 06-71	Y	--	Y	Y
07-00 to 07-51	--	Y	--	Y
08-00	--	Y	--	Y

Legend:

Y: Applicable

--: Not applicable

#1: Refers to the version of JP1/Base on the search target host.

#2: The restriction numbers correspond to the numbers in the following table.

*Table H-22: List of restrictions*

No.	Details
1	You cannot collect any information from hosts.
2	You cannot collect host information other than OS names.
3	You cannot set up event forwarding, log file trapping, or event log trapping on the managed host.
4	You cannot display or set valid configuration information for local actions.

## I. Performance and Estimation

This appendix describes the memory and disk space requirements of JP1/IM, and traffic volumes on the network.

### I.1 Memory requirements

For details on JP1/IM memory requirements, see the *Release Notes* for JP1/IM - Manager and JP1/IM - View.

### I.2 Disk space requirements

For details on JP1/IM disk space requirements, see the *Release Notes* for JP1/IM - Manager and JP1/IM - View.

### I.3 Network traffic volumes

The following describes traffic volumes generated at communication based on the Central Console and Central Scope. Traffic arising from other types of communication is minimal and is not covered in this explanation.

#### (1) Central Console traffic

The following describes the amounts of data generated during communication based on the Central Console.

##### (a) Estimated traffic volumes between JP1/IM - View and JP1/IM - Manager (JP1/IM - Central Console)

*Table I-1:* Traffic volumes between JP1/IM - View and JP1/IM - Manager (JP1/IM - Central Console)

Activity	Estimated data transferred (bytes)
Display events in the Event Console window.	$((5,000 + \{\text{average data size per event}\}^{\#1} \times 1.5) \times (\text{number of events acquired when window refreshed})^{\#2} + 2,500)$ $\times (\{\text{number of events generated since window was last refreshed}\}^{\#3} / \{\text{number of events acquired when window refreshed}\}^{\#2})$
Open the Event Search Conditions window, or click the <b>OK</b> button in the Event Search Conditions window.	Data transferred = $\{\text{total size of condition groups}\}^{\#4} + (\{\text{name of search target host}\} \times 1.5)$ $\{\text{condition group}\} = (400 \text{ bytes} + \{\text{total of attribute values specified for the condition group}\} + (\{\text{condition group name}\} \times 1.5))$
Perform an event search.	$((5,000 + \{\text{average data size per event}\}^{\#1} \times 1.5) \times (\text{number of events acquired when window refreshed})^{\#2} + 2,500)$ $\times (\{\text{number of retrieved events}\}^{\#5} / \{\text{number of events acquired when window refreshed}\}^{\#2})$

Activity	Estimated data transferred (bytes)
Open the Event Details window.	20,000 + {total byte size of the attribute names defined in the definition file for the extended event attributes for the event in question} x 1.5 + {average data size per event} <sup>#1</sup> x 1.5 + {length of event-guide messages (max. 409,600)}
Open the System Environment Settings window, or click the <b>Apply</b> button in the System Environment Settings window.	Data transferred = {total event acquisition filter data} + {data of active event acquisition filters} + {data of common exclusion condition groups} + 1,200  {event acquisition filter data} = {total size of condition groups} <sup>#4</sup> + ({length of event acquisition filter name} x 1.5) {condition group} = (400 bytes + {total of attribute values specified for the condition group} + ({condition group name} x 1.5)) {common exclusion condition groups} = (400 bytes + {total of attribute values specified for common exclusion condition groups} + ({condition group name} x 1.5))
Open the Settings for Event Receiver Filter window, or click the <b>Apply</b> button in the Settings for Event Receiver Filter window.	Data transferred = {total event receiver filter data}  {event receiver filter data} = {total size of condition groups} <sup>#4</sup> + ({length of event receiver filter name} x 1.5) + ({user names associated with filter} x 1.5) {condition group} = (410 bytes + {total of attribute values specified for the condition group} + ({condition group name} x 1.5))
Open the Severe Event Definitions window, or click the <b>OK</b> button in the Severe Event Definitions window.	Data transferred = {total size of condition groups} <sup>#4</sup> {condition group} = (400 bytes + {total of attribute values specified for the condition group} + ({condition group name} x 1.5))
Click the <b>OK</b> button in the Settings for View Filter window, or click the <b>OK</b> button in the View List of Filters window.	Data transferred = {total size of view filters}  {view filter} = {total size of condition groups} <sup>#4</sup> + ({view filter names} x 1.5) {condition group} = (400 bytes + {total of attribute values specified for the condition group} + ({condition group name} x 1.5))
Apply the settings in the Preferences window.	6,000
Open the Action Parameter Definitions window.	1,750 + ({byte size of one action definition} + 140) x (number of action definitions)
Click the <b>Apply</b> button in the Action Parameter Definitions window.	3,200 + ( ({byte size of one action definition} + 140) x (number of action definitions) ) x 2
Open the Action Log window.	2,400 + ({byte size of the action command} + {length of the messages displayed in the Action Log Details window})

Activity	Estimated data transferred (bytes)
Open the List of Action Results window.	1,850 + (500 + {byte size of the action command} + {length of the messages displayed in the Action Log Details window}) x (number of displayed actions)
Click the <b>OK</b> button in the Conditions for Updating List of Action Results window, or close the List of Action Results window.	1,600

## #1: Example of calculating the average data size per event

To find the average data size per event:

1. Using the `jevexport` command, output all the events generated during a set period of time to a CSV file. For details on the `jevexport` command, see the *Job Management Partner 1/Base User's Guide*.
2. Find the total number of bytes in the output CSV file.
3. Divide the total byte count by the number of generated events.

If events that generate data greater than the average size are output in close succession, the above estimation may be exceeded.

#2: This is the value set in **Num. of events to acquire at update** in the Preferences window. The default is 20 events.

#3: Find the number of events issued since window was last refreshed using the equation given below.

#4: A *condition group* is a pass condition group or exclusion condition group.

#5: This is the value set in **Num. of events to acquire in 1 search** in the Preferences window. The default is 20 events.

Equation for {number of events generated since window was last refreshed}

- When **Apply** is set for **Automatic refresh** in the Preferences window:

Number of events generated since window was last refreshed =

{value set in **Interval** (default 5 sec.)}

x {number of events generated per second}

- When **Do not apply** is set for **Automatic refresh** in the Preferences window:

Number of events generated since window was last refreshed =

{interval at which user refreshes Event Console (sec.)}

x {number of events generated per second}



**(b) Estimated traffic volumes between JP1/IM - View and JP1/Base (manager)**

*Table I-2: Traffic volumes between JP1/IM - View and JP1/Base (manager)*

Activity	Estimated data transferred (bytes)
Execute a command from the Execute Command window.	$(928 + \{\text{command length}\}) \times (4^{\#} + \{\text{number of lines in the execution result}\})$

#: The number increases if a warning message (KAVB2xxx-W) is output about the command execution, but this is an exceptional case and is not counted in the estimate.

**(c) Estimated traffic volumes between JP1/IM - Manager (JP1/IM - Central Console) and JP1/Base**

*Table I-3: Traffic volumes between JP1/IM - Manager (JP1/IM - Central Console) and JP1/Base*

Activity	Estimated data transferred (bytes)
Execute a command in an automated action (data relayed between JP1/IM - Manager (JP1/IM - Central Console) and JP1/Base on the same host).	$(5,024 \times 4^{\#1})^{\#2}$
Click <b>Event Search Conditions</b> on the <b>Search Events</b> page to search for events (data relayed between JP1/IM - Manager (JP1/IM - Central Console) and JP1/Base on the target host).	$140^{\#3} + (600^{\#4} \times \{\text{number of JP1 events matching the search conditions}\})$

#1: The number increases if a warning message (KAVB2xxx-W) is output about the command execution, but this is an exceptional case and is not counted in the estimate.

#2: Maximum amount of data for one automated action request issued to JP1/Base 08-00 or later.

#3: Amount of data when the name of the destination event server is 16 bytes and the event ID is the only search condition.

#4: Data size of the JP1 event issued when a character string of about 100 bytes is trapped by the log file trapping function.

**(d) Estimated traffic volumes between JP1/Base and JP1/Base***Table I-4: Traffic volumes between JP1/Base and JP1/Base*

Activity	Estimated data transferred (bytes)
Execute a command from the Execute Command window or execute a command in an automated action (data relayed among JP1/Base that received the request, JP1/Base on the relay host, and JP1/Base on the target host).	$5,540^{\#1} + (1,700 \times (3^{\#2} + \{\text{number of lines in the execution result}\}))^{\#3}$

#1: Maximum amount of data for a command execution request.

#2: The number increases if a warning message (KAVB2xxx-W) is output about the command execution, but this is an exceptional case and is not counted in the estimate.

#3: Maximum amount of data in the command execution result. You can adjust the amount of data using the `jccomddef` command. For details on this command, see the chapter on commands in the *Job Management Partner 1/Base User's Guide*.

**(2) Central Scope traffic**

The following describes the amounts of data generated during communication based on the Central Scope.

**(a) Estimated traffic volumes between JP1/IM - View and JP1/IM - Manager (JP1/IM - Central Scope)***Table I-5: Traffic volumes between JP1/IM - View and JP1/IM - Manager (JP1/IM - Central Scope)*

Activity	Estimated data transferred (bytes)
Update of the data being monitored in the Visual Monitoring window since the last poll (where polling takes place at 5-second intervals).	500 + (number of nodes) x 40
Change in the status or monitoring status of nodes being monitored in the Monitoring Tree window since the last poll (where polling takes place at 5-second intervals).	64 + (number of nodes whose status or monitoring status has changed since the last poll) x 20

Activity	Estimated data transferred (bytes)
Update of the tree configuration information of JP1/IM - Manager (JP1/IM - Central Scope) since the last poll, during monitoring from the Monitoring Tree window (where polling takes place at 5-second intervals).	Sum of the data amount for each monitoring object <sup>#1</sup> + sum of the data amount for each monitoring group <sup>#2</sup> + sum of the data amount for each common condition <sup>#3</sup>
Display the Guide window by choosing <b>View</b> and then <b>Guide</b> in the Monitoring Tree window, or by choosing <b>Guide</b> from the pop-up menu in the Visual Monitoring window.	1,400 + size of the guide-message
Search for status change events by choosing <b>View</b> and then <b>Search Status-Change Events</b> in the Monitoring Tree window.	90 x number of status change events for the selected monitoring node
Add or change a common condition in the Common Condition Detailed Settings window. Note that no communication is entailed when the Common Condition Detailed Settings window is opened from the Monitoring Tree (Editing) window.	100 + data amount for the common condition <sup>#3</sup>
Apply tree configuration information to JP1/IM - Manager (JP1/IM - Central Scope) by choosing <b>File</b> and then <b>Update Server Tree</b> in the Monitoring Tree (Editing) window.	100 + sum of the data amount for each monitoring object <sup>#1</sup> + sum of the data amount for each monitoring group <sup>#2</sup> + sum of the data amount for each common condition <sup>#3</sup>
Acquire all common conditions from JP1/IM - Manager (JP1/IM - Central Scope) by choosing <b>Options</b> and then <b>Acquire Latest Definition</b> in the Monitoring Tree (Editing) window.	100 + sum of the data amount for each common condition <sup>#3</sup>

