

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

3020-3-R77-01(E)

■ Relevant program products

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

For Windows Server 2003 and Windows XP Professional:

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

For Windows Server 2008 and Windows Vista:

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

For Windows Server 2003:

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

For Windows Server 2008:

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

For Solaris:

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

For AIX:

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

■ Trademarks

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

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

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

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

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

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

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

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

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

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

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

RSA Security Inc. All rights reserved.

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

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

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

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

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

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

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

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

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

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

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

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

Portions of this software were developed at the National Center for Supercomputing Applications (NCSA) at the University of

Illinois at Urbana-Champaign.

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

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

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

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



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

HITACHI
Inspire the Next

 Hitachi, Ltd.



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

■ Restrictions

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

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

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

Printed in Japan.

■ Edition history

Edition 1 (3020-3-R77-01(E)): November 2009

■ Copyright

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

Preface

This manual explains how to set up Job Management Partner 1/Integrated Management - Manager and Job Management Partner 1/Integrated Management - View systems.

In this manual, *Job Management Partner 1* is abbreviated as *JP1*, and *JP1/Integrated Management* is abbreviated as *JP1/IM*.

Intended readers

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

- Apply centralized monitoring of the events that occur in a system, and take appropriate action in response to those events.
- Implement centralized monitoring of the system by associating the status of the infrastructure used to manage the system with the events that occur in the system.

Organization of this manual

This manual is organized into the following chapters:

1. *Installation and Setup (for Windows)*

Chapter 1 explains how to install and set up JP1/IM in a Windows environment.

2. *Installation and Setup (for UNIX)*

Chapter 2 explains how to install and set up JP1/IM in a UNIX environment.

3. *Using IM Configuration Management to Set the System Hierarchy*

Chapter 3 explains how to use IM Configuration Management to set the system's hierarchical structure.

4. *Setting up Central Console*

Chapter 4 explains how to set up an environment for using Central Console.

5. *Setting up Central Scope*

Chapter 5 explains how to set up an environment for using Central Scope.

6. *Operation and Environment Configuration in a Cluster System*

Chapter 6 describes the operation and environment configuration of JP1/IM -

Manager in a cluster system.

7. Operation and Environment Configuration Depending on the Network Configuration

Chapter 7 describes the operation and environment configuration depending on the network configuration (such as a configuration in which the JP1/IM - Manager host is connected to multiple networks, or a configuration with a firewall).

8. Settings for Linking to Other Integrated Management Products

Chapter 8 explains how to set up an environment for linking JP1/IM to other Integrated Management products (such as JP1/IM - Rule Operation).

Related publications

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

Manuals related to JP1/IM

- *Job Management Partner 1/Integrated Management - Manager Quick Reference (3020-3-R75(E))*
- *Job Management Partner 1/Integrated Management - Manager Overview and System Design Guide (3020-3-R76(E))*
- *Job Management Partner 1/Integrated Management - Manager 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))*

Manuals related to JP1

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

- *Job Management Partner 1/Performance Management User's Guide* (3020-3-R32(E))
- *Job Management Partner 1/Performance Management - Analysis Description, Operator's Guide and Reference* (3020-3-K77(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/Software Distribution Setup Guide* (3020-3-S80(E)), for Windows systems
- *Job Management Partner 1/Software Distribution Administrator's Guide Volume 1* (3020-3-S81(E)), for Windows systems
- *Job Management Partner 1/Software Distribution Administrator's Guide Volume 2* (3020-3-S82(E)), for Windows systems
- *Job Management Partner 1/Software Distribution Client Description and User's Guide* (3020-3-S85(E)), for UNIX systems
- *Job Management Partner 1/Automatic Job Management System 2 Linkage Guide* (3020-3-K27(E))

Manual related to Cosminexus

- *Cosminexus Simple Setup and Operation Guide* (3020-3-M05(E))

Manuals related to HiRDB

- *For UNIX Systems HiRDB Version 8 Installation and Design Guide* (3000-6-352(E))
- *For Windows Systems HiRDB Version 8 Installation and Design Guide* (3020-6-352(E))
- *For UNIX Systems HiRDB Version 8 System Definition* (3000-6-353(E))
- *For Windows Systems HiRDB Version 8 System Definition* (3020-6-353(E))

Conventions: Abbreviations

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

Abbreviation		Full name or meaning
AIX		AIX(R) 5L 5.2
		AIX(R) 5L 5.3
		AIX(R) 6.1
Cosminexus	Cosminexus Application Server	uCosminexus Application Server Standard
		uCosminexus Application Server Enterprise
		uCosminexus Web Redirector
		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
	JP1/AJS - View	Job Management Partner 1/Automatic Job Management System 2 - View
		Job Management Partner 1/Automatic Job Management System 3 - View

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

Abbreviation		Full name or meaning
	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	Group of agent products such as Job Management Partner 1/Performance Management - Agent for Platform and other components of the Agent product suite
	JP1/PFM - Manager	Job Management Partner 1/Performance Management - Manager
	JP1/PFM - View	Job Management Partner 1/Performance Management - View
	JP1/PFM - Web Console	Job Management Partner 1/Performance Management - Web Console
JP1/SES		Job Management Partner 1/System Event Service
JP1/Software Distribution		Job Management Partner 1/Software Distribution Manager
		Job Management Partner 1/Software Distribution SubManager
		Job Management Partner 1/Software Distribution Client
NNM	HP NNM	HP Network Node Manager Software Version 6 or earlier
		HP Network Node Manager Starter Edition Software Version 7.5 or earlier

Abbreviation		Full name or meaning	
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
			Microsoft(R) Windows Server(R) 2008 Standard
	Windows Server 2008 (IPF)		Microsoft(R) Windows Server(R) 2008 for Itanium-based Systems

Abbreviation	Full name or meaning
Windows Vista	Microsoft(R) Windows Vista(R) Business
	Microsoft(R) Windows Vista(R) Enterprise
	Microsoft(R) Windows Vista(R) Ultimate
Windows XP Professional	Microsoft(R) Windows(R) XP Professional Operating System

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

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

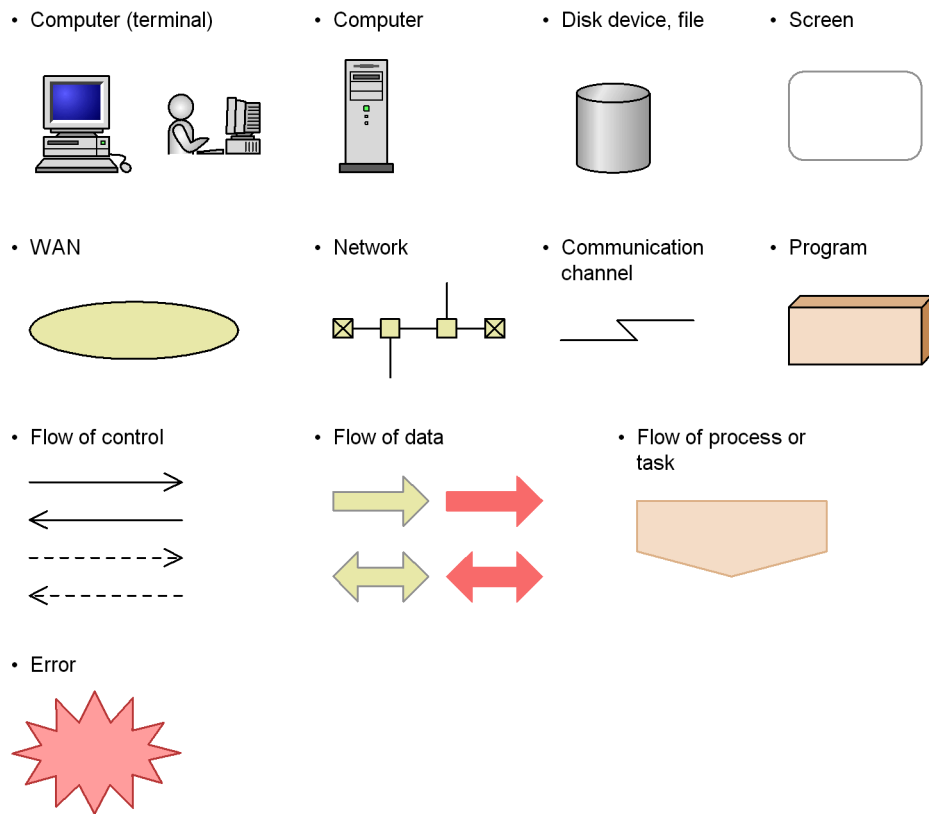
This manual also uses the following abbreviations:

Abbreviation	Full name or meaning
ASCII	American Standard Code for Information Interchange
CMT	Container-Managed Transaction
CRLF	Carriage Return/Line Feed
CSV	Comma Separated Value
DB	Database
DBMS	Database Management System
DNS	Domain Name System
FQDN	Fully Qualified Domain Name
GMT	Greenwich Mean Time
GUI	Graphical User Interface
HTML	Hyper Text Markup Language
HTTP	HyperText Transfer Protocol
IP	Internet Protocol
IPF	Itanium(R) Processor Family

Abbreviation	Full name or meaning
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: Diagrams

This manual uses the following conventions in diagrams:



Conventions: Fonts and symbols

Font and symbol conventions are classified as:

- General font conventions
- Conventions in syntax explanations

These conventions are described below.

General font conventions

The following table lists the general font conventions:

Font	Convention
Bold	Bold type indicates text on a window, other than the window title. Such text includes menus, menu options, buttons, radio box options, and explanatory labels. For example, bold is used in sentences such as the following: <ul style="list-style-type: none"> • From the File menu, choose Open. • Click the Cancel button. • In the Enter name entry box, type your name.
<i>Italics</i>	Italics are used to indicate a placeholder for some actual text provided by the user or the system. Italics are also used for emphasis. For example: <ul style="list-style-type: none"> • Write the command as follows: <i>copy source-file target-file</i> • Do <i>not</i> delete the configuration file.
Code font	A code font indicates text that the user enters without change, or text (such as messages) output by the system. For example: <ul style="list-style-type: none"> • At the prompt, enter <code>dir</code>. • Use the <code>send</code> command to send mail. • The following message is displayed: <code>The password is incorrect.</code>

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

```
MakeDatabase
...
StoreDatabase temp DB32
```

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

Conventions in syntax explanations

Syntax definitions appear as follows:

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

The following table lists the conventions used in syntax explanations:

Example font or symbol	Convention
<code>StoreDatabase</code>	Code-font characters must be entered exactly as shown.
<i>database-name</i>	This font style marks a placeholder that indicates where appropriate characters are to be entered in an actual command.
SD	Bold code-font characters indicate the abbreviation for a command.
<u>perm</u>	Underlined characters indicate the default value.

Example font or symbol	Convention
[]	Square brackets enclose an item or set of items whose specification is optional. If multiple items are enclosed, either omit them all or select one of them. Example: [A] means either nothing or A must be specified. [B C] means nothing, or B, or C must be specified.
	Only one of the options separated by a vertical bar can be specified at the same time. Example: A B C means A, or B, or C.
...	An ellipsis (...) indicates that the item or items enclosed in () or [] immediately preceding the ellipsis may be specified as many times as necessary.
{ }	One of the items or sets of items enclosed in curly brackets must be selected. Inside the curly brackets, each item or set of items is separated by a vertical bar (). Example: {A B C} means that A, or B, or C must be specified.
Δ	Indicates a space. Δ ₀ : Zero or more spaces (space can be omitted). Δ ₁ : One or more spaces (space cannot be omitted).
▲	Indicates a tab. Example: ▲ A means that a tab character precedes A.

Conventions for mathematical expressions

This manual uses the following symbols in mathematical expressions:

Symbol	Meaning
x	Multiplication sign
/	Division sign

Conventions: Installation folders for the Windows version of JP1/IM and JP1/Base

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

Product name	Installation folder	Default installation folder [#]
JP1/IM - View	<i>View-path</i>	<i>system-drive:\Program Files\HITACHI\JP1CoView</i>
JP1/IM - Manager	<i>Manager-path</i>	<i>system-drive:\Program Files\HITACHI\JP1IMM</i>

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

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

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

Conventions: KB, MB, GB, and TB

This manual uses the following conventions:

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

Conventions: Version numbers

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

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

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

Change in the product lineup for version 8

In version 8, the JP1/IM product lineup has been changed as follows:

- JP1/IM - Central Console and JP1/IM - Central Scope are now bundled in one package called JP1/IM - Manager.
- JP1/IM - Central Console Upgrade has been discontinued.
- JP1/IM - Rule Operation has been added. For details, see the manual *Job*

Administrator permissions

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

Online manuals

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

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

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

To display the table of contents for this online manual:

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

Note:

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

Contents

Preface	i
Intended readers	i
Organization of this manual	i
Related publications	ii
Conventions: Abbreviations	iii
Conventions: Diagrams	x
Conventions: Fonts and symbols	x
Conventions: Installation folders for the Windows version of JP1/IM and JP1/Base	xii
Conventions: KB, MB, GB, and TB	xiii
Conventions: Version numbers	xiii
Change in the product lineup for version 8	xiii
Administrator permissions	xiv
Online manuals	xiv
1. Installation and Setup (for Windows)	1
1.1 Installation and setup procedures	2
1.2 Preparations required before installation	4
1.2.1 Designing the setup details	4
1.2.2 Configuring the system environment	4
1.2.3 Installing the prerequisite program	4
1.3 Installing	5
1.3.1 Installation procedure	5
1.3.2 Uninstallation procedure	7
1.3.3 Notes about installing and uninstalling	8
1.4 Creating an IM database	10
1.5 Settings for using the functions of IM Configuration Management	13
1.6 Setting the startup sequence for services	14
1.7 Settings for user authentication and user mapping	15
1.7.1 Specifying the authentication server	16
1.7.2 Registering JP1 users	16
1.7.3 Setting operation permissions for the JP1 users	16
1.7.4 Copying the primary authentication server settings	17
1.7.5 Setting user mapping	17
1.8 Settings for handling JP1/Base failures	19
1.9 Setting the system hierarchy (when IM Configuration Management is used)	20
1.9.1 Setting using IM Configuration Management - View	20
1.9.2 Setting using the export and import functions	22

1.9.3	Settings for managing and monitoring a virtualization system configuration	23
1.10	Setting the system hierarchy (when IM Configuration Management is not used)	24
1.10.1	Setting the configuration definition information	24
1.10.2	Deleting the configuration definition information	25
1.10.3	Changing the configuration definition information	25
1.10.4	Notes about setting the configuration definition information	25
1.11	Setting Event Service	27
1.12	Setting JP1 event forwarding (when IM Configuration Management is used)	28
1.13	Setting JP1 event forwarding (when IM Configuration Management is not used)	29
1.14	Collecting and distributing Event Service definition information (when IM Configuration Management is used)	30
1.15	Collecting and distributing Event Service definition information (when IM Configuration Management is not used)	31
1.16	Setting up a command execution environment	32
1.17	Settings for using the source host name of Event Service in the FQDN format ...	34
1.17.1	Prerequisites	34
1.17.2	Setting method	34
1.17.3	Startup method	34
1.18	Setting up JP1/IM - Manager	36
1.18.1	Settings for using the functions of Central Scope	36
1.18.2	Settings for handling JP1/IM - Manager failures	36
1.18.3	Settings during upgrading	41
1.19	Setting up JP1/IM - View	45
1.19.1	Settings for handling JP1/IM - View failures	45
1.19.2	Setting up IM Configuration Management - View	45
1.19.3	Setting up the JP1/IM - Rule Operation linkage	46
2.	Installation and Setup (for UNIX)	49
2.1	Installation and setup procedures	50
2.2	Preparations required before installation	52
2.2.1	Designing the setup details	52
2.2.2	Configuring the system environment	52
2.2.3	Installing the prerequisite program	52
2.3	Installing	53
2.3.1	Installation procedure	53
2.3.2	How to use the Hitachi Program Product Installer	54
2.3.3	Uninstallation procedure	56
2.3.4	Notes about installing and uninstalling	57
2.4	Creating an IM database	59
2.5	Settings for using the functions of IM Configuration Management	62
2.6	Settings for user authentication and user mapping	63
2.6.1	Specifying the authentication server	64
2.6.2	Registering JP1 users	64

2.6.3	Setting operation permissions for the JP1 users.....	64
2.6.4	Copying the primary authentication server settings.....	65
2.6.5	Setting user mapping.....	65
2.7	Settings for handling JP1/Base failures.....	67
2.8	Setting the system hierarchy (when IM Configuration Management is used).....	68
2.8.1	Setting using IM Configuration Management - View.....	68
2.8.2	Setting using the export and import functions.....	70
2.8.3	Settings for managing and monitoring a virtualization system configuration.....	71
2.9	Setting the system hierarchy (when IM Configuration Management is not used).....	72
2.9.1	Setting the configuration definition information.....	72
2.9.2	Deleting the configuration definition information.....	73
2.9.3	Changing the configuration definition information.....	73
2.9.4	Notes about setting the configuration definition information.....	74
2.10	Setting Event Service.....	75
2.11	Setting JP1 event forwarding (when IM Configuration Management is used).....	76
2.12	Setting JP1 event forwarding (when IM Configuration Management is not used).....	77
2.13	Collecting and distributing Event Service definition information (when IM Configuration Management is used).....	78
2.14	Collecting and distributing Event Service definition information (when IM Configuration Management is not used).....	79
2.15	Setting up a command execution environment.....	80
2.16	Settings for using the source host name of Event Service in the FQDN format.....	82
2.16.1	Prerequisites.....	82
2.16.2	Setting method.....	82
2.16.3	Startup method.....	83
2.17	Setting up JP1/IM - Manager.....	84
2.17.1	Executing the setup program.....	84
2.17.2	Setting automatic startup and automatic stop.....	84
2.17.3	Settings for using the functions of Central Scope.....	86
2.17.4	Settings for handling JP1/IM - Manager failures.....	86
2.17.5	Settings during upgrading.....	90

3. Using IM Configuration Management to Set the System Hierarchy 93

3.1	Registering hosts.....	94
3.1.1	Registering hosts.....	94
3.1.2	Displaying host information.....	94
3.1.3	Deleting hosts.....	95
3.1.4	Changing host information.....	95
3.1.5	Collecting information from hosts.....	96
3.2	Setting the system hierarchy.....	98
3.2.1	Collecting the system hierarchy.....	98
3.2.2	Displaying the system hierarchy.....	99
3.2.3	Verifying the system hierarchy.....	99

3.2.4	Editing the system hierarchy	100
3.2.5	Applying the system hierarchy	102
3.2.6	Synchronizing the system hierarchy	103
3.3	Setting the profiles	104
3.3.1	Collecting profiles	104
3.3.2	Collecting profile lists	106
3.3.3	Displaying profiles	107
3.3.4	Editing configuration files	108
3.3.5	Applying edited information in configuration files	110
3.4	Importing and exporting the management information in IM Configuration Management	113
3.5	Setting a virtualization system configuration	115
3.5.1	Using IM Configuration Management to manage a virtualization configuration	115
3.5.2	Using Central Scope to monitor a virtualization configuration	120
4.	Setting up Central Console	123
4.1	Settings for the operations to be performed during JP1/IM event acquisition	124
4.2	Setting JP1 event filtering	125
4.2.1	Settings for view filters	125
4.2.2	Settings for event receiver filters	128
4.2.3	Settings for severe events filters	130
4.2.4	Settings for event acquisition filters	132
4.3	Setting automated actions	139
4.3.1	Setting up an execution environment for the automated action function ...	139
4.3.2	Setting the execution conditions and details of automated actions	140
4.3.3	Settings for monitoring the automated action execution status	142
4.3.4	Setting suppression of automated action execution	143
4.4	Setting correlation event generation	144
4.4.1	Setting startup of the correlation event generation function	144
4.4.2	Setting the size and number of correlation event generation history files ..	144
4.4.3	Setting startup options	146
4.4.4	Creating and applying a correlation event generation definition	146
4.5	Setting memo entries	148
4.6	Editing event guide information	149
4.6.1	How to edit event guide information	149
4.7	Setting JP1 event issuance during action status change	152
4.8	How to display user-specific event attributes	153
4.8.1	Creating the definition files	156
4.8.2	Enabling the definition files	159
4.9	Setting the severity changing function	160
4.10	Setting JP1/IM - View for each login user	161
4.11	Customizing the JP1/IM - View operation	163
4.12	Setting monitor startup for linked products	164

4.12.1	How to open monitor windows	164
4.12.2	Determining the window to be used for opening monitor windows	165
4.12.3	Creating the definition files	165
4.13	Setting the Tool Launcher window	167
4.13.1	Settings for opening the GUI of linked products from the Tool Launcher window	167
4.13.2	How to add new menus	168
4.13.3	Determining a window to be opened from the Tool Launcher window	168
4.13.4	Creating the definition files	169
4.13.5	Settings for opening the Web page of a linked product from the Tool Launcher window	172
4.14	Settings for using a Web-based JP1/IM - View	174
4.14.1	Installing an HTTP server	174
4.14.2	Setting up the HTTP server	174
4.14.3	Setting up a Web browser	174
4.14.4	Specifying display settings for the Java Console window	175
4.14.5	Setting timeout values for Web-based operation	175

5. Setting up Central Scope 177

5.1	Overview of the Central Scope environment setup	178
5.2	Registering host information	179
5.3	Using the GUI to create a monitoring tree	180
5.3.1	Opening the Monitoring Tree (Editing) window	180
5.3.2	Acquiring an existing monitoring tree	183
5.3.3	Generating a monitoring tree automatically	184
5.3.4	Customizing a monitoring tree	186
5.3.5	Saving a customized monitoring tree at the local host	197
5.3.6	Applying a customized monitoring tree to the manager	198
5.4	Using the GUI to create a Visual Monitoring window	200
5.4.1	Opening an edit window for the Visual Monitoring window	200
5.4.2	Acquiring an existing Visual Monitoring window	201
5.4.3	Customizing a Visual Monitoring window	202
5.4.4	Saving a customized Visual Monitoring window at the local host	207
5.4.5	Applying a customized Visual Monitoring window to the manager	207
5.4.6	Editing the list of Visual Monitoring windows and deleting Visual Monitoring windows	209
5.5	Using saved CSV files to create monitoring windows	210
5.6	Editing guide information	211
5.6.1	How to edit guide information	211
5.7	Setting up a Central Scope operating environment	213
5.7.1	Setting for the maximum number of status change events	213
5.7.2	Setting the completed-action linkage function	213
5.7.3	Settings for automatically deleting status change events when JP1 event handling is completed	214

5.7.4	Settings for initializing monitoring objects when JP1 events are received	215
5.7.5	Setting the memory-resident status change condition function.....	215
5.7.6	Customizing the toolbar for the monitoring tree	216
5.8	Setting up for linked products.....	218
5.8.1	Setup for linkage with JP1/AJS	218
5.8.2	Setup for linkage with JP1/PFM.....	219
5.8.3	Setup for linkage with HP NNM	221
5.8.4	Setup for linkage with JP1/Software Distribution	222
5.8.5	Setup for linkage with JP1/PAM	223
5.8.6	Setup for linkage with Cosminexus.....	223
5.8.7	Setup for linkage with HiRDB	224
5.9	Examples of monitoring object creation.....	226
5.9.1	Example of creating system-monitoring objects (JP1/AJS jobnet monitoring).....	226
5.9.2	Example of creating a general-purpose monitoring object (HiRDB monitoring).....	228
6.	Operation and Environment Configuration in a Cluster System	237
6.1	Overview of cluster operation.....	238
6.1.1	Overview of a cluster system.....	239
6.1.2	Prerequisites for cluster operation	240
6.1.3	JP1/IM configuration in a cluster system	243
6.2	Environment setup for cluster operation (for Windows)	248
6.2.1	Environment setup procedure.....	248
6.2.2	Installing and setting up the logical host	250
6.2.3	Registering into the cluster software (for Windows).....	266
6.2.4	Procedures for changing settings.....	268
6.2.5	Deleting the IM databases and logical host.....	269
6.3	Environment setup for cluster operation (for UNIX)	272
6.3.1	Environment setup procedure.....	272
6.3.2	Installing and setting up the logical host	273
6.3.3	Registering into the cluster software (for UNIX).....	285
6.3.4	Procedures for changing settings.....	289
6.3.5	Deleting the IM databases and logical host.....	290
6.4	Notes about cluster operation	293
6.5	Logical host operation and environment configuration in a non-cluster system ...	294
6.5.1	Evaluating the configuration for running logical hosts in a non-cluster system.....	294
6.5.2	Environment setup for running logical hosts in a non-cluster system.....	294
6.5.3	Logical host operation in the non-cluster system	295
7.	Operation and Environment Configuration Depending on the Network Configuration	301
7.1	Controlling communications by JP1/Base.....	302

7.2	Operating in multiple networks	303
7.2.1	Example 1 (non-cluster operation with JP1/IM - View connection).....	303
7.2.2	Example 2 (non-cluster operation with command execution)	304
7.2.3	Example 3 (cluster operation with JP1/IM - View connection)	306
7.2.4	Example 4 (cluster operation with command execution).....	307
7.3	Operating in a firewall environment.....	310
7.3.1	Basic information about firewalls	310
7.3.2	JP1/IM communication	317
8.	Settings for Linking to Other Integrated Management Products	325
8.1	Linking to JP1/IM - Rule Operation.....	326
8.1.1	Settings for enabling the JP1/IM - Rule Operation linkage function	326
8.1.2	Settings for sending notifications to JP1/IM - Rule Operation	327
8.1.3	Settings for checking notifications on the Event Console window.....	328
Index		329

Chapter

1. Installation and Setup (for Windows)

This chapter explains how to install and set up JP1/IM in a Windows environment.

- 1.1 Installation and setup procedures
- 1.2 Preparations required before installation
- 1.3 Installing
- 1.4 Creating an IM database
- 1.5 Settings for using the functions of IM Configuration Management
- 1.6 Setting the startup sequence for services
- 1.7 Settings for user authentication and user mapping
- 1.8 Settings for handling JP1/Base failures
- 1.9 Setting the system hierarchy (when IM Configuration Management is used)
- 1.10 Setting the system hierarchy (when IM Configuration Management is not used)
- 1.11 Setting Event Service
- 1.12 Setting JP1 event forwarding (when IM Configuration Management is used)
- 1.13 Setting JP1 event forwarding (when IM Configuration Management is not used)
- 1.14 Collecting and distributing Event Service definition information (when IM Configuration Management is used)
- 1.15 Collecting and distributing Event Service definition information (when IM Configuration Management is not used)
- 1.16 Setting up a command execution environment
- 1.17 Settings for using the source host name of Event Service in the FQDN format
- 1.18 Setting up JP1/IM - Manager
- 1.19 Setting up JP1/IM - View

1.1 Installation and setup procedures

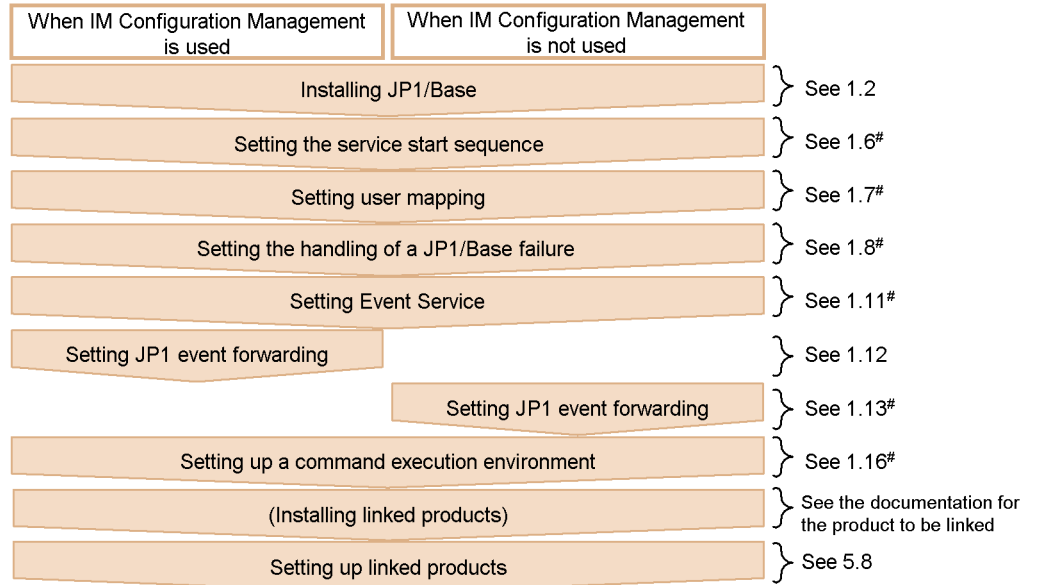
This section describes the procedure from the start of installation to the end of setup for the manager, agent, and viewer.

Figure 1-1: Installation and setup procedure (manager)

When IM Configuration Management is used	When IM Configuration Management is not used	
Installing the prerequisite program • Installing JP1/Base		} See 1.2
Installing JP1/IM - Manager		} See 1.3
Creating an IM database		} See 1.4
Setting use of IM Configuration Management		} See 1.5
Setting the service start sequence		} See 1.6#
Setting user authentication and user mapping		} See 1.7#
Setting the handling of a JP1/Base failure		} See 1.8#
Setting the system hierarchy		} See 1.9
	Setting the system hierarchy	} See 1.10#
Setting Event Service		} See 1.11#
Setting JP1 event forwarding		} See 1.12
	Setting JP1 event forwarding	} See 1.13#
Collecting and distributing Event Service definition information		} See 1.14
	Collecting and distributing Event Service definition information	} See 1.15#
Setting up a command execution environment		} See 1.16#
Setting use of the Event Service's source host name in FQDN format		} See 1.17#
Setting up JP1/IM - Manager • Setting use of the functions of Central Scope • Setting the handling of a JP1/IM - Manager failure • Setting up for upgrading		} See 1.18
(Installing linked products)		} See the documentation for the product to be linked
Setting up linked products		} See 5.8

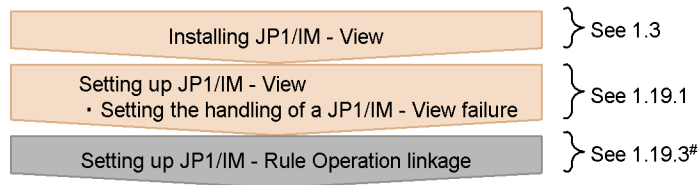
#: For details, see the *Job Management Partner 1/Base User's Guide*.

Figure 1-2: Installation and setup procedure (agent)



#: For details, see the *Job Management Partner 1/Base User's Guide*.

Figure 1-3: Installation and setup procedure (viewer)



#: For details, see the *Job Management Partner 1/Integrated Management - Rule Operation System Configuration and User's Guide*.

1.2 Preparations required before installation

1.2.1 Designing the setup details

Before you start installation, evaluate the details of JP1/IM setup and prepare the setup items.

For details about how to design the setup details, see *Part 3. Design* in the *Job Management Partner 1/Integrated Management - Manager Overview and System Design Guide*.

1.2.2 Configuring the system environment

(1) Configuring the OS environment

Before you install JP1/IM, configure an OS environment that satisfies the following conditions:

- The OS version being used is supported by JP1/IM.
- Service packs and patches required by JP1/IM have been applied.

See the release notes for JP1/IM - Manager and JP1/IM - View to check the service packs and patches required by JP1/IM, and then apply them to the OS.

1.2.3 Installing the prerequisite program

(1) Installing JP1/Base

To use JP1/IM managers and agents, you must install JP1/Base, which is the prerequisite program for JP1/IM.

To check the system configuration, see *1.5 JP1/IM - Manager system configuration* in the *Job Management Partner 1/Integrated Management - Manager Overview and System Design Guide*. For details about how to install JP1/Base, see the *Job Management Partner 1/Base User's Guide*.

1.3 Installing

This section explains how to install and uninstall JP1/IM - Manager and JP1/IM - View. The user who will be performing the installation must have Administrator permissions.

1.3.1 Installation procedure

This subsection explains how to install JP1/IM - Manager and JP1/IM - View.

(1) *How to install*

To install JP1/IM:

1. Terminate all programs.

Before you start the installation, terminate all programs.

Stop the JP1/Base services.

If you are performing an upgrade installation, stop the JP1/Console service. If a JP1/IM - View is connected, log out.

2. Insert the distribution medium in the CD-ROM drive and start the installation.

Follow the instructions of the installer, which starts automatically.

Enter the following items:

- User information

Enter this information only if you are performing a new installation. If you are upgrading from an old version of JP1/IM - Manager, JP1/IM - Central Console, or JP1/IM - Central Scope, the information specified for the old version will be inherited.

- Installation folders

The installation folders listed below are created when you install JP1/IM - Manager and JP1/IM - View.

Table 1-1: Folders created during installation

Product	Folder that is created ^{#1}	Description
JP1/IM - Manager	<i>installation-folder</i> \JP1IMM\#2	Stores JP1/IM - Manager information
	<i>installation-folder</i> \JP1Cons\#2	Stores Central Console information
	<i>installation-folder</i> \JP1Scope\#2	Stores Central Scope information

1. Installation and Setup (for Windows)

Product	Folder that is created ^{#1}	Description
JP1/IM - View	<i>installation-folder</i> \JP1CoView\ ^{#2}	Stores JP1/IM - View information

#1: The default installation folder is "system-drive:\Program Files\HITACHI".

#2: If an old version of JP1/IM - Manager, JP1/IM - Central Console, JP1/IM - Central Scope, or JP1/IM - View was installed in a different folder, that installation folder is inherited and the folders listed above are not created.

Note that the drive that is specified as the installation folder for JP1/IM - Manager and JP1/IM - View must be a fixed disk.

- Program folder (specification of registration location in the **Start** menu)

Specify this information only when you install JP1/IM - View.

Note that a program folder can not be specified if you are installing a Windows Vista or Windows Server 2008 version of JP1/IM - View.

3. If you are prompted to restart the system, restart Windows.

Windows must be restarted when Hitachi Network Objectplaza Trace Library (HNTRLib2) is installed. For details, see the notes below.

When JP1/IM - Manager and JP1/IM - View are installed, the files listed below are created as logs. These files contain maintenance information that is used in the event of abnormal termination of installation. Once JP1/IM - Manager and JP1/IM - View have been installed successfully, start them. If there are no problems, delete the following files:

- *Windows-installation-folder*\Temp\HITACHI_JP1_INST_LOG\jplimm_inst{1|2|3|4|5}.log
- *Windows-installation-folder*\Temp\HITACHI_JP1_INST_LOG\jplcoview_inst{1|2|3|4|5}.log

Note:

You must specify a fixed disk as the drive for the JP1/IM - Manager and JP1/IM - View installation folders. JP1/IM - Manager and JP1/IM - View must not be installed on a removable disk, network drive, or UNC path.

It will not be possible to upgrade JP1/IM - Central Console, JP1/IM - Central Scope, and JP1/IM - View if they are installed anywhere other than on a fixed disk.

(2) About the types of installation**Upgrade installation**

If you are upgrading from an old version, first read the notes about upgrading that you will find in *12.2 Upgrading from a previous version of JP1/IM* in the *Job Management Partner 1/Integrated Management - Manager Overview and System Design Guide*.

Remote installation using JP1/Software Distribution

JP1/IM supports remote installation (software distribution) using JP1/Software Distribution.

By running JP1/Software Distribution on the server where JP1/IM is run, you can perform a new installation as well as an upgrade installation of JP1/IM. For details about how to perform remote installation using JP1/Software Distribution, see the *Job Management Partner 1/Software Distribution Administrator's Guide Volume 1*.

1.3.2 Uninstallation procedure

This subsection explains how to uninstall JP1/IM - Manager and JP1/IM - View.

(1) How to uninstall

To uninstall:

1. Terminate the programs.

Before you start the uninstallation procedure, terminate all programs.

Terminate JP1/IM - Manager Service and the JP1/Base services. If a JP1/IM - View is connected, log out.

2. In Windows, close the Services dialog box.

If the Services dialog box is open in Windows, close it before you start uninstalling the product.

3. In Windows, choose **Control Panel, Add or Remove Programs**, and then select the product that you want to uninstall.

Follow the instructions of the installer to perform uninstallation.

No entries are required during uninstallation.

4. Restart Windows, if requested.
5. Delete user files.

Definition files and log files that were created after installation, as well as files that may be edited by the user, are not deleted during uninstallation. To delete these files, use Windows Explorer to delete the folder in which JP1/IM - Manager

or JP1/IM - View had been installed.

When JP1/IM - Manager or JP1/IM - View is uninstalled, the applicable file listed below is created for installer logs. This file contains maintenance information that can be used in the event of abnormal termination of uninstallation. After uninstallation has terminated normally, delete these files.

- *Windows-installation-folder*\Temp\HITACHI_JP1_INST_LOG\jplimm_inst{1|2|3|4|5}.log
- *Windows-installation-folder*\Temp\HITACHI_JP1_INST_LOG\jplcoview_inst{1|2|3|4|5}.log

1.3.3 Notes about installing and uninstalling

■ Relationship between products

JP1/IM - Manager requires JP1/Base. When you install and uninstall the products, note the following:

- Any prerequisite products must be installed first and in the correct order.
Install JP1/Base and then JP1/IM - Manager, in this order.
- Stop JP1/Base before you install or uninstall JP1/IM - Manager. If you forgot to stop JP1/Base, make sure that you restart JP1/Base. If you do not restart JP1/Base, it will not be possible to manage system configuration information correctly.

■ About Hitachi Network Objectplaza Trace Library (HNTRLib2)

- When you install JP1/IM - View or JP1/Base, Hitachi Network Objectplaza Trace Library (HNTRLib2) is installed, and the path of HNTRLib2 (*system-drive*:\Program Files\Common Files\Hitachi) is added to the Path Windows system environment variable.
- When you uninstall JP1/IM - View or JP1/Base, Hitachi Network Objectplaza Trace Library (HNTRLib2) is deleted unless another product is using it.

■ Settings in the Windows environment

- During installation, the information listed below is set in Windows.

The bin folder path of JP1/IM and the HNTRLib2 path are as follows in the system environment variables:

- *Console-path*\bin

This information is added during installation of JP1/IM - Manager.

- *View-path*\bin

This information is added during installation of JP1/IM - View.

- *system-drive*:\Program Files\Common Files\Hitachi

This information is added when either JP1/IM - View or JP1/Base is installed.

In the *services* file, the port numbers indicated in *C. Port Numbers* in the *Job Management Partner 1/Integrated Management - Manager Overview and System Design Guide* are set. The port numbers are deleted during uninstallation.

- The *Path* system environment variable value that was added during installation is deleted. However, if any program is using Hitachi Network Objectplaza Trace Library (HNTRLib2), the path of HNTRLib2 (*system-drive*:\Program Files\Common Files\Hitachi) is not deleted.
- About changing an installation path
- To change an installation path, first uninstall and then install again.
 - If you are changing the installation path of JP1/Base (by uninstalling it and then reinstalling in a different folder), you must first uninstall JP1/IM - Manager and then reinstall it.
- To reinstall JP1/IM - View on the same host as for JP1/Base, uninstall JP1/IM - View first, delete the files under the *conf* and *bin* folders at the installation destination, and then reinstall JP1/IM - View.
- When you change the installation path of JP1/IM - Manager, JP1/IM - View, or JP1/Base, definitions cannot be recovered from a backup. You must re-specify individual definitions after reinstallation.
- About reinstallation

When JP1/IM - Manager or JP1/IM - View is uninstalled, definition files and log files that were created after installation, as well as files that may be edited by the user, are not deleted. If you reinstall the program while these files remain in the system, the program may not function correctly. Therefore, if you reinstall JP1/IM - Manager or JP1/IM - View, use Windows Explorer to delete the folder in which JP1/IM - Manager or JP1/IM - View had been installed, and then reinstall the program.

1.4 Creating an IM database

To use the IM Configuration Management database to manage a system hierarchy and to use the integrated monitoring database to manage JP1 events, you must create an IM database, which is the collective name for these two databases.

If you do not use the IM Configuration Management database during system configuration or you do not use the integrated monitoring database or the IM Configuration Management database when you start operations, there is no need to create an IM database. You can create the IM database when you need either or both of the integrated monitoring database and the IM Configuration Management database after operations have started.

This section explains how to create an IM database.

(1) Preparations for creating an IM database

You must prepare a *setup information file* that specifies the size of the database area required in order to create an IM database and information about the database storage directory.

To prepare for IM database creation:

1. Edit the setup information file

The following shows an example of the settings:

```
IMDBSIZE=S #IM DATABASE SERVICE - DB Size
IMDBDIR=Manager-path\database #IM DATABASE SERVICE - Data
Storage Directory
IMDBPORT=20700 #IM DATABASE SERVICE - Port Number
IMDBENVDIR=Manager-path\dbms #IM DATABASE SERVICE - DB
Install Directory
```

For details about the setup information file, 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*.

(2) Setting up the integrated monitoring database

Create an integrated monitoring database and use the Central Console functions to set up the database so you can use it. If you do not use the integrated monitoring database, there is no need to perform this procedure.

To execute the `jcodbsetup` command that creates an integrated monitoring database, one of the following conditions must be satisfied:

- Central Console Service is stopped.

- The integrated monitoring database settings are disabled and the IM Configuration Management service is stopped.

To set up the integrated monitoring database:

1. Execute the `jcodbsetup` command to create an integrated monitoring database.

- When an IM Configuration Management database has been set up

```
jcodbsetup -s [-h logical-host-name -c {online|standby}] [-q]
```

- When no IM Configuration Management database has been set up

```
jcodbsetup -f setup-information-file-name [-h logical-host-name -c {online|standby}] [-q]
```

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

2. Execute the `jcoimdef` command to enable the integrated monitoring database.

```
jcoimdef -db ON
```

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*.

To start JP1/IM - Manager and use the integrated monitoring database, the IM database service must be running (return value: 0). Execute the `jimdbstatus` command to check the settings of the integrated monitoring database and the status of the IM database service.

If the operating status is that the IM database service is engaged in start or stop processing (return value: 4), is stopped (return value: 8), or is not running (return value: 16), processing is placed on wait status for the amount of time (in milliseconds) specified in the common definition.

Define the parameter as follows:

```
[logical-host-name\JP1CONSOLEMANAGER\IMDB]
"DB_START_RETRY_INTERVAL"=dword:hexadecimal-value
```

Specify a hexadecimal value in the range 3,000 to 3,600,000 (milliseconds). The default is `dword:0000xbb8` (3,000 milliseconds).

The operating status of the IM database service is checked again.

Checking of the operating status of the IM database service is performed as many times as is specified in the common definition.

Define the parameter as follows:

```
[logical-host-name\JP1CONSOLEMANAGER\IMDB]
```

1. Installation and Setup (for Windows)

```
"DB_START_RETRY_COUNT"=dword:hexadecimal-value
```

Specify a hexadecimal value in the range 0 to 10,000 (times). The default is `dword:0000x12c` (300 times).

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

(3) Setting up the IM Configuration Management database

Create an IM Configuration Management database and set it up so that the IM Configuration Management service can be started from process management. If you do not use the IM Configuration Management database, there is no need to perform this procedure.

To execute the `jcfdbsetup` command that creates an IM Configuration Management database, one of the following conditions must be satisfied:

- Central Console Service is stopped.
- The integrated monitoring database settings are disabled and the IM Configuration Management service is stopped.

To set up the IM Configuration Management database:

1. Execute the `jcfdbsetup` command to create an IM Configuration Management database.

- When an integrated monitoring database has been set up

```
jcfdbsetup -s [-h logical-host-name -c {online|standby}]  
[-q]
```

- When no integrated monitoring database has been set up

```
jcfdbsetup -f setup-information-file-name [-h logical-host-name -c  
{online|standby}] [-q]
```

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

1.5 Settings for using the functions of IM Configuration Management

When a new installation of JP1/IM - Manager is performed, the default is that the functions of IM Configuration Management are disabled. To use IM Configuration Management during system configuration or system operations, you must create an IM Configuration Management database using the procedure described in *1.4 Creating an IM database*, and then enable the functions of IM Configuration Management.

To enable the functions of IM Configuration Management:

1. Execute the `jcoimdef` command to enable the IM Configuration Management service (`jcfmain`).

```
jcoimdef -cf ON
```

2. Restart JP1/IM - Manager.
3. Execute the `jco_spm�_status` command to ensure that the IM Configuration Management service (`jcfmain`) is displayed in the active processes.

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*.

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

1.6 Setting the startup sequence for services

To use the startup control service in JP1/Base to set the startup sequence for the JP1 services:

1. Specify the startup sequence control settings.

Normally, there is no problem with the default settings, but you must customize the settings in the following cases:

- JP1/Power Monitor is being used to manage starting and stopping.
- The IM database is being used.

For details about the settings, see the chapter that describes the settings for the service startup and stop sequences in the *Job Management Partner 1/Base User's Guide*. For details about how to start the IM database, see *3.1 Starting JP1/IM - Manager* in the *Job Management Partner 1/Integrated Management - Manager Administration Guide*.

1.7 Settings for user authentication and user mapping

You must specify information that is required for JP1 user management, such as the authentication server, registration of JP1 users, and user mapping.

Specify the settings as appropriate to the host's role, as shown below.

Table 1-2: Settings depending on host's role

Setting item	Used as authentication server		Not used as authentication server	
	Primary authentication server	Secondary authentication server	Manager host	Agent host
Authentication server specification	Y	Y	Y	--
JP1 user setting	Y	--	--	--
Operation permission setting	Y	--	--	--
Copy of authentication server setting	--	Y	--	--
User mapping	Y	Y	Y	Y

Legend:

Y: Setting is required

--: Setting is not required

You specify the settings using either the JP1/Base Environment Settings dialog box or JP1/Base commands.

You must set user mapping at all hosts where commands are executed by an automated action or a JP1/IM - View operation.

Table 1-3: User mapping when commands are executed by an automated action or JP1/IM - View

Operation	JP1 user name	Server host name	OS user name
When executing commands from JP1/IM - View	User who logs on to the manager	Manager to which JP1/IM - View connects [#]	User who is registered in the OS of the host where the command is executed

Operation	JP1 user name	Server host name	OS user name
When executing an automated action	User name specified in the action definition	Manager that defined the automated action [#]	User who is registered in the OS of the host where the action is executed

#

You can also specify an asterisk (*) as the server host name, in which case user mapping is permitted at all hosts.

The JP1 user `jp1admin` is registered by default. For `jp1admin`, operation permissions whose JP1 resource group is * and JP1 authority level is `JP1_Console_Admin` have been set (JP1 resource group * can access all JP1 resource groups).

1.7.1 Specifying the authentication server

Specify the host name of the authentication server. This setting is required for the host and the JP1/IM manager, but not for the agent.

To specify the authentication server:

1. Specify the authentication server.

Specify the authentication server in **Order of authentication server** on the **Authentication Server** page.

You can set a maximum of two authentication servers (primary and secondary servers).

For details about how to specify the settings, see the chapter that describes user management settings in the *Job Management Partner 1/Base User's Guide*.

1.7.2 Registering JP1 users

Register the JP1 users who will use JP1/IM. This is required at the host of the primary authentication server.

To register JP1 users:

1. Register JP1 users.

In **JP1 user** on the **Authentication Server** page, register the JP1 users and set passwords for them.

1.7.3 Setting operation permissions for the JP1 users

Register operation permissions for the JP1 users who will use JP1/IM. This is required at the host of the primary authentication server.

To set operation permissions for the JP1 users:

1. Set operation permissions for the JP1 users.

In **Authority level for JP1 resource group** on the **Authentication Server** page, set operation permissions for the JP1 users.

For example, as JP1/IM operation permissions, you can specify `JP1_Console` for a JP1 resource group and `JP1_Console_Admin` for a permission level.

As operation permissions for IM Configuration Management, you must set `JP1_Console` for the JP1 resource group and both JP1/IM permission level and IM Configuration Management permission level as permission levels. If you do not set any permission level for IM Configuration Management, you can execute operations only within the range of the JP1 permission level `JP1_CF_User` for IM Configuration Management.

For details about the operation permissions for JP1/IM, see *7.4.1 Managing JP1 users* and *Appendix E. Operating Permissions* in the *Job Management Partner 1/Integrated Management - Manager Overview and System Design Guide*.

1.7.4 Copying the primary authentication server settings

Copy the settings files for the primary authentication server. These settings are required at the host of the secondary authentication server.

To copy the primary authentication server settings:

1. Copy the settings files for the authentication server.

Copy the settings files `JP1_Group`, `JP1_Passwd`, and `JP1_UserLevel` that are stored in the *Base-path*\conf\user_acl\ folder. These are text files. Use a method such as an ASCII transfer by FTP.

1.7.5 Setting user mapping

At a host where you execute commands by automated action and JP1/IM - View operations, set user mapping between JP1 user names and OS user names. This setting is required for all hosts that execute commands from JP1/IM.

To set user mapping:

1. Register the OS user names and passwords.

Set the information in **Password management** on the **User Mapping** page.

2. Set the JP1 user names and host names.

Set the information in **JP1 user** on the **User Mapping** page.

3. Map JP1 users and OS users.

In the JP1 User dialog box, click the **OK** button to display the OS User Mapping

Details dialog box, and then set user mapping.

If there are multiple users, you must set user mapping for all of them. User mapping is required even when a JP1 user name is the same as the OS user name.

The commands that are executed by automated action and JP1/IM - View operations are executed by a primary user who has been mapped to a JP1 user. To execute commands by a specific OS user, register that OS user as the primary user.

For details about user mapping, see the description of the user management settings in the *Job Management Partner 1/Base User's Guide*.

1.8 Settings for handling JP1/Base failures

JP1/Base provides the following functions to minimize the effects of JP1/Base failures on system operation:

- Function for detecting process errors (health check function)
- Function for automatically restarting processes in the event of abnormal process termination
- Function for issuing JP1 events when abnormalities are detected in processes and authentication servers
- Tool for collecting data necessary for investigation in the event of a JP1/Base failure

By default, all functions for detecting process errors, restarting processes, and issuing JP1 events are disabled. To change the settings, see the chapter that describes installation and setup in the *Job Management Partner 1/Base User's Guide*.

JP1/Base also provides the data collection tool to enable the user to collect troubleshooting data promptly.

For details about the data that can be collected by JP1/Base's data collection tool, see the *Job Management Partner 1/Base User's Guide*. The data that can be collected by this tool includes memory dumps and crash dumps. You must set these dumps to be output beforehand. For details, see the *Job Management Partner 1/Base User's Guide*.

1.9 Setting the system hierarchy (when IM Configuration Management is used)

This section explains how to set the system hierarchy when IM Configuration Management is used. For details about how to set the system hierarchy when IM Configuration Management is not used, see *1.10 Setting the system hierarchy (when IM Configuration Management is not used)*.

When you use IM Configuration Management, you must use IM Configuration Management - View to set the manager and agent hierarchical structure of the system that is managed by JP1/IM.

You can also use the export and import functions of IM Configuration Management to migrate a system configuration from a test environment to the operating environment or from the environment before a change to the environment after the change.

The export and import functions of IM Configuration Management enable you to specify settings for managing a system hierarchy that includes virtual hosts (virtualization system configuration), as well as settings for using Central Scope for monitoring.

When you use IM Configuration Management to manage your system hierarchy, do not edit the configuration management function settings file provided by JP1/Base, or execute commands.

1.9.1 Setting using IM Configuration Management - View

This subsection explains how to use IM Configuration Management - View to set the system hierarchy.

If you have added IM Configuration Management to an existing JP1/IM system that does not use IM Configuration Management, IM Configuration Management - View enables you to edit the configuration definition information collected from the existing JP1/IM system and set the system hierarchy.

This subsection explains how to set a new system hierarchy and how to edit the hierarchy of an existing system.

(1) Setting a new system hierarchy

There are two ways to define a system hierarchy: by using the highest manager to define the entire system hierarchy in batch mode, and by dividing the system hierarchy into smaller sections that are managed by individual managers, and then defining each section.

For examples of the management and configuration definition of a system hierarchy, see *6.2.1 Hierarchical configurations managed by IM Configuration Management* in the *Job Management Partner 1/Integrated Management - Manager Overview and*

System Design Guide.

The following provides an overview of how to set a new system hierarchy.

To set a new system hierarchy:

1. Register a host that is to be added to the system hierarchy as a management target of IM Configuration Management.
 - For details about how to register hosts and how to set information about hosts, see *3.1.1 Registering hosts*.
 - For details about how to view information about the registered hosts, see *3.1.2 Displaying host information*.
 - For details about how to delete hosts, see *3.1.3 Deleting hosts*.
 - For details about how to change information about the registered hosts, see *3.1.4 Changing host information*.

2. Add the host registered in IM Configuration Management to the system hierarchy and set the hierarchy between managers and agents.

Add the host registered to IM Configuration Management to the system that is managed by JP1/IM, and set the hierarchy between the managers and the agents.

- For details about how to add hosts to a JP1/IM system, see *3.2.4(1) Adding hosts*.
- For details about how to set a hierarchy between managers and agents, see *3.2.4(2) Moving hosts*.
- For details about how to delete hosts from the JP1/IM system, see *3.2.4(3) Deleting hosts*.

3. Apply the set system hierarchy to the system.

Apply the system hierarchy that was set by IM Configuration Management - View to the system that is managed by JP1/IM.

- For details about how to apply the set system hierarchy to the system, see *3.2.5 Applying the system hierarchy*.
- For details about how to check the set system hierarchy, see *3.2.2 Displaying the system hierarchy*.

If you divide the system hierarchy into integrated manager and site managers, perform the above procedure for each manager. After that, use the IM Configuration Management - View that is connected to the integrated manager to perform the procedure described below to create a definition for the entire system.

To set a new system hierarchy:

1. Synchronize the system hierarchy.

Synchronize the configuration definition information between the integrated manager and site managers.

For details about how to synchronize the system hierarchy, see 3.2.6 *Synchronizing the system hierarchy*.

(2) Editing an existing system hierarchy

The following provides an overview of how to edit the configuration definition information that is collected from an existing JP1/IM system.

To edit an existing system hierarchy:

1. Collect the configuration definition information from the existing JP1/IM system.

For details about how to collect configuration definition information from an existing JP1/IM system, see 3.2.1 *Collecting the system hierarchy*.

2. Verify that the collected configuration definition information matches the configuration definition information held by IM Configuration Management.

For details about how to verify configuration definition information, see 3.2.3 *Verifying the system hierarchy*.

3. Edit the system hierarchy.

- For details about how to add hosts to the JP1/IM system, see 3.2.4(1) *Adding hosts*.
- For details about how to set the hierarchy between managers and agents, see 3.2.4(2) *Moving hosts*.
- For details about how to delete hosts from the JP1/IM system, see 3.2.4(3) *Deleting hosts*.

4. Apply the set system hierarchy to the system.

Apply the system hierarchy that was set by IM Configuration Management - View to the system that is managed by JP1/IM.

- For details about how to apply the set system hierarchy to the system, see 3.2.5 *Applying the system hierarchy*.
- For details about how to check the set system hierarchy, see 3.2.2 *Displaying the system hierarchy*.

1.9.2 Setting using the export and import functions

The export and import functions of IM Configuration Management enable you to migrate a system configuration from a test environment to an operating environment and to migrate a system hierarchy from the environment before a change to the environment after the change. For details about how to set the system hierarchy using the export and import functions, see 3.4 *Importing and exporting the management*

information in IM Configuration Management.

1.9.3 Settings for managing and monitoring a virtualization system configuration

The export and import functions of IM Configuration Management enable you to use IM Configuration Management to manage the configuration definition information for a virtualization system configuration, and to use Central Scope to monitor the virtualization system configuration. For details about how to set up an environment for managing and monitoring a virtualization system configuration, see *3.5 Setting a virtualization system configuration.*

1.10 Setting the system hierarchy (when IM Configuration Management is not used)

This section describes the system hierarchy settings when IM Configuration Management is not used. For details about the system hierarchy settings when IM Configuration Management is used, see *1.9 Setting the system hierarchy (when IM Configuration Management is used)*.

When you are not using IM Configuration Management, you must use the configuration management function provided by JP1/Base to set the hierarchical structure between managers and agents in a system that is managed by JP1/IM.

There are two ways to define a system hierarchy: by using the highest manager to define the entire system hierarchy in batch mode, and by dividing the system hierarchy into smaller sections that are managed by individual managers, and then defining each section.

If you are using IM Configuration Management to manage your system hierarchy, do not edit the definition files for the configuration management function provided by JP1/Base, or execute commands.

For examples of system hierarchy management and configuration definitions, see *7.4.3 Managing the system hierarchy* in the *Job Management Partner 1/Integrated Management - Manager Overview and System Design Guide*.

1.10.1 Setting the configuration definition information

To set the configuration definition information:

1. At the manager, create a configuration definition file (`jbs_route.conf`).
To define the system hierarchy in batch mode, specify the entire system hierarchy in the definition file. To divide the system hierarchy into multiple sections, specify in the definition file the managed hosts and managers that are under that manager.
2. At the manager, execute the setting command (`jbsrt_distrib`).
The command will update the definition information.

If you divide the system hierarchy into multiple sections, perform the above procedure for each manager. After that, perform the procedure described below at the highest manager to create a definition for the entire system.

To set the configuration definition information:

1. At the highest manager, create the configuration definition file. (`jbs_route.conf`).

Specify the system hierarchy from the highest manager to the next highest manager in the definition file.

2. At the highest manager, execute the setting command (`jbsrt_sync`).

To check the contents of the configuration definition information, execute the `jbsrt_get` command on each host.

1.10.2 Deleting the configuration definition information

To delete the configuration definition information, such as clearing the definitions:

1. At the manager, provide a configuration definition file (`jbs_route.conf`).
If there is no configuration definition file, create a file that specifies only the local host name.
If there is an existing file, use it as is.
2. At the manager, execute the setting command (`jbsrt_distrib`).

If configuration definition information was not deleted from a host because JP1/Base was not running, execute the `jbsrt_del` command at that host to delete the configuration definition information, and then execute the `jbsrt_distrib` command at the highest manager.

1.10.3 Changing the configuration definition information

If you change the configuration definition information, follow the same procedure as in *1.10.1 Setting the configuration definition information*. This will distribute the post-change configuration definition information.

Changing the highest manager

To change the highest manager in the system:

1. First, delete the configuration definition information at the highest manager.
At the highest manager before the change, delete the configuration definition information using the procedure described in *1.10.2 Deleting the configuration definition information*.
2. At the highest manager after the change, set the configuration definition information.
At the highest manager after the change, set the configuration definition information using the procedure described in *1.10.1 Setting the configuration definition information*.

1.10.4 Notes about setting the configuration definition information

When configuration definition information is distributed, JP1/Base must be running at each host. This subsection describes the effects when JP1/Base is inactive, and the

actions to be taken.

■ Effects of inactive JP1/Base

Configuration definition information is managed by JP1/Base. If JP1/Base is not running at a host that is defined in the configuration definition information, distribution of configuration definition information will fail. In such a case, take the following actions:

1. Continue processing even if the message KAVB3107-E Cannot set configuration in the host is displayed when the `jbsrt_distrib` command executes.

The configuration definition information will be distributed to the hosts where JP1/Base is running.

2. Start JP1/Base at the host where definition was not distributed, and then execute the `jbsrt_distrib` command again.

■ Effects of inactive JP1/Base Event Service

The configuration definition information is related to JP1 event forwarding. When the `jbsrt_distrib` or `jbsrt_del` command is executed, the `jevreload` command executes automatically and the Event Service's forwarding settings are updated (reloaded). If Event Service is not running during this reload processing, configuration definition information will be distributed, but the JP1 event destination information will not be updated. In such a case, restart Event Service.

For details about the configuration definition information, see the *Job Management Partner 1/Base User's Guide*.

1.11 Setting Event Service

To set each host in order to manage events by means of JP1/IM using JP1 events:

1. Set up an Event Service environment.

Normally, the default settings can be used for operation, but in the following cases, you must customize the settings:

- The capacity of the event database is to be increased.
- JP1/IM manages events that are in the JP1/SES format.

JP1/IM - Manager collects JP1 events from JP1/Base (Event Service) using the user name `SYSTEM`. If you specify the `users` parameter in the event server settings file (`conf`) of the JP1/Base (Event Service) that is running on the same host, include `SYSTEM`. If `SYSTEM` is not included, JP1/IM - Manager will no longer start successfully.

2. Set event conversions.

To use JP1 events to manage log files, SNMP traps, and Windows event logs, set the event conversions.

For details about the settings, see the chapter that describes the setting of an Event Service environment and event conversion in the *Job Management Partner 1/Base User's Guide*.

1.12 Setting JP1 event forwarding (when IM Configuration Management is used)

This section describes the JP1 event forwarding settings when IM Configuration Management is used.

When you use IM Configuration Management, you use IM Configuration Management - View to specify JP1 event forwarding settings.

In the JP1 event forwarding settings, you set each host in such a manner that the JP1 events managed by JP1/IM are forwarded to the higher JP1/IM manager.

Normally, the default settings can be used for operation, but in the following cases, you must customize the settings:

- JP1/IM manages JP1 event severity notification and information events.
- JP1/IM manages events that are in the JP1/SES format.

By default, events are forwarded according to the hierarchy definition that is specified as explained in *1.9 Setting the system hierarchy (when IM Configuration Management is used)*.

If you use IM Configuration Management, you can change the event forwarding settings by editing the event forwarding information settings file on the **Configuration File** page in the Display/Edit Profiles window. For details about how to edit the settings file, see *3.3.4 Editing configuration files*.

1.13 Setting JP1 event forwarding (when IM Configuration Management is not used)

This section describes the JP1 event forwarding settings when IM Configuration Management is not used.

If you do not use IM Configuration Management, you use the configuration management function provided by JP1/Base to specify the JP1 event forwarding settings.

In the JP1 event forwarding settings, you set each host in such a manner that the JP1 events managed by JP1/IM are forwarded to the higher JP1/IM manager.

Normally, the default settings can be used for operation, but in the following cases, you must customize the settings:

- JP1/IM manages JP1 event severity notification and information events.
- JP1/IM manages events that are in the JP1/SES format.

By default, events are forwarded according to the hierarchy definition that is specified as explained in *1.10 Setting the system hierarchy (when IM Configuration Management is not used)*.

For details about the settings, see the chapter that provides details of the forwarding settings file in the *Job Management Partner 1/Base User's Guide*.

1.14 Collecting and distributing Event Service definition information (when IM Configuration Management is used)

This section describes the collection and distribution of Event Service definition information when IM Configuration Management is used.

When you use IM Configuration Management, you use IM Configuration Management - View to collect and distribute Event Service definition information.

In a system consisting of JP1/Base and JP1/IM, the manager can collect and distribute in batch mode Event Service definition information from and to multiple hosts on which JP1/Base version 9 is running. This means that you can use the manager to centrally manage Event Service definition information for each host without having to check and define the definition information at each host.

When you use IM Configuration Management, you can collect and distribute the following definition information:

- Forwarding settings file
- Log file trap operation definition file
- Event log trap operation definition file
- Local action definition file

When you use IM Configuration Management, you can collect Event Service definition information by collecting profiles (valid configuration information and configuration files) on the **Host List** or **IM Configuration** page in the IM Configuration Management window. For details about how to collect profiles, see *3.3.1 Collecting profiles*.

Furthermore, if you use IM Configuration Management, you can distribute Event Service definition information to the hosts on which JP1/Base is running by applying edited information to the configuration file on the **Host List** or **IM Configuration** page in the IM Configuration Management window. For details about how to apply edited information to the configuration files, see *3.3.5 Applying edited information in configuration files*.

1.15 Collecting and distributing Event Service definition information (when IM Configuration Management is not used)

This section describes the collection and distribution of Event Service definition information when IM Configuration Management is not used.

When you do not use IM Configuration Management, you use the definition collection and distribution function provided by JP1/Base to collect and distribute Event Service definition information.

In a system consisting of JP1/Base and JP1/IM, the manager can collect and distribute Event Service definition information from and to multiple hosts in batch mode. This means that you can use the manager to centrally manage Event Service definition information for each host without having to check and define the definition information at each host.

You can collect and distribute information in the following files:

- Forwarding settings file
- Log file trap operation definition file
- Event log trap operation definition file

For details about how to collect and distribute definition information without using IM Configuration Management, see the chapter that describes collection and distribution of Event Service definition information in the *Job Management Partner 1/Base User's Guide*.

1.16 Setting up a command execution environment

You must specify the settings described below in order to set up a command execution environment in which the automated action function and commands are executed from the Execute Command window of JP1/IM - View.

Of the steps below, step 1 is used only once at the time of upgrading from JP1/Base version 7 or earlier. In the case of a new installation, start the procedure from step 2.

To set up a command execution environment:

1. Migrating command execution log files to version 8

Execute the `jcocmdconv` command to migrate the command execution logs accumulated by version 7 or earlier to command execution log files for version 8.

For details about how to migrate command execution logs, see the following:

12.2.6 Upgrading from JP1/Base version 7 in the Job Management Partner 1/ Integrated Management - Manager Overview and System Design Guide

12.2.7 Upgrading from JP1/Base version 6 in the Job Management Partner 1/ Integrated Management - Manager Overview and System Design Guide

2. Setting up a command execution environment

Execute the `jcocmddef` command to set up a command execution environment.

We recommend that you adjust the number of commands that can be executed concurrently. To do this, execute the command as follows:

Example: Set the number of commands that can be executed concurrently to 3

```
jcocmddef -execnum 3
```

3. Creating an environment variable file

If you will use an environment variable file during command execution, create it.

4. Defining host groups

If necessary, define host groups (groups of hosts at which a command can be executed simultaneously).

For details about the command execution environment, see the following:

About command execution environments

- `jcocmdconv` command

See the chapter that describes commands in the *Job Management Partner 1/ Base User's Guide*.

- `jcocmddef` command

See the chapter that describes commands in the *Job Management Partner 1/ Base User's Guide*.

- Creation of an environment variable file

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

- Host group definition

See *Host group definition file* in 2. *Definition Files* in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.

1.17 Settings for using the source host name of Event Service in the FQDN format

JP1/IM - Manager supports operation in which the source host name of Event Service is used in the FQDN format. By using the source host name of Event Service in the FQDN format, you can monitor JP1 events in a system that consists of multiple domains.

This section describes the prerequisites and the setting and startup methods for using the source host name of Event Service on the manager in the FQDN format. The setting described here is not needed when you use the source host name of Event Service on an agent in the FQDN format.

1.17.1 Prerequisites

To use the source host name of JP1/Base Event Service on the JP1/IM host in the FQDN format, the following conditions must be satisfied:

- This is a physical host environment.
- The `hostname` command executed on the JP1/IM - Manager host returns a host name in the short name format.

1.17.2 Setting method

You must release the dependencies between JP1/IM - Manager Service and JP1/Base Event Service. At JP1/Base, set the event server in the FQDN format and then use the following procedure to release the service dependencies.

To set:

1. At the command prompt, execute the following command to release the dependencies between JP1/IM - Manager Service and JP1/Base Event Service:
`SpmSetSvcCon -setdepend no`

For details about how to set the event server in the FQDN format, see the following descriptions in the *Job Management Partner 1/Base User's Guide*:

- Setting the event server in a system using DNS
- Notes about Event Service

For details about the `SpmSetSvcCon` command, see the Release Notes for JP1/IM - Manager.

1.17.3 Startup method

Because no dependencies are set between JP1/IM - Manager Service and the FQDN-format JP1/Base Event Service, you must start the FQDN-format JP1/Base

Event and JP1/Base services before you start JP1/IM - Manager Service. Start the services in the order shown below.

To start services:

1. Start the JP1/Base `Event_FQDN-host-name` service.
2. Start the JP1/Base service.
3. Start the JP1/IM - Manager Service.

1.18 Setting up JP1/IM - Manager

This section describes the setup items for JP1/IM - Manager.

The user who performs this setup must have Administrator permissions.

1.18.1 Settings for using the functions of Central Scope

When a new installation of JP1/IM - Manager is performed, the functions of Central Scope are disabled by default.

To use the functions of Central Scope:

1. Create a Central Scope database.
Execute the `jcsdbsetup` command.
2. Enable Central Scope Service (`jcsmain`).
Execute `jcoimdef -s ON`.
3. Restart JP1/IM - Manager.
4. Verify that Central Scope Service is running.
Execute the `jco_spmd_status` command. Make sure that `jcsmain` is displayed as an active process.

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

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*.

1.18.2 Settings for handling JP1/IM - Manager failures

JP1/IM - Manager provides functions to protect against its own failures, such as the tool for collecting data needed for resolving problems and the function for automatic restart in the event of abnormal process termination.