Activity	Estimated data transferred (bytes)
Apply visual monitoring data to JP1/IM - Manager (JP1/IM - Central Scope) by clicking the <b>Update the Visual Monitoring Data of Server</b> button in the Visual Monitoring (Editing) window.	500 + (number of nodes) x 40

#1: Data amount for each monitoring object =

$$\begin{aligned}
&200 + \{\text{length of monitoring node name}\} + \{\text{length of icon file name (when sent)}\} \\
&+ \{\text{length of icon file name (when expanded)}\} + \{\text{length of background image file name}\} \\
&+ \{\text{sum of attribute name lengths}\} + \{\text{sum of attribute value lengths}\} \\
&+ \{\text{sum of individual condition attribute name lengths}\} \\
&+ \{\text{sum of individual condition attribute name values}\} \\
&+ \{\text{sum of lengths of status change condition names in monitoring group}\}
\end{aligned}$$

#2: Data amount for each monitoring group =

$$\begin{aligned}
&200 + \{\text{length of monitoring node name}\} + \{\text{length of icon file name (when sent)}\} \\
&+ \{\text{length of icon file name (when expanded)}\} + \{\text{length of background image file name}\} \\
&+ \{\text{sum of attribute name lengths}\} + \{\text{sum of attribute value lengths}\} \\
&+ \{\text{sum of lengths of status change condition names in monitoring group}\} \\
&+ \{\text{number of status change conditions in monitoring group}\} \times 40
\end{aligned}$$

#3: Data amount for each common condition =

$$\begin{aligned}
&250 + \{\text{length of common condition name}\} + 10 \times \{\text{number of specified event levels}\} \\
&+ \{\text{sum of lengths of source event server names}\} + \{\text{length of object type}\} \\
&+ \{\text{sum of lengths of object names}\} + \{\text{length of root object name}\} \\
&+ \{\text{length of occurrence name}\} + \{\text{sum of user name lengths}\} + \{\text{message length}\} \\
&+ \{\text{product name length}\} + \{\text{event ID}\} \times 10 \\
&+ \{\text{sum of lengths of extended attribute names}\} \\
&+ \{\text{sum of lengths of extended attribute values}\}
\end{aligned}$$

**(b) Estimated traffic volumes between JP1/IM - Manager (JP1/IM - Central Scope) and JP1/Base on a managed host**

*Table I-6: Traffic volumes between JP1/IM - Manager (JP1/IM - Central Scope) and JP1/Base on a managed host*

Activity	Estimated data transferred (bytes)
Select the <b>Generate</b> , <b>Show Differences</b> , or <b>Add</b> button in the Auto-generation - Select Configuration window.	For work-oriented or server-oriented trees: JP1/AJS data amounts <sup>#</sup> + JP1/PFM data amounts <sup>#</sup> + Cosminexus data amounts <sup>#</sup>

<sup>#</sup>: Estimate these data amounts using the tables below.

■ Estimating JP1/AJS data amounts

*Table I-7: JP1/AJS data amounts*

Equation	Item	Estimated data transferred for each item (bytes)
200 + sum of <i>a</i> + sum of <i>b</i> + sum of <i>c</i> + sum of <i>d</i>	<i>a</i> : Scheduler service	10 + length of the scheduler service name + length of the character code
	<i>b</i> : Job group	20 + length of the scheduler service name + length of the full name of the unit + length of the job group name + length of the comment name
	<i>c</i> : Root jobnet	20 + length of the scheduler service name + length of the full name of the unit + length of the jobnet name + length of the comment name
	<i>d</i> : Execution agent	10 + length of the scheduler service name + length of the root jobnet path + length of the job execution agent name

■ Estimating JP1/PFM data amounts

Table I-8: JP1/PFM data amounts

Equation	Item	Estimated data transferred for each item (bytes)
200 + sum of $e$	$e$ : Service	310 + length of host name + length of instance name

## ■ Estimating Cosminexus data amounts

Table I-9: Cosminexus data amounts

Equation	Item	Estimated data transferred for each item (bytes)
200 + sum of $h$ + sum of $i$  + sum of $j$ + sum of $k$ + sum of $l$ + sum of $m$  + sum of $n$ + sum of $o$ + sum of $p$ + sum of $q$ + sum of $r$ + sum of $s$ + sum of $t$ + sum of $u$ + sum of $v$	$h$ : Operations management domain	10 + length of operations management domain name + length of operations management domain display name
	$i$ : Host	10 + length of operations management domain name + length of the name or IP address of the operations management agent machine + length of host display name
	$j$ : Logical J2EE server	320 + length of operations management domain name + length of logical server name x 7 + length of host name + length of logical server display name + length of logical server name of the logical naming service being used + length of logical server name of the logical OTS being used + length of logical server name of the logical CTM being used + length of logical server name of the logical TCS being used + length of logical server name of the logical performance tracer being used + length of logical server name of the logical SFO being used

Equation	Item	Estimated data transferred for each item (bytes)
	<i>k</i> : Logical naming service	70 + length of operations management domain name + length of logical server name + length of host name + length of logical server display name + length of logical server name of the logical smart agent being used
	<i>l</i> : Logical smart agent	20 + length of operations management domain name + length of logical server name + length of host name + length of logical server display name
	<i>m</i> : Logical OTS	70 + length of operations management domain name + length of logical server name + length of host name + length of logical server display name + length of logical server name of the logical smart agent being used
	<i>n</i> : Logical TCS	70 + length of operations management domain name + length of logical server name + length of host name + length of logical server display name + length of logical server name of the logical TCS being used
	<i>o</i> : Logical CTM domain manager	120 + length of operations management domain name + length of logical server name + length of host name + length of logical server display name + length of logical server name of the logical smart agent being used + length of logical server name of the logical performance tracer being used
	<i>p</i> : Logical CTM	70 + length of operations management domain name + length of logical server name + length of host name + length of logical server display name + length of logical server name of the logical CTM domain manager being used

Equation	Item	Estimated data transferred for each item (bytes)
	<i>q</i> : Logical performance tracer	20 + length of operations management domain name + length of logical server name + length of host name + length of logical server display name
	<i>r</i> : Logical SFO	70 + length of operations management domain name + length of logical server name + length of host name + length of logical server display name + length of logical server name of the logical performance tracer being used
	<i>s</i> : Logical Web server	70 + length of operations management domain name + length of logical server name x 2 + length of host name + length of logical server display name + length of logical server name of the logical performance tracer being used
	<i>t</i> : J2EE application	20 + length of operations management domain name + length of display name of J2EE application properties
	<i>u</i> : Imported J2EE application	50 + length of display name of J2EE application properties + length of logical server name of imported logical J2EE server
	<i>v</i> : J2EE server mapping definition	50 + length of logical server name of the logical Web server + length of logical server name of mapped logical J2EE server



---

## J. Kernel Parameters

---

To use JP1/IM in a UNIX environment, adjust the OS kernel parameters to allocate the resources needed to run JP1/IM.

For details about the kernel parameters you need to adjust, see the JP1/IM - Manager *Release Notes*.

---

## K. Version Changes

---

This appendix describes the changes between versions.

### K.1 Changes in version 09-00

- Event levels of events received from JP1/Base can now be changed according to predefined conditions, and the events can be managed by JP1/IM - Manager under the new event level (function for changing the severity level of JP1 events).
- A dedicated database for JP1/IM - Manager (the *IM database*) can now be created.
- A maximum of 1,500,000 events can now be managed (when using the IM database).
- Memo entries can now be added to events (when using the IM database) (addition of memo entries).
- An event can be issued when a correlation event fails to establish a correlation (event generation).
- Action definitions can now be set from a GUI (Action Parameter Detailed Definitions window) (simplified automatic action function).
- By specifying a date and time or by moving the slider, users can limit the range of events displayed in the event list (addition of event display start-time specification area).
- Managed hosts can now be registered, deleted, and viewed in list form from IM Configuration Management - View, allowing centralized management of information related to registered hosts (host management).
- The system hierarchy can be centrally managed from IM Configuration Management - View (system hierarchy management).
- IM Configuration Management - View can be used to centrally manage the profiles in JP1/Base on the hosts (profile management).
- Activity information about the JP1/Base services running on each host can be checked from IM Configuration Management - View (management of service activity information).
- Commands are now available for exporting and importing management information associated with IM Configuration Management (import and export of IM Configuration Management information).
- System hierarchies that incorporate virtual hosts can now be managed in IM Configuration Management - View. Also, information about a system hierarchy

that has virtual hosts can be imported and used in the Central Scope (virtualization configuration management).

- Troubleshooting data can be collected by the data collection tool.
- Actions can now be performed locally by JP1/Base on a stand-alone basis.
- JP1/IM can be linked with JP1/AJS3.
- NNMi incidents generated by HP NNMi can now be converted into JP1 events by JP1/IM - EG for NNMi and be monitored by JP1/IM.
- Messages have been added, deleted, and changed.
- JP1 events have been added.
- The JP1/IM - Manager manuals have been reorganized.
- Windows Server 2008 is now supported.
- JP1/Integrated Management - Service Support has been added as an integrated management products capable of linking with JP1/Integrated Management.
- Windows 2000 has been removed as a prerequisite operating system for JP1/Base.
- Common exclusion conditions have been added to the event acquisition filter to temporarily prevent the system from acquiring JP1 events issued by hosts under maintenance.
- Exclusion conditions which exclude JP1 events from display (or acquisition) have been added to the following filters and as conditions for event searches:
  - Event acquisition filter
  - Event receiver filter
  - Severe events filter
  - View filter
- A function has been added for making status change conditions for monitoring objects resident in memory.
- A function has been added for automatically setting a monitoring object to Initial status on receipt of a specific JP1 event.
- A function has been added for automatically deleting status change events when the response status of a JP1 event changes to **Processed**.
- The method of specifying the source host for the event service in FQDN format has been changed.
- Cautionary notes associated with the setup for linking with HP NNM System Observer have been amended.