This subsection describes the settings for handling JP1/IM - Manager failures.

(1) Preparations for collecting data in the event of a failure

JP1/IM - Manager provides a batch file (`jim_log.bat`) as a tool for collecting data in the event of a problem. This tool enables you to collect data needed for resolving problems in batch mode.

The data collection tool of JP1/IM - Manager can collect troubleshooting data for JP1/IM - Manager, JP1/Base, and JP1/IM - View (on the same host). For details about the

data that can be collected, see 9.3 *Data that needs to be collected when a problem occurs* in the *Job Management Partner 1/Integrated Management - Manager Administration Guide*.

About the data collection tool

- About jim_log.bat

See *jim_log.bat (Windows only)* in *1. Commands* in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.

In the event of a problem, it may be advisable to obtain a memory dump and a crash dump. To collect these dumps, specify the settings described below so that memory and crash dumps are output (when these output settings are specified, these dumps can also be collected by the data collection tool).

Memory dump output settings

- In Windows Server 2003
 1. From **Control Panel**, double-click **System**.
 2. On the **Advanced** page, in **Startup and Recovery**, click the **Settings** button.
 3. In **Write debugging information**, select **Kernel memory dump**, and then specify an output file.

Note:

The size of a memory dump depends on the size of the real memory. If the installed physical memory is large, the size of a memory dump will also be large. Take care to allocate sufficient disk space for collecting a memory dump. For details, see the Windows Help topic **Stop error**.

Crash dump output settings

- In Windows Server 2003
 1. From the **Start** menu, choose **Run**.
 2. In the text box, enter `drwtsn32` and then click the **OK** button.
The Dr. Watson for Windows dialog box appears.
 3. Select the **Create Crash Dump File** check box and then specify the output file in the **Crash Dump** text box.
 4. Click the **OK** button.

Note:

In addition to JP1 information, error information for other application programs is also output to the crash dump. For this reason, output of a crash dump requires a fair amount of disk space. If you specify the setting to output crash dumps, take care that sufficient disk space is available.

(2) Restart settings in the event of abnormal process termination

To specify restart settings in the event of abnormal process termination:

1. Define process restart.

Edit the following extended startup process definition file so that process restart is enabled:

Console-path\conf\jplco_service.conf

The restart parameter is the fourth value separated by the vertical bars (|). Set either 0 (do not restart (default)) or 1 (restart). Do not change any of the first three values.

2. Apply the definition information.

If JP1/IM - Manager is running, execute JP1/IM - Manager's reload command so that the process restart setting is enabled:

jco_spmc_reload

3. Set Dr. Watson (applicable to Windows Server 2003).

To enable process restart, set the Dr. Watson dialog box to be hidden. This is because a process cannot restart if the Dr. Watson dialog box is displayed in the event of an applicable error.

From the **Start** menu, choose **Run**, then execute **drwtsn32**. When the Dr. Watson dialog box appears, clear the **Visual Notification** check box.

Note that because the Dr. Watson settings are common settings, the setting specified here applies to all programs in the entire system.

To enable the Dr. Watson settings, execute the following command at the command prompt:

drwtsn32 -i

Dr. Watson is installed as the default application debugger.

4. Suppress error reporting to Microsoft.

In Windows Server 2003

When you enable process restart, you must specify settings so that the Microsoft error reporting dialog box, which is displayed in the event of an error detection, is not displayed. This is because a process cannot restart if

this dialog box is displayed.

1. From **Control Panel**, double-click **System**.
2. On the **Advanced** page, click the **Error Reporting** button.
3. Choose **Disable error reporting** and make sure that the **But notify me when critical errors occur** check box is not selected.

In Windows Server 2008

1. In the **Run** text box, enter `wercn` and then click the **OK** button.
The Problem Reports and Solutions dialog box appears.
2. In the left-hand frame, click **Change settings**.
3. Choose **Advanced settings**.
4. In **Advanced settings for problem reporting**, choose **Off**, and then click the **OK** button.

About process restart definition

- About the extended startup process definition file (`jp1co_service.conf`)
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*.

(3) Setting JP1 event issuance in the event of abnormal process termination

To set JP1 event issuance in the event of abnormal process termination:

1. Set JP1 event issuance.

Edit the following IM parameter definition file:
`Console-path\conf\jp1co_param_v7.conf`

In this file, `SEND_PROCESS_TERMINATED_ABNORMALLY_EVENT` and `SEND_PROCESS_RESTART_EVENT` are the JP1 event issuance setting parameters. To issue JP1 events, change the value to `dword:1`.

2. Execute the `jbssetcnf` command to apply the definition information.
`jbssetcnf Console-path\conf\jp1co_param_v7.conf`
3. Restart JP1/Base and the products that require JP1/Base.

The specified settings take effect after the restart.

About JP1 event issuance settings

- About the IM parameter definition file (`jp1co_param_v7.conf`)
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.

(4) Setting the health check function

To set the health check function in order to detect JP1/IM - Manager process hang-ups:

1. Open the health check definition file (`jcohc.conf`) and specify parameters.

To enable the health check function, specify `ENABLE=true`.

Specify `EVENT=true` to issue a JP1 event and `COMMAND=command-to-be-executed` to execute a notification command when a hang-up is detected.

2. If you specified a notification command, execute the `jcohcetest` command to check the notification command's execution validity.

Execute the `jcohcetest` command to determine whether the command specified in `COMMAND` executes correctly. If the operation is not valid, check and, if necessary, revise the specification.

3. Use the `jco_spmc_reload` command to reload JP1/IM - Manager, or restart JP1/IM - Manager.

About the health check function settings

- About the health check definition file (`jcohc.conf`)

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*.

- About the `jcohcetest` command

See *jcohcetest* in 1. *Commands* in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.

(5) Automatic backup and recovery settings for a monitoring object database

You specify these settings when you will be using the functions of Central Scope.

If the OS shuts down while the monitoring tree is being updated, or a failover occurs during cluster operation, the monitoring object database may be corrupted. Therefore, you must set the monitoring object database to be backed up and recovered automatically when the monitoring tree is being updated.

These settings are enabled when you have performed a new installation, and they are disabled if the settings were disabled in the old version of JP1/IM - Manager or JP1/IM - Central Scope. Change the settings as appropriate to your operation.

To specify automatic backup and recovery settings for a monitoring object database:

1. Terminate JP1/IM - Manager.
2. Execute the `jbssetcnf` command using the following file for the parameters:

To enable the automatic backup and recovery functions for the monitoring object database: `auto_dbbackup_on.conf`

To disable the automatic backup and recovery functions for the monitoring object database: `auto_dbbackup_off.conf`

When you execute the `jbssetcnf` command, the settings are applied to the JP1 common definition information.

For details about the `jbssetcnf` command, see the *Job Management Partner 1/Base User's Guide*.

About the settings in the file

For details about the settings in the file, 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*.

3. Start JP1/IM - Manager.

1.18.3 Settings during upgrading

This subsection describes the setup items to be specified during upgrade installation of JP1/IM - Manager.

(1) **Changing the location of the event acquisition filter**

If you have upgraded JP1/IM - Central Console, you can use the event acquisition filter (for compatibility).

If you had been using an event acquisition filter (for compatibility) with an old version of JP1/IM - Manager or JP1/IM - Central Console, you can change the location of the event acquisition filter from Event Console Service to Event Base Service by executing the `jcochafmode` command. If you change the location of the event acquisition filter to Event Base Service, the filter can be used not only for monitoring JP1 events but also for monitoring the status of automated actions and monitored objects. You can also define detailed filter conditions. Note that if you want to continue using the pre-upgrade event acquisition filter, there is no need to change the filter location.

Note:

Once you change the location of the event acquisition filter, you can no longer restore the previous event acquisition filter. Carefully consider the location of the event acquisition filter before you execute the `jcochafmode` command.

To change the location of the event acquisition filter:

1. Terminate JP1/IM - Manager.
2. Execute the `jcochafmode` command to change the location of the filter.
3. Start JP1/IM - Manager.

- About the functions of the event acquisition filter

See 3.2.2 *Event acquisition filter* in the *Job Management Partner 1/Integrated Management - Manager Overview and System Design Guide*.

- About inheriting the settings of the event acquisition filter (for compatibility)

See 12.2.3(2) *Upgrading from JP1/IM - Central Console version 7* in the *Job Management Partner 1/Integrated Management - Manager Overview and System Design Guide*.

- About the `jcochafmode` command

See `jcochafmode` in 1. *Commands* in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.

(2) Executing the Central Scope upgrade command

If you have upgraded JP1/IM - Central Scope from version 8 or earlier, apply the procedure below to execute the upgrade command. Until you execute the upgrade command, JP1/IM - Central Scope will run in the mode that is compatible with the old version of JP1/IM - Central Scope (no new functions can be used).

To execute the Central Scope upgrade command:

1. Terminate JP1/IM - Manager.
2. Check the available disk capacity.

To execute the `jp1csverup.bat` command in the next step, you will need sufficient free space for the monitoring object database. The monitoring object database includes all the data in the following folder:

Scope-path\database\jcsdb\

3. Execute the `jp1csverup.bat` command.
4. Execute the `jbssetcnf` command.

Whether the following functions are enabled or disabled depends on the settings of the old version of JP1/IM - Central Scope:

- Completed-action linkage function
- Monitoring of the maximum number of status change events

To enable these functions, execute the `jbssetcnf` command using the files shown in the table below as arguments.

Table 1-4: Setting files for enabling functions

File name	Description
<code>action_complete_on.conf</code>	File for enabling the completed-action linkage function
<code>evhist_warn_event_on.conf</code>	File for enabling the JP1 event issuance function when the number of status change events for the monitored object exceeds the maximum value (100)

5. Start JP1/IM - Manager.
6. Use JP1/IM - View to connect to JP1/IM - Manager (JP1/IM - Central Scope) to check for any problems.

- About the `jp1csverup.bat` command

See *jp1csverup.bat (Windows only)* in *1. Commands* in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.

(3) Updating the automated action definition file

If you have upgraded JP1/IM - Central Console from version 08-01 or earlier, apply the procedure below to update the automated action definition file.

If you want to continue using the automated action definition file for version 08-01 or earlier as is, there is no need to perform this procedure.

To update the automated action definition file:

1. Terminate JP1/IM - Manager.
2. Execute the following `jcadefconv` command to update the automated action definition file:

```
jcadefconv -i action-definition-file-name-before-conversion -o
action-definition-file-name-after-conversion
```

3. Start JP1/IM - Manager.

1. Installation and Setup (for Windows)

- About the automated action function

See *5. Command Execution by Automated Action* in the *Job Management Partner 1/Integrated Management - Manager Overview and System Design Guide*.

- About the `jcdefconv` command

See `jcdefconv` in *1. Commands* in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.

1.19 Setting up JP1/IM - View

This section describes the setup items for JP1/IM - View.

The user who performs this setup must have Administrator permissions.

1.19.1 Settings for handling JP1/IM - View failures

To protect against failures, JP1/IM - View provides a tool for collecting data needed for resolving problems. We recommend that you specify dump output settings so that a Windows crash dump and memory dump can be collected when the tool is used in conjunction with a JP1/IM - View failure.

JP1/IM - View provides as a batch file (`jcoview_log.bat`) a tool for collecting data in the event of an error. The data collection tool of JP1/IM - View can collect troubleshooting data for JP1/IM - View. For details about the data that can be collected, see *9.3 Data that needs to be collected when a problem occurs* in the *Job Management Partner 1/Integrated Management - Manager Administration Guide*.

About the data collection tool

- About `jcoview_log.bat`

See `jcoview_log.bat` (*Windows only*) in *1. Commands* in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.

Specify the settings that enable output of a memory dump and crash dump by referencing *1.18.2(1) Preparations for collecting data in the event of a failure*.

IM Configuration Management provides the `jcfthreaddmp` command for collecting a thread dump in the event of a failure in IM Configuration Management - View. For details about the `jcfthreaddmp` command, see `jcfthreaddmp` (*Windows only*) in *1. Commands* in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.

1.19.2 Setting up IM Configuration Management - View

There are two ways to start IM Configuration Management - View:

- From the Windows **Start** menu
- By executing the `jcfview` command

This subsection describes the setup for using the Windows **Start** menu to start IM Configuration Management - View. This setup is not needed if you will use the `jcfview` command to start IM Configuration Management - View.

A shortcut to JP1/IM - Manager is created in the **Start** menu when you install JP1/IM - View, but no shortcut to IM Configuration Management - View is created.

To create a shortcut to IM Configuration Management - View:

1. Stop JP1/IM - View.
2. Execute the following command:

```
jcovcfsetup -i (the -i option can be omitted)
```

A shortcut to IM Configuration Management - View is added in **Programs** in the Windows **Start** menu under **JP1_Integrated Management - View**. The name is **Configuration Management**.

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

Note:

If you have changed the location or name of **JP1_Integrated Management - View** (shortcut) registered in the **Start** menu, the shortcut is not added.

1.19.3 Setting up the JP1/IM - Rule Operation linkage

This subsection describes the setup for using JP1/IM - View (the JP1/IM - Rule Operation linkage part).

When you install JP1/IM - View, shortcuts to JP1/IM - Manager are created in the **Start** menu, but no shortcuts are created to JP1/IM - Rule Operation.

The names of the shortcuts to JP1/IM - Manager are **Integrated View** and **Edit Monitoring Tree**.

To create shortcuts to JP1/IM - Rule Operation:

1. Stop JP1/IM - View.
2. Execute the following command:

```
jcovrmsetup -i (the -i option can be omitted)
```

Shortcuts to JP1/IM - Rule Operation are added in **Programs** in the Windows **Start** menu under **JP1_Integrated Management - View**. The names are **Rule Management** and **Help (Rule Management)**.

For details about JP1/IM - Rule Operation and JP1/IM - View (the JP1/IM - Rule Operation linkage part), 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*

Note:

If you have changed the location or name of **JPI_Integrated Management - View** (shortcut) registered in the **Start** menu, the shortcuts are not added.

Chapter

2. Installation and Setup (for UNIX)

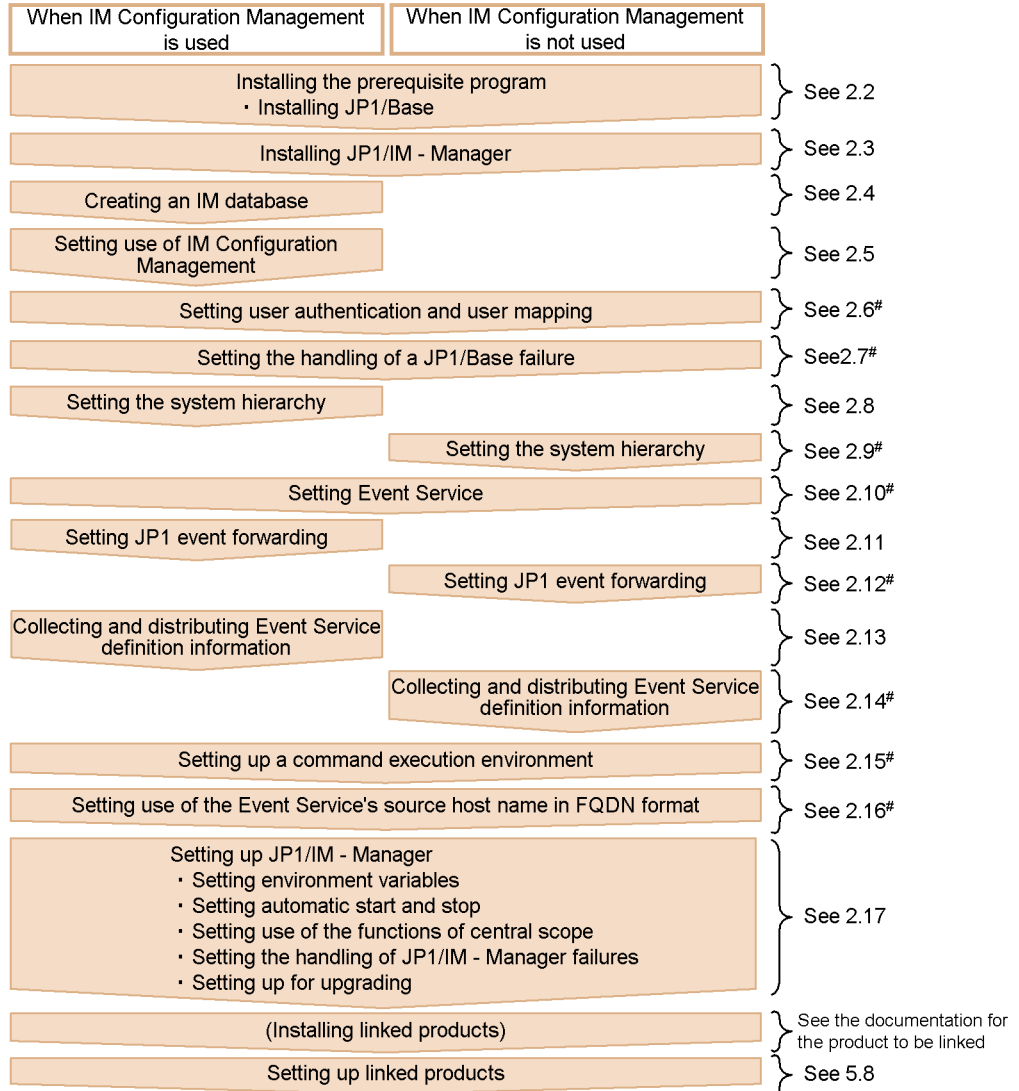
This chapter explains how to install and set up JP1/IM in a UNIX environment.

- 2.1 Installation and setup procedures
- 2.2 Preparations required before installation
- 2.3 Installing
- 2.4 Creating an IM database
- 2.5 Settings for using the functions of IM Configuration Management
- 2.6 Settings for user authentication and user mapping
- 2.7 Settings for handling JP1/Base failures
- 2.8 Setting the system hierarchy (when IM Configuration Management is used)
- 2.9 Setting the system hierarchy (when IM Configuration Management is not used)
- 2.10 Setting Event Service
- 2.11 Setting JP1 event forwarding (when IM Configuration Management is used)
- 2.12 Setting JP1 event forwarding (when IM Configuration Management is not used)
- 2.13 Collecting and distributing Event Service definition information (when IM Configuration Management is used)
- 2.14 Collecting and distributing Event Service definition information (when IM Configuration Management is not used)
- 2.15 Setting up a command execution environment
- 2.16 Settings for using the source host name of Event Service in the FQDN format
- 2.17 Setting up JP1/IM - Manager

2.1 Installation and setup procedures

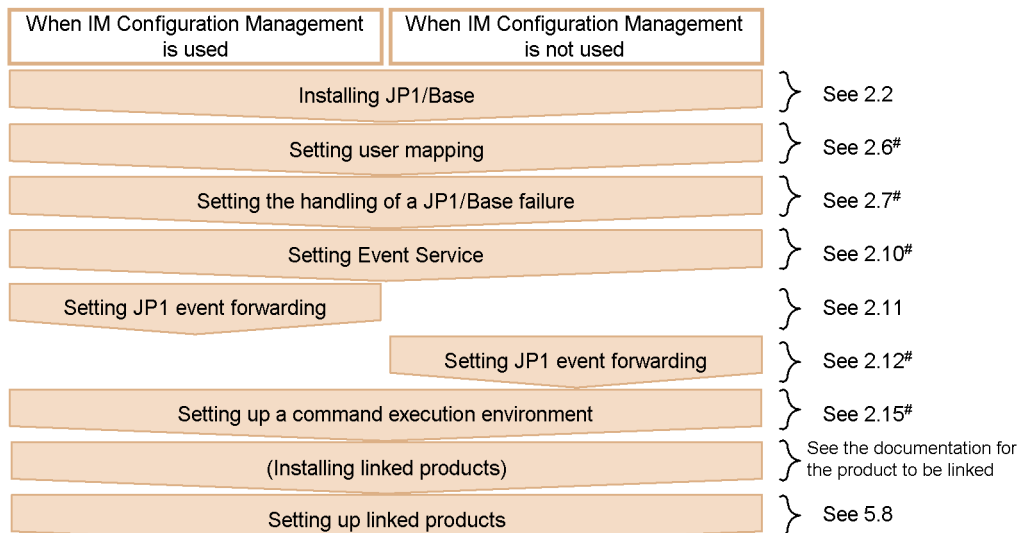
This section describes the procedure from the start of installation to the end of setup for the manager and agent.

Figure 2-1: Installation and setup procedure (manager)



#: For details, see the *Job Management Partner 1/Base User's Guide*.

Figure 2-2: Installation and setup procedure (agent)



#: For details, see the *Job Management Partner 1/Base User's Guide*.

2.2 Preparations required before installation

2.2.1 Designing the setup details

Before you start installation, evaluate the details of JP1/IM setup and prepare the setup items.

For details about how to design the setup details, see *Part 3. Design* in the *Job Management Partner 1/Integrated Management - Manager Overview and System Design Guide*.

2.2.2 Configuring the system environment

(1) Configuring the OS environment

Before you install JP1/IM, configure an OS environment that satisfies the following conditions:

- The OS version being used is supported by JP1/IM.
- Service packs and patches required by JP1/IM have been applied.
- Kernel parameters have been adjusted appropriately to the configuration of JP1/IM.

See the release notes for JP1/IM - Manager and JP1/IM - View and perform the following:

- Check the patches required by JP1/IM and then apply them to the OS.
- Adjust the kernel parameters appropriately to the configuration of JP1/IM.

2.2.3 Installing the prerequisite program

(1) Installing JP1/Base

To use JP1/IM managers and agents, you must install JP1/Base, which is the prerequisite program for JP1/IM - Manager.

To check the system configuration, see *1.5 JP1/IM - Manager system configuration* in the *Job Management Partner 1/Integrated Management - Manager Overview and System Design Guide*. For details about how to install JP1/Base, see the *Job Management Partner 1/Base User's Guide*.

2.3 Installing

This section explains how to install and uninstall JP1/IM - Manager.

The user who will be performing the installation must have Administrator permissions.

2.3.1 Installation procedure

This subsection explains how to install JP1/IM - Manager.

(1) How to install

You need `root` permissions to perform this procedure.

To install JP1/IM - Manager:

1. Terminate all programs.

Before you start the installation, terminate JP1/Base and all programs that require JP1/Base.

If you are performing an upgrade installation, stop JP1/IM - Manager. If a JP1/IM - View is connected, log out.

2. Run the Hitachi Program Product Installer.

Follow the instructions of the Hitachi Program Product Installer. For details about how to use the Hitachi Program Product Installer, see *2.3.2 How to use the Hitachi Program Product Installer*.

When JP1/IM - Manager is installed, the file shown below is created as a log. This file contains maintenance information that is used in the event of abnormal termination of installation. Once JP1/IM - Manager has been installed successfully, start it. If there are no problems, delete the following file:

```
/tmp/HITACHI_JP1_INST_LOG/jp1imm_inst{1|2|3|4|5}.log
```

(2) About the types of installation

Upgrade installation

If you are upgrading from an old version of JP1/IM - Manager, first read the notes about upgrading that you will find in *12.2 Upgrading from a previous version of JP1/IM* in the *Job Management Partner 1/Integrated Management - Manager Overview and System Design Guide*.

Remote installation using JP1/Software Distribution

JP1/IM supports remote installation (software distribution) using JP1/Software Distribution.

By running JP1/Software Distribution at the server where JP1/IM is run, you can

perform a new installation as well as an upgrade installation of JP1/IM. For details about how to perform remote installation using JP1/Software Distribution, see the *Job Management Partner 1/Software Distribution Setup Guide, for Windows systems* and the manual *Job Management Partner 1/Software Distribution Client Description and User's Guide, for UNIX systems*.

2.3.2 How to use the Hitachi Program Product Installer

The Hitachi Program Product Installer is on the JP1/IM distribution medium. This subsection describes the following procedures:

- How to start the Hitachi Program Product Installer
- How to use the Hitachi Program Product Installer to install JP1/IM - Manager
- How to use the Hitachi Program Product Installer to remove JP1/IM - Manager
- How to use the Hitachi Program Product Installer to check the versions of currently installed Hitachi products

User permissions for execution of the Hitachi Program Product Installer

- To use the Hitachi Program Product Installer, you need `root` permissions. Either log on as `root` or use the `su` command to change the user to `root`.

(1) Starting the Hitachi Program Product Installer

To start the Hitachi Program Product Installer:

1. Insert the JP1/IM - Manager distribution medium CD-ROM in the drive.
2. Mount the CD-ROM.

The mounting method depends on the OS, hardware, and environment in use. For details about the mounting method, see the OS documentation.

- In Solaris

Normally when you insert the CD-ROM, it mounts automatically.

```
/usr/sbin/mount (checks to see if the CD-ROM is mounted)
```

If the CD-ROM has not mounted automatically, enter the following command:

```
/usr/sbin/mount -r -F hsf s /dev/dsk/c0t4d0s0 /cdrom
```

- In AIX

```
/usr/sbin/mount -r -v cdrfs /dev/cd0 /cdrom
```

Note that the device special file name indicated in bold type and the underlined CD-ROM file system mount directory name depend on the environment.

3. Start the Hitachi Program Product Installer.

The directory and file names on the CD-ROM may differ depending on the machine environment. Use the `ls` command to check the directory and file names, and then use the displayed names.

- In Solaris

```
/cdrom/cdrom0/solaris/setup /cdrom/cdrom0
```

- In AIX

```
/cdrom/aix/setup /cdrom
```

Replace the underlined part with the actual CD-ROM mount directory name.

4. Unmount the CD-ROM.

After you finish the installation, unmount the CD-ROM. For details about how to unmount a CD-ROM, see the OS documentation.

- In Solaris

```
/usr/bin/eject (ejects the CD-ROM that was mounted automatically)
```

If you used the `mount` command to mount the CD-ROM manually, enter the following command:

```
/usr/sbin/umount /cdrom
```

- In AIX

```
/usr/sbin/umount /cdrom
```

Replace the underlined part with the actual CD-ROM mount directory name.

(2) Installing JP1/IM - Manager

This subsection explains how to use the Hitachi Program Product Installer to install JP1/IM - Manager. When you start the Hitachi Program Product Installer, the initial window appears.

Figure 2-3: Example of the Hitachi Program Product Installer's initial window

```
L) List Installed Software.
I) Install Software.
D) Delete Software.
Q) Quit.

Select Procedure ==>

+-----+
| CAUTION!                                     |
| YOU SHALL INSTALL AND USE THE SOFTWARE PRODUCT LISTED IN THE |
| "List Installed Software." UNDER THE TERMS AND CONDITION OF  |
| THE SOFTWARE LICENSE AGREEMENT ATTACHED TO SUCH SOFTWARE    |
| PRODUCT.                                                     |
+-----+
```

In **Select Procedure** in the initial window, enter **I** to display a list of software programs that can be installed. Move the cursor to the software program that you want to install, and then press the space bar to select it. Entering **I** again installs JP1/IM - Manager. After installation is completed, enter **Q** to return to the initial window.

(3) Removing JP1/IM - Manager

Enter the following command to start the Hitachi Program Product Installer:
`/etc/hitachi_setup`

The Hitachi Program Product Installer's initial window is displayed. For details about the initial window, see Figure 2-3 Example of the Hitachi Program Product Installer's initial window.

In **Select Procedure** in the initial window, enter **D** to display a list of software programs that can be removed. Move the cursor to the software program that you want to remove, and then press the space bar to select it. Entering **D** again removes the software program. After the software program has been removed, enter **Q** to return to the initial window.

(4) Displaying version information

Execute the following command to start the Hitachi Program Product Installer:
`/etc/hitachi_setup`

The Hitachi Program Product Installer's initial window is displayed. For details about the initial window, see Figure 2-3 Example of the Hitachi Program Product Installer's initial window.

In **Select Procedure** in the initial window, enter **L** to display a list of Hitachi products that have been installed.

2.3.3 Uninstallation procedure

This subsection explains how to uninstall JP1/IM - Manager.

(1) How to uninstall

You need `root` permissions to perform this procedure.

To uninstall JP1/IM - Manager:

1. Terminate the programs.

Before you start the uninstallation procedure, terminate JP1/IM - Manager, JP1/Base, and all programs that require JP1/Base. If a JP1/IM - View is connected, stop it.

2. Back up user files.

When you uninstall JP1/IM - Manager, folders containing files, such as definition files and log files, are also deleted. If necessary, back them up.

3. Run the Hitachi Program Product Installer.

Follow the instructions of the Hitachi Program Product Installer to perform uninstallation.

4. Delete user files.

If a process uses files, those files may remain. Check the following directories and manually delete any user files:

- `/opt/jp1imm/`
- `/var/opt/jp1imm/`
- `/etc/opt/jp1cons/`
- `/opt/jp1cons/`
- `/var/opt/jp1cons/`
- `/etc/opt/jp1scope/`
- `/opt/jp1scope/`
- `/var/opt/jp1scope/`

When JP1/IM - Manager is uninstalled, the file shown below is created as installer logs. This file contains maintenance information that can be used in the event of abnormal termination of uninstallation. After the uninstallation has terminated normally, delete this file.

- `/tmp/HITACHI_JP1_INST_LOG/jp1imm_inst{1|2|3|4|5}.log`

2.3.4 Notes about installing and uninstalling

- Relationship between products

JP1/IM - Manager requires JP1/Base. When you install and uninstall the products,

note the following:

- Any prerequisite products must be installed first and in the correct order.
Install JP1/Base and then JP1/IM - Manager, in this order.
- Stop JP1/Base before you install or uninstall JP1/IM - Manager. If you forgot to stop JP1/Base, make sure that you restart JP1/Base. If you do not restart JP1/Base, it will not be possible to manage system configuration information correctly.
- The common definition information for JP1/IM - Manager is deleted when you uninstall JP1/Base. If you have reinstalled JP1/Base, execute the `jp1cc_setup` and `jp1cs_setup` commands.
- About Hitachi Network Objectplaza Trace Library (HNTRLib2)
 - When you install JP1/Base, Hitachi Network Objectplaza Trace Library (HNTRLib2) is installed.
 - When you uninstall JP1/Base, Hitachi Network Objectplaza Trace Library (HNTRLib2) is deleted unless another product is using it.
- Settings in the OS environment
 - During installation, the following information is set in the OS:
In the `services` file, the port numbers indicated in *C. Port Numbers* in the *Job Management Partner 1/Integrated Management - Manager Overview and System Design Guide* are set.
 - During uninstallation of JP1/IM - Manager, the port numbers indicated in *C. Port Numbers* in the *Job Management Partner 1/Integrated Management - Manager Overview and System Design Guide* are deleted.

2.4 Creating an IM database

To use the IM Configuration Management database to manage a system hierarchy and to use the integrated monitoring database to manage JP1 events, you must create an IM database, which is the collective name for these two databases.

If you do not use the IM Configuration Management database during system configuration or you do not use the integrated monitoring database or the IM Configuration Management database when you start operations, there is no need to create an IM database. You can create the IM database when you need either or both of the integrated monitoring database and the IM Configuration Management database after operations have started.

This section explains how to create an IM database.

(1) Preparations for creating an IM database

You must prepare a *setup information file* that specifies the size of the database area required in order to create an IM database and information about the database storage directory.

To prepare for IM database creation:

1. Edit the setup information file

The following shows an example of the settings:

```
IMDBSIZE=S #IM DATABASE SERVICE - DB Size
IMDBDIR=/var/opt/jplimm/database #IM DATABASE SERVICE -
Data Storage Directory
IMDBPORT=20700 #IM DATABASE SERVICE - Port Number
IMDBENVDIR=/var/opt/jplimm/dbms #IM DATABASE SERVICE - DB
Install Directory
```

For details about the setup information file, 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*.

(2) Setting up the integrated monitoring database

Create an integrated monitoring database and use Central Console functions to set up the database so you can use it. If you do not use the integrated monitoring database, there is no need to perform this procedure.

To execute the `jcodbsetup` command that creates an integrated monitoring database, one of the following conditions must be satisfied:

- Central Console Service is stopped.

- The integrated monitoring database settings are disabled and the IM Configuration Management service is stopped.

To set up the integrated monitoring database:

1. Execute the `jcodbsetup` command to create an integrated monitoring database.

- When an IM Configuration Management database has been set up

```
jcodbsetup -s [-h logical-host-name -c {online|standby}]  
[-q]
```

- When no IM Configuration Management database has been set up

```
jcodbsetup -f setup-information-file-name [-h logical-host-name -c  
{online|standby}] [-q]
```

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

2. Execute the `jcoimdef` command to enable the integrated monitoring database.
`jcoimdef -db ON`

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*.

To start JP1/IM - Manager and use the integrated monitoring database, the IM database service must be running (return value: 0). Execute the `jimdbstatus` command to check the settings of the integrated monitoring database and the status of the IM database service.

If the operating status is that the IM database service is engaged in start or stop processing (return value: 4), is stopped (return value: 8), or is not running (return value: 16), processing is placed on wait status for the amount of time (in milliseconds) specified in the common definition.

Define the parameter as follows:

```
[logical-host-name\JP1CONSOLEMANAGER\IMDB]  
"DB_START_RETRY_INTERVAL"=dword:hexadecimal-value
```

Specify a hexadecimal value in the range 3,000 to 3,600,000 (milliseconds). The default is `dword:0000xbb8` (3,000 milliseconds).

The operating status of the IM database service is checked again.

Checking of the operating status of the IM database service is performed as many times as is specified in the common definition.

Define the parameter as follows:

```
[logical-host-name\JP1CONSOLEMANAGER\IMDB]
```

"DB_START_RETRY_COUNT"=dword:*hexadecimal-value*

Specify a hexadecimal value in the range 0 to 10,000 (times). The default is dword:0000x12c (300 times).

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

(3) Setting up the IM Configuration Management database

Create an IM Configuration Management database and set it up so that the IM Configuration Management service can be started from process management. If you do not use the IM Configuration Management database, there is no need to perform this procedure.

To execute the jcfdbsetup command that creates an IM Configuration Management database, one of the following conditions must be satisfied:

- Central Console Service is stopped.
- The integrated monitoring database settings are disabled and the IM Configuration Management service is stopped.

To set up the IM Configuration Management database:

1. Execute the jcfdbsetup command to create an IM Configuration Management database.

- When an IM Configuration Management database has been set up

```
jcfdbsetup -s [-h logical-host-name -c {online|standby}] [-q]
```

- When no IM Configuration Management database has been set up

```
jcfdbsetup -f setup-information-file-name [-h logical-host-name -c {online|standby}] [-q]
```

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

2.5 Settings for using the functions of IM Configuration Management

When a new installation of JP1/IM - Manager is performed, the default is that the functions of IM Configuration Management are disabled. To use IM Configuration Management during system configuration or system operations, you must create an IM Configuration Management database using the procedure described in *2.4 Creating an IM database*, and then enable the functions of IM Configuration Management.

To enable the functions of IM Configuration Management:

1. Execute the `jcoimdef` command to enable the IM Configuration Management service (`jcfmain`).

```
jcoimdef -cf ON
```
2. Restart JP1/IM - Manager.
3. Execute the `jco_spmc_status` command to ensure that the IM Configuration Management service (`jcfmain`) is displayed in the active processes.

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*.

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

2.6 Settings for user authentication and user mapping

You must specify information that is required for JP1 user management, such as the authentication server, registration of JP1 users, and user mapping.

Specify the settings as appropriate to the host's role, as shown below.

Table 2-1: Settings depending on host's role

Setting item	Used as authentication server		Not used as authentication server	
	Primary authentication server	Secondary authentication server	Manager host	Agent host
Authentication server specification	Y	Y	Y	--
JP1 user setting	Y	--	--	--
Operation permission setting	Y	--	--	--
Copy of authentication server setting	--	Y	--	--
User mapping	Y	Y	Y	Y

Legend:

Y: Setting is required

--: Setting is not required

You specify the settings using JP1/Base commands.

You must set user mapping at all hosts where commands are executed by an automated action or a JP1/IM - View operation.

Table 2-2: User mapping when commands are executed by an automated action or JP1/IM - View

Operation	JP1 user name	Server host name	OS user name
When executing commands from JP1/IM - View	User who logs on to the manager	Manager to which JP1/IM - View connects [#]	User who is registered in the OS of the host where the command is executed

Operation	JP1 user name	Server host name	OS user name
When executing an automated action	User name specified in the action definition	Manager that defined the automated action [#]	User who is registered in the OS of the host where the action is executed

#

You can also specify an asterisk (*) as the server host name, in which case user mapping is permitted at all hosts.

The JP1 user `jp1admin` is registered by default. For `jp1admin`, operation permissions whose JP1 resource group is `*` and JP1 authority level is `JP1_Console_Admin` have been set (JP1 resource group `*` can access all JP1 resource groups).

2.6.1 Specifying the authentication server

Specify the host name of the authentication server. This setting is required for the host and the JP1/IM manager, but not for the agent.

To specify the authentication server:

1. Specify the authentication server.

```
/opt/jp1base/bin/jbssetusrsv host-name-1 [host-name-2]
```

You can set a maximum of two authentication servers (primary and secondary servers). *host-name-1* specifies the primary authentication server and *host-name-2* specifies the secondary authentication server.

For details about how to specify the settings, see the chapter that describes user management settings in the *Job Management Partner 1/Base User's Guide*.

2.6.2 Registering JP1 users

Register the JP1 users who will use JP1/IM. This is required at the host of the primary authentication server.

To register JP1 users:

1. Register a JP1 user.

```
/opt/jp1base/bin/jbsadduser JP1-user-name
```

2.6.3 Setting operation permissions for the JP1 users

Register operation permissions for the JP1 users who will use JP1/IM. This is required at the host of the primary authentication server.

To set operation permissions for the JP1 users:

1. Set operation permissions for the JP1 users.

At the host of the authentication server, edit the user permissions level file (`JP1_UserLevel`) and set operation permissions for the JP1 users.

For details about the settings, see the description of setting operation permissions for JP1 users in the *Job Management Partner 1/Base User's Guide*.

For example, as JP1/IM operation permissions, you can specify `JP1_Console` for a JP1 resource group and `JP1_Console_Admin` for a permission level.

As operation permissions for IM Configuration Management, you must set `JP1_Console` for the JP1 resource group and both JP1/IM permission level and IM Configuration Management permission level as permission levels. If you do not set any permission level for IM Configuration Management, you can execute operations only within the range of the JP1 permission level `JP1_CF_User` for IM Configuration Management.

For details about the operation permissions for JP1/IM, see *7.4.1 Managing JP1 users* and *Appendix E. Operating Permissions* in the *Job Management Partner 1/Integrated Management - Manager Overview and System Design Guide*.

2.6.4 Copying the primary authentication server settings

Copy the settings files for the primary authentication server. These settings are required at the host of the secondary authentication server.

To copy the primary authentication server settings:

1. Copy the settings files for the authentication server.

Copy the settings files `JP1_Group`, `JP1_Passwd`, and `JP1_UserLevel` that are stored in the `/etc/opt/jp1base/conf/user_acl` directory. These are text files. Use a method such as an ASCII transfer by FTP.

2.6.5 Setting user mapping

At the host where you execute commands by automated action and JP1/IM - View operations, set user mapping between JP1 user names and OS user names. This is required at all hosts that execute commands from JP1/IM.

To set user mapping:

1. Set the user mapping definition.

At each host where commands are executed, edit the user mapping definition file (`jp1BsUmap.conf`) to specify user mapping between JP1 users and OS users.

2. Execute the following user mapping definition command:
`/opt/jp1base/bin/jbsmkumap`

2. Installation and Setup (for UNIX)

If there are multiple users, you must set user mapping for all of them. User mapping is required even when a JP1 user name is the same as the OS user name.

The commands that are executed by automated action and JP1/IM - View operation are executed by a primary user who has been mapped to a JP1 user. To execute commands by a specific OS user, register that OS user as a primary user.

For details about the user mapping definition file (`jp1BsUmap.conf`) and the `jbsmkumap` command, see the description of the user management settings in the *Job Management Partner 1/Base User's Guide*.

2.7 Settings for handling JP1/Base failures

JP1/Base provides the following functions to minimize the effects of JP1/Base failures on system operation:

- Function for detecting process errors (health check function)
- Function for automatically restarting processes in the event of abnormal process termination
- Function for issuing JP1 events when abnormalities are detected in processes and authentication servers
- Tool for collecting data necessary for investigation in the event of a JP1/Base failure

By default, all functions for detecting process errors, restarting processes, and issuing JP1 events are disabled. To change the settings, see the chapter that describes installation and setup in the *Job Management Partner 1/Base User's Guide*.

2.8 Setting the system hierarchy (when IM Configuration Management is used)

This section explains how to set the system hierarchy when IM Configuration Management is used. For details about how to set the system hierarchy when IM Configuration Management is not used, see *2.9 Setting the system hierarchy (when IM Configuration Management is not used)*.

When you use IM Configuration Management, you must use IM Configuration Management - View to set the manager and agent hierarchical structure of the system that is managed by JP1/IM.

You can also use the export and import functions of IM Configuration Management to migrate a system configuration from a test environment to the operating environment or from the environment before a change to the environment after the change.

The export and import functions of IM Configuration Management enable you to specify settings for managing a system hierarchy that includes virtual hosts (virtualization system configuration), as well as settings for using Central Scope for monitoring.

When you use IM Configuration Management to manage your system hierarchy, do not edit the configuration management function settings file provided by JP1/Base, or execute commands.

2.8.1 Setting using IM Configuration Management - View

This subsection explains how to use IM Configuration Management - View to set the system hierarchy.

If you have added IM Configuration Management to an existing JP1/IM system that does not use IM Configuration Management, IM Configuration Management - View enables you to edit the configuration definition information collected from the existing JP1/IM system and set the system hierarchy.

This subsection explains how to set a new system hierarchy and how to edit the hierarchy of an existing system.

(1) *Setting a new system hierarchy*

There are two ways to define a system hierarchy: by using the highest manager to define the entire system hierarchy in batch mode, and by dividing the system hierarchy into smaller sections that are managed by individual managers, and then defining each section.

For examples of the management and configuration definition of a system hierarchy, see *6.2.1 Hierarchical configurations managed by IM Configuration Management* in the *Job Management Partner 1/Integrated Management - Manager Overview and*

System Design Guide.

The following provides an overview of how to set a new system hierarchy.

To set a new system hierarchy:

1. Register a host that is to be added to the system hierarchy as a management target of IM Configuration Management.
 - For details about how to register hosts and how to set information about hosts, see *3.1.1 Registering hosts*.
 - For details about how to view information about the registered hosts, see *3.1.2 Displaying host information*.
 - For details about how to delete hosts, see *3.1.3 Deleting hosts*.
 - For details about how to change information about the registered hosts, see *3.1.4 Changing host information*.

2. Add the host registered in IM Configuration Management to the system hierarchy and set the hierarchy between managers and agents.

Add the host registered to IM Configuration Management to the system that is managed by JP1/IM, and set the hierarchy between the managers and the agents.

- For details about how to add hosts to a JP1/IM system, see *3.2.4(1) Adding hosts*.
 - For details about how to delete hosts from the JP1/IM system, see *3.2.4(3) Deleting hosts*.
 - For details about how to set a hierarchy between managers and agents, see *3.2.4(2) Moving hosts*.
3. Apply the set system hierarchy to the system.

Apply the system hierarchy that was set by IM Configuration Management - View to the system that is managed by JP1/IM.

 - For details about how to apply the set system hierarchy to the system, see *3.2.5 Applying the system hierarchy*.
 - For details about how to check the set system hierarchy, see *3.2.2 Displaying the system hierarchy*.

If you divide the system hierarchy into integrated manager and site managers, perform the above procedure for each manager. After that, use the IM Configuration Management - View that is connected to the integrated manager to perform the procedure described below to create a definition for the entire system.

To set a new system hierarchy:

1. Synchronize the system hierarchy.

Synchronize the configuration definition information between the integrated manager and site managers.

For details about how to synchronize the system hierarchy, see 3.2.6 *Synchronizing the system hierarchy*.

(2) Editing an existing system hierarchy

The following provides an overview of how to edit the configuration definition information that is collected from an existing JP1/IM system.

To edit an existing system hierarchy:

1. Collect the configuration definition information from the existing JP1/IM system.

For details about how to collect configuration definition information from an existing JP1/IM system, see 3.2.1 *Collecting the system hierarchy*.

2. Verify that the collected configuration definition information matches the configuration definition information held by IM Configuration Management.

For details about how to verify configuration definition information, see 3.2.3 *Verifying the system hierarchy*.

3. Edit the system hierarchy.

- For details about how to add hosts to the JP1/IM system, see 3.2.4(1) *Adding hosts*.
- For details about how to delete hosts from the JP1/IM system, see 3.2.4(3) *Deleting hosts*.
- For details about how to set the hierarchy between managers and agents, see 3.2.4(2) *Moving hosts*.

4. Apply the set system hierarchy to the system.

Apply the system hierarchy that was set by IM Configuration Management - View to the system that is managed by JP1/IM.

- For details about how to apply the set system hierarchy to the system, see 3.2.5 *Applying the system hierarchy*.
- For details about how to check the set system hierarchy, see 3.2.2 *Displaying the system hierarchy*.

2.8.2 Setting using the export and import functions

The export and import functions of IM Configuration Management enable you to migrate a system configuration from a test environment to an operating environment, and to migrate a system hierarchy from the environment before a change to the environment after the change. For details about how to set the system hierarchy using the export and import functions, see 3.4 *Importing and exporting the management*

information in IM Configuration Management.

2.8.3 Settings for managing and monitoring a virtualization system configuration

The export and import functions of IM Configuration Management enable you to use IM Configuration Management to manage the configuration definition information for a virtualization system configuration, and to use Central Scope to monitor the virtualization system configuration. For details about how to set up an environment for managing and monitoring a virtualization system configuration, see *3.5 Setting a virtualization system configuration.*

2.9 Setting the system hierarchy (when IM Configuration Management is not used)

This section describes the system hierarchy settings when IM Configuration Management is not used. For details about the system hierarchy settings when IM Configuration Management is used, see *2.8 Setting the system hierarchy (when IM Configuration Management is used)*.

When you are not using IM Configuration Management, you must use commands to set the hierarchical structure between managers and agents in a system that is managed by JP1/IM.

There are two ways to define a system hierarchy: by using the highest manager to define the entire system hierarchy in batch mode, and by dividing the system hierarchy into smaller sections that are managed by individual managers, and then defining each section.

If you are using IM Configuration Management to manage your system hierarchy, do not edit the definition files for the configuration management function provided by JP1/Base, or execute commands.

For examples of system hierarchy management and configuration definitions, see *7.4.3 Managing the system hierarchy* in the *Job Management Partner 1/Integrated Management - Manager Overview and System Design Guide*.

This section explains how to set, delete, and change configuration definition information.

2.9.1 Setting the configuration definition information

To set the configuration definition information:

1. At the manager, create a configuration definition file (`jbs_route.conf`).
To define the system hierarchy in batch mode, specify the entire system hierarchy in the definition file. To divide the system hierarchy into multiple sections, specify in the definition file the managed hosts and managers that are under that manager.
2. At the manager, execute the setting command (`jbsrt_distrib`).
The command will update the definition information.

If you divide the system hierarchy into multiple sections, perform the above procedure for each manager. After that, perform the procedure described below at the highest manager to create a definition for the entire system.

To set the configuration definition information:

1. At the highest manager, create the configuration definition file (`jbs_route.conf`).

Specify the system hierarchy from the highest manager to the next highest manager in the definition file.

2. At the highest manager, execute the setting command (`jbsrt_sync`).

To check the contents of the configuration definition information, execute the `jbsrt_get` command on each host.

2.9.2 Deleting the configuration definition information

To delete the configuration definition information, such as clearing the definitions:

1. At the manager, provide a configuration definition file (`jbs_route.conf`).

If there is no configuration definition file, create a file that specifies only the local host name.

If there is an existing file, use it as is.

2. At the manager, execute the setting command (`jbsrt_distrib`).

If configuration definition information was not deleted from a host because JP1/Base was not running, execute the `jbsrt_del` command at that host to delete the configuration definition information, and then execute the `jbsrt_distrib` command at the highest manager.

2.9.3 Changing the configuration definition information

If you change the configuration definition information, follow the same procedure as in *2.9.1 Setting the configuration definition information*. This will distribute the post-change configuration definition information.

Changing the highest manager

To change the highest manager in the system:

1. First, delete the configuration definition information at the highest manager.

At the highest manager before the change, delete the configuration definition information using the procedure described in *2.9.2 Deleting the configuration definition information*.

2. At the highest manager after the change, set the configuration definition information.

At the highest manager after the change, set the configuration definition information using the procedure described in *2.9.1 Setting the configuration definition information*.

2.9.4 Notes about setting the configuration definition information

When configuration definition information is distributed, JP1/Base must be running at each host. This subsection describes the effects when JP1/Base is inactive, and the actions to be taken.

■ Effects of inactive JP1/Base

Configuration definition information is managed by JP1/Base. If JP1/Base is not running at a host that is defined in the configuration definition information, distribution of configuration definition information will fail. In such a case, take the following actions:

1. Continue processing even if the message KAVB3107-E Cannot set configuration in the host is displayed when the `jbsrt_distrib` command executes.

The configuration definition information will be distributed to the hosts where JP1/Base is running.

2. Start JP1/Base at the host where definition was not distributed, and then execute the `jbsrt_distrib` command again.

■ Effects of inactive JP1/Base Event Service

The configuration definition information is related to JP1 event forwarding. When the `jbsrt_distrib` or `jbsrt_del` command is executed, the `jevreload` command executes automatically and the Event Service's forwarding settings are updated (reloaded). If Event Service is not running during this reload processing, configuration definition information will be distributed, but the JP1 event destination information will not be updated. Restart Event Service.

For details about the configuration definition information, see the *Job Management Partner I/Base User's Guide*.

2.10 Setting Event Service

To set each host in order to manage events by means of JP1/IM using JP1 events:

1. Set up an Event Service environment.

Normally, the default settings can be used for operation, but in the following cases, customize the settings:

- The capacity of the event database is to be increased.
- JP1/IM manages events that are in the JP1/SES format.

JP1/IM - Manager collects JP1 events from JP1/Base (Event Service) using the user name `root`. If you specify the `users` parameter in the event server settings file (`conf`) of the JP1/Base (Event Service) that is running on the same host, include `root`. If `root` is not included, JP1/IM - Manager will no longer start successfully.

2. Set event conversions.

To use JP1 events to manage log files, SNMP traps, and Windows event logs, set the event conversions.

For details about the settings, see the chapter that describes the setting of an Event Service environment and event conversion in the *Job Management Partner 1/Base User's Guide*.

2.11 Setting JP1 event forwarding (when IM Configuration Management is used)

This section describes JP1 event forwarding settings when IM Configuration Management is used.

When you use IM Configuration Management, you use IM Configuration Management - View to specify JP1 event forwarding settings.

In the JP1 event forwarding settings, you set each host in such a manner that the JP1 events managed by JP1/IM are forwarded to the higher JP1/IM manager.

Normally, the default settings can be used for operation, but in the following cases, you must customize the settings:

- JP1/IM manages JP1 event severity notification and information events.
- JP1/IM manages events that are in the JP1/SES format.

By default, events are forwarded according to the hierarchy definition that is specified as explained in *2.8 Setting the system hierarchy (when IM Configuration Management is used)*.

If you use IM Configuration Management, you can change the event forwarding settings by editing the event forwarding information settings file on the **Configuration File** page in the Display/Edit Profiles window. For details about how to edit the settings files, see *3.3.4 Editing configuration files*.

2.12 Setting JP1 event forwarding (when IM Configuration Management is not used)

Set each host in such a manner that the JP1 events managed by JP1/IM are forwarded to the higher JP1/IM manager. This procedure is executed when the IM Configuration Management database is not used in the JP1/IM system configuration.

To set JP1 event forwarding:

1. Set event forwarding.

Normally, the default settings can be used for operation, but in the following cases, you must customize the settings:

- JP1/IM manages JP1 event severity notification and information events.
- JP1/IM manages events that are in the JP1/SES format.

By default, events are forwarded according to the hierarchy definition that is specified as explained in *2.9 Setting the system hierarchy (when IM Configuration Management is not used)*.

For details about the settings, see the chapter that provides details of the forwarding settings file in the *Job Management Partner 1/Base User's Guide*.

2.13 Collecting and distributing Event Service definition information (when IM Configuration Management is used)

This section describes the collection and distribution of Event Service definition information when IM Configuration Management is used.

When you use IM Configuration Management, you use IM Configuration Management - View to collect and distribute Event Service definition information.

In a system consisting of JP1/Base and JP1/IM, the manager can collect and distribute in batch mode Event Service definition information from and to multiple hosts on which JP1/Base version 9 is running. This means that you can use the manager to centrally manage Event Service definition information for each host without having to check and define the definition information at each host.

When you use IM Configuration Management, you can collect and distribute the following definition information:

- Forwarding settings file
- Log file trap operation definition file
- Local action definition file

When you use IM Configuration Management, you can collect Event Service definition information by collecting profiles (valid configuration information and configuration files) on the **Host List** or **IM Configuration** page in the IM Configuration Management window. For details about how to collect profiles, see *3.3.1 Collecting profiles*.

Furthermore, if you use IM Configuration Management, you can distribute Event Service definition information to the hosts on which JP1/Base is running by applying edited information to the configuration file on the **Host List** or **IM Configuration** page in the IM Configuration Management window. For details about how to apply edited information to the configuration files, see *3.3.5 Applying edited information in configuration files*.

2.14 Collecting and distributing Event Service definition information (when IM Configuration Management is not used)

This section describes the collection and distribution of Event Service definition information when IM Configuration Management is not used. Perform this operation if you do not use the IM Configuration Management database in the JP1/IM system configuration.

When you do not use IM Configuration Management, you use commands provided by JP1/Base to collect and distribute Event Service definition information.

In a system consisting of JP1/Base and JP1/IM, the manager can collect and distribute Event Service definition information from and to multiple hosts in batch mode. This means that you can use the manager to centrally manage Event Service definition information for each host without having to check and define the definition information at each host.

You can collect and distribute information in the following files:

- Forwarding settings file
- Log file trap operation definition file
- Event log trap operation definition file

For details about how to collect and distribute definition information without using IM Configuration Management, see the chapter that describes collection and distribution of Event Service definition information in the *Job Management Partner 1/Base User's Guide*.

2.15 Setting up a command execution environment

You must specify the settings described below in order to set up a command execution environment in which the automated action function and commands are executed from the Execute Command window of JP1/IM - View.

Of the steps below, step 1 is used only once at the time of upgrading from JP1/Base version 7 or earlier. In the case of a new installation, start the procedure from step 2.

To set up a command execution environment:

1. Migrating command execution log files to version 8

Execute the `jcocmdconv` command to migrate the command execution logs accumulated by version 7 or earlier to command execution log files for version 8.

For details about how to migrate command execution logs, see the following:

12.2.6 Upgrading from JP1/Base version 7 in the Job Management Partner 1/ Integrated Management - Manager Overview and System Design Guide

12.2.7 Upgrading from JP1/Base version 6 in the Job Management Partner 1/ Integrated Management - Manager Overview and System Design Guide

2. Setting up a command execution environment

Execute the `jcocmddef` command to set up a command execution environment.

We recommend that you adjust the number of commands that can be executed concurrently. To do this, execute the command as follows:

Example: Set the number of commands that can be executed concurrently to 3

```
/opt/jp1base/bin/jcocmddef -execnum 3
```

3. Creating an environment variable file

If you will use an environment variable file during command execution, create it.

4. Defining host groups

If necessary, define host groups (groups of hosts at which a command can be executed simultaneously).

For details about the command execution environment, see the following:

About command execution environments

- `jcocmdconv` command

See the chapter that describes commands in the *Job Management Partner 1/ Base User's Guide*.

- `jcocmddef` command

See the chapter that describes commands in the *Job Management Partner 1/ Base User's Guide*.

- Creation of an environment variable file

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

- Host group definition

See *Host group definition file* in 2. *Definition Files* in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.

2.16 Settings for using the source host name of Event Service in the FQDN format

JP1/IM - Manager supports operation in which the source host name of Event Service is used in the FQDN format. By using the source host name of Event Service in the FQDN format, you can monitor JP1 events in a system that consists of multiple domains.

This section describes the prerequisites and the setting and startup methods for using the source host name of Event Service on the manager in the FQDN format. The setting described here is not needed when you use the source host name of Event Service on an agent in the FQDN format.

2.16.1 Prerequisites

To use the source host name of JP1/Base Event Service on the JP1/IM host in the FQDN format, the following conditions must be satisfied:

- This is a physical host environment.
- The `hostname` command executed on the JP1/IM - Manager host returns a host name in the short name format.

2.16.2 Setting method

Edit the `jco_start` command that starts JP1/IM - Manager automatically. Before starting JP1/IM - Manager, the `jco_start` command checks the active status of JP1/Base. If you use the event server in the FQDN format, you must check the active status of the event server in the FQDN format. At JP1/Base, set the event server in the FQDN format and then use the following procedure to edit the `jco_start` command.

To set:

1. Copy `jco_start.model` with any desired name.


```
cd /etc/opt/jplcons
cp -p jco_start.model any-name
```
2. Use a text editor to open the script copied in step 1 and then edit it as follows:


```
Before change: EVS_HOST=`hostname`
After change: EVS_HOST=FQDN-format-host-name
```

For details about how to set the event server in the FQDN format, see the following descriptions in the *Job Management Partner 1/Base User's Guide*:

- Setting the event server in a system using DNS
- Notes about Event Service

2.16.3 Startup method

The startup method is the same as the normal startup method. For details, see *3.1.2 In UNIX* in the *Job Management Partner 1/Integrated Management - Manager Administration Guide*.

2.17 Setting up JP1/IM - Manager

This section describes the setup items for JP1/IM - Manager.

The user who performs this setup must have `root` permissions.

2.17.1 Executing the setup program

To execute the setup program after you have installed JP1/IM - Manager:

1. Execute the setup program.
 - `/opt/jp1cons/bin/jp1cc_setup`
 - `/opt/jp1scope/bin/jp1cs_setup`
 - `/opt/jp1imm/bin/imcf/jp1cf_setup`

Depending on the installation status, execution of the setup program may not be required, as explained below.

- When execution of the setup program is required
JP1/Base was uninstalled and then reinstalled.
- When execution of the setup program is not required
A new installation of JP1/IM - Manager was performed.
The same version of JP1/IM - Manager was installed by overwriting.

2.17.2 Setting automatic startup and automatic stop

This subsection describes the procedure for implementing automatic startup and stopping of JP1/IM - Manager at the time the host is started and stopped.

(1) In Solaris

To set automatic startup and automatic stop:

1. Copy the automatic startup and automatic stop scripts.

```
# cd /etc/opt/jp1cons
# cp -p jco_start.model jco_start
# cp -p jco_stop.model jco_stop
```

(2) In AIX

To set automatic startup and automatic stop:

1. Copy the automatic startup and automatic stop scripts.

```
# cd /etc/opt/jp1cons
```

```
# cp -p jco_start.model jco_start
# cp -p jco_stop.model jco_stop
```

2. Specify the automatic startup settings.

Use the `mkitab` command to add the startup entries for JP1/Base and JP1/IM - Manager to the `/etc/inittab` file. Perform this step in the following order:

```
# mkitab -i hntr2mon "jplbase:2:wait:/etc/opt/jplbase/
jbs_start"
# mkitab -i jplbase "jplcons:2:wait:/etc/opt/jplcons/
jco_start"
```

After you have added the above settings, use the `lsitab` command to check the settings.

```
# lsitab -a
init:2:initdefault:
brc::sysinit:/sbin/rc.boot 3 >/dev/console 2>&1 # Phase 3 of
system boot
:
:
hntr2mon:2:once:/opt/hitachi/HNTRLib2/etc/D002start
jplbase:2:wait:/etc/opt/jplbase/jbs_start
jplcons:2:wait:/etc/opt/jplcons/jco_start
#
```

The settings are correct if the added entries are specified in the order of `hntr2mon` (Hitachi Network Objectplaza Trace Library (HNTRLib2)), `jplbase`, and `jplcons`.

3. Specify the automatic stop settings.

Use a text editor to add the stop entries for JP1/Base and JP1/IM - Manager to the `/etc/rc.shutdown` file.

Perform this step in the following order:

File name: `/etc/rc.shutdown`

```
:  
    test Δ -x Δ /etc/opt/jp1cons/jco_stop Δ && Δ /etc/opt/jp1cons/  
jco_stop  
    test Δ -x Δ /etc/opt/jp1base/jbs_stop Δ && Δ /etc/opt/jp1base/  
jbs_stop  
:
```

Note:

The `/etc/rc.shutdown` script detects an error and cancels shutdown processing when the termination code of the last command executed is anything other than zero. Therefore, we recommend that you add a code such as the following at the end of the `/etc/rc.shutdown` script:

```
exit 0
```

The automatic startup and stop scripts are now enabled.

2.17.3 Settings for using the functions of Central Scope

When a new installation of JP1/IM - Manager is performed, the functions of Central Scope are disabled by default.

To use the functions of Central Scope:

1. Create a Central Scope database.
Execute the `jcsdbsetup` command.
2. Enable Central Scope Service (`jcsmain`).
Execute `jcoimdef -s ON`.
3. Restart JP1/IM - Manager.
4. Verify that Central Scope Service is running.
Execute the `jco_spm_status` command. Make sure that `jcsmain` is displayed as an active process.

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

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*.

2.17.4 Settings for handling JP1/IM - Manager failures

JP1/IM - Manager provides functions to protect against its own failures, such as the

tool for collecting data needed for resolving problems and the function for automatic restart in the event of abnormal process termination.

This subsection describes the settings for handling JP1/IM - Manager failures.

(1) Preparations for collecting data in the event of a failure

JP1/IM - Manager provides a shell script (`jim_log.sh`) as a tool for collecting data in the event of a problem. This tool enables you to collect data needed for resolving problems in batch mode.

The data collection tool of JP1/IM - Manager can collect troubleshooting data for JP1/IM - Manager and JP1/Base. For details about the data that can be collected, see 9.3 *Data that needs to be collected when a problem occurs* in the *Job Management Partner 1/Integrated Management - Manager Administration Guide*.

About the data collection tool

- About `jim_log.sh`

See *jim_log.sh (UNIX only)* in 1. *Commands* in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.

In the event of a problem, it may be advisable to obtain a core dump to facilitate investigation of the cause. Output of a core dump depends on the user environment settings. Check the settings described below.

(a) Setting the size of a core dump file

The maximum size of a core dump file depends on the `root` user's core dump file size setting (`ulimit -c`). In JP1/IM - Manager, the following setting is specified in the `jco_start` and `jco_start.cluster` scripts so that output of core dump files does not depend on the user's environment settings:

```
ulimit -c unlimited
```

If this setting violates your machine's security policies, comment out the setting in the scripts, as shown below:

```
# ulimit -c unlimited
```

Note:

If the setting is commented out, you may not be able to investigate problems because no core dump will be output in the event of a segmentation failure in a JP1/IM - Manager process or a bus failure, or when a core dump file is to be output by the `jcogencore` command.

(2) Restart settings in the event of abnormal process termination

To specify restart settings in the event of abnormal process termination:

2. Installation and Setup (for UNIX)

1. Define process restart.

Edit the following extended startup process definition file so that process restart is enabled:

```
/etc/opt/jplcons/conf/jplco_service.conf
```

The restart parameter is the fourth value that is separated by the vertical bars (|). Set either 0 (do not restart (default)) or 1 (restart).

2. Apply the definition information.

If JP1/IM - Manager is running, execute JP1/IM - Manager's reload command so that the process restart setting is enabled:

```
/opt/jplcons/bin/jco_spmc_reload
```

About process restart definition

- About the extended startup process definition file (`jplco_service.conf`)

See *Extended startup process definition file (jplco_service.conf)* in 2. *Definition Files* in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.

(3) Setting JP1 event issuance in the event of abnormal process termination

To set JP1 event issuance in the event of abnormal process termination:

1. Set JP1 event issuance.

Edit the following IM parameter definition file:

```
/etc/opt/jplcons/conf/jplco_param_v7.conf
```

In this file, `SEND_PROCESS_TERMINATED_ABNORMALLY_EVENT` and `SEND_PROCESS_RESTART_EVENT` are JP1 event issuance setting parameters. To issue JP1 events, change the value to `dword:1`.

2. Execute the `jbssetcnf` command to apply the definition information.

```
/opt/jplbase/bin/jbssetcnf /etc/opt/jplcons/conf/jplco_param_v7.conf
```

3. Restart JP1/Base and the products that require JP1/Base.

The specified settings take effect after the restart.

About JP1 event issuance settings

- About the IM parameter definition file (`jplco_param_v7.conf`)

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*.

(4) Setting the health check function

To set the health check function in order to detect JP1/IM - Manager process hang-ups:

1. Open the health check definition file (`jcohc.conf`) and specify parameters.

To enable the health check function, specify `ENABLE=true`.

Specify `EVENT=true` to issue a JP1 event and

`COMMAND=command-to-be-executed` to execute a notification command when a hang-up is detected.

2. If you specified the notification command, execute the `jcohcetest` command to check the notification command's execution validity.

Execute the `jcohcetest` command to determine whether the command specified in `COMMAND` executes correctly. If the operation is not valid, check and, if necessary, revise the specification.

3. Use the `jco_spmd_reload` command to reload JP1/IM - Manager, or restart JP1/IM - Manager.

About the health check function settings

- About the health check definition file (`jcohc.conf`)

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*.

- About the `jcohcetest` command

See `jcohcetest` in *1. Commands* in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.

(5) Automatic backup and recovery settings for a monitoring object database

You specify these settings when you will be using the functions of Central Scope.

If the OS shuts down while the monitoring tree is being updated or a failover occurs during cluster operation, the monitoring object database may be corrupted. Therefore, you must set the monitoring object database to be backed up and recovered automatically when the monitoring tree is being updated.

These settings are enabled when you have performed a new installation, and they are disabled if the settings were disabled in the old version of JP1/IM - Manager or JP1/IM - Central Scope. Change the settings as appropriate to your operation.

To specify automatic backup and recovery settings for a monitoring object database:

1. Terminate JP1/IM - Manager.
2. Execute the `jbssetcnf` command using the following file for the parameters:

2. Installation and Setup (for UNIX)

To enable the automatic backup and recovery functions for the monitoring object database: `auto_dbbackup_on.conf`

To disable the automatic backup and recovery functions for the monitoring object database: `auto_dbbackup_off.conf`

When you execute the `jbssetcnf` command, the settings are applied to the JP1 common definition information.

For details about the `jbssetcnf` command, see the *Job Management Partner 1/Base User's Guide*.

About the settings in the file

For details about the settings in the file, 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*.

3. Start JP1/IM - Manager.

2.17.5 Settings during upgrading

This subsection describes the setup items to be specified during upgrade installation of JP1/IM - Manager.

(1) **Changing the location of the event acquisition filter**

If you have upgraded JP1/IM - Central Console, you can use the event acquisition filter (for compatibility).

If you had been using an event acquisition filter (for compatibility) with an old version of JP1/IM - Manager or JP1/IM - Central Console, you can change the location of the event acquisition filter from Event Console Service to Event Base Service by executing the `jcochafmode` command. If you change the location of the event acquisition filter to Event Base Service, the filter can be used not only for monitoring JP1 events but also for monitoring the status of automated actions and monitored objects. You can also define detailed filter conditions. Note that if you want to continue using the pre-upgrade event acquisition filter, there is no need to change the filter location.

Note:

Once you change the location of the event acquisition filter, you can no longer restore the previous event acquisition filter. Carefully consider the location of the event acquisition filter before you execute the `jcochafmode` command.

To change the location of the event acquisition filter:

1. Terminate JP1/IM - Manager.

2. Execute the `jcochafmode` command to change the location of the filter.
3. Start JP1/IM - Manager.
 - About the functions of the event acquisition filter
See 3.2.2 *Event acquisition filter* in the *Job Management Partner 1/Integrated Management - Manager Overview and System Design Guide*.
 - About inheriting the settings of the event acquisition filter (for compatibility)
See 12.2.3(2) *Upgrading from JP1/IM - Central Console version 7* in the *Job Management Partner 1/Integrated Management - Manager Overview and System Design Guide*.
 - About the `jcochafmode` command
See `jcochafmode` in 1. *Commands* in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.

(2) Executing the Central Scope upgrade command

If you have upgraded JP1/IM - Central Scope from version 8 or earlier, apply the procedure below to execute the upgrade command. Until you execute the upgrade command, JP1/IM - Central Scope will run in the mode that is compatible with the old version of JP1/IM - Central Scope (no new functions can be used).