- The following files have been added to the list of log files and directories:  
Install log, event console log, plugin log
- The file count for event flow control trace logs, the maximum disk usage, and the timing when the file is switched have been changed.
- The maximum disk usage of the action hosts file has been changed.
- The maximum length of an event acquisition filter has been changed.
- The **Central Scope** button and menu command become unavailable in the Event Console window when the Central Scope service is inactive.
- The number of entries saved in the **Target host** and **Command** fields in the Execute Command window has been augmented.
- A description of the title bar has been added to the description of the elements in the Monitoring Tree window.
- Because the JP1/Base commands described in this manual apply to manager hosts, a note has been added to direct readers to the JP1/Base manuals for details of agent host commands.
- Users must now have superuser permission to execute the `jcocmddef` command.
- A note about the message output when the `jcocmddef` command is executed has been added.
- The values specifiable in the `-runevinterval` option of the `jcocmddef` command have been changed (interval for issuing elapsed time events).
- The triggers for JP1 events have been changed.
- The arrival time attribute has been renamed.
- Some product names have changed.
- The event log has been added as an output destination for messages.
- A `Source` field has been added to the list of Windows event log entries output by JP1/Integrated Management.
- User-specified images of any size can now be used as icons representing monitoring nodes (Visual Icon).
- JP1/Integrated Management - View is now supported on Windows Vista.
- A feature for copying information to the clipboard has been added.
- There are now additional files that need to be backed up:
  - Guide information file (`jcs_guide.txt`)
  - Action profiles (`actprofile2_JP1-user-name`)

- Files under *View-path\image\icon\*
- Files under *View-path\image\visual\*
- Files under *View-path\image\map\*
- The list of files has been updated.
- The list of limits has been updated.
- Connectivity with previous versions has been updated.
- In a non-cluster environment, a method of configuring and operating logical hosts that are not subject to failover has been added.
- An explanation of the integrated trace log has been added.

## K.2 Changes from version 07-00 to version 08-01

- Support was added for the following features related to correlation event issue:
  - The range of JP1 events subject to correlation event issue processing can be restricted.
  - By grouping JP1 events matching an event condition on the basis of an attribute value, correlation events can be issued on a group basis.
  - Users can change the number of sets of JP1 events that can be kept for one correlation event generation condition.
- Additional files needed to be backed up.
- JP1/IM - Central Console and JP1/IM - Central Scope were integrated and renamed *JP1/IM - Manager*.
- The version 7 data collection tools (*jco\_log.bat* and *jco\_log.sh*) were discontinued. They were replaced by a data collection tool for JP1/IM - View (*jcoview\_log.bat*) and data collection tools for JP1/IM - Manager (*jim\_log.bat* and *jim\_log.sh*).
- Correlation events can be issued.
- JP1/IM could be linked with JP1/IM - Rule Operation.
- The Event Issue Service (*evgen*) could be monitored by the health check function.
- In windows other than the **Severe Events** page of the Event Console window, users could select multiple JP1 events and change their response status in one operation.
- Information about the JP1 events displayed in the Event Console window could be saved as a CSV snapshot.

- The maximum length of a command executed remotely from JP1/IM - View or executed in an automated action was changed to 4,096 bytes.
- The maximum number of lines that can be displayed in the **Log** area of the Execute Command window was increased from 100 to 10,000. The execution results could also be sorted by column header (**Time**, **Host**, and **Message**).
- A Related Events window was added for viewing related events (repeated events and correlation source events).
- The permitted monitoring range of a monitoring tree could be changed for individual JP1 users. Also, the operations users are permitted to perform on monitoring nodes within a permitted monitoring range could be individually controlled (using JP1 resource groups).
- An **Add** option was added to the feature for automatically generating monitoring trees.
- Items in the Monitoring Tree window and Search window could be sorted according to their status.
- The same attribute name could be used in more than one individual condition in the Status-Change Condition Settings window.
- The following operations in the Monitoring Tree (Editing) window were supported:
  - Acquire and apply changes to information from a previous version of JP1/IM - Central Scope.
  - Read and edit CSV files saved in a previous version of JP1/IM - View, and save the edited information to a previous version of JP1/IM - Central Scope.
- The programs that can be launched from the Tool Launcher window were changed.
- JP1 events were added.
- Additional files needed to be backed up.
- The list of log files was updated in accordance with version 08-00.
- The list of files was updated in accordance with version 08-00.
- Connectivity with previous versions was updated in accordance with version 08-00.
- Messages were added, deleted, and changed.
- The `jcocmdconv` command was added, allowing the user to import command execution logs from version 7 to the version 8 environment (JP1/Base enhancement).

### Changes related to the Central Console:

- A JP1 event with the following event ID could be issued when the response status of a JP1 event changes:

Event ID: 3F11

- The response status of a JP1 event could be changed from the **Search Event** page.
- Performance of the following actions during an event search was enhanced:
  - Access another window
  - Cancel the search
  - Redisplay the **Search Events** page
  - List search results sequentially
- The functionality for outputting command execution logs in CSV format was enhanced, allowing the user to specify a date and time range (JP1/Base control component).
- Guide information on investigating and dealing with JP1 events could be registered and viewed.
- Support was provided for running JP1/Integrated Manager - Central Console on an IPF server.
- The programs that can be launched from the Tool Launcher window were changed.
- Support was provided for running JP1/Integrated Manager - Central Scope on a UNIX-based operating system.
- The status of monitoring objects could be changed according to changes in the JP1 event response status in the Central Console.
- Support was provided for a feature that prevents the database being corrupted by errors during the database update processing (automatic backup and recovery of the monitoring objects database).
- A warning JP1 event (00003FB1) was output when the number of status change events associated with a monitoring object exceeded 100.
- The HiRDB and System Manager system-monitoring objects were added.

### K.3 Changes in version 07-11

- A function was added to detect hangups in JP1/IM - Central Console processes and JP1/Base processes (event service) on managers (health check function).
- Support was provided for multiple event acquisition filters that can be switched by the user.

- A function was added for summarizing events in the Event Console window when JP1 events with identical contents are received in succession by JP1/IM - View (consolidated display of repeated events).
- The execution statuses of automated actions was further classified, making their processing status easier to understand.
- Suppression of identical actions executed within a set time was supported (suppression of identical actions).
- Monitoring of the execution status of automated actions was supported (delay monitoring and status monitoring of automated actions).
- Automated actions could be cancelled.
- In line with the further classification of automated action statuses, the values `Deterrent`, `Cancel`, and `Kill` were added to the statuses of re-executable automated actions.

Automated actions could be re-executed from the following windows:

- Action Log window
- Action Log Details window
- A command (`jcothreaddmp`) was added for outputting a Java thread dump as troubleshooting data when a hangup occurs in JP1/IM - View.
- Operability of the Event Search Conditions window was enhanced (**Registered timeframe** could be specified as a condition).
- Setting conditions were added for displaying the execution results of automated actions in the Conditions for Updating List of Action Results window and List of Action Results window.
- JP1 events were added.
- A threshold parameter was added, enabling the command queue count for commands executed by automated actions to be monitored (JP1/Base control component).
- The amount of data transferred as command execution results could be controlled (JP1/Base control component).
- Support was added for automatically generating a monitoring tree for Cosminexus.
- The specification of an OR condition (for multiple condition groups) when setting filter conditions was supported in the following windows:
  - Event Acquisition Settings window
  - Detailed Settings for Event Receiver Filter window



- Severe Event Definitions window
- Settings for View Filter window
- Event Search Conditions window
- The use of an event acquisition filter in an automated action was supported.
- Multiple view filters could be set.
- A command (`jplcohaveup`) for upgrading JP1/IM in a cluster environment was added.
- The data collection tools (`jco_log.bat` and `jco_log.sh`) were enhanced (improvement of data collection tools).
- A command for checking the status of an executing command (`jcocmdshow`) and a command for deleting an executing command (`jcocmddel`) were added (JP1/Base control component).
- Support was provided for a JP1 event (00003FA3) to be issued automatically when command execution takes too long (JP1/Base control component).
- Support was provided for suppressing output of detailed results to the command execution log for automated actions (JP1/Base control component).
- The search function for status change events was enhanced (to allow a maximum of 100 results).
- Commands (`jplcsverup.bat` and `jplcshaverup.bat`) for upgrading JP1/IM were added.
- Linkage with other products (Cosminexus) was enhanced (addition of system-monitoring objects).
- Offline editing of common conditions was supported.
- User monitoring objects could be created for the host information database (lifting a restriction).
- The use of regular expressions and host name comparisons in individual conditions was supported.

---

## L. Glossary

---

### agent

In JP1/IM, a host managed by a manager, or a program managed by a manager program.

JP1/Base acts as the agent program in a JP1/IM system, receiving processing requests from JP1/IM - View and JP1/IM - Manager, and performing tasks such as managing JP1 events and executing commands.

Each agent runs JP1/Base, which provides the core functionality for the JP1/IM system.

### auto-generation

A function that automatically generates a monitoring tree in the JP1/IM Central Scope.

By generating a tree automatically, and then customizing it to suit your mode of operation, you can easily set up an environment to perform system monitoring based on a monitoring tree.

A monitoring tree represents the system to be monitored by JP1/IM in tree format, with the nodes to be monitored arranged upon it. Every node in the tree needs to be defined, and the JP1/IM auto-generation function can produce this huge amount of definition information automatically. Using this function, you can automatically collect definition information from the hosts to be monitored by JP1/IM, and automatically create a monitoring tree. If the system is reconfigured, you can extract the differences between the new and existing monitoring trees as difference information.

### automated actions

A function that automatically executes a command as an action when a specific JP1 event is received.

Using an automated action, you can, for example, execute a command to inform the system administrator of an important event that occurred while JP1/IM was monitoring the system. In an automated action definition, you can specify conditions for executing the action and the command to be executed as the action.

### basic attribute

Information (an attribute) held by all JP1 events.

See also *JP1 event*.

### basic information

Basic information held by the monitoring nodes that make up a monitoring tree in the JP1/IM Central Scope.

In the case of a monitoring group, the name that identifies the group is basic information.

For example, you can assign a group name such as *Daily accounting routines* or *Database server group* to jobs or servers grouped according to the monitoring objectives.

In the case of a monitoring object, the information for identifying the object is basic information.

For example, you can define a combination of information, such as a jobnet name together with a host name, for identifying the monitoring object within the system.

Basic information can be used, for example, when searching for monitoring nodes or in the conditions (individual conditions in a status change condition) for identifying the node concerned when a JP1 event occurs in the job or resource being monitored.

### **Central Console**

A program that enables integrated system management by centrally managing events in the system based on JP1 events.

In the Central Console, events occurring on the various hosts in the system are managed using JP1 events. The more important JP1 events, which need to be managed or dealt with in some way, are forwarded to a manager where they can be centrally managed. By monitoring these JP1 events in a viewer (the Event Console window), the user can monitor the whole system.

The Central Console also supports automated actions that execute a command automatically in response to specific JP1 events, and provides functionality for operating on the system from a viewer.

These features of the Central Console enable the user to efficiently perform the monitoring, error investigation, and troubleshooting tasks involved in system management.

### **Central Scope**

A program that enables objective-oriented system monitoring via a graphical user interface matched to the objectives of the system administrator.

In the Central Scope, the hosts, programs, jobs, and other system resources that need to be monitored are displayed in a tree view in a Monitoring Tree window. Because the relationships between the monitored objects are presented visually, the user has a clear picture of the likely impact of any problem in the system.

The Visual Monitoring window lets you display key resources and functions that you need to watch closely in a map view. You can arrange the monitoring points as icons on a map, organizational chart, or other background image. This allows the administrator to centrally monitor the system, no matter how large, from the required viewpoints.

## **cluster system**

A system in which multiple servers work together as a single system.

A cluster system is designed to ensure uninterrupted job processing and to enhance availability by having another server continue processing if a failure occurs. The processing of another server taking over processing is known as *failover*.

If the active server (primary node) fails, the standby server (secondary node) takes over. Because the job processing is switched from the active to the standby node, a cluster system is also called a *node switching system*.

Cluster systems include load-sharing systems with multiple servers that perform parallel processing. In this manual, however, *cluster system* refers only to failover functionality for preventing interruption of job processing.

## **command execution log**

A generic name for the database in which an execution log is recorded when a command is executed from JP1/IM - View or a command is executed in an automated action.

The logs for command execution from JP1/IM - View and for command execution in automated actions are managed separately. The file names generated in practice are as follows.

- Command execution logs for command execution from JP1/IM - View:  
CMDISAMLOGV8 . \*
- Command execution logs for command execution in automated actions:  
ACTISAMLOGV8 . \*

## **common condition**

A status change condition that applies to all monitoring objects of the same type in the JP1/IM Central Scope.

See also *status change condition*.

## **common definition information**

A database containing the definition parameters for the JP1 execution environment.

Common definition information is managed by JP1/Base and is used by JP1/Base, JP1/IM, JP1/AJS, and JP1/Power Monitor 06-02 or later. The database resides on a local disk of each server, and the definition parameters are sorted according to the physical host or logical host to which they apply.

When JP1 is used in a cluster system, the logical host settings in the common definition information residing on the primary and secondary servers must be identical. For this reason, after completing the setup and environment settings on the primary server, you must copy the defined parameters to the secondary server.

### common exclusion conditions

Conditions that form part of an event acquisition filter and consist of a group of conditions for filtering out JP1 events monitored by JP1/IM.

### configuration definition

Information defining the configuration of the system managed by JP1/IM.

A configuration definition defines the hierarchy of managers and agents in JP1/IM. Managers can be defined at different levels. For example, you can define lower-level base managers under a higher-level integrated manager.

Configuration definitions are managed by the JP1/IM configuration management functionality.

The information about the host relationships defined in a configuration definition can be used in JP1/IM to specify the hosts to which important JP1 events should be forwarded, for example, or to define the target host for executing a command in an automated action.

### configuration management

Functionality for managing the hosts in the JP1/IM system as a hierarchy of managers and agents.

You can manage the system configuration by using IM Configuration Management, or by editing the definition files directly.

Configuration definition information is used to manage the hosts.

See also *IM Configuration Management* and *configuration definition*.

### consolidated display of repeated events

A function that summarizes identical JP1 events received in succession by JP1/IM - View into a single JP1 event for display on the **Monitor Events** page or **Severe Events** page of the Event Console window. By using this function, you can prevent other important JP1 events from being overlooked.

Under this function, an event that summarizes identical JP1 events is known as a *consolidation event*. There are two types of consolidation events: an event in which repeated events are still being consolidated (*event being consolidated*) and an event in which the consolidation processing has been completed (*consolidation completion event*).

The first of identical JP1 events received by JP1/IM - View is known as a *consolidation start event*. The subsequently received identical JP1 events are called *repeated events*, and events that are not repeated, and therefore not consolidated, are known as *non-consolidation events*.

**consolidation completion event**

See *consolidated display of repeated events*.

**consolidation event**

See *consolidated display of repeated events*.

**consolidation start event**

See *consolidated display of repeated events*.

**correlation event**

A JP1 event issued by correlation processing. JP1/IM can issue a new JP1 event as a correlation event whenever a related JP1 event is issued. The correlation event and the association between the JP1 events can be defined by the user as a *correlation event generation definition*.

**correlation event generation definition**

A definition for issuing correlation events, specifying which types of JP1 events to associate, and the nature of the issued correlation event. A correlation event generation definition consists of a correlation event generation condition name, a filtering condition for the correlation target range, one or more event conditions, a timeout period, an event correlation type, a duplicate attribute value condition, a maximum correlation number, a correlation approval event, and a correlation failure event.

**correlation source event**

A JP1 event that triggers issue of a correlation event. Correlation source events can be listed in the Related Events (Correlation) window.

See also *correlation event*.

**Cosminexus**

A core product used to build application server-based systems for developing and running business applications that provide high performance and reliability.

**delay monitoring**

Monitoring of the execution time of an automated action, from start to completion. Delay monitoring is able to detect and notify the user of any automated action that fails to complete within a set time.

**event acquisition filter**

A filter for setting detailed conditions about the JP1 events to be acquired by JP1/IM - Manager for display in the Event Console window.

You can use an event acquisition filter to acquire events in JP1/SES format or to suppress acquisition of specific JP1 events.

**event being consolidated**

*See consolidated display of repeated events.*

**event buffer**

An area of memory used by JP1/IM - Manager (JP1/IM - Central Console) to store JP1 events extracted from the event service of JP1/Base.

JP1 events are stored in the event buffer when:

- JP1/IM - Manager (JP1/IM - Central Console) starts
- JP1 events are stored in the event database of JP1/Base

JP1/IM - View acquires events from the event buffer, not directly from the event service of JP1/Base.

**Event Console window**

A JP1/IM - View windows that shows the JP1 events received by the Central Console in a time series. The Event Console window is the first window that appears when you log in to JP1/IM - Central Console.

JP1/IM centrally manages the events generated on the various hosts by recording them as JP1 events and forwarding the more important ones to a JP1/IM manager. By viewing these JP1 events in the Event Console window, you can centrally monitor events occurring in the system.

**event display start-time specification**

When you use the integrated monitoring database, you can change the JP1 events listed in the Event Console window of JP1/IM - View by specifying a date and time or by moving the slider in the **event display start-time specification** area.

**event generation condition**

A condition that determines the type of status change in a monitoring node in the JP1/IM Central Scope that will cause the node to issue a JP1 event.

A monitoring node manages the status of the job or resource it is monitoring based on JP1 events issued by that job or resource. By defining an event generation condition, a JP1 event can be issued when a monitoring node changes status (that is, when a problem of some kind occurs in the job or resource being monitored), enabling early detection and swift response to any problems.

The JP1 event issued as a result of this condition has the event ID 00003FB0.

**event guide function**

A function that displays guide information in the JP1/IM Central Console for investigating and resolving JP1 events that occur during system monitoring.

By displaying troubleshooting procedures and other advice on handling JP1 events that

could impact on the system, you can reduce the system administrator's workload when a problem occurs.

The event guide function displays guidance targeted to a specific JP1 event. The JP1/IM Central Scope provides a similar function, but targeted to a specific monitoring node.

See also *guide function*.

### **event ID**

One of the attributes of a JP1 event. An event ID is an identifier indicating the program that issued the event and the nature of the JP1 event. It is a basic attribute and has the attribute name `B.ID`.

Event IDs are hexadecimal values, such as 7FFF8000.

Event IDs are uniquely assigned by each of the programs in the JP1 series. For details on the JP1 events issued by a specific program, see the documentation for the product concerned.

The values from 0 to 1FFF, and from 7FFF8000 to 7FFFFFFF, are available as user-specifiable event IDs.

A JP1 event is an 8-byte number consisting of a basic code (upper four bytes) and extended code (lower four bytes). Usually only the basic code is used, representing a 4-byte event ID. The extended code is 0, except in special cases, as when set by the user in the API. When both the basic and extended codes need to be included, they are joined with a colon (:) and appear as 7FFF8000:0, for example.

### **event level**

One of the attributes of a JP1 event, indicating the severity of an event that occurred in the system.

The event level is common information in the extended attributes of a JP1 event, and the attribute name is `E.SEVERITY`.

Event levels are Emergency, Alert, Critical, Error, Warning, Notice, Information, and Debug.

### **event receiver filter**

A filter for setting conditions, for individual JP1 users, about the JP1 events that can be viewed in the Event Console window.

Use an event receiver filter when you want to restrict the JP1 events that can be viewed by a particular user who performs operational tasks.

### **exclusion condition**

A filter condition that filters out JP1 events that match the condition. An exclusion condition can be specified in an event acquisition filter, view filter, severe events filter,



event receiver filter, or event search.

### **extended attribute**

Information (an attribute) held by a JP1 event, optionally set by the source program when issuing a JP1 event.

See also *JP1 event*.

### **failover**

Uninterrupted JP1 processing by transferring JP1 operations to another server when a failure occurs on the active server. Or, switching by the system administrator of the server that is currently executing JP1 processing.

Because the server on a secondary node takes over from the server on the primary node, failover is also known as *node switching*.

### **forwarding filter**

A filter set on each JP1/IM host, specifying conditions for the JP1 events to be forwarded from that host and the destination manager to which they are sent.

These settings are registered with the JP1/Base event service, and are known as a *forwarding filter* in JP1/IM.

In JP1/IM, events occurring in the system are centrally managed as JP1 events. To enable centralized management, JP1 events are forwarded to JP1/IM managers. The particular types of JP1 events to be forwarded are defined in a forwarding filter.

### **general monitoring object**

A monitoring object whose target can be set by the user. A system-monitoring object when edited becomes a general monitoring object.

The monitoring node type is *User Monitoring Object*.

See also *monitoring object*.

### **guide function**

A function that displays error causes and action procedures in the JP1/IM Central Scope relating to problems occurring in the system.

By displaying troubleshooting procedures and other advice on handling problems arising during system monitoring, you can reduce the system administrator's workload at the initial response stage.

The guide function displays guidance targeted to a specific monitoring node. The JP1/IM Central Console provides a similar function, but targeted to a specific JP1 event.

See also *event guide function*.

### **health check function**

A function that informs the user, by means of a JP1 event or notification command, when a hangup occurs in a JP1/IM or JP1/Base process.