To execute the Central Scope upgrade command:

1. Terminate JP1/IM - Manager.
2. Check the available disk capacity.

To execute the `jplcsverup` command in the next step, you will need sufficient free space for the monitoring object database. The monitoring object database includes all the data in the following directory:

```
/var/opt/jplscope/database/jcsdb/
```

3. Execute the `jplcsverup` command.
4. Execute the `jbssetcnf` command.

Whether the following functions are enabled or disabled depends on the settings of the old version of JP1/IM - Central Scope:

- Completed-action linkage function
- Monitoring of the maximum number of status change events

To enable these functions, execute the `jbssetcnf` command using the files shown in the table below as arguments.

Table 2-3: Setting files for enabling functions

File name	Description
action_complete_on.conf	File for enabling the completed-action linkage function
evhist_warn_event_on.conf	File for enabling the JP1 event issuance function when the number of status change events for the monitored object exceeds the maximum value (100)

5. Start JP1/IM - Manager.
6. Use JP1/IM - View to connect to JP1/IM - Manager (JP1/IM - Central Scope) to check for any problems.
 - About the `jp1csverup` command
See *jp1csverup (UNIX only)* in *1. Commands* in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.

(3) Updating the automated action definition file

If you have upgraded JP1/IM - Central Console from version 08-01 or earlier, apply the procedure below to update the automated action definition file.

If you want to continue using the automated action definition file for version 08-01 or earlier as is, there is no need to perform this procedure.

To update the automated action definition file:

1. Terminate JP1/IM - Manager.
2. Execute the following `jcadefconv` command to update the automated action definition file:

```
jcadefconv -i action-definition-file-name-before-conversion -o
action-definition-file-name-after-conversion
```
3. Start JP1/IM - Manager.
 - About the automated action function
See *5. Command Execution by Automated Action* in the *Job Management Partner 1/Integrated Management - Manager Overview and System Design Guide*.
 - About the `jcadefconv` command
See *jcadefconv* in *1. Commands* in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.

Chapter

3. Using IM Configuration Management to Set the System Hierarchy

This chapter explains how to use IM Configuration Management to set the system's hierarchical structure.

- 3.1 Registering hosts
- 3.2 Setting the system hierarchy
- 3.3 Setting the profiles
- 3.4 Importing and exporting the management information in IM Configuration Management
- 3.5 Setting a virtualization system configuration

3.1 Registering hosts

This section explains how to use IM Configuration Management - View to register hosts into IM Configuration Management.

3.1.1 Registering hosts

To register a new host into the IM Configuration Management database:

1. In the IM Configuration Management window, click the **Host List** tab.
The **Host List** page is displayed.
2. Use one of the following methods to display the Register Host window:
 - In the tree area, select **Host List**, and then from the menu bar, choose **Edit**, and then **Register Host**.
 - In the tree area, select **Host List**, and then from the pop-up menu that is displayed by right-clicking, choose **Register Host**.
3. Register a new host by specifying the items that are displayed in the Register Host window.

For details about the items displayed in the Register Host window, see 4.2 *Register Host window* in the manual *Job Management Partner 1/Integrated Management - Manager GUI Reference*.

4. Click the **OK** button.

3.1.2 Displaying host information

To display information about the hosts that have been registered into the IM Configuration Management database:

1. In the IM Configuration Management window, click the **Host List** tab.
The **Host List** page is displayed.

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

2. Choose **Host List**.

If you choose **Host List** from the tree area, hosts are listed as lower host information in the node information display area.

To view host information, do the following:

To display basic information:

From the tree area or the node information display area, select a host, and

then click the **Basic Information** button. The basic information and detailed information are displayed in the node information display area.

To display product information:

From the tree area or the node information display area, select a host, and then click the **Product Information** button. The product information and detailed information are displayed in the node information display area.

To display service information:

From the tree area or the node information display area, select a host, and then click the **Service Information** button. The service information and detailed information are displayed in the node information display area.

3.1.3 Deleting hosts

To delete hosts from the IM Configuration Management database:

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

The **Host List** page is displayed.

2. From the tree area, choose a host.

If the selected host has lower hosts, you can also select hosts from the **Lower Host Information** list that is displayed by clicking the **Lower Host Information** button. In this case, you can select multiple hosts at the same time.

3. Use one of the following methods to delete the selected host or hosts:

- From the menu bar, choose **Edit**, and then **Delete Host**.
- From the pop-up menu that is displayed by right-clicking, choose **Delete Host**.

When a confirmation message asking whether you wish to delete the selected host or hosts is displayed, choose **Yes**.

The selected host or hosts are deleted from the IM Configuration Management database. If deletion processing fails, an error message is displayed.

3.1.4 Changing host information

To change host information that has been registered into the IM Configuration Management database:

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

The **Host List** page is displayed.

2. From the tree area, choose a host.

If the selected host has lower hosts, you can also select a host from the **Lower**

Host Information list that is displayed by clicking the **Lower Host Information** button.

3. Use one of the following methods to display the Edit Host Properties window:
 - From the menu bar, choose **Edit**, and then choose **Edit Host Properties**.
 - From the pop-up menu that is displayed by right-clicking, choose **Edit Host Properties**.
4. Change host information by changing the items that are displayed in the Edit Host Properties window.

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

3.1.5 Collecting information from hosts

You can collect host information about specified hosts. Execute this processing immediately after you have registered a host or when information about a host or the installed software has been updated for a reason such as the following:

- The OS has been replaced
- The IP address has changed
- Software has been replaced
 - Software was installed or uninstalled
 - Software was upgraded

Once you collect host information, the profile lists are cleared. When the Display/Edit Profiles window is opened after host information has been collected, the most recent profile lists are collected.

To collect host information from the IM Configuration Management database:

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

The **Host List** page or the **IM Configuration** page is displayed.

2. From the tree area, choose a host.

If the chosen host has lower hosts, you can also select hosts from the **Lower Host Information** list that is displayed by clicking the **Lower Host Information** button. In this case, you can select multiple hosts at the same time.

3. Use one of the following methods to collect host information:

- From the menu bar, choose **Operation**, then **Collect Host Information**.
- From the pop-up menu that is displayed by right-clicking, choose **Collect Host Information**.

When a confirmation message asking whether you wish to collect information about the selected host or hosts is displayed, choose **Yes**. Information about the selected host or hosts is collected. In the case of multiple hosts, you can check the execution results in the Execution Results window.

You can use the **Host List** page to check a host's status after host information has been collected. If collection of a host's information has failed, the host icon is displayed in gray in the tree area on the **Host List** page. To display the detailed information, click the **Basic Information** button in the node information display area on the **Host List** page.

3.2 Setting the system hierarchy

This section explains how to use IM Configuration Management to set the system hierarchy when a JP1/IM system is configured.

3.2.1 Collecting the system hierarchy

To collect the system hierarchy:

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

The **Host List** page or the **IM Configuration** page is displayed.

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

When a confirmation message asking whether you wish to collect configuration definition information is displayed, choose **Yes**. The collected configuration definition information is saved in the manager where IM Configuration Management is running.

- If the collected configuration definition information contains a host that has not been registered into IM Configuration Management, that host is automatically registered into the IM Configuration Management database. However, host information is not collected; to collect host information, use the **Host List** page or **IM Configuration** page in the IM Configuration Management window.
- If the collected configuration definition information contains duplicated host names, an error message is displayed, and the collected information is not applied to the configuration definition information that is maintained by the IM Configuration Management database.
- If the collected configuration definition information contains duplicated host names, the collected configuration definition information is discarded, and the IM configuration tree is displayed in gray on the **IM Configuration** page.
- If the collected configuration definition information does not match the configuration definition information maintained by the IM Configuration Management database, the system hierarchy is displayed in gray in the tree area of the **IM Configuration** page.
- If the configuration definition information maintained by JP1/Base at the manager where IM Configuration Management is running has been deleted, the message KNAN20230-Q IM configuration does not exist. Do you want to delete the IM configuration maintained in the Server? is displayed.

If you click the **Yes** button, the configuration definition information maintained by the IM Configuration Management database is deleted. If you click the **No** button, the system hierarchy is displayed in gray in the tree area of the **IM Configuration** page, but the configuration definition information maintained by the IM Configuration Management database is not deleted.

3.2.2 Displaying the system hierarchy

You can view the system hierarchy on the **IM Configuration** page in the IM Configuration Management window.

To display the **Host List** page in the IM Configuration Management window:

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

The **IM Configuration** page is displayed.

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

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

Selecting a host from the tree area and then clicking the **Lower Host Information** button displays in the node information display area information about the selected host's lower hosts.

3.2.3 Verifying the system hierarchy

To verify whether the configuration definition information collected from all hosts that constitute the system matches the configuration definition information maintained by IM Configuration Management:

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

The **Host List** page or the **IM Configuration** page is displayed.

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

When a confirmation message asking whether you wish to verify the configuration definition information is displayed, choose **Yes**.

When you execute verification of configuration definition information, the system collects configuration definition information for the selected hosts and verifies whether it matches the configuration definition information maintained by IM Configuration Management.

If the configuration definition information maintained by JP1/Base at the manager where IM Configuration Management is running does not match the configuration definition information maintained by the IM Configuration Management database, a host icon indicating the error status is displayed in the tree area on the **IM**

Configuration page in the Configuration Management window.

If verification fails, a host icon indicating the error status is displayed in the tree area on the **IM Configuration** page in the Configuration Management window.

If the version of JP1/Base running at the host is earlier than 9, verification of system hierarchy is not supported. Therefore, a host icon indicating unknown configuration status is displayed in the tree area on the **IM Configuration** page in the IM Configuration Management window of IM Configuration Management - View.

If the manager's configuration definition information is missing or corrupted, manager verification results in an error and the processing is cancelled.

3.2.4 Editing the system hierarchy

This subsection explains how to set and change the system hierarchy.

(1) Adding hosts

To add hosts:

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

The **Host List** page or the **IM Configuration** page is displayed.

2. From the menu bar, choose **Edit**, then **Edit IM Configuration**.

The Edit IM Configuration window appears.

3. From the tree area of the Edit IM Configuration window, choose the higher host under which a host is to be added.

Lower Host Information displays information about the hosts already under the selected host. **Host List** displays information about the hosts that can be added to the selected host.

4. Use one of the following methods to register a host:

- In the Edit IM Configuration window, from **Host List**, select the host to be added, and then drag and drop it in the tree area.
- From the menu bar in the Edit IM Configuration window, choose **Edit**, then **Add Host**.

The Select Hosts window appears. From the hosts displayed in **Select host(s):**, select the host (or hosts) to be added, and then move them to the list of **Selected host(s):**. When you have finished selecting hosts, click the **OK** button.

- In the tree area of the Edit IM Configuration window, from the pop-up menu that is displayed by right-clicking, choose **Add Host**.

The Select Hosts window appears. From the hosts displayed in **Select host(s)**, select the host (or hosts) to be added, and then move them to the list of **Selected host(s)**. When you have finished selecting hosts, click the **OK** button.

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

(2) Moving hosts

To move hosts:

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

The **Host List** page or the **IM Configuration** page is displayed.

2. From the menu bar, choose **Edit**, then **Edit IM Configuration**.

The Edit IM Configuration window appears.

3. From the tree area of the Edit IM Configuration window, select the host to be moved.
4. Use one of the following methods to select the host to be moved:
 - Select the host from the tree area in the Edit IM Configuration window, and then drag and drop it onto another hierarchy in the tree area.
 - From the menu bar in the Edit IM Configuration window, choose **Edit** then **Cut**, and in the tree area, select a higher host at the destination, and then choose **Edit** then **Paste**.
 - In the tree area of the Edit IM Configuration window, from the pop-up menu that is displayed by right-clicking, choose **Cut**, and in the tree area, select a higher host at the destination, and then from the pop-up menu that is displayed by right-clicking, choose **Paste**.

If you move a higher host, its lower hosts also move.

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

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

(3) **Deleting hosts**

To delete hosts:

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

The **Host List** page or the **IM Configuration** page is displayed.

2. From the menu bar, choose **Edit**, then **Edit IM Configuration**.

The Edit IM Configuration window appears.

3. From the tree area of the Edit IM Configuration window, select the hosts to be deleted.

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

- From the tree area in the Edit IM Configuration window, select a host to be deleted, and then drag and drop it on to **Host List**.
- From the menu bar in the Edit IM Configuration window, choose **Edit**, then **Delete Host**.
- In the tree area of the Edit IM Configuration window, from the pop-up menu that is displayed by right-clicking, choose **Delete Host**.

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

If you delete a higher host, its lower hosts are also deleted at the same time.

3.2.5 **Applying the system hierarchy**

To apply the system hierarchy to the system that is managed by IM Configuration Management:

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

The **Host List** page or the **IM Configuration** page is displayed.

2. From the menu bar, choose **Edit**, then **Edit IM Configuration**.

The Edit IM Configuration window appears.

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

Configuration of the JP1/IM system can now be applied. While you possess update rights and are editing the configuration, no other user can edit the configuration of the JP1/IM system.

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

Update Host Information.

The information displayed in the Edit IM Configuration window is applied to the host information, and the most recent configuration definition information is obtained.

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

The most recent configuration definition information set by IM Configuration Management is distributed to all the hosts in the system, and the existing configuration definition information is updated by overwriting.

The result of applying the system hierarchy is displayed in a dialog box. You can check the resulting system hierarchy on the **IM Configuration** page in the IM Configuration Management window. If this reflection processing fails, a host icon indicating the error status is displayed in the tree area on the **IM Configuration** page. To view the detailed information, click the **Basic Information** button in the node information display area on the **IM Configuration** page.

3.2.6 Synchronizing the system hierarchy

To synchronize the system hierarchy:

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

The **Host List** page or the **IM Configuration** page is displayed.

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

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

If no site managers are defined under the integrated manager, the system configuration definition information is not synchronized.

3.3 Setting the profiles

This section explains how to set the JP1/Base profiles that are run on each host during JP1/IM system configuration.

There are two types of information for a JP1/Base profile:

- Valid configuration information

This consists of the settings currently used by each service of the agent. When each service starts normally, this information is updated by the agent. Each service is run based on this valid configuration information.

- Information in the configuration file

This is the configuration file stored at the agent. The definition information specified in this configuration file may not always be used to start each service. For example, if information in the definition file has been edited but has not yet been applied to the services, the valid configuration information does not match the information in the configuration file.

3.3.1 Collecting profiles

There are two ways to collect the JP1/Base profiles from the agents, depending on the collection range. This subsection describes the two methods.

(1) Collecting profiles in batch mode

This subsection explains how to collect the JP1/Base profiles in batch mode from all hosts that are defined in the system hierarchy.

Note that profile collection cannot be performed in batch mode in the following cases:

- Another user has exclusive editing rights for one of the configuration files.
- Another user is performing batch collection of profiles.
- Another user is performing batch reflection of edited information in the configuration files.

To collect profiles in batch mode:

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

The **Host List** page or the **IM Configuration** page is displayed.

2. From the menu bar, choose **Operation**, then **Batch Collect Profiles**.

Batch collection of all profiles is executed. The execution result is displayed in the Execution Results window.

When a confirmation message asking whether you wish to collect profiles in batch mode is displayed, choose **Yes**. Profiles are collected and stored in the manager where IM Configuration Management is running.

After executing the batch collection, you can check profile status in the Display/Edit Profiles window. If there is a profile whose collection has failed, its **Configuration file contents** in the node information display area is grayed out, and the profile status is displayed in **Status**.

After executing batch collection of profiles, you can check host status on the **IM Configuration** page in the Configuration Management window. If there is a profile whose collection has failed, a host icon indicating the error status is displayed in the tree area on the **IM Configuration** page. To view the detailed information, click the **Basic Information** button in the node information display area on the **IM Configuration** page.

(2) Collecting profiles from individual hosts

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

This function is applicable to hosts that are running JP1/Base version 9. You can use the Display/Edit Profiles window to collect an individual host's JP1/Base profile.

Note that profiles cannot be collected while another user has exclusive editing rights for the configuration files.

To collect the profile from a specific host:

1. In the IM Configuration Management window, click the **IM Configuration** tab. The **IM Configuration** page is displayed.
2. From the tree area, choose the host whose profile is to be collected.
3. Use one of the following methods to display the Display/Edit Profiles window:
 - From the menu bar, choose **Display**, and then **Display Profiles**.
 - From the pop-up menu that is displayed by right-clicking, choose **Display Profiles**.
4. From the tree area, choose a JP1 product name (JP1/Base), and then use one of the following methods to obtain exclusive editing rights:
 - From the menu bar, choose **Edit**, and then **Exclusive Editing Settings**.
 - From the pop-up menu that is displayed by right-clicking, choose **Exclusive Editing Settings**.

You can obtain exclusive editing rights on the JP1 product (JP1/Base) on the target host.

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

The **Configuration File** page is displayed.

If you have never collected configuration files, clicking the **Configuration File** button automatically starts configuration file collection.

6. From the tree area, choose a profile to be edited, and then use one of the following methods to collect it:
 - From the menu bar, choose **Operation**, and then **Collect Profiles**.
 - From the pop-up menu that is displayed by right-clicking, choose **Collect Profiles**.

When a confirmation message asking whether you wish to collect the target profile from the agent is displayed, choose **Yes**. Profiles are collected and stored in the manager where IM Configuration Management is running.

3.3.2 Collecting profile lists

Lists of profiles that are to be managed by IM Configuration Management can be collected from the agents. The collected information is displayed in the tree area of the Display/Edit Profiles window.

The profile lists are placed in unregistered status at the time of any of the following operations:

- Initial startup of IM Configuration Management
- Collection of host information
- Reflection of system hierarchy
- Execution of the `jcfimport` command

To collect profile lists:

1. In the IM Configuration Management window, click the **IM Configuration** tab. The **IM Configuration** page is displayed.
2. Use one of the following methods to display the Display/Edit Profiles window:
 - From the menu bar, choose **Display**, and then **Display Profiles**.
 - From the pop-up menu that is displayed by right-clicking, choose **Display Profiles**.
3. From the tree area, choose a JP1 product name (JP1/Base), and then use one of the following methods to update a profile list:
 - From the menu bar, choose **Operation**, and then **Rebuild Profile Tree**.
 - From the pop-up menu that is displayed by right-clicking, choose **Rebuild**

Profile Tree.

The profile tree is rebuilt and the profile list is updated. If you have restarted the agent or the agent's JP1/Base, rebuild the profile tree before you edit or apply the profile.

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

The profile lists to be managed by IM Configuration Management are collected from the agents.

Notes

- If profile tree rebuild processing fails, an error message is displayed, together with the profile tree that existed before the rebuild processing was executed. Although you can perform operations on the profiles that existed before the rebuild processing and on profiles whose information is still the same as at the agents, such operations may have adverse effects on future operations. It is better to eliminate the cause of the error and then re-execute the profile tree rebuild processing.
- Collection of profile lists fails if multiple event log traps are started using the same operation definition file or using operation definition files with the same name in different directories.

3.3.3 Displaying profiles

There are two ways to display JP1/Base profiles, depending on the type of information to be displayed. This subsection describes both methods.

(1) *Displaying the valid configuration information*

This subsection explains how to display the valid configuration information for JP1/Base for each host. This function is applicable to hosts that are running JP1/Base version 9.

To display the valid configuration information:

1. In the IM Configuration Management window, click the **IM Configuration** tab. The **IM Configuration** page is displayed.
2. From the tree area, choose a host whose valid configuration information is to be displayed.
3. Use one of the following methods to display the Display/Edit Profiles window:
 - From the menu bar, choose **Display**, and then **Display Profiles**.
 - From the pop-up menu that is displayed by right-clicking, choose **Display Profiles**.

3. Using IM Configuration Management to Set the System Hierarchy

4. From the tree area of the Display/Edit Profiles window, choose an item for which valid configuration information is to be displayed.
5. Click the **Valid Configuration Information** button.

The valid configuration information that is displayed depends on the item selected in the tree area of the Display/Edit Profiles window. For details about the relationship between the selected item and the displayed information, see *4.6.1 Valid Configuration Information page* in the manual *Job Management Partner 1/Integrated Management - Manager GUI Reference*.

(2) Displaying configuration files

This subsection explains how to display the configuration files for JP1/Base for individual hosts. These configuration files are displayed in the Display/Edit Profiles window.

To display configuration files:

1. In the IM Configuration Management window, click the **IM Configuration** tab. The **IM Configuration** page is displayed.
2. From the tree area, choose the host whose configuration file is to be displayed.
3. Use one of the following methods to display the Display/Edit Profiles window:
 - From the menu bar, choose **Display**, and then **Display Profiles**.
 - From the pop-up menu that is displayed by right-clicking, choose **Display Profiles**.
4. From the tree area of the Display/Edit Profiles window, choose an item for which the configuration file is to be displayed.
5. Click the **Configuration File** button.

The contents of the configuration file that is displayed depends on the item selected in the tree area of the Display/Edit Profiles window. For details, see *4.6.2 Configuration File page* in the manual *Job Management Partner 1/Integrated Management - Manager GUI Reference*.

Whether the information displayed in a configuration file can be edited depends on the item. For details about how to edit the configuration files, see *3.3.4 Editing configuration files*.

3.3.4 Editing configuration files

This subsection explains how to edit and save collected JP1/Base configuration files. For details about how to collect configuration files, see *3.3.1 Collecting profiles*. You can use the Display/Edit Profiles window to edit and save a configuration file.

Note that the types of profiles that can be edited in the configuration files are the event

forwarding information, log file trap information, event log trap information, and local action information.

To edit and save a configuration file:

1. In the IM Configuration Management window, click the **IM Configuration** tab. The **IM Configuration** page is displayed.
2. From the tree area, choose a host whose configuration file is to be edited.
3. Use one of the following methods to display the Display/Edit Profiles window:
 - From the menu bar, choose **Display**, and then **Display Profiles**.
 - From the pop-up menu that is displayed by right-clicking, choose **Display Profiles**.
4. From the tree area, choose a JP1 product name (JP1/Base) and then use one of the following methods to obtain exclusive editing rights.[#]
 - From the menu bar, choose **Edit**, and then **Exclusive Editing Settings**.
 - From the pop-up menu that is displayed by right-clicking, choose **Exclusive Editing Settings**.
5. From the tree area in the Display/Edit Profiles window, choose the configuration file that is to be edited.
6. In the node information display area in the Display/Edit Profiles window, click the **Configuration File** button.

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

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

The edited configuration file is saved in the manager where IM Configuration Management is running.

Note that the contents of the configuration file that was stored in the manager where IM Configuration Management is running are not forwarded to the host. When you perform reflection processing on the configuration file, its contents are saved automatically. For details about how to forward and apply the contents of configuration files, see *3.3.5 Applying edited information in configuration files*.

If you save the contents of a configuration file in the manager where IM Configuration Management is running and then collect the profile from the host,

the configuration file will be overwritten by the collected information.

#

- If you cut and paste character strings in a configuration file, you must perform step 4 to obtain exclusive editing rights.
- If you will only be copying character strings in a configuration file, there is no need to perform step 4.
- If you have already obtained exclusive editing rights, there is no need to perform step 4.

3.3.5 Applying edited information in configuration files

There are two ways to apply edited information in configuration files, depending on the range to which the information is to be applied. This subsection describes both methods.

In the case of JP1/Base version 9, if configuration file reflection processing fails, the agent's configuration file is rolled back to the original configuration file.

(1) Using the batch mode to apply edited information in configuration files

This subsection explains how to use the batch mode to apply edited information in configuration files to all hosts that are registered in the system hierarchy.

Note that the types of profiles in the configuration files that can be applied are the event forwarding information, event log trap information, and local action information.

The batch mode cannot be used to apply edited information in configuration files in the following cases:

- Another user has exclusive editing rights for one of the configuration files.
- Another user is performing batch collection of profiles.
- Another user is performing batch reflection of edited information in configuration files.

To use the batch mode to apply edited information in configuration files:

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

The **Host List** page or the **IM Configuration** page is displayed.

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

Batch reflection of profiles is executed. The execution result is displayed in the Execution Results window.

When a confirmation message asking whether you wish to perform batch reflection of configuration files is displayed, choose **Yes**. The contents of the

configuration files stored at the manager where IM Configuration Management is running are applied to all hosts.

After executing batch reflection, you can check the status of the configuration files in the Display/Edit Profiles window. If there is a configuration file whose reflection failed or whose status is **Saved on the server**, an icon indicating that the editing process is underway is displayed for the configuration file in the tree area.

After executing batch reflection of configuration files, you can check host status on the **IM Configuration** page in the Configuration Management window. If there is a configuration file whose reflection failed or whose status is **Saved on the server**, a host icon indicating the error status is displayed in the tree area. To view the detailed information, click the **Basic Information** button in the node information display area on the **IM Configuration** page.

(2) Applying edited information in configuration files to individual hosts

This subsection explains how to apply edited information in configuration files to individual hosts.

Note that the types of profiles in configuration files that can be applied to individual hosts are the event forwarding information, log file trap information, event log trap information, and local action information.

To apply edited information in a configuration file to an individual host:

1. In the IM Configuration Management window, click the **IM Configuration** tab.^{#1}
The **IM Configuration** page is displayed.
2. From the tree area, choose the host whose configuration file is to be applied.^{#1}
3. Use one of the following methods to display the Display/Edit Profiles window.^{#1}
 - From the menu bar, choose **Display**, and then **Display Profiles**.
 - From the pop-up menu that is displayed by right-clicking, choose **Display Profiles**.
4. From the tree area, choose a JP1 product name (JP1/Base) and then use one of the following methods to obtain exclusive editing rights.^{#1}
 - From the menu bar, choose **Edit**, and then **Exclusive Editing Settings**.
 - From the pop-up menu that is displayed by right-clicking, choose **Exclusive Editing Settings**.
5. From the tree area, choose the profile that is to be applied, and then click the **Configuration File** button.^{#2}
The **Configuration File** page is displayed.

3. Using IM Configuration Management to Set the System Hierarchy

6. From the menu bar, choose **Operation, Reflect Profiles**, and then **Apply by Reloading**.

The profile is applied.

When a confirmation message asking whether you wish to apply the contents of the configuration file is displayed, choose **Yes**.

#1

If you have already obtained exclusive editing rights, there is no need to perform steps 1 through 4.

#2

If you have edited the configuration file that contains the profile to be applied, there is no need to perform step 5.

3.4 Importing and exporting the management information in IM Configuration Management

This section explains how to set the system hierarchy during JP1/IM system configuration by importing and exporting the management information in IM Configuration Management.

We recommend that you make a backup before importing because the data maintained by IM Configuration Management is altered by import processing. If an error occurs during import processing, the data is rolled back to its status before the import processing began.

To import and export the management information in IM Configuration Management:

1. Export the management information in IM Configuration Management.

At the manager where the source IM Configuration Management is running, execute the `jcfexport` command to export the management information in IM Configuration Management that is registered in the IM Configuration Management database.

For details about the export function, see *6.5 Importing and exporting IM Configuration Management information* in the *Job Management Partner 1/ Integrated Management - Manager Overview and System Design Guide*.

For details about the export procedure, see *8.5.1 Exporting management information of IM Configuration Management* in the *Job Management Partner 1/ Integrated Management - Manager Administration Guide*.

2. Edit the management information in IM Configuration Management that was exported.

For example, to rename a host, edit the management information in IM Configuration Management that was exported.

3. Import into IM Configuration Management the management information that was exported.

At the manager where the target IM Configuration Management is running, execute the `jcfimport` command to import into IM Configuration Management the management information that was exported and edited.

For details about the import function, see *6.5 Importing and exporting IM Configuration Management information* in the *Job Management Partner 1/ Integrated Management - Manager Overview and System Design Guide*.

For details about the import procedure, see *8.5.2 Importing management information of IM Configuration Management* in the *Job Management Partner 1/*

3. Using IM Configuration Management to Set the System Hierarchy

Integrated Management - Manager Administration Guide.

4. Apply the system hierarchy to the system.

Use IM Configuration Management - View to apply the imported system hierarchy to the system that is to be managed by JP1/IM. For details about how to apply the system hierarchy to a system, see *3.2.5 Applying the system hierarchy*.

3.5 Setting a virtualization system configuration

This section describes the settings for using IM Configuration Management to manage a virtualization configuration by importing and exporting the management information in IM Configuration Management during system configuration; it also describes the settings for using Central Scope for monitoring.

3.5.1 Using IM Configuration Management to manage a virtualization configuration

This subsection describes the settings for using IM Configuration Management to manage a virtualization configuration.

To manage a virtualization configuration, you need VMware ESX.

(1) Setting information about virtual hosts

Use one of the following methods to specify information about the virtual hosts that are to be added to the JP1/IM system:

- Use IM Configuration Management - View to register the virtual hosts into IM Configuration Management.

For details about how to register hosts, see *3.1 Registering hosts*.

- Import into the manager where IM Configuration Management is running the virtualization configuration information acquired from VMware ESX where the virtual hosts are running.

To import into the manager where IM Configuration Management is running the virtualization configuration information acquired from VMware ESX:

1. Export the management information in IM Configuration Management.

At the manager where IM Configuration Management is running, execute the `jcfexport` command to export the management information in IM Configuration Management registered in the IM Configuration Management database.

2. Output the virtualization configuration information of VMware ESX to a file.

At the same manager, execute the `jcfcolvmesx` command to output the virtualization configuration information of VMware ESX to a virtualization configuration information file.

If you use SSL (https) for communication, you must install a certificate for VMware ESX. For details about how to install a certificate, see *3.5.1(4) Installing a certificate for VMware ESX*.

3. Apply the contents of the virtualization configuration information file to the

3. Using IM Configuration Management to Set the System Hierarchy

exported management information in IM Configuration Management.

At the same manager, execute the `jcfmkhostsdata` command to apply the contents of the virtualization configuration information file to the exported management information in IM Configuration Management.

4. Import the updated management information in IM Configuration Management.

At the same manager, execute the `jcfimport` command to import the management information in IM Configuration Management that was updated in step 3.

(2) Adding virtual hosts to the system hierarchy

Use IM Configuration Management - View to add to the system hierarchy virtual hosts registered in 3.5.1(1) *Setting information about virtual hosts*. For details about how to add hosts to the JP1/IM system configuration, see 3.2.4 *Editing the system hierarchy*.

(3) Applying the system hierarchy to the system

Use IM Configuration Management - View to apply to the system the system hierarchy that was set in 3.5.1(2) *Adding virtual hosts to the system hierarchy*. For details about how to apply the system hierarchy to a system, see 3.2.5 *Applying the system hierarchy*.

Once you have applied the system hierarchy to the system, you can view the hierarchical relationships between physical and virtual hosts on the **IM Configuration** page in the IM Configuration Management window.

(4) Installing a certificate for VMware ESX

Two communication methods are available for acquiring virtualization configuration information from VMware ESX with the `jcfcolvmesx` command. One method uses SSL (https), and the other method does not use SSL (http).

If you use SSL for communication with VMware ESX, you must install a certificate for the target VMware ESX host on the manager where JP1/IM - Manager is running. Install as many certificates as there are VMware ESXs with which communication is to be established.

This subsection explains how to install a certificate for a VMware ESX host. For details, see the VMware ESX documentation.

(a) Obtaining certificates

The two ways to obtain an SSL certificate from VMware ESX are by using Internet Explorer and by obtaining the certificate files directly. This subsection describes both methods.

■ Using Internet Explorer

The procedure that uses Internet Explorer 6.0 with Windows Server 2003 is explained

below. If you are using any other browser, see the browser's Help.

To obtain a certificate:

1. Access `https://VMware-ESX-host-name`.

A Security Alert dialog box appears.

If the **View Certificate** button is displayed in the Security Alert dialog box, proceed to step 3.

If the Security Alert dialog box is not displayed, double-click the key icon (SSL authentication) that is displayed in the lower right part of the browser, and then proceed to step 4.

2. Click the **OK** button.

Another Security Alert dialog box, which is different from the one in step 1, is displayed.

3. Click the **View Certificate** button.

The Certificate dialog box is displayed.

4. Click the **Details** tab and then click the **Copy to File** button.

The Certificate Export Wizard dialog box is displayed.

5. Click the **Next** button.

6. Select **DER encoded binary X509 (CER)** and then click the **Next** button.

7. In the **File name** text box, specify the name of the certificate file that is to be saved, and then click the **Next** button.

8. Click the **Finish** button.

■ Obtaining certificate files directly

In the case of VMware ESX 3.5, a certificate file is stored in `/etc/vmware/ssl/rui.crt` on the VMware ESX host.

(b) Installing certificates in IM Configuration Management

Install the obtained certificate in IM Configuration Management using the procedure described below.

■ In Windows

This procedure must be performed by a user with Administrator permissions.

To install a certificate in IM Configuration Management:

1. Open a command prompt and move to `Manager-path\bin\jre\bin`.
2. Execute the `keytool` command to install the certificate in IM Configuration

Management.

```
keytool -import -file certificate-file-name -alias  
VMware-ESX-host-name -keystore  
..\..\..\data\imcf\vmware.keystore
```

For *certificate-file-name*, specify the name of the certificate file (including path) that was acquired in (a) *Obtaining certificates*.

For *VMware-ESX-host-name*, specify the name of the VMware ESX host from which the certificate was acquired.

3. Enter any password for the key store.
If you install multiple certificates, enter the same password for each of them.
4. When a message asking whether the certificate is to be trusted is displayed, enter **yes**.
The certificate is installed in IM Configuration Management.
5. Repeat steps 1 through 4 as many times as there are VMware ESX hosts.

■ **In UNIX**

This procedure must be performed by a user with superuser permissions.

To install a certificate in IM Configuration Management:

1. Open the console or terminal, and then execute `cd /opt/jplimm/bin/jre/bin`.
2. Execute the `keytool` command to install the certificate in IM Configuration Management.

```
./keytool -import -file certificate-file-name -alias  
VMware-ESX-host-name -keystore /var/opt/jplimm/data/imcf/  
vmware.keystore
```

For *certificate-file-name*, specify the name of the certificate file (including path) that was acquired in (a) *Obtaining certificates*.

For *VMware-ESX-host-name*, specify the name of the VMware ESX host from which the certificate was acquired.

3. Enter any password for the key store.
If you install multiple certificates, enter the same password for each of them.
4. When a message asking whether the certificate is to be trusted is displayed, enter **yes**.
The certificate is installed in IM Configuration Management.
5. Repeat steps 1 through 4 as many times as there are VMware ESX hosts.

(c) Deleting certificates

This subsection explains how to delete certificates from IM Configuration Management.