The JP1/IM health check function can detect hangups in JP1/IM - Manager processes<sup>#</sup> and in the JP1/Base event service on managers. Detection is reported via a JP1 event or notification command.

The JP1/Base health check function can detect hangups in JP1/Base processes on the local host and on remote hosts. Detection is reported via a JP1 event.

By using the JP1/IM and JP1/Base health check functions in conjunction, you can quickly detect and respond to process errors in JP1/IM or in any instance of JP1/Base configured in the JP1/IM system.

#

The central scope service, IM Configuration Management service, and IM database service are not supported.

### **HiRDB**

A database management system (DBMS) product for building a relational database scalable to business operations.

### **HP NNM**

A generic name for a suite of integrated network management tools for managing the network configuration, performance, and failures.

### **IM Configuration Management**

Functionality that lets you centrally manage the hierarchical structure and host settings of a system managed by JP1/IM, using the configuration management features of JP1/IM - Manager accessed from IM Configuration Management - View. By using IM Configuration Management, you can check JP1/Base service activity information and manage the status of the JP1/Base profiles on each host.

See also *configuration management*.

### **IM Configuration Management database**

A database used by JP1/IM - Manager when implementing IM Configuration Management.

### **IM database**

A database provided by JP1/IM - Manager. *IM database* is a generic term for the IM Configuration Management database and the integrated monitoring database.

See also *IM Configuration Management database* and *integrated monitoring database*.

**incident**

A single occurrence of an event that can lower the quality of an IT service or impede normal system operation.

**individual condition**

A status change condition defined for a specific monitoring object in the JP1/IM Central Scope.

See also *status change condition*.

**initial status**

The status when the JP1/IM Central Scope has no information about the status of a monitoring node in the monitoring tree.

See also *status*.

**integrated monitoring database**

A database provided by JP1/IM - Manager for use with the Central Console functionality.

**JP1 common definition information**

See *common definition information*.

**JP1 event**

Information for managing events occurring in the system within the JP1 framework.

The information recorded in a JP1 event is categorized by attribute as follows:

- Basic attributes

Held by all JP1 events.

The basic attribute name for an event ID, for example, is written as B.ID (or simply ID).

- Extended attributes

Attributes that are optionally set by the program that issued the JP1 event. An extended attribute consists of the following common information and program-specific information:

- Common information (extended attribute information in a standard format for all JP1 events)

- Program-specific information (other information in a format specific to the program issuing the event)

The extended attribute name for an event level, for example, is written as E.SEVERITY (or simply SEVERITY).

JP1 events are managed by the JP1/Base event service. Events generated in the system are recorded in a database as JP1 events.

### **JP1/AJS**

A program for running jobs automatically.

Using JP1/AJS, you can execute processing in order according to a set schedule, or initiate processing when a specific event occurs.

### **JP1/Base**

A program that provides the core functionality of JP1/IM.

JP1/Base carries out processing such as the sending and receiving of JP1 events, user management, and startup control. It also serves as the agent in a JP1/IM system.

JP1/Base is a prerequisite program for JP1/IM - Manager.

### **JP1/IM - Central Console**

A feature of JP1/IM - Manager that provides the manager functionality of the Central Console. JP1/IM - Central Console oversees the entire system by centrally managing events in the system as JP1 events.

See also *Central Console*.

### **JP1/IM - Central Scope**

A feature of JP1/IM - Manager that provides the manager functionality of the Central Scope. JP1/IM - Central Scope enables objective-oriented system monitoring matched to the requirements of the system administrator.

See also *Central Scope*.

### **JP1/IM - Manager**

A program that enables integrated system management by providing centralized monitoring and operation across all system resources.

JP1/IM - Manager consists of three components: the *Central Console*, the *Central Scope*, and *IM Configuration Management*.

### **JP1/IM - Rule Operation**

A program that supports rapid failure recovery by predefining recovery procedures or *rules* for the errors that may occur in the system, and executing them automatically.

### **JP1/IM - View**

A GUI program that provides the viewer functionality for realizing integrated system management in JP1/IM.

The same JP1/IM - View is used with both JP1/IM - Manager and JP1/IM - Rule Operation. It can be connected to either program as required, for monitoring and

managing the system.

This manual does not cover the use of JP1/IM - View connected to JP1/IM - Rule Operation.

See also *viewer*.

### **JP1/SES event**

An event that was output by an obsolete JP1 product or by a product that does not support JP1 event output. JP1/SES events have basic attributes only (whereas JP1 events also have extended attributes).

### **JP1/Software Distribution**

A generic name for a system that performs software distribution and client management as batch operations over a network.

### **jp1hosts information**

Host information that associates JP1-specific host names with IP addresses.

This information can be used for customizing JP1 communication procedures in an environment with inter-connected networks, for example. `jp1hosts` information is managed by JP1/Base and is used by programs such as JP1/Base, JP1/IM, and JP1/AJS.

When `jp1hosts` information has been defined, the settings take precedence in JP1 communication over the OS `hosts` file settings. This allows you to associate host names and IP addresses differently from the OS settings, specifically for JP1 communication.

### **logical host**

A logical server that provides the JP1 execution environment for running JP1 in a cluster system. If a failure occurs, a failover between logical hosts takes place.

Each logical host has a logical IP address and a shared disk, which are inherited at failover. A logical host consists of JP1 programs and other applications which run using the logical IP address and the shared disk.

At failover, the secondary node takes over the logical IP address and shared disk, and JP1 continues running. Thus, even if the physical server running JP1 is switched, other hosts can access the server using the same IP address and it appears that one host is operating continuously.

### **manager**

A program whose role is to manage other programs or a host whose role is to manage other hosts in the JP1/IM system.

In the JP1/IM system, JP1/IM - Manager serves as the manager program, and manages the agent program JP1/Base.

The managers run JP1/Base, which provides the core functionality, and JP1/IM - Manager.

### memo entry setting function

When you use the integrated monitoring database, this functionality allows users to set additional information about a JP1 event displayed in the Event Console window.

### monitoring group

A group of monitoring objects in the JP1/IM Central Scope, or an icon in the Monitoring Tree window representing a group of monitoring objects.

Monitoring groups can be tailored to objectives. For example, you can define a job group or host group, depending on what you want to monitor.

The status of a monitoring group changes according to the highest severity among the statuses passed from the lower-level monitoring objects and groups it contains, or according to the conditions defined in a status change condition.

### monitoring node

A generic name for any monitoring object or monitoring group that is part of a monitoring tree in the JP1/IM Central Scope.

See also *monitoring object* and *monitoring group*.

### monitoring object

An object that you monitor using the JP1/IM Central Scope, or an icon in the Monitoring Tree window showing the status of an object being monitored.

When the Central Scope receives a JP1 event from an object being monitored, the event is judged using a *status change condition*, and the status of the monitoring object is displayed accordingly. (For example, a status change condition might set the status to *Emergency* on receipt of a JP1 event of *Emergency* level.) This allows you to manage the status of the various operations and resources being monitored in the system.

### monitoring status

An attribute that determines whether to monitor the status of a monitoring node in the JP1/IM Central Scope.

There are two monitoring statuses: **Monitor** and **Do not monitor**.

When **Monitor** is set for a node, that node will react to any change in the status of whatever it is monitoring. In the case of a monitoring object, its status changes on receipt of a JP1 event that matches the monitoring conditions defined in a status change condition. In the case of a monitoring group, its status changes according to the highest severity among the statuses passed from its lower-level monitoring objects and groups (any status change in a monitoring node is always passed to the higher-level node), or

according to the conditions defined in a status change condition. In JP1/IM - View, icons are color-coded to show the status of each monitoring node.

When **Do not monitor** is set for a node, its status does not change regardless of any JP1 event received from the job or host being monitored, or any status passed from a lower-level node. In JP1/IM - View, the icons of **Do not monitor** nodes are grayed out. You can set **Do not monitor** for a node when you need to maintain the resource it is monitoring, or when an automatically generated node does not need to be monitored.

### monitoring tree

Functionality provided by the JP1/IM Central Scope for managing the objects being monitored in the system in form of a tree, drawn according to the viewpoints required by the system administrator. *Monitoring tree* may also refer to the Monitoring Tree window in JP1/IM - View which provides this functionality.

See also *Central Scope*.

### node switching system

See *cluster system*.

### non-consolidation event

See *consolidated display of repeated events*.

### pass conditions

A set of conditions for JP1 events that you want to display (acquire). A pass condition can be specified in an event acquisition filter, view filter, severe events filter, event receiver filter, or event search.

### physical host

A physical server configured in a cluster system in which JP1 operates. The term *physical host* is used in contrast with *logical host* (a logical server that can be failed over independently of the physical servers).

### scroll buffer

An area of memory used by JP1/IM - View to store JP1 events extracted from the event buffer of JP1/IM - Manager.

A scroll buffer is kept for each of the **Monitor Events** page, **Severe Events** page, and **Search Events** page.

The JP1 events that JP1/IM - View displays on each page is determined by the contents of the scroll buffer for that page.

JP1 events are stored in the scroll buffer of the **Monitor Events** page, **Severe Events** page when:

- JP1/IM - View starts<sup>#</sup>

- The page is automatically refreshed<sup>#</sup>
- The user selects **Refresh** in a menu or the toolbar

#: If **Apply** is selected for **Automatic refresh** in the Preferences window.

At the above times, JP1/IM - View communicates with JP1/IM - Manager as long as unacquired events are present in the event buffer. The number of events acquired in one transmission is determined by the value set in **Num. of events to acquire at update** in the Preferences window.

JP1 events are stored in the scroll buffer of the **Search Events** page when a user runs an event search.

The number of events acquired in one search is determined by the value set in **Num. of events to acquire in 1 search** in the Preferences window. To display the events that could not be acquired in one search, click **Search for Next Event**.

### **severe events filter**

A filter that defines the severe events to be displayed in the **Severe Events** page of the Event Console window.

A *severe event* is a particularly important JP1 event that needs to be addressed, such as a failure of some sort. JP1/IM provides a **Severe Events** page so that users can reliably detect and deal with every severe event. On this page, as well as listing up only severe events, you can also manage the response status of each one.

### **severity level changing function**

A function that lets users freely change the event level of a JP1 event, so that JP1 events can be managed in accordance with the system's operating environment.

### **status**

The status of a resource being managed by a monitoring node in the JP1/IM Central Scope.

A monitoring node can have any of the following statuses: Emergency, Alert, Critical, Error, Warning, Normal, Debug, or Initial. Initial status means that the Central Scope does not yet have any information about the status of the resource being monitored.

For example, if a failure occurs and the node issues a JP1 event of Emergency level, the Central Scope will manage the event according to the status of the monitoring node.