■ In Windows

1. Open a command prompt and move to *Manager-path*\bin\jre\bin.
2. Execute the `keytool` command to delete a certificate from IM Configuration Management.

```
keytool -delete -alias VMware-ESX-host-name -keystore
..\..\..\data\imcf\vmware.keystore
```

For *VMware-ESX-host-name*, specify the name of the VMware ESX host that corresponds to the certificate that is to be deleted.

3. Enter the password that was specified in (b) *Installing certificates in IM Configuration Management*.

The certificate for the specified VMware ESX host is deleted from IM Configuration Management.

■ In UNIX

1. Open the console or terminal, and then execute `cd /opt/jplimm/bin/jre/bin`.
2. Execute the `keytool` command to delete a certificate from IM Configuration Management.

```
./keytool -delete -alias VMware-ESX-host-name -keystore /var/
opt/jplimm/data/imcf/vmware.keystore
```

For *VMware-ESX-host-name*, specify the name of the VMware ESX host that corresponds to the certificate that is to be deleted.

3. Enter the password that was specified in (b) *Installing certificates in IM Configuration Management*.

The certificate for the specified VMware ESX host is deleted from IM Configuration Management.

(5) Changing the communication type for VMware ESX

The `jcfcolvmesx` command enables you to communicate with VMware ESX using an interface of VMware Infrastructure SDK in order to acquire virtualization configuration information.

In VMware Infrastructure SDK, you can select the setting that allows only the method that uses SSL (https) or the setting that allows only the method that does not use SSL (http) during communication with VMware ESX. The default is the setting that allows only the method that uses SSL (https).

This subsection provides an overview of how to change the communication type permitted by VMware Infrastructure SDK. For details, see the VMware ESX documentation.

To change the communication type for VMware ESX:

1. Log on to the service console of VMware ESX with superuser permissions.
2. Move to `/etc/vmware/hostd`.
3. Use a text editor to open the `proxy.xml` file.
4. Change the VMware Infrastructure SDK item in the `<EndpointList>` tag in the `proxy.xml` file and then save the file.

In the following example, change the item in bold type according to the communication type that is to be used.

```
...
<e id="1">
  <_type>vim.ProxyService.NamedPipeServiceSpec</_type>
  <accessMode>httpsWithRedirect</accessMode>
  <pipeName>/var/run/vmware/proxy-sdk</pipeName>
  <serverNamespace>/sdk</serverNamespace>
</e>
...
```

- To allow only the method that uses SSL (https), specify `httpsWithRedirect`.
 - To allow only the method that does not use SSL (http), specify `httpOnly`.
 - To allow both the method that uses SSL (https) and the method that does not use SSL (http), specify `httpAndHttps`.
5. Execute the following command to restart the `vmware-hostd` process:

```
service mgmt-vmware restart
```

3.5.2 Using Central Scope to monitor a virtualization configuration

This subsection describes the settings for creating a monitoring tree to be used by Central Scope to monitor a virtualization configuration.

(1) *Setting procedure*

To create a monitoring tree to be used by Central Scope to monitor a virtualization configuration:

1. Export the management information in IM Configuration Management.

At the manager where the IM Configuration Management that manages the virtualization configuration is running, execute the `jcfeexport` command to export the management information in IM Configuration Management registered

in the IM Configuration Management database.

For details about the management information in IM Configuration Management that can be exported, see *6.5.1 Types of information that can be imported or exported* in the *Job Management Partner 1/Integrated Management - Manager Overview and System Design Guide*.

2. Export the monitoring tree information to Central Scope.

At the same manager, execute the `jcsdbexport` command to export the monitoring tree information to Central Scope.

3. Merge the management information in IM Configuration Management and the monitoring tree information in Central Scope that were exported.

At the same manager, execute the `jcfmkcsdata` command to merge the management information in IM Configuration Management and the monitoring tree information in Central Scope that were exported.

4. Import the information that was merged in step 3 to Central Scope.

At the same manager, execute the `jcsdbimport` command to import the management information in IM Configuration Management that was exported. The monitoring tree of the virtualization configuration is added to Central Scope's monitoring tree.

(2) Prerequisites for the monitoring tree of Central Scope

To monitor a virtualization configuration, the tree part of the monitored hosts displayed in Central Scope's monitoring tree is grouped. A monitoring tree of a virtualization configuration is then created. Therefore, in order to create a monitoring tree of a virtualization configuration, Central Scope must provide a server-oriented monitoring tree in which monitored objects are grouped by server.

If you create a monitoring tree of a virtualization configuration from a monitoring tree that is not server-oriented, you must modify the created monitoring tree.

Chapter

4. Setting up Central Console

This chapter explains how to set up the functions of Central Console, such as JP1 event filtering and automated actions.

- 4.1 Settings for the operations to be performed during JP1/IM event acquisition
- 4.2 Setting JP1 event filtering
- 4.3 Setting automated actions
- 4.4 Setting correlation event generation
- 4.5 Setting memo entries
- 4.6 Editing event guide information
- 4.7 Setting JP1 event issuance during action status change
- 4.8 How to display user-specific event attributes
- 4.9 Setting the severity changing function
- 4.10 Setting JP1/IM - View for each login user
- 4.11 Customizing the JP1/IM - View operation
- 4.12 Setting monitor startup for linked products
- 4.13 Setting the Tool Launcher window
- 4.14 Settings for using a Web-based JP1/IM - View

4.1 Settings for the operations to be performed during JP1/IM event acquisition

You can specify settings for the operations to be performed when JP1/IM - Manager acquires JP1 events that are registered in Event Service, such as setting event acquisition filter conditions and setting the buffer size when JP1 events are buffered in the manager's memory.

Normally, you can use the default settings, but you may customize the settings if necessary. The following settings can be specified:

- Event acquisition filter settings
- Maximum number of events when JP1 events are extracted and buffered in the manager (event buffer)
- Retry count and interval when Event Service is to be reconnected
- `jcochstat` command use permissions

You use the System Environment Settings window to specify the settings. The specified settings are saved in the manager's JP1/IM - Manager, which means that the identical information is displayed by all JP1/IM - Views that are connected to the same JP1/IM - Manager.

To specify settings for the operations to be performed during JP1/IM event acquisition:

1. Start the System Environment Settings window.

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

2. Adjust parameters.

Adjust parameters as necessary, such as the number of event buffers and the retry count for connecting to Event Service.

For details about the System Environment Settings window, see *2.11 System Environment Settings window* in the manual *Job Management Partner 1/Integrated Management - Manager GUI Reference*.

Note:

Information about these settings is also included in the system profile (`.system`). However, directly editing this file is not recommended; if any of the settings are wrong, JP1/IM - Manager may not function correctly.

4.2 Setting JP1 event filtering

You can set filters to limit the types of JP1 events that will be displayed in the Event Console window. This enables you to display only the JP1 events that satisfy your monitoring purposes. There are four types of filters that can be set from the Event Console window:

- View filters

View filters define conditions for displaying JP1 events on the **Monitor Events** page in the Event Console window. You can define a maximum of 50 view filters per JP1 user.

- Event receiver filters

Event receiver filters define the types of JP1 events that can be monitored by the user. The system administrator can define a maximum of 128 event receiver filters.

- Severe events filters

Severe events filters define the severe events that are to be displayed on the **Severe Events** page in the Event Console window.

- Event acquisition filters[#]

Event acquisition filters define filter conditions to be applied when JP1/IM - Manager (Event Base Service) acquires events from JP1/Base (Event Service). You can define a maximum of 50 event acquisition filters per manager.

#

Event acquisition filters are for compatibility. They provide filter conditions to be applied when JP1/IM - Manager control (Event Console Service) acquires events from JP1/IM - Manager control (Event Base Service).

The following subsections describe how to set each type of filter.

4.2.1 Settings for view filters

View filters set conditions for the JP1 events that are to be displayed on the **Monitor Events** page in the Event Console window.

(1) *Creating a new view filter*

To create a new view filter:

1. If you use the attribute value of a JP1 event displayed in the events list as the view condition, select a JP1 event from the list.

2. From the Event Console window, choose **View**, and then **View List of Filters**.
The View List of Filters window appears. This window displays filter names.
3. To create a new view filter, click the **Add** button. To use an existing filter, click the **Copy** button, and then click the **Edit** button.

Clicking the **Add** button displays the Settings for View Filter window.

Clicking the **Copy** button adds **Copy *view-filter-name*** to the filters. In this case, select **Copy *view-filter-name*** and then click the **Edit** button to display the Settings for View Filter window.

4. In the Settings for View Filter window, set the filter.

In the Settings for View Filter window, you can specify the following settings:

- Filter name

Specify a name for the filter in order to distinguish setting conditions.

- Condition group

Specify a name for a group of conditions in order to distinguish sets of pass conditions or exclusion conditions.

You can set a maximum of five pass-conditions groups and five exclusion-conditions groups; the relationship between condition groups is the OR condition.

To set condition groups, you must click the **Show List** button to keep **List** displayed.

To add a condition group: Click the **Add** button to add an unnamed **Condition group *n*** (*n*: number).

To copy a condition group: Select a condition group and then click the **Copy** button to add **Copy *selected-condition-group-name***.

To delete a condition group: Select a condition group and then click the **Delete** button to delete the selected condition group.

To rename a condition group: Select a condition group to display its name in **Condition group name**. Edit this name and move the focus to rename the condition group.

- To set conditions (detailed settings for a condition group)

Specify pass conditions or exclusion conditions for the filter.

You can combine multiple conditions, in which case the relationship between conditions is the AND condition.

The items that you can specify include source host, event level, object type,

object name, root object type, root object name, occurrence, user name, message, product name, event ID, status, and action status. If an integrated monitoring database is used, original severity level and memo can also be specified.

To apply the attribute value of the JP1 event selected from the Event Console window to the conditions list, click the **Read From Selected Event** button.

5. Click the **OK** button.

The Settings for View Filter window closes and the View List of Filters window is displayed again.

6. Click the **OK** button.

The specified settings (for creating a filter) take effect and the View List of Filters window closes.

(2) Changing a view filter

To change the contents of an existing view filter:

1. If you use the attribute value of a JP1 event displayed in the events list as the view condition, select a JP1 event from the list.
2. Display the Settings for View Filter window.

Use one of the following methods to display the Settings for View Filter window:

- From the Event Console window, choose **View**, and then **View List of Filters** to display the View List of Filters window.

Next, in the View List of Filters window, select the view filter that is to be changed, and then click the **Edit** button.

- In the Event Console window, on the **Monitor Events** page, from the **Filter name** list box, select the view filter that is to be changed, and then click the **View Filter Settings** button, or from the menu bar, choose **View**, and then **View Filter Settings**.

3. In the Settings for View Filter window, edit the filter settings.

To apply the attribute values of the JP1 event selected from the Event Console window to the conditions list, click the **Read From Selected Event** button.

4. Click the **OK** button.

The Settings for View Filter window closes, and the window that called the Settings for View Filter window is displayed again. When the View List of Filters window is displayed again, click **OK** to apply the specified settings (for changing a filter).

(3) Deleting a view filter

To delete an existing view filter:

1. From the Event Console window, choose **View**, and then **View List of Filters**.

The View List of Filters window appears. This window displays filter names.

2. Select the view filter to be deleted, and then click the **Delete** button.

The selected view filter is deleted.

3. Click the **OK** button.

The specified settings (for deleting a filter) take effect and the View List of Filters window closes.

4.2.2 Settings for event receiver filters

You can limit the JP1 events that can be monitored by the user in the Event Console window.

The specified settings are applied to the events that are distributed to JP1/IM - View after you click the **Apply** button in the Settings for Event Receiver Filter window. A user for whom no event receiver filters have been set can monitor all JP1 events.

To set event receiver filters, you need `JP1_Console_Admin` permissions.

(1) Creating a new event receiver filter

To create a new event receiver filter:

1. If you use the attribute value of a JP1 event displayed in the events list as the view condition, select a JP1 event from the list.

2. From the Event Console window, choose **Options**, and then **Event Receiver Filter Settings**.

The Settings for Event Receiver Filter window appears.

This window displays filter names and user names.

3. Click the **Add** button.

The Detailed Settings for Event Receiver Filter window appears.

4. In the Detailed Settings for Event Receiver Filter window, specify filter settings.

Specify the following settings in the Detailed Settings for Event Receiver Filter window:

- Filter name

Specify a name for the filter in order to distinguish setting conditions.

- Name of the user subject to this filter

Specify the name of the user who will be restricted by this filter. To enter multiple user names, separate the names with the comma.

The same user cannot be subject to multiple filters.

- Condition group

Specify a name for a group of conditions in order to distinguish sets of pass conditions or exclusion conditions.

You can set a maximum of 30 pass-conditions groups and 30 exclusion-conditions groups; the relationship between condition groups is the OR condition.

To set condition groups, you must click the **Show List** button to keep **List** displayed.

To add a condition group: Click the **Add** button to add an unnamed **Condition group** *n* (*n*: number).

To copy a condition group: Select a condition group and then click the **Copy** button to add **Copy** *selected-condition-group-name*.

To delete a condition group: Select a condition group and then click the **Delete** button to delete the selected condition group.

To rename a condition group: Select a condition group to display its name in **Condition group name**. Edit this name and move the focus to rename the condition group.

- To set conditions (detailed settings for a condition group)

Specify pass conditions or exclusion conditions for the filter.

You can combine multiple conditions, in which case the relationship between conditions is the AND condition.

The items that you can specify include source host, event level, object type, object name, root object type, root object name, occurrence, user name, message, product name, event ID, status, and action status.

To apply the attribute value of the JP1 event selected from the Event Console window to the conditions list, click the **Read From Selected Event** button.

5. Click the **OK** button.

The Detailed Settings for Event Receiver Filter window closes and the Settings for Event Receiver Filter window is displayed again.

6. Click the **Apply** button.

The settings are applied.

(2) Changing an event receiver filter

To change the contents of an existing event receiver filter:

1. If you use the attribute value of a JP1 event displayed in the events list as the view condition, select a JP1 event from the list.
2. From the Event Console window, choose **Options**, and then **Event Receiver Filter Settings**.

The Settings for Event Receiver Filter window appears.

3. Select the event receiver filter to be changed, and then click the **Edit** button.

The Detailed Settings for Event Receiver Filter window appears.

4. In the Detailed Settings for Event Receiver Filter window, edit the filter settings.

To apply the attribute value of the JP1 event selected from the Event Console window to the conditions list, click the **Read From Selected Event** button.

5. Click the **OK** button.

The Detailed Settings for Event Receiver Filter window closes and the Settings for Event Receiver Filter window is displayed again.

6. Click the **Apply** button.

The settings are applied.

(3) Deleting an event receiver filter

To delete an existing event receiver filter:

1. From the Event Console window, choose **Options**, and then **Event Receiver Filter Settings**.

The Settings for Event Receiver Filter window appears.

2. Select the event receiver filter to be deleted, and then click the **Delete** button.

The selected event receiver filter is deleted.

3. Click the **Apply** button.

The settings are applied.

4.2.3 Settings for severe events filters

You can set conditions for the severe events that are to be displayed on the **Severe Events** page in the Event Console window. By setting severe events filters, you can define specific JP1 events as severe events.

Because the specified settings are saved in the manager's JP1/IM - Manager, the same information is displayed by all JP1/IM - Views that are connected to the same JP1/IM

- Manager.

To set a severe events filter, you need JP1_Console_Admin permissions.

To set a severe events filter:

1. Select a JP1 event from the events list to use its attribute value as the severe event definition conditions.
2. In the Event Console window, choose **Options**, and then **Severe Event Definitions**.

The Severe Event Definitions window appears.

3. In the Severe Event Definitions window, define a severe event.

In the Severe Event Definitions window, you can specify the following settings:

- Condition group

Specify a name for a group of conditions in order to distinguish sets of pass conditions or exclusion conditions.

You can set a maximum of 30 pass-conditions groups and 30 exclusion-conditions groups; the relationship between condition groups is the OR condition.

To set condition groups, you must click the **Show List** button to keep **List** displayed.

To add a condition group: Click the **Add** button to add an unnamed **Condition group n** (*n*: number).

To copy a condition group: Select a condition group and then click the **Copy** button to add **Copy selected-condition-group-name**.

To delete a condition group: Select a condition group and then click the **Delete** button to delete the selected condition group.

To rename a condition group: Select a condition group to display its name in **Condition group name**. Edit this name and move the focus to rename the condition group.

- To set conditions (detailed settings for a condition group)

Specify pass conditions or exclusion conditions for the filter.

You can combine multiple conditions, in which case the relationship between conditions is the AND condition.

The items that you can specify include source host name, event level, object type, object name, root object type, root object name, occurrence, user name, message, product name, event ID, and action status.

To apply the attribute value of the JP1 event selected from the Event Console window to the conditions list, click the **Read From Selected Event** button.

4. Click the **OK** button.

The specified definition takes effect and the Severe Event Definitions window closes.

Note:

You can create one severe event definition for each manager. The same information is displayed by all JP1/IM - Views that are connected to the same manager's JP1/IM - Manager. Carefully evaluate the settings before you specify them.

4.2.4 Settings for event acquisition filters

This subsection explains how to set only one event acquisition filter, how to set an event acquisition filter by switching the filter conditions, and how to set an event acquisition filter (for compatibility).

Event acquisition filters are set whether or not the integrated monitoring database is used. Therefore, if you set an event acquisition filter (for compatibility), it is used even when the integrated monitoring database is used.

The event acquisition filters set here, except for the event acquisition filter (for compatibility), limit the JP1 events that are distributed to all services of JP1/IM - Manager.

(1) Setting only one event acquisition filter

This subsection explains how to set only one filter condition that is to be applied when JP1/IM - Manager acquires events from the JP1/Base event database. This method is not applicable when an event acquisition filter (for compatibility) is used. In order to start the System Environment Settings window, you need JP1_Console_Admin permissions.

To set only one event acquisition filter:

1. Select a JP1 event from the events list to use its attribute value as the condition.
2. In the Event Console window, choose **Options**, and then **System Environment Settings**.

The System Environment Settings window appears.

3. In **A filter is being applied**, click the **Configure** button.

The Event Acquisition Settings window appears.

To edit an existing event acquisition filter, select the desired event acquisition filter from the drop-down list in **Event acquisition conditions**, and then click the **Configure** button. Details of the selected event acquisition filter are displayed in the Event Acquisition Settings window to enable you to edit the settings.

4. In the Event Acquisition Settings window, specify the filter settings.

In the Event Acquisition Settings window, you can specify the following settings:

- Filter name and filter ID

If you are creating a new event acquisition filter, specify a name for the filter. The smallest filter ID that is available in the list of event acquisition conditions is automatically assigned to the filter.

To edit an event acquisition filter, the name and ID of the event acquisition filter to be edited are displayed. You can edit the filter name and filter ID. Note that simply changing the filter name or filter ID does not result in creation of a new event acquisition filter. An existing filter name or filter ID cannot be specified.

- Condition group

Specify a name for a group of conditions in order to distinguish sets of pass conditions or exclusion conditions. Note that the same name cannot be assigned to a pass-conditions group and an exclusion-conditions group.

You can set a maximum of 30 pass-conditions groups and 30 exclusion-conditions groups; the relationship between condition groups is the OR condition.

To set condition groups, you must click the **Show List** button to keep **List** displayed.

To add a condition group: Click the **Add** button to add an unnamed **Condition group *n*** (*n*: number).

To copy a condition group: Select a condition group and then click the **Copy** button to add **Copy *selected-condition-group-name***.

To delete a condition group: Select a condition group and then click the **Delete** button to delete the selected condition group.

To rename a condition group: Select a condition group to display its name in **Condition group name**. Edit this name and move the focus to rename the condition group.

- To set conditions (detailed settings for a condition group)

Specify pass conditions or exclusion conditions for the filter.

You can combine multiple conditions, in which case the relationship between

conditions is the AND condition.

The items that you can specify include source host, event level (or JP1/SES event), object type, object name, root object type, root object name, occurrence, user name, message, product name, action, and event ID.

To apply the attribute value of the JP1 event selected from the Event Console window to the conditions list, click the **Read From Selected Event** button.

5. Click the **OK** button.

The Event Acquisition Settings window closes and the System Environment Settings window is displayed again.

6. Click the **Apply** button.

The specified settings take effect.

(2) Setting an event acquisition filter by switching the filter conditions

This subsection explains how to set an event acquisition filter by switching the filter conditions that are used when JP1/IM - Manager acquires events from the JP1/Base event database.

To set an event acquisition filter by switching, you first display the Event Acquisition Conditions List window from the System Environment Settings window, and then set the event acquisition filter. This method enables you to create a new event acquisition filter by editing, copying, or deleting an existing event acquisition filter. Note that this method is not applicable when an event acquisition filter (for compatibility) is used.

In order to start the System Environment Settings window, you need JP1_Console_Admin permissions.

To set an event acquisition filter by switching:

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

The System Environment Settings window appears.

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

The Event Acquisition Conditions List window appears.

3. To edit, copy, or delete an existing event acquisition filter, select the desired event acquisition filter from **Filter list**.

4. Click the **Add**, **Edit**, **Copy**, or **Delete** button, as appropriate.

When you click the **Add** button:

The Event Acquisition Settings window is displayed so that you can set a new event acquisition filter.

When you click the **Edit** button:

The Event Acquisition Settings window is displayed to enable you to edit the event acquisition filter selected in step 3. For an overview of the settings that can be specified in the Event Acquisition Settings window, see *4.2.4(1) Setting only one event acquisition filter*.

When you click the **Copy** button:

The selected event acquisition filter is copied and then added to **Filter list**. **Copy** is added to the beginning of the name of the copied event acquisition filter. The name of the copied event acquisition filter cannot be changed here.

To rename the event acquisition filter, use the Event Acquisition Settings window that is displayed by clicking the **Edit** button.

When you click the **Delete** button:

The selected event acquisition filter is deleted.

5. Click the **OK** button.

The Event Acquisition Conditions List window closes and the System Environment Settings window is displayed again.

6. Click the **Apply** button.

The specified settings take effect.

(3) Setting an event acquisition filter (for compatibility)

You can set filter conditions to be applied when Event Console Service acquires events from Event Base Service. Note that this method is applicable only when an event acquisition filter (for compatibility) is used.

In order to start the System Environment Settings window, you need `JP1_Console_Admin` permissions.

To set an event acquisition filter (for compatibility):

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

The System Environment Settings window appears.

2. In **Event acquisition conditions**, click the **Configure** button.

The Event Acquisition Settings (for compatibility) window appears.

3. Set filter conditions to be applied when events are acquired from Event Service.

To display JP1/SES events in the Event Console window, select the **Acquire** check box in **JP1/SES events**.

To specify JP1 event severity levels, select all applicable items (**Emergency**,

Alert, Critical, Error, Warning, Notice, Information, and Debug). If the **Event level** check box is not selected, all events for which a severity has been defined become the target.

To specify an event ID, select the **Event ID** check box, and then specify a desired JP1 event ID. To specify multiple event IDs, separate the IDs with the comma.

Conditions set here are passed to Event Service as an AND condition between a JP1/SES event and an event ID or as an AND condition between an event level and an event ID.

4. Click the **OK** button.

The System Environment Settings window is displayed again.

5. Click the **Apply** button.

The specified settings take effect.

(4) Setting common exclusion conditions

This subsection explains how to set common exclusion conditions for temporarily excluding JP1 events that are issued by a host to be maintained from the acquisition target. In order to start the System Environment Settings window, you need JP1_Console_Admin permissions.

To set common exclusion conditions:

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

The System Environment Settings window appears.

2. To edit existing common exclusion conditions, select their common exclusion-conditions group name, and then in **Common exclusion-conditions groups**, click the **Configure** button.

The Common Exclusion-Conditions Settings window appears. Proceed to step 4.

3. To define new common exclusion conditions, click the **Editing list** button.

The Event Acquisition Conditions List window appears.

In the Event Acquisition Conditions List window, you can add, edit, copy, and delete common exclusion conditions. You can set a maximum of 30 common exclusion-conditions groups. The relationship between condition groups is the OR condition.

- Adding a condition group: Click the **Add** button to display the Common Exclusion-Conditions Settings window in order to set a new common exclusion-conditions group.
- Editing a condition group: Click the **Edit** button to display the Common

Exclusion-Conditions Settings window. You can edit the selected common exclusion-conditions group.

- Copying a condition group: Select a common exclusion-conditions group and then click the **Copy** button to add **Copy selected-condition-group-name**.
- Deleting a condition group: Select a common exclusion-conditions group and then click the **Delete** button to delete the selected condition group.

4. Set the conditions in the Common Exclusion-Conditions Settings window.

- Common exclusion-conditions group ID

From the drop-down list, select a common exclusion-conditions group ID.

If you are adding common exclusion conditions, the smallest common exclusion-conditions group ID that is available in the common exclusion-conditions groups list is assigned automatically to the common exclusion conditions.

If you are editing common exclusion conditions, the common exclusion-conditions group ID selected from the common exclusion-conditions groups list is displayed.

A duplicate common exclusion-conditions group ID cannot be specified.

- Common exclusion-conditions group name

Specify a name for the common exclusion-conditions group.

If you have selected an existing common exclusion-conditions group and then renamed it, the group's name is overwritten by the new name.

- Setting conditions (detailed settings for a condition group)

Set conditions for the JP1 events that are to be excluded as acquisition targets.

You can combine multiple conditions, in which case the relationship between conditions is the AND condition.

The items that you can specify include source host, event level (JP1/SES event), object type, object name, root object type, root object name, occurrence, user name, message, product name, and event ID.

To apply the attribute value of the JP1 event selected from the Event Console window to the conditions list, click the **Read From Selected Event** button.

5. Click the **OK** button.

The Common Exclusion-Conditions Settings window closes and the System Environment Settings window is displayed again.

6. To apply the specified common exclusion conditions, select the applicable check

4. Setting up Central Console

boxes under **Apply**.

7. Click the **Apply** button.

The specified settings take effect.

4.3 Setting automated actions

This section describes the settings for using the automated action function.

4.3.1 Setting up an execution environment for the automated action function

You can set up an execution environment for automated actions by editing the automated action environment definition file (`action.conf`). You specify in the automated action environment definition file such information as the default user who executes automated actions and the regular expressions to be used by the automated action function.

To set up an execution environment for the automated action function:

1. Copy the model file, rename it to the definition file name (`action.conf`), and then edit the definitions.

Copy the model file of the automated action execution environment definition files, rename it, and then edit the definition file (`action.conf`). Execute the following:

In Windows:

```
cd Console-path
copy default\action.conf.update conf\action.conf
notepad conf\action.conf
```

In UNIX:

```
cd /etc/opt/jplcons
cp -p default/action.conf.update conf/action.conf
vi conf/action.conf
```

For details about the definitions in the automated action environment definition file, 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*.

2. Terminate JP1/IM - Manager.
3. Execute the `jbssetcnf` command to apply the definitions.

In Windows:

```
jbssetcnf Console-path\conf\action.conf
```

In UNIX:

```
/opt/jp1base/bin/jbssetcnf /etc/opt/jp1cons/conf/  
action.conf
```

When you execute the `jbssetcnf` command, the execution environment settings for the automated action function are applied to the JP1 common definition information. For details about the `jbssetcnf` command, see the *Job Management Partner 1/Base User's Guide*.

4. Start JP1/IM - Manager.

4.3.2 Setting the execution conditions and details of automated actions

You can use the GUI of JP1/IM - View or the definition file to set the execution conditions and details of automated actions. This subsection describes both methods.

Note:

If you have upgraded your installation of Central Console from version 08-01 or earlier, you must update the definition file.

For details about the updating procedure, see *1.18.3(3) Updating the automated action definition file (Windows)* or *2.17.5(3) Updating the automated action definition file (UNIX)*. If you use the definition file for version 08-01 or earlier, there is no need to update the file.

(1) Using the GUI of JP1/IM - View

To set the execution conditions and details of automated actions:

1. In the Event Console window, choose **Options**, and then **Automated Action Parameter Settings**.

The Action Parameter Definitions window appears.

2. Click the **Add**, **Edit**, or **Delete** button, as appropriate.

To set a new automated action:

Click the **Add** button. In the Action Parameter Detailed Definitions window, specify the execution conditions and details of an automated action.

Clicking the **OK** button displays the Action Parameter Definitions window again.

To edit existing automated action conditions:

From the list, select an automated action to be edited, and then click the **Edit** button. In the Action Parameter Detailed Definitions window, edit the execution conditions and details of the existing automated action.

Clicking the **OK** button displays the Action Parameter Definitions window again.

To delete an existing automated action:

From the list, select an automated action to be deleted, and then click the **Delete** button.

3. Click the **Apply** button.

The specified settings take effect.

For details about the Action Parameter Definitions window, see 2.24 *Action Parameter Definitions window* in the manual *Job Management Partner 1/Integrated Management - Manager GUI Reference*.

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*.

(2) Editing the definition file

To set the execution conditions and details of automated actions:

1. Edit the automated action definition file (`actdef.conf`).

The following table lists the storage location of the automated action definition file.

Table 4-1: Storage location of automated action definition file

OS	Storage location
Windows	<code>Console-path\conf\action\</code>
	<code>shared-folder\jplcons\conf\action\</code> (logical host)
UNIX	<code>/etc/opt/jplcons/conf/action/</code>
	<code>shared-directory/jplcons/conf/action/</code> (logical host)

To check the automated action definition file for errors, execute the `jcamakea` command.

2. Apply the edited information.

To apply the edited automated action definition file, perform one of the following:

- Restart JP1/IM - Manager.
- Execute the `jcachange` command.
- In the Action Parameter Definitions window of JP1/IM - View, click the **Apply** button.

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*.

4.3.3 Settings for monitoring the automated action execution status

The two types of monitoring of the automated action execution status are *status monitoring* and *delay monitoring*. If an error is detected during status monitoring or delay monitoring, you can report the automated action error by issuing a JP1 event or by executing a notification command.

This subsection describes the settings for both types of monitoring.

(1) Setting status monitoring and delay monitoring of automated actions

You can set monitoring of the automated action execution status by using the GUI of JP1/IM - View or by editing the definition file.

Using the GUI of JP1/IM - View

Use the Action Parameter Definitions window to set status monitoring and the Action Parameter Detailed Definitions window to set delay monitoring. For details about the Action Parameter Definitions window and the Action Parameter Detailed Definitions window, see the following:

- 2.24 *Action Parameter Definitions window* in the manual *Job Management Partner 1/Integrated Management - Manager GUI Reference*
- 2.25.1 *Action Parameter Detailed Definitions window* in the manual *Job Management Partner 1/Integrated Management - Manager GUI Reference*

Editing the definition file

Status monitoring and delay monitoring can both be set by editing the automated action definition file (`actdef.conf`).

For details, 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*.

(2) Setting notification when an error is detected during status monitoring or delay monitoring

To set notification when an error is detected during status monitoring or delay monitoring requires that you edit the automatic action notification definition file (`actnotice.conf`).

For details, 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*.

4.3.4 Setting suppression of automated action execution

Suppression of automated action execution can be set for each automated action. You can use the GUI of JP1/IM - View or you can edit the definition file to set suppression of automated execution of an action.

(1) Using the GUI of JP1/IM - View

Use the Action Parameter Detailed Definitions window to suppress execution of an automated action.

For details, see *2.25.1 Action Parameter Detailed Definitions window* in the manual *Job Management Partner 1/Integrated Management - Manager GUI Reference*.

(2) Editing the definition file

To suppress execution of an automated action, edit the automated action definition file (`actdef.conf`).

For details, 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*.

4.4 Setting correlation event generation

To generate correlation events, you must do the following:

- Set startup of the correlation event generation function
- Set the size and number of correlation event generation history files
- Set startup options
- Create and apply a correlation event generation definition

4.4.1 Setting startup of the correlation event generation function

To specify settings for starting the correlation event generation function:

1. Execute the startup command for the correlation event generation function:
`jcoimdef -egs ON`

When the integrated monitoring database is not used:

Event Generation Service starts automatically when JP1/IM - Manager starts.

When the integrated monitoring database is used:

The correlation event generation function of Event Base Service starts automatically when JP1/IM - Manager starts.

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*.

4.4.2 Setting the size and number of correlation event generation history files

This subsection explains how to set the size and number of correlation event generation history files. If you use the default settings, there is no need to perform the procedure described below.

The following table shows the default size and number of correlation event generation history files.

Table 4-2: Default size and number of correlation event generation history files

Item	Default value
Size	10 MB
Number of files	3

To set the size and number of correlation event generation history files:

1. Create a correlation event generation environment definition file.

Create a desired correlation event generation environment definition file.

For details about the parameters and values that are to be specified in the correlation event generation environment definition file, 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*.

We recommend that you store the created correlation event generation environment definition file in the following folder/directory:

Table 4-3: Folder/directory for storing the correlation event generation environment definition file

OS	Storage location [#]
Windows	<i>Console-path</i> \default\
	<i>shared-folder</i> \jplcons\default\ (logical host)
UNIX	/etc/opt/jplcons/default/
	<i>shared-directory</i> /jplcons/default/ (logical host)

#

By storing the correlation event generation environment definition file in the indicated folder/directory, the data collection tool can automatically collect from it in the same manner as with other definition files.

2. Execute the `jbssetcnf` command.

Execute the `jbssetcnf` command with the created correlation event generation environment definition file specified as an argument.

When you execute the `jbssetcnf` command, the settings in the correlation event generation environment definition file are applied to the JP1 common definition information. For details about the `jbssetcnf` command, see the *Job Management Partner 1/Base User's Guide*.

3. Either execute the `jco_spmd_reload` command or restart JP1/IM - Manager.

The defined information takes effect. For details about the `jco_spmd_reload` command, see *jco_spmd_reload* in *1. Commands* in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.

4.4.3 Setting startup options

To set startup options for the correlation event generation function:

1. Edit the correlation event generation system profile (`egs_system.conf`).

For details about the correlation event generation system profile, see *Correlation event generation system profile (egs_system.conf)* in *2. Definition Files* in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.

2. Either execute the `jco_spm�_reload` command or restart JP1/IM - Manager.

The defined information takes effect.

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

4.4.4 Creating and applying a correlation event generation definition

To create and apply a correlation event generation definition:

1. Create a correlation event generation definition file.

Create a desired correlation event generation definition file. The file name and extension must observe the naming rules described in the table below.