### **status change condition**

A condition that determines when to change the status of a monitoring object or monitoring group in the JP1/IM Central Scope.



- Status change condition for a monitoring object

Defines the types of JP1 events in the job or resource being monitored that will cause the monitoring object to change status. A status change condition for a monitoring object consists of one or more common conditions and individual conditions, and the resulting status when the status change condition is satisfied.

A *common condition* is one that applies to all monitoring objects of the same type. For example, an event ID indicating that a job has ended abnormally is used for all monitoring objects that monitor jobs. A condition of this nature is defined as a common condition.

An *individual condition* is one whose value is specific to the monitoring object concerned. For example, an individual condition might identify what is being monitored by a value such as the name of the job or the name of the host that executes the job. Conditions of this nature are defined as individual conditions. In the case of a system-monitoring object, the same attribute as specified in the basic information of the monitoring object is defined in the individual condition contained in a status change condition.

- Status change condition for a monitoring group

Defines the status of a lower-level node that will cause the monitoring group to change status. A status change condition for a monitoring group consists of a child node status, a comparison condition, and the resulting status when the status change condition is satisfied.

*Child node status* refers to the status of a monitoring node at the next level below (immediately under) the monitoring group. When the child node status is set as `Alert`, for example, applicable statuses will include `Emergency`, which has higher priority than `Alert`.

The *comparison condition* calculates lower-level nodes whose status has changed to the defined child node status, by a percentage or a count. The former is calculated as the number of child nodes in the specified status, as a percentage (%) of the total number of child nodes in the monitoring group. The latter is the number of child nodes in the specified status.

### **status monitoring**

Monitoring for abnormal termination of an automated action. Status monitoring is able to detect and notify the user of any abnormally ended automated action whose status has changed to `Fail`, `Error`, or `Error (Miss)`.

### **system information management**

A structure for realizing integrated management of a system by centrally managing information about the system's myriad resources.

### **system-monitoring object**

A monitoring object provided by the JP1/IM Central Scope.

Each system-monitoring object contains predefined basic settings for monitoring a particular product in the JP1 series. The use of such objects facilitates environment setup.

See also *monitoring object*.

### **Tool Launcher window**

A JP1/IM - View window for registering and launching applications of the user's choice.

By registering applications needed for job processing in the Tool Launcher window, you can integrate operations under JP1/IM - View in running your JP1/IM system.

The Tool Launcher window has preset links for launching the GUI of products in the JP1 series.

### **variable binding**

A variable binding of an SNMP trap. When a SNMP trap is converted into a JP1 event in JP1/Base, the variable bindings are read into the program-specific information contained in the extended attributes of the JP1 event.

As basic information, an SNMP trap indicates the source program (enterprise name) and the trap type (generic or specific). In addition, when detailed trap-specific information needs to be included, variable bindings (also written as VarBind) are appended to the SNMP trap when it is issued.

A variable binding contains an object identifier (OID) and data.

For details on SNMP traps, see RFC1157 and other network-related documentation. For details on the information contained in the variable bindings, see the manual for the specific program that issues SNMP traps.

### **view filter**

A filter that sets conditions about the JP1 events to be displayed in the Event Console window.

Use a view filter when you want to temporarily restrict an event listing to specific JP1 events only.

### **viewer**

A GUI program that provides purpose-built windows for integrated system management in JP1/IM. *Viewer* may also refer to the host running the GUI program.

The viewer connects to the Central Console, Central Scope, IM Configuration Management, system information management, and rule operation manager to

perform system monitoring and management tasks.

### **virtual root node**

Appears only when the monitoring range settings are enabled for the monitoring tree.

Unlike a monitoring object or monitoring group, the information in a virtual root node cannot be edited (in the Properties window). Neither can you change the node status or perform any other direct operations on the virtual root node. (Its status changes accordingly when the status of a monitoring node below it changes, but you cannot change the virtual root node status directly. To change its status, you must change the status of a lower-level monitoring node.)

### **Visual Icon**

An icon displayed in the JP1/IM Central Scope which can be any size and based on any image. A visual icon is set as an attribute of a monitoring node. Because a visual icon can be any size, this feature offers the user a greater degree of freedom when creating monitoring windows. Visual Icon is displayed only in map view and in the Visual Monitoring window.

### **visual monitoring**

Functionality provided by the JP1/IM Central Scope for displaying the objects in the system that need to be monitored particularly closely as icons arranged on a map, organizational chart, or other image. *Visual monitoring* may also refer to the Visual Monitoring window in JP1/IM - View which provides the map view functionality.

See also *Central Scope*.

### **Web page**

A generic name for the GUI provided by another product and viewed in a Web browser (refers to the Web-based JP1/IM - View in the JP1/IM context).

### **Web-based JP1/IM - View**

A light version of JP1/IM - View, forming part of JP1/IM - Manager (JP1/IM - Central Console). The program has a number of functional limitations, such as not being able to open the Tool Launcher window or Execute Command window. To use the Web-based JP1/IM - View, in addition to a Web browser, the Java Runtime Environment (JRE) and its accompanying plug-ins are required on the viewer. For details, see the *Release Notes* for JP1/IM - Manager. A Web server is required on the manager.



---

# Index

---

## A

- access control 366
- agent 28, 29
  - glossary 682
- authentication block 365
- auto-generation
  - conditions 187
  - flow of processing 234
  - generation types 191
  - glossary 682
  - monitoring tree structures 189
  - processing 234
- automated action 237
  - canceling 264
  - checking execution results 263
  - checking execution status 263
  - command execution (under JP1/Base control) 378
  - command execution environment (JP1/Base component) 537
  - considerations 478
  - defining 246
  - delay monitoring 260
  - error monitoring based on execution monitoring 262
  - executable commands 255
  - execution condition precedence 250
  - execution flow 268
  - execution monitoring 260
  - flow of processing 269
  - glossary 682
  - notes 480
  - operation settings 267
  - overview 238
  - parameter groups and AND condition 251
  - re-executing 266
  - setting up execution monitoring 261
  - specifiable conditions 247
  - specifying command to execute 255

- status management 240
- status monitoring 261
- status transition 240
- suppressing 256
- target host 255
- user account 255

## B

- backing up
  - requirements 546
- basic attribute (glossary) 682
- basic configuration 506
- basic information (glossary) 682

## C

- Central Console
  - automated actions 237
  - centralized system monitoring 51
  - command execution 160
  - consolidated display of repeated events 109
  - correlation event issue 74
  - event guide function 121
  - JP1 event filtering 64
  - limits 603
  - monitor startup 154
  - operating permissions for system monitoring 614
  - saving event information (event report output) 134
  - saving event listings (CSV snapshot) 129
  - searching for events 115
  - Tool Launcher 157
- Central Console (glossary) 683
- Central Scope
  - automatic backup and recovery of monitoring objects database 235
  - completed-action linkage function 222
  - considerations for system monitoring 466

- databases 235
- event issued when status change events exceed 100 210
- guide function 214
- host information 230
- limits 608
- objective-oriented system monitoring 167
- operating permissions for system monitoring 618
- overview of functions 168
- searching for status change events 207
- setting monitoring windows 203
- system monitoring 232
- Tool Launcher 229
- using 230
- central scope
  - system design considerations 539
- Central Scope (glossary) 683
- centralized monitoring using JP1 events 52
- changes from version 07-00 to 08-01 677
- changes in version 07-11 679
- changes in version 09-00 674
- changing
  - response status 58
- changing event levels of JP1 events
  - considerations 456
  - supported event types 457
- child node status 181
- cluster system
  - glossary 684
  - JP1/IM operation 414
  - system configuration examples 517
- collecting and distributing definitions 390
  - auto-generation of monitoring tree (Central Scope) 392
  - event service definitions 390
- command concurrent execution count 538
- command execution
  - checking result 162
  - checking status 162
  - command execution environment (JP1/Base component) 537
  - commands for troubleshooting 386
  - conditions 162
  - conditions for command execution 388
  - considerations 475
  - executable commands 161
  - flow of processing 163
  - functionality 160
  - issuing JP1 events based on command execution statuses 386
  - notes 476
  - OS command execution 382
  - under JP1/Base control 378
  - users permitted to execute commands 381
  - using host groups to execute commands on multiple hosts 385
- command execution log (glossary) 684
- common condition 177
  - glossary 684
- common definition information
  - glossary 684
- common exclusion conditions 71
  - glossary 685
- communicating
  - with JP1/IM - Rule Operation 363
  - within local host 362
- communication 358
  - between manager and agent 359
  - between manager and authentication server 359
  - between viewer and manager 358
  - changing settings 631
  - connection status 600
  - direction through firewall 599
  - JP1/IM port numbers 598
  - timeout period 540
- comparison condition 181
- completed-action linkage 222
  - behavior 222
  - disabled 225
- configuration definition
  - glossary 685
- configuration file
  - editing 326
  - obtaining and releasing exclusive editing rights 330
- configuration for differing product versions 519

- configuration for monitoring Cosminexus system environment 513
- configuration for monitoring JP1 events from Web browser 512
- configuration management
  - considerations for system hierarchy 526
  - glossary 685
- configuration with HP NNM for network monitoring 509
- configuration with JP1/AJS for monitoring job execution 508
- configuration with JP1/IM - Rule Operation 515
- connection status 600
- connectivity
  - version 7 products 650
  - version 8 products 644
  - with previous versions 644
  - with previous versions of JP1/Base 658
- considerations for JP1 event forwarding 429
- considerations for system hierarchy 526
- consolidated display
  - consolidation completion event (glossary) 686
  - consolidation event (glossary) 686
  - consolidation start event (glossary) 686
  - event being consolidated (glossary) 687
  - non-consolidation event (glossary) 695
- consolidated display of repeated events 109
  - considerations 451
  - example of processing 112
  - glossary 685
  - process 110
- consolidation of repeated events 109
- copying to clipboard
  - CSV output items 142
  - JP1 event information and action execution results 140
  - notes 144
  - output format 141
  - screenshot 141
  - target windows and information 140
- correlation approval event 98
- correlation event generation function
  - JP1 event acquisition after startup 80
  - startup processing 78
- correlation event generation history file
  - contents 100, 101
  - format 101
  - output example 105
- correlation event issue 74, 77
  - after JP1 event issue 91
  - condition name 95
  - considerations 436
  - correlation event (glossary) 686
  - correlation event generation definition (glossary) 686
  - correlation source event (glossary) 686
  - defining 94
  - definition considerations 437
  - failure conditions 106
  - filtering condition 95
  - generation condition satisfied 105
  - issued correlation event 107
  - notes 449
  - required environment 448
  - service operation settings 99
  - service status transition 99
  - status 99
  - target JP1 events 105
  - timeout 95
- correlation failure event 99
- Cosminexus
  - adding to monitoring tree 467
  - auto-generation of monitoring tree 186
  - glossary 686
  - system configuration example 513
- CSV image and format
  - copying to clipboard 141
  - saving event listings 129
- CSV output
  - copying window to clipboard 140
  - from integrated monitoring database 134
  - from JP1/IM - View 129
- CSV output items
  - copying to clipboard 142
  - saving event listings 130
- CSV snapshot
  - timing 134

types of information 129

## D

data collection tools 533

database

    maintenance considerations 546

delay monitoring 260

    glossary 686

design overview 421

designing or considering 417

    automated actions 478

    backup 546

    basic configuration 506

    central scope system design 539

    changing event levels of JP1 events 456

    command execution environment 537

    command execution from JP1/IM - View 475

    communication timeout period 540

    configuration for cluster use 517

    configuration for differing product

    versions 519

    configuration for monitoring Cosminexus

    system environment 513

    configuration for monitoring JP1 events from

    Web browser 512

    configuration with HP NNM for network

    monitoring 509

    configuration with JP1/AJS for monitoring job

    execution 508

    configuration with JP1/IM - Rule

    Operation 515

    consolidated display of repeated events 451

    correlation event generation 436

    database maintenance 546

    design considerations 419

    design overview 421

    disk space checks 546

    error detection and reporting 424

    error investigation in JP1/IM 475

    event guide information 459

    event management using JP1 events 428

    event monitoring from Web-based JP1/IM -

    View 541

    failure report usage 547

flow of JP1/IM deployment 418

guide information 469

host name and IP address 522

IM database capacity requirements 488

issuing JP1 events at status change 536

JP1 event filtering 430

JP1 event forwarding to managers 429

JP1 user environment 535

JP1/IM - Manager system environment 534

JP1/IM - View environment 541

JP1/IM and JP1/Base environments 531

JP1/IM and JP1/Base troubleshooting 531

JP1/IM maintenance 546

JP1/IM processing performance 560

JP1/IM system design 487

JP1/IM system-wide maintenance 548

JP1/IM system-wide maintenance

(example) 550

kernel parameters (UNIX) 491

language environment 491

linking with other integrated management

products 544

maintenance of agent (example) 556

maintenance preparation 548

managing system hierarchy 485

memory and disk and database space

requirements for monitor servers 566

memory and disk space requirements 488

memory and disk space requirements for

monitor machines 567

model for performance evaluation 561

monitor startup 475

monitoring 421

monitoring objects database automatic backup

and recovery 500

monitoring trees 466

network configuration 522

operating environment 488

operation behind firewall 524

operation management 427

operation on multiple networks 524

overview of designing JP1/IM

deployment 421

performance and estimates 559



- prerequisite OSs and patches 488
- regular expressions 531
- saving event information (event report output) 465
- saving monitoring information (CSV snapshot) 464
- server network configuration 523
- setting event acquisition start location 542
- status change condition for monitoring group 470
- system configuration 506
- system design for JP1/IM - Rule Operation linkage 544
- system hierarchy 526
- system monitoring from Central Scope 466
- system monitoring using JP1 events 428
- Tool Launcher 475
- upgrade from JP1/Base version 6 505
- upgrade from JP1/Base version 7 505
- upgrade from JP1/Base version 8 505
- upgrade from JP1/IM - View version 7 504
- upgrade from previous version of JP1/IM 496
- upgrade from version 7 JP1/IM - Manager products 502
- upgrade from version 8 JP1/IM - Manager products 496
- upgrading from JP1/IM - View version 8 501
- user authentication 528
- user requirements 562
- visual monitoring 468
- WAN connection 525
- directories list 570
- disk space checks 546
- disk space requirements 662
- dump output commands 532
- duplicate attribute value condition 96

## E

- error detection and reporting (design)
  - JP1 event levels 424
  - monitoring from Central Scope 426
  - response procedures 425
- error investigation
  - considerations 475

- error reporting and action
  - JP1/IM - Manager health check function 352
  - managing JP1/Base processes 397
  - managing JP1/IM - Manager processes 348
- estimating disk space requirements 488
- estimating memory requirements 488
- event acquisition filter 67
  - common exclusion conditions 71
  - considerations 432
  - considerations for setting multiple filters 433
  - customizing considerations 433
  - events issued when filter switched 68
  - glossary 686
  - multiple filters 68
- event buffer 534
  - glossary 687
- event condition 95
- Event Console window 53
  - glossary 687
- event correlation type 96
- event generation condition (glossary) 687
- event guide function 121
  - considerations 459
  - differences between two functions 470
  - glossary 687
  - restricting applicable JP1 events 459
  - setting appropriate information 461
  - using variables (placeholder strings) 462
- event guide information
  - coding example 125
  - display example 121
  - settings 122
- event ID (glossary) 688
- event level
  - glossary 688
  - JP1 event attribute 369
- event management using JP1 events 428
  - converting non-JP1 events 428
  - linkage with programs that issue JP1 events 428
  - using JP1 event-issuing commands 428
- event receiver filter 69
  - considerations 434
  - glossary 688

- event report
  - command options 138
  - export maintenance information 139
  - image and format 135
  - output items 135
  - save events before deletion 139
  - types of information 134
- event report output 134
  - considerations 465
- event search 115
- event search conditions 117
- event search process 118
- event service 368
- exclusion condition 72
  - glossary 688
- exclusive editing rights
  - obtaining and releasing 330
- extended attribute (glossary) 689

**F**

- failover
  - glossary 689
- failure report usage 547
- files list 570
- filtering JP1 events 64
- filters
  - defining conditions 70
  - event acquisition filter 67
  - event receiver filter 69
  - forwarding filter 66
  - severe events filter 69
  - view filter 70
- firewall
  - communication direction 599
  - considerations 524
  - firewall support 414
  - notes 525
- flow of processing
  - auto-generation of monitoring tree 234
  - automated actions 269
  - command execution 163
  - JP1 event search 118
  - monitoring object status change 233
- forwarding events 371

- forwarding filter 66
  - glossary 689
- functionality 407
- functions list 43

## G

- general monitoring object 195
  - glossary 689
- glossary 682
- guide function
  - differences between two functions 470
  - functionality 214
  - glossary 689
- guide information 215
  - considerations 469
  - differences between two functions 470
  - display conditions 216
  - display contents 217
  - settings 215
  - utilizing 219

## H

- health check function
  - enabling and disabling 354
  - glossary 690
  - JP1/IM - Manager 352
  - mechanism 354
  - monitored processes 353
- HiRDB
  - adding to monitoring tree 467
  - glossary 690
- Hitachi Network Objectplaza Trace Library 394
- host information 230
  - collecting 280
  - considerations 539
- host management
  - changing information 285
  - collecting information 280
  - deleting hosts (Edit IM Configuration window) 305
  - deleting hosts (IM Configuration Management window) 288
  - displaying information 285
  - host information 274

- registering hosts 277
- host name
  - considerations 522
- HP NNM
  - glossary 690

## I

- IM Configuration Management
  - glossary 690
  - host management 274
  - importing and exporting management information 337
  - managing service activity information 332
  - managing virtualization configurations 343
  - profile management 311
  - system hierarchy management 291
- IM Configuration Management database
  - glossary 690
- IM database
  - estimating capacity requirements 488
  - glossary 690
- incident
  - glossary 691
- individual condition 178
  - glossary 691
- inherited event information 252
  - converting 254
- initial status (glossary) 691
- integrated console
  - JP1/IM - Rule Operation linkage 400
- integrated management using JP1 events 10
- integrated monitoring database
  - glossary 691
- IP address considerations 522

## J

- jcachstat
  - connection permission 534
- JP1 common definition information (glossary) 691
- JP1 event
  - attributes 369
  - centralized event management 370
  - considerations for generating at response status change 536

- consolidated display 109
  - display process 110
  - filtering 64
  - filtering considerations 430
  - forwarding 371
  - forwarding considerations 429
  - glossary 691
  - management considerations 428
  - managing through JP1/Base 368
  - monitoring process 59
  - searching 115
  - setting response status 58
  - use as historical and statistical information 374
- JP1 event forwarding 371
  - definition collection and distribution 374
  - relationship to configuration management 374
  - retry 374
- JP1 event information and action execution results
  - copying to clipboard 140
- JP1 event search 115
  - canceling 117
  - conditions 117
  - flow of processing 118
- JP1 permission level 613
- JP1 user environment
  - considerations 535
- JP1 users 364
- JP1/AJS
  - auto-generation of monitoring tree 186
  - glossary 692
  - monitoring automated actions 479
  - system configuration examples 508
- JP1/Base 28
  - agent maintenance 550
  - collecting and distributing definitions 390
  - connectivity 410
  - failure report usage 547
  - firewall support 414
  - forwarding filter 66
  - glossary 692
  - Hitachi Network Objectplaza Trace Library 394

- JP1 event filtering 64
- JP1/IM core functionality 364
- list of functions 43
- managing command execution 378
- managing JP1 events 368
- managing JP1 users 364
- managing service startup 393
- multiple LAN support 414
- prerequisite OSs 412
- prerequisite programs 413
- process management 397
- regular expressions 531
- troubleshooting considerations 531
- upgrading from version 6 505
- upgrading from version 7 505
- upgrading from version 8 505
- JP1/IM
  - automated action considerations 478
  - automated actions 237
  - centralized system monitoring with Central Console 51
  - communication in JP1/IM system environment 358
  - communication settings 631
  - configuration 408
  - connectivity with previous versions 644
  - considerations for error investigation 475
  - considerations for managing system hierarchy 485
  - considerations for system hierarchy 526
  - considerations for system monitoring from Central Scope 466
  - considerations for system monitoring using JP1 events 428
  - core functionality provided by JP1/Base 364
  - design items 419
  - design overview 417
  - files and directories 570
  - flow of deployment 418
  - functionality 407
  - glossary 682
  - JP1/IM and JP1/Base environment considerations 531
  - limits 603
  - linking with JP1/IM - Rule Operation 400
  - linking with other integrated management products 544
  - linking with other JP1/IM products 399
  - list of processes 592
  - maintenance considerations 546
  - model for performance evaluation 561
  - network considerations 522
  - objective-oriented system monitoring using Central Scope 167
  - operating environment considerations 488
  - operating permissions 613
  - operation control 347
  - operation management design 427
  - overview 1
  - overview of deployment design 421
  - performance and estimates 559
  - port numbers 598
  - processing performance 560
  - product connectivity 410
  - product structure 409
  - regular expressions 633
  - series 2
  - system configuration design 506
  - system configuration support 414
  - system design 487
  - system hierarchy 29
  - system hierarchy management 291
  - system operation (Central Console) 154
  - system operation (Central Scope) 229
  - system-wide maintenance 548
  - troubleshooting considerations 531
  - upgrading from previous version 496
  - user authentication considerations 528
  - version changes 674
- JP1/IM - Central Console
  - glossary 692
- JP1/IM - Central Scope
  - glossary 692
- JP1/IM - Manager 28
  - component products 28
  - features 10
  - files list (UNIX) 579
  - files list (Windows) 571