Table 4-4: Naming rules for a correlation event generation definition file

Item	Rule
File name	Permitted characters are alphanumeric characters and the underscore (_) only.
Extension	Extension must be <code>.conf</code> .

For details about the definitions to be specified in 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*.

We recommend that you store the created correlation event generation definition file in the following folder/directory:

Table 4-5: Folder/directory for storing the correlation event generation definition file

OS	Storage location [#]
Windows	<code>Console-path\conf\evgen\define\</code>

OS	Storage location [#]
	<i>shared-folder\jplcons\conf\evgen\define\</i> (logical host)
UNIX	<i>/etc/opt/jplcons/conf/evgen/define/</i>
	<i>shared-directory/jplcons/conf/evgen/define/</i> (logical host)

#

By storing the correlation event generation definition file in the indicated folder/directory, the data collection tool can automatically collect from it in the same manner as with other definition files. During cluster operation, store the correlation event generation definition file on the shared disk to synchronize operations between the executing and standby systems.

- Execute the `jcoegscheck` command to check for errors in the correlation event generation definition.

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*.

- Execute the `jcoegschange` command.

The defined information takes effect.

If JP1/IM - Manager is not running, the definition applied by the `jcoegschange` command will take effect the next time JP1/IM - Manager starts.

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

4.5 Setting memo entries

This section explains how to enable the memory entry setting function. To edit memo entries, you need `JP1_Console_Admin` or `JP1_Console_Operator` permissions. All users can view memo entries.

To set memo entries:

1. Enable the memo entry setting function.

Execute `jcoimdef -memo ON`.

2. Restart JP1/IM - Manager.

If you executed the `jcoimdef` command with the `-i` option specified, there is no need to restart JP1/IM - Manager.

3. Restart JP1/IM - View.

The memo entry settings are applied.

4. In the Preferences window, set the memo entries that are to be displayed.

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 how to edit memo entries, see *5.4 Editing memo entries* in the *Job Management Partner 1/Integrated Management - Manager Administration Guide*.

4.6 Editing event guide information

In the event of a problem during system monitoring, event guide information for JP1 events can be displayed in the Event Details window. You can reduce the system administrator's workload by displaying as event guide information such items as examples of problems that may arise and examples of the actions that can be taken. You can also accumulate information, such as past records of problem handling, as operational know-how.

The information to be displayed as event guides is set in the event guide information file that is located at the JP1/IM - Manager host.

This section explains how to edit event guide information.

For details about the information to be set as event guides, the event guide concept, and the event guide function, see the following:

About editing and setting event guide information:

- About the event guide function
See *3.6 Event guide function* in the *Job Management Partner 1/Integrated Management - Manager Overview and System Design Guide*.
- About the concept of event guides
See *11.1.7 Considerations for setting event guide information* in the *Job Management Partner 1/Integrated Management - Manager Overview and System Design Guide*.
- About the format of the event guide information file
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*.

4.6.1 How to edit event guide information

After you have edited the event guide information file, you can display the new information by refreshing the Event Details window.

To edit event guide information:

1. Copy the sample event guide information file (`sample_jco_guide.txt`) and rename the copy to `jco_guide.txt`.

Store the event guide information file (`jco_guide.txt`) in the same folder/directory as for the sample event guide information file, as shown below.

Table 4-6: Folder/directory for the sample event guide information file

OS	Folder/directory for the sample file
Windows	<i>Console-path</i> \conf\guide\sample_jco_guide.txt
	<i>shared-folder</i> \conf\guide\sample_jco_guide.txt
UNIX	/etc/opt/jplcons/conf/guide/sample_jco_guide.txt
	<i>shared-directory</i> /jplcons/conf/sample_guide/jco_guide.txt

2. Edit the event guide information file (`jco_guide.txt`).

The event guide information file is a TXT-format file. Use a text editor to edit the file. Use the language encoding set for JP1/IM - Manager to describe information in the event guide information file.

If you use an event guide message file, use a program such as a text editor to create the file.

3. Apply the settings for the event guide information.

The event guide information file is loaded when JP1/IM - Manager is reloaded or restarted.

Do one of the following:

- Execute the `jco_spmd_reload` command to reload JP1/IM.
- Terminate JP1/IM - Manager and then restart it (also restart JP1/IM - View).

4. Check that the event guide information has been loaded successfully.

If the event guide information file contains invalid information, an error will occur when JP1/IM - Manager loads the event guide information file. Check the integrated trace log to make sure that the event guide information file loaded successfully.

Table 4-7: Folder/directory for the integrated trace log

OS	Integrated trace log
Windows	<i>system-drive</i> :\Program Files\HITACHI\HNTRLib2\spool\
UNIX	/var/opt/hitachi/HNTRLib2/spool/

- When the event guide information file loaded successfully

The `KAVB1585-I` message is output to the integrated trace log. Check that this message has been output.

- When a loading error has occurred for the event guide information file
The KAVB1586-W or KAVB1587-E message is output to the integrated trace log. In the event of an error, check the message for the cause of the error and then correct the problem. After that, reload or restart JP1/IM - Manager.

4.7 Setting JP1 event issuance during action status change

You use the status event definition file (`processupdate.conf`) to set JP1 event issuance (3F11) when the action status for a JP1 event changes.

To set JP1 event issuance during action status change:

1. Edit the status event definition file (`processupdate.conf`) with a program such as a text editor.
2. Restart JP1/IM - Manager.

The settings take effect once JP1/IM - Manager has restarted.

About the JP1 event issuance settings:

- About the status event definition file (`processupdate.conf`)

See *Status event definition file (processupdate.conf)* in 2. *Definition Files* in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.

4.8 How to display user-specific event attributes

This section describes the procedures for displaying user-specific event attributes (user-specific information for extended attributes).

Before you start using JP1/IM, you can set JP1/Base to issue user-specific events. For details about how to set JP1/Base to issue user-specific events, see the manual *Job Management Partner 1/Base Function Reference*.

You can also use the `jevsend` and `jevsendd` commands in JP1/Base to issue user-specific events. In such cases, you might also need to specify information such as definition files for the extended event attributes. For details about how to set user-specific events to be issued by using the `jevsend` and `jevsendd` commands in JP1/Base, see the *Job Management Partner 1/Base User's Guide*.

To display user-specific event attributes in JP1/IM:

1. Create definition files.

Create the following definition files on the machine where JP1/IM - Manager is installed:

- Definition file for the extended event attributes
Defines the user-specific event attributes that you want to display.
- Definition file for objects types
Defines the display items on the JP1/IM - View window that are used to display user-specific event attributes.

2. Apply the definition files.

The details of each step are provided in the subsections below. The following explains how to create the definition files for displaying the attributes of sample JP1 events.

Sample JP1 events

This example uses the startup and abnormal termination events that are issued when a Windows application named `SAMPLE` starts and terminates.

The following are the details of each event:

Types of JP1 events to be displayed

- JP1 event that is issued when the `SAMPLE` application starts (startup event)
Event ID: `0x00000001`
Message: `The SAMPLE application now starts.`

4. Setting up Central Console

- JP1 event that is issued when the SAMPLE application terminates abnormally (abnormal termination event)

Event ID: 0x00000002

Message: The SAMPLE application terminated abnormally.

Attribute definition for the startup event (extended attributes (extattrs))

The following attributes have been defined for the startup event of the SAMPLE application:

Table 4-8: Attributes of the startup event

Attribute type	Item	Attribute name	Description
Basic attribute	Event ID	--	0x00000001
	Message	--	The SAMPLE application now starts.
Extended attribute (common information)	Event level	SEVERITY	Notice
	User name	USER_NAME	SAMPLE_USER
	Product name	PRODUCT_NAME	/COMPANY/APP1/ SAMPLE_PRODUCT (product name)
	Object type	OBJECT_TYPE	SAMPLE
	Object name	OBJECT_NAME	SAMPLE_NAME
	Root object type	ROOT_OBJECT_TYPE	ROOT_SAMPLE
	Root object name	ROOT_OBJECT_NAME	ROOT_SAMPLE_NAME
	Object ID	OBJECT_ID	SAMPLE_ID
	Occurrence	OCCURRENCE	START
	Start time	START_TIME	SAMPLE application start time. This is the number of seconds from UTC 01/01/1970 00:00:00.
	Platform type	PLATFORM	NT
Version information	ACTION_VERSION	0600	
Extended attribute	SAMPLE common attribute 1	COMMON_ATTR1	NATIVE

Attribute type	Item	Attribute name	Description
(user-specific information)	SAMPLE common attribute 2	COMMON_ATTR2	TRUE
	SAMPLE start attribute 1	START_ATTR1	SAMPLE1
	SAMPLE start attribute 2	START_ATTR2	SAMPLE2

Attribute definition for the abnormal termination event (extended attributes (extattrs))

The following attributes have been defined for the abnormal termination event of the SAMPLE application:

Table 4-9: Attributes of the abnormal termination event

Attribute type	Item	Attribute name	Description
Basic attribute	Event ID	--	0x00000002
	Message	--	The SAMPLE application terminated abnormally.
Extended attribute (common information)	Event level	SEVERITY	Error
	User name	USER_NAME	SAMPLE_USER
	Product name	PRODUCT_NAME	/COMPANY/APP1/ SAMPLE_PRODUCT (product name)
	Object type	OBJECT_TYPE	SAMPLE
	Object name	OBJECT_NAME	SAMPLE_NAME
	Root object type	ROOT_OBJECT_TYPE	ROOT_SAMPLE
	Root object name	ROOT_OBJECT_NAME	ROOT_SAMPLE_NAME
	Object ID	OBJECT_ID	SAMPLE_ID
	Occurrence	OCCURRENCE	END
	End time	END_TIME	SAMPLE application end time. This is the number of seconds from UTC 01/01/1970 00:00:00.

Attribute type	Item	Attribute name	Description
	Termination code	RESULT_CODE	Termination code of the SAMPLE application
	Platform type	PLATFORM	NT
	Version information	ACTION_VERSION	0600
Extended attribute (user-specific information)	SAMPLE common attribute 1	COMMON_ATTR1	NATIVE
	SAMPLE common attribute 2	COMMON_ATTR2	TRUE
	SAMPLE end attribute 1	END_ATTR1	SAMPLE1
	SAMPLE end attribute 2	END_ATTR2	SAMPLE2

4.8.1 Creating the definition files

To display user-specific event attributes, you must create a definition file for the extended event attributes as well as a definition file for objects types. This subsection describes these files.

(1) Definition file for the extended event attributes

In the definition file for the extended event attributes, define only those event attributes that you want to display as details from among all the event attributes set for the user-specific events that are to be displayed. There is no need to define the basic attributes and the common information of the extended attributes because these attributes are set automatically. Define only the user-specific information. The following shows the storage location for the definition file for the extended event attributes.

In Windows:

Console-path\conf\console\attribute\

In the case of cluster operation, the storage location is *shared-folder*\jplcons\conf\console\attribute\.

In UNIX:

/etc/opt/jplcons/conf/console/attribute/

In the case of cluster operation, the storage location is *shared-directory*/jplcons/conf/console/attribute/.

When the definitions take effect:

The definitions take effect when JP1/IM - Manager is restarted.

For details about the definition file for the extended event attributes, see *Definition file for extended event attributes* in 2. *Definition Files* in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.

JP1/IM provides the `jcoattrfcheck` command for checking the definition file for the extended event attributes. For details about this command, see `jcoattrfcheck` in 1. *Commands* in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.

Example of definition:

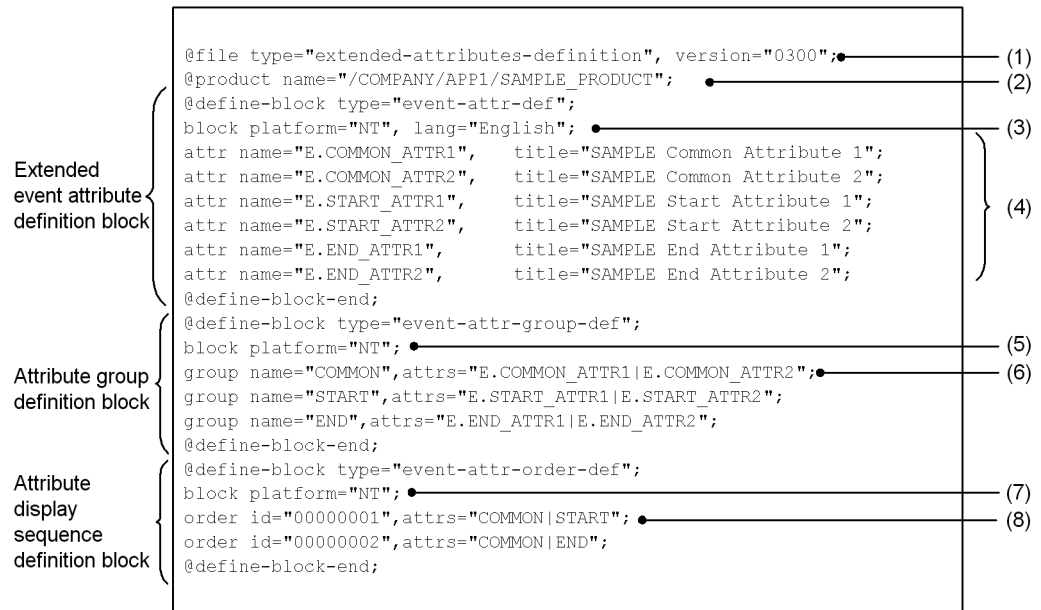
This example defines in the definition file for the extended event attributes the user-specific events that are issued by the `SAMPLE` application. This definition file defines the attributes of all JP1 events that are issued by a single application. This sample defines the JP1 events with event IDs `00000001` and `00000002` that are issued by the `SAMPLE` application. The example uses the following file name:

```
company_sample_attr_en.conf
```

This file name indicates that this is the `SAMPLE` application for a company named `company`.

The following shows an example definition file for the extended event attributes.

Figure 4-1: Example of definition file for the extended event attributes



- (1) Only "0300" can be specified for the version.
- (2) This is the value specified for the `PRODUCT_NAME` extended event attribute.
- (3) The value of `platform=` is the value specified for the `PLATFORM` extended event attribute.
- (4) `title=` defines a name that is displayed in the detailed information.
- (5) The value of `platform=` is the value specified for the `PLATFORM` extended event attribute.
- (6) Defines an attribute group.
- (7) The value of `platform=` is the value specified for the `PLATFORM` extended event attribute.
- (8) The group name specified in (6) is used.

(2) Definition file for objects types

You define in the definition file for objects types the extended attributes of the user-specific events that you want to display, and the items that are to be displayed in **Object type** and **Root object type** in JP1/IM - View windows (such as the Severe Event Definitions window and Event Acquisition Settings window). This definition file is required in order to display detailed information about JP1 events. The following shows the storage location for the definition file for objects types.

In Windows:

Console-path\conf\console\object_type\

In the case of cluster operation, the storage location is
shared-folder\jplcons\conf\console\object_type\.

In UNIX:

```
/etc/opt/jplcons/conf/console/object_type/
```

In the case of cluster operation, the storage location is *shared-directory/jplcons/conf/console/object_type/*.

When the definition takes effect:

The definition takes effect when JP1/IM - View is restarted.

For details about the definition file for objects types, see *Definition file for object types* in 2. *Definition Files* in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.

Example of definition:

This example defines in the definition file for objects types the user-specific events that are issued by the SAMPLE application. Because this example adds new information to ROOT_OBJECT_TYPE and OBJECT_TYPE, the information must be defined in the object definition file.

This example uses the following file name:

```
company_sample_obj.en
```

This file name indicates that this is the SAMPLE application for a company named company.

The following shows an example definition file for objects types:

```
[ObjectType]
# extended-attribute-value, list-display-character-string, comment
ROOT_SAMPLE, ROOT_SAMPLE //Sample's root object name
SAMPLE, SAMPLE //Sample's object name
[End]
```

4.8.2 Enabling the definition files

When the definition files take effect depends on the file. The following table shows when each definition file takes effect.

Table 4-10: When the definition files take effect

Definition file	When it takes effect
Definition file for the extended event attributes	When JP1/IM - Manager is restarted
Definition file for objects types	When JP1/IM - View is restarted

4.9 Setting the severity changing function

This section explains how to set the severity changing function. The severity changing function is related to use of the integrated monitoring database.

To set the severity changing function:

1. Execute the command for setting the severity changing function:

```
jcoimdef -chsev ON
```

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*.

2. Edit the severity changing definition file.

For details about the information to be edited, see *5.3 Changing the severity level of events* in the *Job Management Partner 1/Integrated Management - Manager Administration Guide*.

3. Either execute the `jco_spmc_reload` command or restart JP1/IM - Manager.

The defined information takes effect. For details about the `jco_spmc_reload` command, see *jco_spmc_reload* in *2. Commands* in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.

4.10 Setting JP1/IM - View for each login user

You must set up a JP1/IM - View GUI environment for each JP1 user who logs in to JP1/IM - Manager. You can specify settings such as the viewer memory buffer size for buffering JP1 events and the display items for events.

Customize the settings, if necessary. The following are the items that can be set:

- Whether displayed information is to be refreshed automatically and a *refresh interval* if the information is to be refreshed automatically
If there are JP1 events that cannot be displayed, shorten the refresh interval.
- Number of JP1 events that can be displayed in the Event Console window (scroll buffer)
If there are JP1 events that cannot be displayed, increase this value.
If you want to reduce the amount of memory used, reduce this value.
- Number of events to acquire in the Event Console window at updating
- Number of events to acquire per search
- Items displayed in the events list

You can add and delete the items that are displayed in the events list columns.

The items that you can specify include event level, registered time, source host name, user name, message, object type, event ID, start time, end time, product name, object name, root object type, root object name, arrived time, action, occurrence, serial number, source process ID, source user ID, source group ID, source user name, source group name, source serial number, type, action type, original severity level, new severity level, and memo. If the severity changing function is disabled, the original severity level and the new severity level are not displayed. If the memo entry settings are disabled, no memo is displayed.

- Whether the column widths for the items displayed in the events list in the Event Console window are to be saved
You can change the column width for an item displayed in the events list by dragging the edge of the column with the mouse. If you change a column width on one page (such as the **Monitor Events** page), that column's width also changes on the other two pages (**Severe Events** and **Search Events** pages). You can specify whether column widths are to be saved at the time of logout.
- Whether a background color is to be applied to specific events displayed in the events list in the Event Console window

You can apply background colors to specific types of events that are displayed on

the **Monitor Events** and **Search Events** pages. This setting is applicable to events with the event levels Emergency, Alert, Critical, Error, and Warning.

- Whether consolidated display is to be used for repeated events

You can specify whether to consolidate a large number of identical events that occur in a short period of time for display in the Event Console window.

To use the repeated event consolidated display function, select the **Enable** check box in **Display most significant status**, and then set a timeout value for the events being consolidated.

If you change the **Display most significant status** setting, event consolidation based on the new setting is applied to events that are received after the setting takes effect. If you log in again after changing the setting, event consolidation starts with the new setting.

- Number of rows to be displayed as execution results in the Command window
- Display of events that occurred during a specified period

You use the Preferences window of JP1/IM - View to specify the settings. These settings are specified and saved for each JP1 user who logs in to JP1/IM - Manager.

To set JP1/IM - View for each login user:

1. Start the Preferences window.

In the Event Console window, choose **Options**, and then **User Preferences**.

2. Adjust the parameters.

Adjust each parameter as necessary

For details about the parameters that can be specified, see the following:

About setting up a JP1 user environment:

- About the Preferences window

See *2.16 Preferences window* in the manual *Job Management Partner 1/Integrated Management - Manager GUI Reference*.

Note:

A user profile also contains information about these settings; however, you should not use the user profile to directly change attributes and attribute values that are not listed in *User profile (defaultUser | profile_user-name)* and *Description* in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*. If such changes are made, JP1/IM - View may not function correctly.

4.11 Customizing the JP1/IM - View operation

You can set the operation of JP1/IM - View. You change settings by editing the IM-View settings file (`tuning.conf`). You can set the following items for JP1/IM - View operation:

- Number of connection-target host entries in the Login window
- Whether to start the Tool Launcher window when the Event Console window starts
- Whether to start the List of Action Results window when the Event Console window starts
- Start path of the Web browser that is used when the Tool Launcher window and monitor windows are called
- Whether data can be copied to the clipboard

The settings specified here take effect only on the viewer that was used to edit the IM-View settings file.

To customize the JP1/IM - View operation:

1. Edit the following IM-View settings file with a program such as a text editor:
View-path\conf\tuning.conf
2. Restart JP1/IM - View.

About customizing the JP1/IM - View operation:

- About the IM-View settings file
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*.

4.12 Setting monitor startup for linked products

Monitor startup is a function for starting an application window related to a JP1 event from the JP1 event itself when it is displayed in the Event Console window. If you intend to use monitor startup to link to another product, first check the operating environment of the linked product (such as the supported OSs and browsers).

To set monitor startup:

1. Select the application that is to be handled by monitor startup.
2. Create definition files.

Create the following definition files:

- Definition file for opening monitor windows

For details about this definition file, 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*.

- Definition file for executing applications

For details about this definition file, see *Definition file for executing applications* in 2. *Definition Files* in the manual *Job Management Partner 1/ Integrated Management - Manager Command and Definition File Reference*.

3. Apply the edited contents of the definition files.

- Restart JP1/IM - Manager.
- Restart JP1/IM - View.

For details about this procedure, see 4.12.3 *Creating the definition files*. The following subsections describe the prerequisites for the settings and provide examples.

Note:

Some linked products provide their own definition files. For details about whether a product supports monitor startup and details about the setup procedures, see the documentation for each product.

If you use the definition files provided by a linked product, make sure that you use the character encoding supported by the target JP1/IM - Manager.

4.12.1 How to open monitor windows

To open monitor windows:

1. Determine the window to be used for opening monitor windows.
2. Create definition files.

Create the following definition files:

- Definition file for opening monitor windows
Specify in this definition file the correspondences between JP1 events and the windows to be opened. Create this definition file on the machine where JP1/IM - Manager is installed.
- Definition file for executing applications
Specify in this definition file the information needed by JP1/IM - View to resolve the application paths defined in the definition file for opening monitor windows. Create this definition file on the machine where JP1/IM - View is installed.

3. Apply the definition files.

The following subsections provide details of each step.

4.12.2 Determining the window to be used for opening monitor windows

To open monitor windows, you must first determine the correspondence between JP1 events and the windows to be opened, as well as the arguments to be specified when a window is opened. The purpose of opening a monitor window is to open the details window of a job or application that issued a JP1 event and to directly manipulate the job or application from that details window. Choose a window that serves the appropriate purpose.

You must also consider the attributes of the JP1 events because all the information required for opening the windows is inherited from the attribute values of the JP1 events.

Login authorization for an application that is started by opening a monitor window cannot be standardized. Therefore, if necessary, you must employ a method such as omitting the login process (by using the options of a window opening command) for each application.

The following subsections describe starting application programs and Web pages on JP1/IM - View using the example of event attributes described in *3.8 Displaying user-defined event attributes* in the *Job Management Partner 1/Integrated Management - Manager Overview and System Design Guide*.

4.12.3 Creating the definition files

This subsection describes the information to be defined in the definition file for

opening monitor windows and the definition file for executing applications, explains their storage locations, and provides an example definition.

(1) Creating a definition file for opening monitor windows

In the definition file for opening monitor windows, define information such as the ID and attributes of a JP1 event that is to open a monitor window.

The attributes of JP1 events must match the information in the definition file for the extended event attributes.

For details about the definition file for the extended event attributes, see *Definition file for extended event attributes* in 2. *Definition Files* in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.

Also specify in this definition file the window to be opened and the arguments to be used when the window is opened. To define the window to be opened, specify the application execution definition identifier. The application execution definition identifier is used by JP1/IM - View to identify a window defined in the definition file for opening monitor windows. Therefore, in the definition file for executing applications, you must specify the application execution definition identifier that is specified in the definition file for opening monitor windows. For the specified application execution definition identifier, the path is resolved by the definition file for executing applications. When the executable file is started, the arguments specified in the definition file for opening monitor windows are passed. For details about the 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*.

JP1/IM provides the `jcomonitorfcheck` command for checking the definition file for opening monitor windows. For details about this command, see *jcomonitorfcheck* in 1. *Commands* in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.

(2) Creating a definition file for executing applications

In the definition file for executing applications, define the relationship between an application execution definition identifier defined in the definition file for opening monitor windows and a path.

For details about the definition file for executing applications, see *Definition file for executing applications* in 2. *Definition Files* in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.

JP1/IM provides the `jcoappexecfcheck` command for checking the definition file for executing applications. For details about this command, see *jcoappexecfcheck* in 1. *Commands* in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.

4.13 Setting the Tool Launcher window

You use the Tool Launcher window to specify settings for opening the GUI (application windows) and Web pages of linked products.

4.13.1 Settings for opening the GUI of linked products from the Tool Launcher window

Some of the products linked to JP1/IM - Manager are displayed in the Tool Launcher window by default. You can install these linked products on the same host as for JP1/IM - View, which enables you to open the GUI of the linked products from the Tool Launcher window. 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*.

The procedure below explains how to register a product that is not displayed in the Tool Launcher window.

To open the GUI (application window) of a linked product from the Tool Launcher window:

1. Determine the application that is to be opened from the Tool Launcher window.
2. Create definition files.

Create the following definition files at the host where JP1/IM - View is installed:

- Definition file for the Tool Launcher window
- Definition file for executing applications

Create the definition file for the Tool Launcher window and the definition file for executing applications in the following folder:

View-path\conf\function\en\

3. Restart JP1/IM - View.

For details about the procedure, see *4.13.4 Creating the definition files*. It describes the prerequisites for the settings and provides examples.

Note:

Some linked products may require a different procedures from that shown above. For details about the setup method, also see the documentation for the particular product.

4.13.2 How to add new menus

To add new menus to the Tool Launcher window:

1. Determine a window that is to be opened from the Tool Launcher window.
2. Create definition files.

On the machine where JP1/IM - View is installed, create the following definition files:

- Definition file for the Tool Launcher window

Define in this definition file such information as the new menu to be added and the windows to be opened from the new menu.

- Definition file for executing applications

Define in this definition file the information needed by JP1/IM - View to resolve the application paths defined in the definition file for the Tool Launcher window.

3. Apply the definition files.

The following subsections provide details of each step.

4.13.3 Determining a window to be opened from the Tool Launcher window

Opening windows from the Tool Launcher window enables you to manage systems and applications. Choose the windows that are appropriate to your purposes.

Because login authorization cannot be standardized, if necessary, you must employ a method such as omitting the login process (by using the options of a window opening command) for each application.

To determine a window to be opened from the Tool Launcher window:

1. Determine the name to be displayed in the Tool Launcher window and the ID to be used.

The ID is a menu ID. Specify it in the format *company-name_product-name*. The ID must be unique throughout the entire menu.

2. Determine the folder to be displayed in the Tool Launcher window.

If an appropriate folder is not available, determine the folder name and ID to be used. Specify the ID in the format *company-name_product-name*. The ID must be unique throughout the entire menu.

3. Prepare the icon that is to be displayed in the Tool Launcher window.

Create an icon as a GIF file with a size of 16 x 16 pixels. If you do not specify an icon, the default icon is used.

4.13.4 Creating the definition files

This subsection describes the information to be defined in the definition file for the Tool Launcher window and the definition file for executing applications, explains their storage locations, and provides example definitions.

(1) **Creating a definition file for the Tool Launcher window**

In the definition file for the Tool Launcher window, define such information as the window to be opened from the menu entry, the higher node in the menu tree, and the name to be displayed as the menu entry.

(a) **Information to be defined**

To define the window to be opened from the menu entry, specify the application execution definition identifier. The application execution definition identifier is used by JP1/IM - View to identify the window defined in the definition file for the Tool Launcher window. Therefore, in the definition file for executing applications, you must specify the application execution definition identifier that is specified in the definition file for the Tool Launcher window. For the specified application execution definition identifier, the path is resolved by the definition file for executing applications, so that the window can be opened from the menu entry. For details about the definition file for the Tool Launcher window, see *Definition file for the Tool Launcher window* in 2. *Definition Files* in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*. For details about the definition file for executing applications, see *Definition file for executing applications* in 2. *Definition Files* in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.

JP1/IM provides the `jcofuncfcheck` command for checking the definition file for the Tool Launcher window. For details about this command, see `jcofuncfcheck` in 1. *Commands* in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.

(b) **Storage location**

Store this file in the viewer's directory shown below. The definition takes effect when JP1/IM - View is restarted.

`View-path\conf\function\en\`

(c) **Example of definition**

This subsection presents the following example:

Application

4. Setting up Central Console

COMPANY's product called SAMPLE

Folder name and ID

```
SAMPLE_management, ID = "company_sample_management"
```

Menu name and ID

```
SAMPLE_management_window (application), ID =  
"company_sample_naitive"
```

```
SAMPLE_management_window (WWW), ID = "company_sample_web"
```

Icon file

```
sample_icon.gif
```

Executable file

```
sample.exe
```

URL

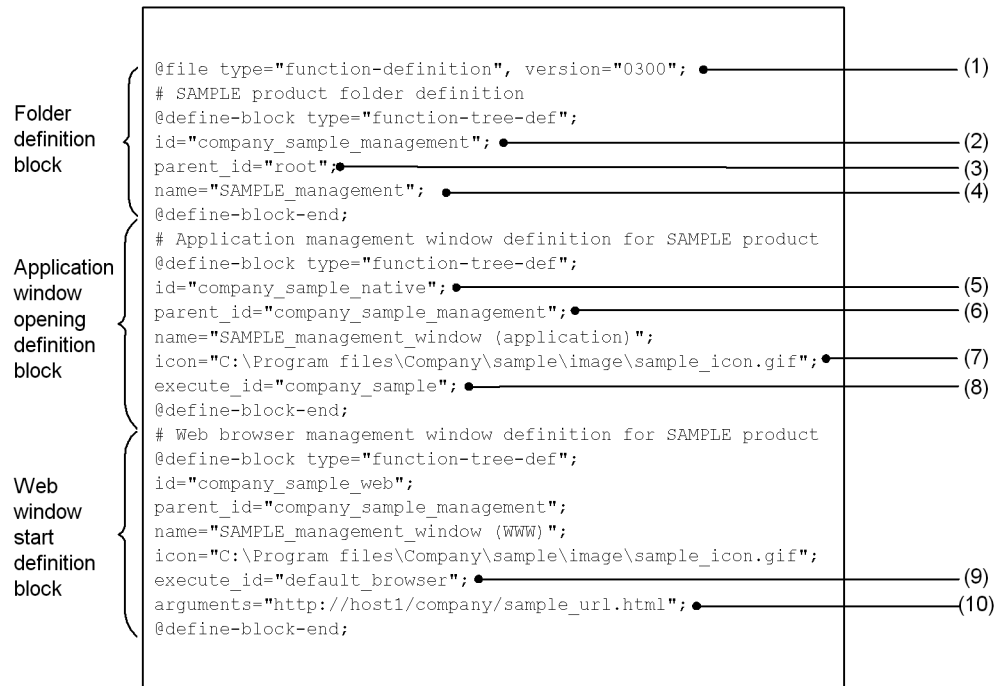
```
http://host1/company/sample_url.html
```

This example uses the following file name:

```
company_sample_tree.conf
```

The following shows the example definition in the definition file for the Tool Launcher window.

Figure 4-2: Example definition in the definition file for the Tool Launcher window



- (1) Only "0300" can be specified for the version.
- (2) Specifies the folder ID.
- (3) Specifies the parent folder. `root` is the highest folder.
- (4) Specifies the folder name.
- (5) Specifies the menu ID.
- (6) Specifies the parent folder.
- (7) Specifies the icon file.
- (8) Specifies the application execution definition identifier.
- (9) Specifies that the default Web browser is to be used.
- (10) Specifies the URL of the Web page that is to be opened.

Based on this definition, the menu entries `SAMPLE_management_window (application)` and `SAMPLE_management_window (WWW)` are displayed in the order defined under the folder named `SAMPLE_management` on the tree in the Tool Launcher window.

(2) Creating the definition file for executing applications

The definition file for executing applications defines an association between an application execution definition identifier specified in the definition file for the Tool Launcher window and the path.

(a) Information to be defined

For details about the definition file for executing applications, see *Definition file for executing applications* in 2. *Definition Files* in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.

JP1/IM provides the `jcoappexecfcheck` command for checking the definition file for executing applications. For details about this command, see *jcoappexecfcheck* in 1. *Commands* in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.

(b) Storage location

Store this file in the viewer's directory shown below. The definition takes effect when JP1/IM - View is restarted.

`View-path\conf\appexecute\en\`

(c) Example of definition

This subsection uses the same example as for opening monitor windows. This example uses the following file name:

`company_sample_app.conf`

The following shows an example definition in the definition file for executing applications.

Figure 4-3: Example of definition in the definition file for executing applications

```
@file type="application-execution-definition", version="0300"; (1)
# Definition of sample.exe for opening the application program window
@define-block type="application-execution-def";
id="company_sample";
path="[\\HKEY_LOCAL_MACHINE\SOFTWARE\COMPANY\SAMPLE\PathName\Path00]\bin\sample.exe"; (2)
@define-block-end;
# Using a Web browser other than the default for displaying Web pages
@define-block type="application-execution-def";
id="company_sample_web";
path="C:\Program files\Netscape\bin\netscape.exe"; (3)
@define-block-end;
```

- (1) Only "0300" can be specified for the version.
 (2) The portion in square brackets is resolved from the registry key.
 (3) If there is no path in the registry information, the full path is specified.

4.13.5 Settings for opening the Web page of a linked product from the Tool Launcher window

To display the Web page of a linked product from the Tool Launcher window of JP1/IM - View, you must set the URL of the Web page to be displayed by editing the Web

page call definition file (*hitachi_jp1_product-name.html*).

To do this:

1. Edit the Web page call definition file (*hitachi_jp1_product-name.html*).

The storage folder for the Web page call definition file is as follows:

View-path\conf\webdata\en

Open the Web page call definition file using a program such as a text editor. Search the file for the <META> tag and specify the URL of the Web page to be opened in the URLs of the CONTENT attribute.

2. Save the edited Web page call definition file.
3. Restart JP1/IM - View.

By creating a definition file for the Tool Launcher window, you can open the Web page of a product for which a Web page call definition file is not provided.

About the URL setting for the Web page:

- About the Web page call definition file

See *Web page call definition file (hitachi_jp1_product-name.html)* in 2. *Definition Files* in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.