- glossary 692
  - health check function 352
  - internal control of JP1 events 61
  - list of functions 43
  - list of processes (UNIX) 595
  - list of processes (Windows) 592
  - process management 348
  - restrictions on connecting from JP1/IM - View 07-00 or 07-01 (using Central Console) 653
  - restrictions on connecting from JP1/IM - View 07-00 or 07-01 (using Central Scope) 657
  - restrictions on connecting from JP1/IM - View 08-01 (using Central Console) 647
  - restrictions on connecting from JP1/IM - View 08-01 (using IM Configuration Management) 649
  - restrictions on connecting from JP1/IM - View 08-01 (when using Central Scope) 648
  - restrictions on managing JP1/Base 06-00 to 08-00 660
  - system configuration 28
  - system operation 18
  - JP1/IM - Rule Operation
    - checking request status and result 404
    - communication in JP1/IM system
    - environment 363
    - glossary 692
    - linkage functions 400
    - monitor startup 406
    - notes 545
    - notification 400
    - settings 544
    - system configuration examples 515
    - system design for linkage 544
  - JP1/IM - View 28
    - command execution 160, 475
    - CSV output 129
    - customizing 541
    - environment considerations 541
    - files list 588
    - glossary 692
    - list of processes 594
    - monitor startup 154
    - restrictions on connecting to JP1/IM - Central Console 07-00 or 07-01 650
    - restrictions on connecting to JP1/IM - Manager 08-01 (when using Central Console) 644
    - restrictions on connecting to JP1/IM - Manager 08-01 (when using Central Scope) 645
    - restrictions on connecting to JP1/IM - Manager 08-01 (when using IM Configuration Management) 646
    - restrictions on event searches in JP1/Base 06-00 to 08-00 658
    - setting up linkage with JP1/IM - Rule Operation 541
    - Tool Launcher 157, 229
  - JP1/IM system-wide maintenance (example) 550
    - JP1/Base setup on base managers and agents 554
    - order of maintenance 551
    - procedures 554
    - settings on integrated manager (JP1/IM - Manager) 552
  - JP1/Integrated Management overview 1
  - JP1/PPM
    - auto-generation of monitoring tree 186
  - JP1/SES event
    - glossary 693
    - monitoring in JP1/IM 433
  - JP1/Software Distribution
    - glossary 693
  - jp1hosts information
    - glossary 693
- ## K
- KAVB5150-W 481
  - KAVB9032-E 503
  - kernel parameters 673
    - adjusting 491
- ## L
- language environment considerations 491
  - limits 603
  - linking with

- JP1/IM - Rule Operation 400
- other integrated management products 544
- other JP1/IM products 399
- list of processes 592
- local host
  - internal communication 362
  - monitoring JP1/Base processes 395
- logical host
  - glossary 693
  - non-cluster system 415
- M**
- maintenance
  - agent (example) 556
  - considerations 546
  - considerations for common exclusion conditions 433
  - entire JP1/IM system 548
- maintenance planning 548
  - agents (JP1/Base) 550
  - entire system 548
  - managers (JP1/IM - Manager) 549
- manager 28, 29
  - glossary 693
- manager/agent communication 359
- manager/authentication server communication 359
- managing
  - command execution 378
  - JP1 events using JP1/Base 368
  - JP1 users 364
  - JP1/Base processes 397
  - service startup 393
- maximum correlation number 97
- memo entries
  - setting 126
- memo entry setting function
  - glossary 694
- memory and disk and database space requirements for monitor servers 566
- memory and disk space estimates 488
- memory and disk space requirements for monitor machines 567
- memory requirements 662
- model for performance evaluation 561
- monitor startup 154
  - considerations 475
  - JP1/IM - Rule Operation 406
- monitor window
  - overview 155
  - prerequisites for opening 157
- monitoring design 421
  - methods 422
  - targets 423
  - viewpoints (Central Scope) 423
- monitoring group 172
  - glossary 694
  - status change condition 470
  - status change condition (examples) 470
  - status change condition (limitations) 473
  - status change conditions 179
- monitoring JP1/Base processes on local hosts 395
- monitoring JP1/Base processes on remote hosts 396
- monitoring node 173
  - glossary 694
  - status 173
- monitoring node search 207
- monitoring object 172
  - automatically initializing 212
  - glossary 694
  - setting to initial status on receipt of JP1 event 212
  - status change conditions 176
  - status change process 233
- monitoring objects database 235
  - automatic backup and recovery considerations 500
- monitoring status (glossary) 694
- monitoring tree 172
  - auto-generated structures 189
  - auto-generation 186
  - auto-generation conditions 187
  - auto-generation process 234
  - auto-generation process flow 234
  - considerations 466
  - editing 195
  - glossary 695
  - map display settings 197
  - monitoring group 172

- monitoring node 173
- monitoring object 172
- monitoring range settings 198
- structure 172
- type 191
- virtual root node 173
- multiple LAN support 414
  - considerations 524

## N

- network
  - considerations 522
  - traffic volumes 662
- node switching system (glossary) 695
- non-consolidation event
  - glossary 695
- notes
  - automated actions 480
  - cluster systems 518
  - command execution 538
  - firewalls 525
  - JP1 event issue at status change 537
  - JP1 system environment 535
  - JP1 user environment 536
  - monitoring trees 467
  - user authentication 530

## O

- operating environment considerations 488
- operating permissions 613
- operation in configuration connected to multiple networks 524
- operation in multi-language environments 491
  - server conditions 495
  - system conditions 492
- operation management design 427

## P

- pass conditions 73
  - glossary 695
- performance and estimates 559
- performance and estimation (appendix) 662
- physical host

- glossary 695
- port numbers 598
- prerequisite OSs 412
- prerequisite OSs and patches 488
- prerequisite programs 413
- process management
  - commands 348
  - issuing JP1 events at error detection 350
  - JP1/Base 397
  - JP1/IM - Manager 348
  - restarting at abnormal termination 349
- product structure 409
- profile management
  - collecting lists 314
  - collecting profiles 317
  - displaying profiles 324
  - types of managed profiles 311

## R

- regular expression 633
  - comparison 638
  - selecting 531
  - syntax 636
  - tips on using 640
  - types 633
  - usage examples 641
- remote host
  - monitoring JP1/Base processes 396
- repeated events
  - consolidated display 109
- response status change
  - considerations for issuing JP1 events 536

## S

- saving event listings 129
  - output format 129
  - output items 130
  - snapshot timing 134
  - types of information 129
- saving monitoring information
  - considerations 464
  - failure report usage 547
- scroll buffer 535
  - glossary 695

- searching
    - for JP1 events 115
    - for monitoring nodes 207
    - for status change events 207
  - server network configuration 523
  - service activity information
    - collecting 332
    - displaying 335
    - managing 332
  - setting
    - event acquisition start location 542
  - settings for event guide information 122
  - severe events filter 69
    - considerations 434
    - glossary 696
  - severity level changing function
    - glossary 696
  - SNMP trap
    - event level after conversion to JP1 event 511
  - specifying event display period 151
  - specifying event display start-time 145
    - glossary 687
  - start options 80
    - cold 80
    - warm 80
  - status
    - glossary 696
    - monitoring node 696
  - status change condition 176
    - considerations 470
    - for monitoring groups 179
    - for monitoring objects 176
    - glossary 696
    - making resident in memory 179
  - status change event
    - automatic deletion 226
    - searching 207
  - status monitoring 261
    - glossary 697
  - support for various system configurations
    - overview 31
  - syntax conventions xi
  - system configuration design 506
  - system configuration examples
    - basic configuration 506
    - cluster system 517
    - differing product versions 519
    - monitoring Cosminexus system environment 513
    - monitoring job execution with JP1/AJS 508
    - monitoring JP1 events from Web browser 512
    - monitoring network with HP NNM 509
  - system configuration support 414
  - system hierarchy management
    - acquiring information 296
    - applying information 306
    - displaying information 298
    - editing information 302
    - managed configurations 291
    - synchronizing information 308
    - verifying information 299
  - system information management
    - glossary 697
  - system life cycle 4
  - system management issues and integrated management 4
  - system monitoring 19
  - system-monitoring object 195
    - glossary 698
- T**
- Tool Launcher 157, 229
    - adding items 127, 159
    - considerations 475
  - Tool Launcher window
    - glossary 698
    - prerequisites for adding items 160
- U**
- upgrade from version 8 JP1/IM - Manager products
    - upgrading from Central Scope version 8 499
  - upgrading
    - JP1/Base version 6 505
    - JP1/Base version 7 505
    - JP1/Base version 8 505
    - JP1/IM - View version 7 504
    - JP1/IM - View version 8 501
    - previous version of JP1/IM 496



- version 7 JP1/IM - Manager products 502
- version 8 JP1/IM - Manager products 496
- upgrading from version 7 JP1/IM - Manager products
  - from JP1/IM - Central Console version 7 503
  - installation directories 502
- upgrading from version 8 JP1/IM - Manager products
  - from Central Console version 8 496
- user authentication 364
  - access permissions of JP1 users 529
  - considerations 528
  - notes 530
  - user authentication blocks 528
- user management 364
  - access control 366
  - user authentication 364
  - user authentication considerations 528
  - user mapping 368
- user mapping 368
- user requirements 562
- user-defined event attributes
  - displaying 127
- UTF-8 492

## V

- variable binding
  - glossary 698
- version changes 674
  - changes from 07-00 to 08-01 677
  - changes in 07-11 679
  - changes in 09-00 674
- view filter 70
  - considerations 435
  - glossary 698
- viewer 28, 29
  - glossary 698
- viewer/manager communication 358
- virtual root node
  - glossary 699
- virtualization configuration
  - managing 343
- Visual Icon 170
  - glossary 699
- visual monitoring 206
  - considerations 468

- glossary 699

## W

- WAN connection 525
- Web page
  - glossary 699
- Web-based JP1/IM - View 409
  - event monitoring 541
  - glossary 699



---

# 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:

<b>Manual name:</b>	
<b>Manual number:</b>	
<b>Your name:</b>	
<b>Company or organization:</b>	
<b>Street address:</b>	
<b>Comment:</b>	

<b>(For Hitachi use)</b>
--------------------------