If an attempt is made to display a Web page without setting the URL as explained above, the system displays a window that explains how to specify the settings. Set the URL according to the information provided in the window. This window depends on the product name (window name) for which the Web page opening was attempted.

4.14 Settings for using a Web-based JP1/IM - View

This section explains how to specify the settings for using a Web-based JP1/IM - View to monitor system operation. The following is an outline of the procedure:

1. Install an HTTP server.
2. Set up the HTTP server.
3. Change the port number.
4. Set up a Web browser.
5. Specify display settings for the Java Console window.
6. Set timeout values.

4.14.1 Installing an HTTP server

To use a Web-based JP1/IM - View, you must install an HTTP server on the host where JP1/IM - Manager is installed.

4.14.2 Setting up the HTTP server

This setup is for the host where JP1/IM - Manager is installed. Add the alias shown below to the HTTP server.

Table 4-11: Alias to be added to the HTTP server

Alias name	Reference path
/JP1IM	<i>Console-path</i> \www\

(1) Changing the port number

A Web-based JP1/IM - View uses not only the HTTP server port but also the event console port (`jp1imevtcon`).

If you have changed the port number of the event console from its default (20115), make the same change to the parameter value in the HTML file shown in the table below.

Table 4-12: Parameter in the HTML file

HTML file	Parameter
<i>Console-path</i> \www\console.html	<code><param name="PORT" value="value"></code>

4.14.3 Setting up a Web browser

This setting is required for the Web browser of the viewer that displays Web-based JP1/

IM - View.

For the Web browser, you need JRE and the plug-ins that are included in JRE. For details, see the Release Notes of JP1/IM - Manager for the applicable product.

4.14.4 Specifying display settings for the Java Console window

These settings are required for the viewer that displays the Web-based JP1/IM - View.

To specify the display settings for the Java Console window:

1. From **Control Panel**, select **Java**. The Java Control Panel window opens.
2. Choose the **Advanced** tab.
3. From **Settings**, choose **Java console**, and then select the **Show console** check box. Next, from **Settings**, choose **Miscellaneous**, and then select the **Place Java icon in system tray** check box.

When these settings are specified, the Java Console window will be displayed when the Web-based JP1/IM - View is displayed.

4.14.5 Setting timeout values for Web-based operation

To set the timeout values for Web-based operation:

1. Use a program such as a text editor to open the definition file stored at the following location:

Console-path\www\console.html

2. Set the socket timeout value.

Set the wait time for arrival of received data.

For a low-speed line or in an environment with heavy event traffic, set a larger value.

The default is 2,500 milliseconds.

Search for the following line and set the timeout value (milliseconds):

```
<param name="SO_TIMEOUT" value="2500">
```

Specify the value (milliseconds) as a decimal number.

3. Set server processing timeout values.

Set the timeout values for login, logout, automatic refreshing, event status change, event search, user environment setup, severe event setting, automated action setting, filter setting, and command execution operation.

The specified value must be in the range of 60,000 to 3,600,000 milliseconds. The default is 60,000 milliseconds.

If KAVB1205 is displayed frequently, set a longer timeout value.

4. Setting up Central Console

Search for the following line and set the timeout value (milliseconds):

```
<param name="RMI_TIMEOUT" value="60000">
```

Specify the value (milliseconds) as a decimal number.

Chapter

5. Setting up Central Scope

Central Scope enables the system administrator to use the Monitoring Tree window and the Visual Monitoring window to monitor the system for appropriate purposes.

This chapter explains how to set up an environment that supports these monitoring windows.

- 5.1 Overview of the Central Scope environment setup
- 5.2 Registering host information
- 5.3 Using the GUI to create a monitoring tree
- 5.4 Using the GUI to create a Visual Monitoring window
- 5.5 Using saved CSV files to create monitoring windows
- 5.6 Editing guide information
- 5.7 Setting up a Central Scope operating environment
- 5.8 Setting up for linked products
- 5.9 Examples of monitoring object creation

5.1 Overview of the Central Scope environment setup

Central Scope environment setup involves creating Central Scope's monitoring windows so that the administrator can monitor the system in accordance with the configuration of the running system and as appropriate to the purposes for which the system is to be monitored.

You first set the actual system configuration in the Monitoring Tree window in a tree format that is appropriate for the monitoring purposes. Then, in map format in **Visual Monitoring**, you set the items that require intensive monitoring.

The information provided in this chapter assumes that Central Scope has already been set up and is running.

(1) Before starting Central Scope environment setup

Before you start Central Scope environment setup, you should ensure that you are familiar with JP1/IM and with Central Scope.

Becoming familiar with JP1/IM as a whole and with Central Scope

- Overview of how to use Central Scope

See 1. *Overview of JP1/Integrated Management* in the *Job Management Partner 1/Integrated Management - Manager Overview and System Design Guide*.

See 2. *Overview of Functions* in the *Job Management Partner 1/Integrated Management - Manager Overview and System Design Guide*.

- About the functions of Central Scope

See 4. *Objective-Oriented System Monitoring Using the Central Scope* in the *Job Management Partner 1/Integrated Management - Manager Overview and System Design Guide*.

Configuring a JP1/IM operating environment

- Installing and setting up JP1/IM

See 1. *Installation and Setup (for Windows)*.

See 2. *Installation and Setup (for UNIX)*.

5.2 Registering host information

To register host information for Central Scope in the host information database:

1. Create and edit a host information file (`jcs_hosts`).
2. Execute the `jcshostsimport` command.
3. Apply the contents of the host information file.

You can use the following methods to apply the contents of the host information file:

- Restart JP1/IM - Manager
- Execute the `jco_spm�_reload` command

For details about setting host information, see the following:

About setting host information:

- About host information

See (2) *Host information* in 4.10 *Central Scope* in the *Job Management Partner 1/Integrated Management - Manager Overview and System Design Guide*.

- About the format of 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*.

- About the `jcshostsimport` command

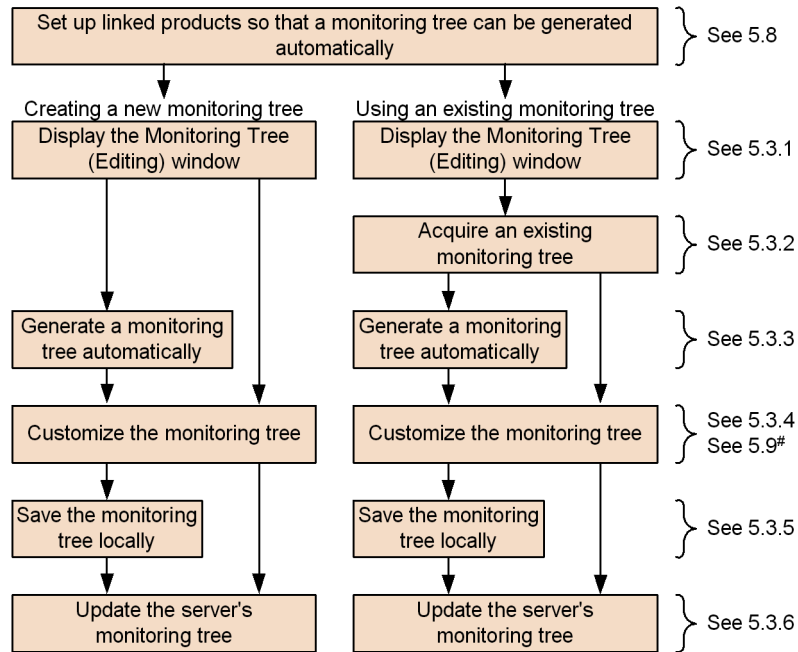
See *jcshostsimport* in 1. *Commands* in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.

5.3 Using the GUI to create a monitoring tree

This section explains how to use the GUI to create a monitoring tree that will be used for monitoring objects.

The following figure shows the procedure.

Figure 5-1: Procedure for using the GUI to create a monitoring tree

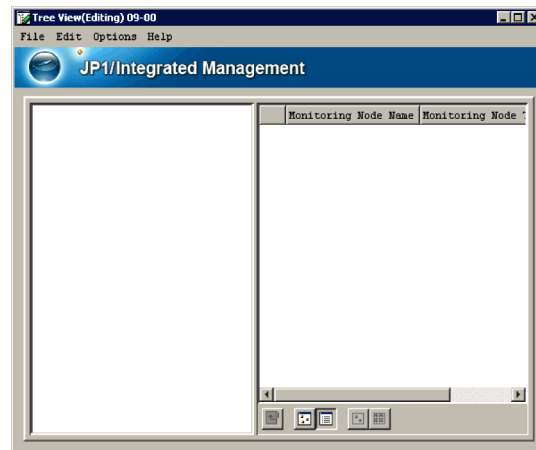


#: This section provides an example of monitoring object creation.

5.3.1 Opening the Monitoring Tree (Editing) window

You can edit the monitoring tree from the Monitoring Tree (Editing) window.

Figure 5-2: Monitoring Tree (Editing) window



To edit the monitoring tree:

1. Open the Monitoring Tree (Editing) window.

Use one of the following methods:

- From the **Start** menu, choose **Programs, JP1_Integrated Management - View**, then **Edit Monitoring Tree**.
- Execute the `jcoview` command.

```
jcoview -e
```
- In the Monitoring Tree window during system monitoring, from the menu bar, choose **Options**, and then **Edit Tree**.

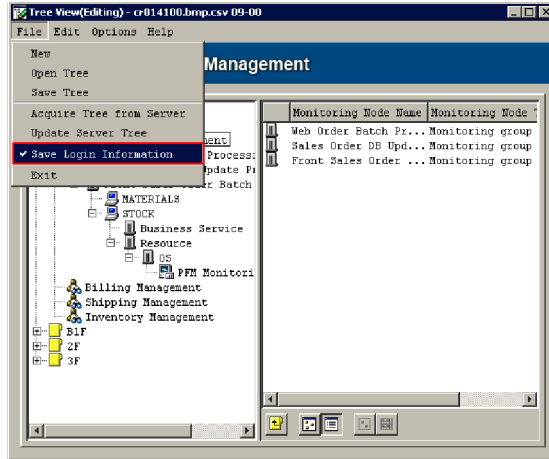
When the Monitoring Tree (Editing) window opens, nothing is displayed initially (there is no monitoring tree information).

Saving the login information

You can set the **Save Login Information** function in the Monitoring Tree (Editing) window. When this function is set, it stores the user name, password, and host to connect at the time of the first login processing when an operation requiring login is performed from the Monitoring Tree (Editing) window. The login operation is not required subsequently.

- From the Monitoring Tree (Editing) window, choose **File**, and then **Save Login Information**.

Figure 5-3: Save Login Information menu



The following table lists and describes the operations that require login.

Table 5-1: List of operations that require login

Window name	Operation	Description
Monitoring Tree (Edit View)	Acquire Tree from Server is chosen from File	Acquires the existing monitoring tree settings from the manager.
	Update Server Tree is chosen from File	Applies the edited contents of the monitoring tree to the manager.
	Auto-generate Tree is chosen from Options	Generates a monitoring tree automatically.
	Acquire Latest Definition is chosen from Options	Acquires the most recent common condition definition from the manager.
	Edit Visual Monitoring Window List is chosen from Edit	Displays the Edit Visual Monitoring Window List window.
Visual Monitoring (Editing)	The Acquire Visual Monitoring Data from Server button is clicked	Loads visual monitoring data from the manager.
	The Update the Visual Monitoring Data of Server button is clicked	Applies the edited visual monitoring data to the manager.

The **Save Login Information** settings are saved when the Monitoring Tree (Editing) window closes. The settings take effect the next time the Monitoring Tree (Editing) window is opened.

5.3.2 Acquiring an existing monitoring tree

If you have already created and been using a monitoring tree, first connect to the manager and then acquire the existing settings.

You can acquire a monitoring tree from the Monitoring Tree (Editing) window or from a CSV file on the local host. In the Monitoring Tree (Editing) window, the title bar displays the version of the JP1/IM - Manager (JP1/IM - Central Scope) being used at the server or the version of the acquired file.

Note:

If you have acquired the monitoring tree from a CSV file at the local host, make sure that the file version displayed on the title bar in the Monitoring Tree (Editing) window matches the version of JP1/IM - Manager (JP1/IM - Central Scope) at the manager. If they do not match, the information edited in the Monitoring Tree (Editing) window cannot be applied to the manager.

(1) Acquiring a monitoring tree from the server

To acquire a monitoring tree from the server:

1. Choose **Acquire Tree from Server**.

From the Monitoring Tree (Editing) window, choose **File**, and then **Acquire Tree from Server**.

2. Log in to the server.

The Login window for logging in to JP1/IM - Manager (JP1/IM - Central Scope) is displayed.

Enter the JP1 user name and password. The JP1 user must belong to the JP1_Console JP1 resource group and have JP1_Console_Admin permissions. For the host to connect, enter the host name of JP1/IM - Manager from which the monitoring tree is to be acquired.

When the login processing is successful, the monitoring tree data is acquired and displayed in the Monitoring Tree (Editing) window.

If monitoring tree settings (a CSV file) are available at the local host, you can also use those settings.

(2) Acquiring a monitoring tree stored locally (CSV file)

To acquire a monitoring tree stored locally as a CSV file:

1. Choose **Open Tree**.

From the Monitoring Tree (Editing) window, choose **File**, and then **Open Tree**.

The Open Tree window appears.

2. Specify a monitoring tree (CSV file).

Select the monitoring tree (the CSV file) to be used and then click the **Open** button.

When a confirmation dialog box appears, click the **Yes** button.

5.3.3 Generating a monitoring tree automatically

You can generate a monitoring tree automatically.

To link other products and generate a monitoring tree automatically, you must have set up the linked products beforehand (such as making the settings for issuing JP1 events and executing adapter commands). See *5.8 Setting up for linked products* and complete the setup before you perform automatic monitoring tree generation.

If you have deleted the `jp1admin` user for some operational reason, a JP1 user who has the appropriate permissions for accessing the definition information of linked products must log in and perform the automatic generation operation.

For details about the monitoring tree automatic generation function, see the following:

About monitoring tree automatic generation:

- About the monitoring tree automatic generation function

See *4.2 Monitoring tree* in the *Job Management Partner 1/Integrated Management - Manager Overview and System Design Guide*.

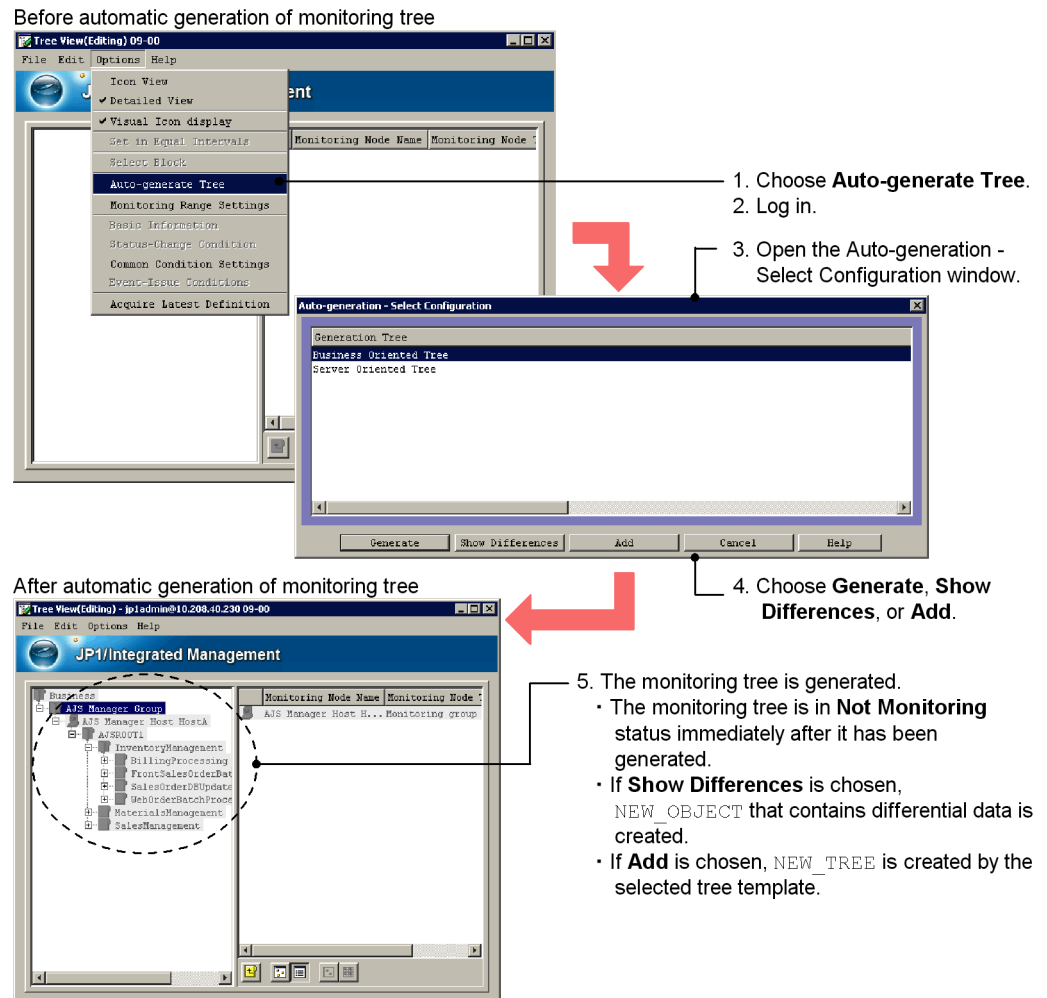
See *4.3 Automatically generating a monitoring tree* in the *Job Management Partner 1/Integrated Management - Manager Overview and System Design Guide*.

- About the monitoring tree model that is generated automatically

See *5. Monitoring Tree Models (for Central Scope)* in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.

The following figure shows the procedure for generating a monitoring tree automatically.

Figure 5-4: Procedure for generating a monitoring tree automatically



To generate a monitoring tree automatically:

1. Choose **Auto-generate Tree**.

From the Monitoring Tree (Editing) window, choose **Options**, and then **Auto-generate Tree**.

If a monitoring tree was already being edited, a confirmation message such as Do you want to replace the current tree configuration information? is displayed. If you choose **Yes**, the current information will be replaced with the automatically generated information.

2. Log in to the server.

The Login window for logging in to JP1/IM - Manager (JP1/IM - Central Scope) is displayed.

Log in as the `jpladmin` user.

For the host to connect, enter the host name of JP1/IM - Manager.

3. In the Auto-generation - Select Configuration window, select a monitoring tree model.

Select the appropriate model for the monitoring tree that is to be generated automatically:

- Work-oriented tree
- Server-oriented tree

4. Click the **Generate**, **Show Differences**, or **Add** button.

- **Generate**: Generates a new monitoring tree from the collected definition information.
- **Show Differences**: Creates differential data from the monitoring tree in the editing window using the collected definition information. The differential data is used to create a monitoring group named `NEW_OBJECT`.
- **Add**: Adds information to the existing monitoring tree in the editing window to create a new monitoring tree. The new monitoring tree is created under a monitoring group named `NEW_TREE`.

5. The monitoring tree is generated automatically.

Definition information is collected from each host managed by JP1/IM and the monitoring tree is generated automatically. Wait for this process to be completed.

Initially, the generated monitoring node is in non-monitoring status.

You can customize the automatically generated monitoring tree before you start using it.

5.3.4 Customizing a monitoring tree

You use the Monitoring Tree (Editing) window to customize an existing monitoring tree as well as to generate a new monitoring tree. The following monitoring tree operations are provided:

- Add monitoring nodes
- Set the attributes of monitoring nodes
- Delete monitoring nodes

- Move monitoring nodes
- Set a monitoring range
- Specify map display settings

This subsection describes these operations and explains how to search for an existing monitoring node.

To customize a monitoring tree, you must know about the functions of and the settings for a monitoring tree. For details, see the following:

About the monitoring tree functions and settings:

- About the functions of monitoring trees

See *4.2 Monitoring tree* in the *Job Management Partner 1/Integrated Management - Manager Overview and System Design Guide*.

See *4.3 Automatically generating a monitoring tree* in the *Job Management Partner 1/Integrated Management - Manager Overview and System Design Guide*.

See *4.4 Editing a monitoring tree* in the *Job Management Partner 1/Integrated Management - Manager Overview and System Design Guide*.

See *4.10 Central Scope* in the *Job Management Partner 1/Integrated Management - Manager Overview and System Design Guide*.

- About the settings for a monitoring tree

See *4.2 Monitoring tree* in the *Job Management Partner 1/Integrated Management - Manager Overview and System Design Guide*.

- About the system-monitoring objects for which basic settings have been defined

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*.

If you set **Common condition** in the monitoring node attribute settings and use common conditions that have already been set, you must apply the operation described below to acquire those common conditions.

If you use a monitoring tree configuration file (CSV file), you can use the common conditions maintained by that configuration file. You can also use the common conditions maintained by JP1/IM - View when you generate a new monitoring tree.

To acquire common conditions:

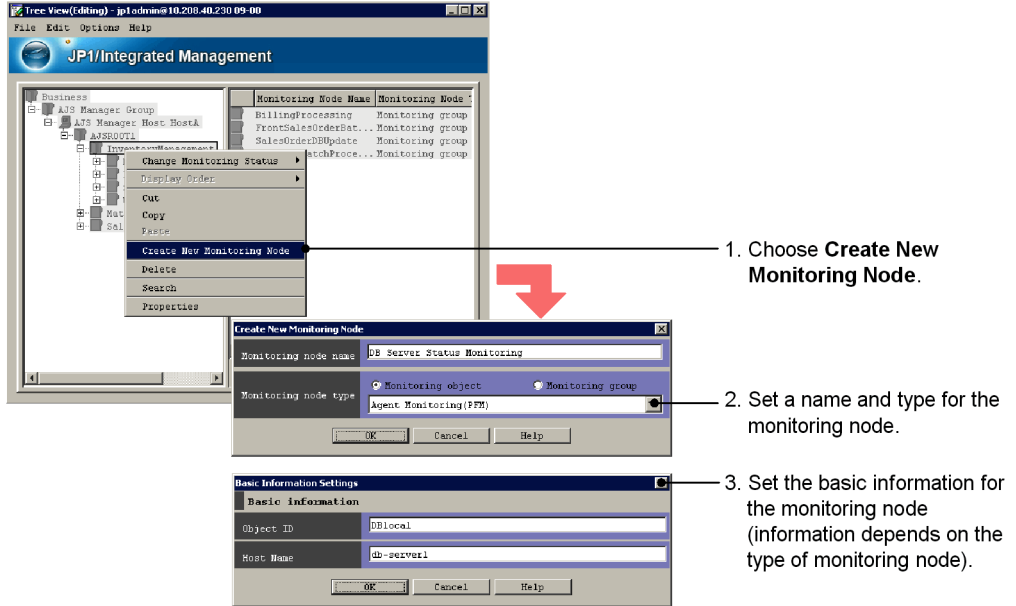
1. In the Monitoring Tree (Editing) window, from the menu bar, choose **Options**, and then **Acquire Latest Definition**.

(1) Adding monitoring nodes

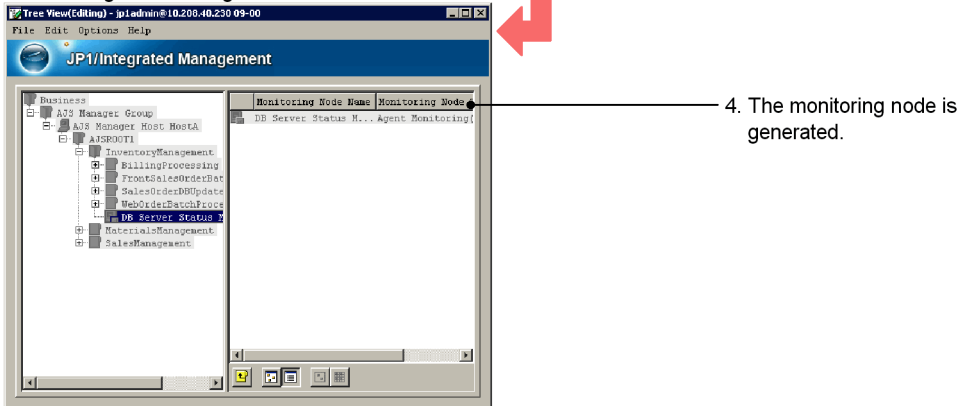
The following figure shows the procedure for adding a monitoring node.

Figure 5-5: Procedure for adding a monitoring node

Before adding a monitoring node



After adding a monitoring node



1. Open the Create New Monitoring Node window.
Use one of the following methods to open the window:
 - Select a monitoring group and then from the right-click pop-up menu, choose

Create New Monitoring Node.

- Select a monitoring group and then from the menu bar, choose **Edit**, then **Create New Monitoring Node**.
- To open the window from the details area, right-click an unselected monitoring node, and then from the pop-up menu, choose **Create New Monitoring Node**.

If there are no monitoring nodes, choose the operation from the menu bar or from the pop-up menu that is displayed by right-clicking the monitoring tree area.

2. Set a name and type for the monitoring node.

In the Create New Monitoring Node window, set the following items:

- Monitoring node name
Specify any desired name.
- Monitoring node type
Select the type of monitoring node.

Select **Monitoring group** or **Monitoring object** and the applicable appropriate type.

For a monitoring object, you can select the type from the system-monitoring objects. The system-monitoring objects are standard monitoring objects provided by the JP1/IM system. Basic settings have already been set for each JP1-series product that is linked with JP1/IM.

If you select **User Monitoring Object** as the type of monitoring object, a general monitoring object is created. Set its attributes using the Properties window for the monitoring node as described below.

If you have selected **Monitoring group** or **Monitoring object** and **User Monitoring Object**, a monitoring node is created without having to specify the following basic information.

3. Set the basic information for the monitoring node.

In the Basic Information Settings window, set the basic information appropriate to the monitoring node type.

The basic information specifies information needed to identify the monitoring object's monitored target. The values to be specified depend on the type of system-monitoring object that was specified as the monitoring node type. For details, see the following:

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. The monitoring node is created.

The monitoring node is created based on the specified settings.

You can also create a monitoring node by copying and pasting an existing monitoring object.

Copying and pasting an existing monitoring object:

To copy and paste an existing monitoring object:

1. Select a monitoring node and then copy it.
 - From the right-click pop-up menu, choose **Copy**.
 - Alternatively, from the menu bar, choose **Edit**, and then **Copy**.
2. Select the target monitoring group.
3. Paste the monitoring node.
 - From the right-click pop-up menu, choose **Paste**.
 - Alternatively, from the menu bar, choose **Edit**, and then **Paste**.

(2) Setting the attributes of monitoring nodes

This subsection explains how to set the attributes of monitoring nodes.

To set the attributes of monitoring nodes, you must be familiar with each setting. This subsection describes the setting procedure and provides a simple example. For details about the settings, check the references provided at the beginning of this section.

To set the attributes of a monitoring node:

1. Open the Properties window for the monitoring node.

Select a monitoring node and then use one of the following methods to open the Properties window:

- Double-click (applicable only to monitoring objects).
- From the right-click pop-up menu, choose **Properties**.
- From the menu bar, choose **Edit**, and then **Properties**.
- From the menu bar, choose **Options**, **Basic Information**, and then **Status-Change Condition** or **Event-Issue Conditions**.

2. Specify the settings on the **General** page.

Specify the monitoring node name, icon to be used, visual icon to be used,^{#1} background image settings (monitoring groups only), monitoring status, and JP1 resource group.^{#2}

3. Specify the settings on the **Basic Information** page.
Specify basic information for the monitoring node.
4. Specify the settings on the **Status-Change Condition** page.
 - When a monitoring object is selected
Specify the JP1 events that are to change the status of the monitoring node when those events are received by JP1/IM - Manager.

For details about the settings for a monitoring object's status change conditions, 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*.
 - When a monitoring group is selected
Specify the status of a lower monitoring node in the monitoring group that is to change the status of the monitoring group.
5. Specify the settings on the **Event-Issue Conditions** page.
Specify the status of the monitoring node that is to trigger issuance of a JP1 event.

If an automated action is to be executed based on the status of the monitoring node, specify the settings in **Event-Issue Conditions**, and then set an automated action for the JP1 event whose event ID is 00003FB0.
6. Click the **OK** or **Apply** button.
#1: Certain advance preparations are required in order to use visual icons, such as creating folders and storing files. For details, see 5.3.4(7) *Settings for using visual icons*.
#2: You can set this item if the monitoring range setting is enabled for the monitoring tree. For details about the monitoring range setting for a monitoring tree, see 5.3.4(6) *Setting the monitoring range*.
The following provides an example of property settings.

5. Setting up Central Scope

Figure 5-6: Example of using the General page to set a monitoring node's monitoring status to Monitoring

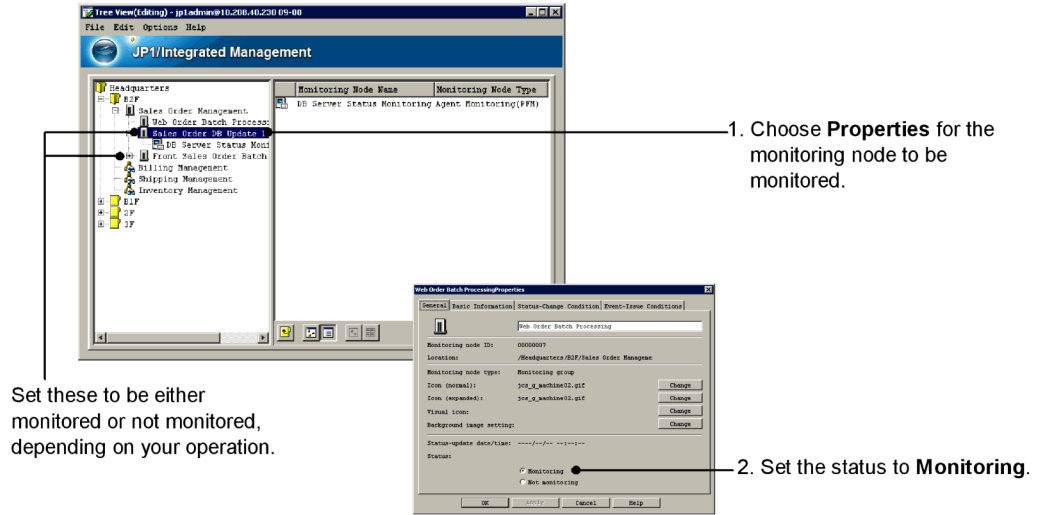


Figure 5-7: Example of settings on the Basic Information page

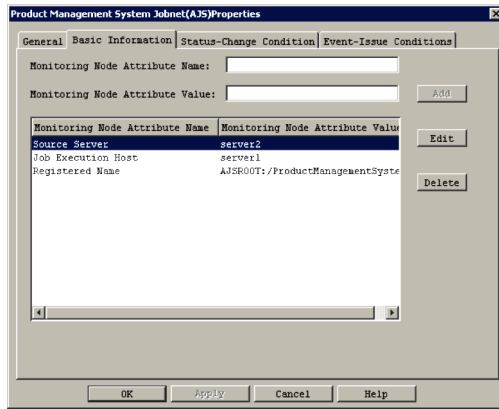


Figure 5-8: Example of using the Status-Change Condition page to set the status change condition for a monitoring node

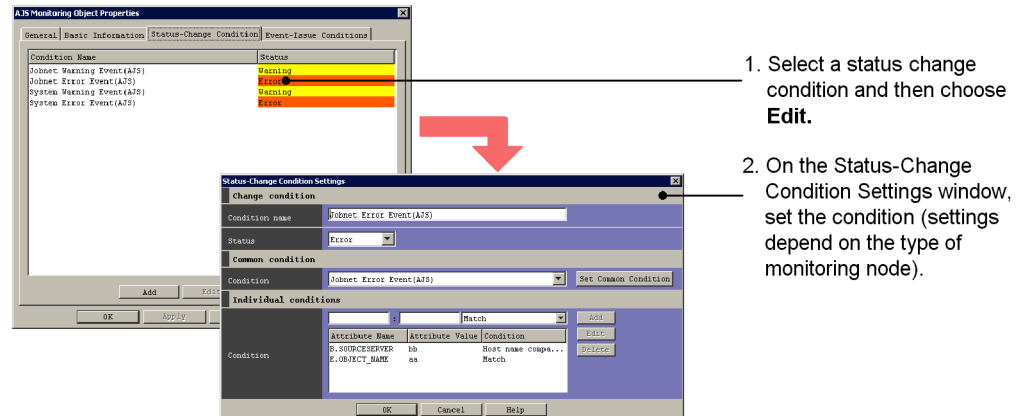
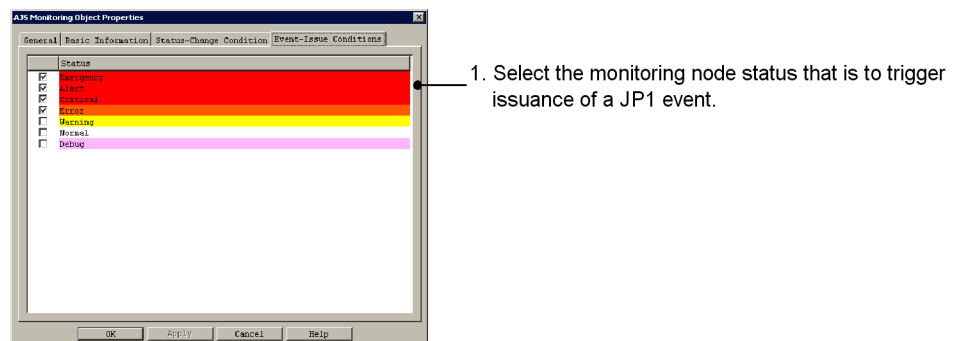


Figure 5-9: Example of setting JP1 event issuance on the Event-Issue Conditions page



(3) Deleting monitoring nodes

This subsection explains how to delete monitoring nodes.

If you delete a monitoring group, all the monitoring nodes under it are also deleted.

To delete a monitoring node:

1. Select a monitoring node.
2. Delete the monitoring node.
 - From the menu bar, choose **Edit**, and then **Delete**.
 - From the right-click pop-up menu, choose **Delete**.

The Confirm Deletion dialog box appears. If you want to delete the monitoring

node, click the **Yes** button.

You can also delete all monitoring nodes by the following method:

1. From the menu bar, choose **Edit**, and then **Delete All**.

A configuration dialog box appears. If you want to delete all monitoring nodes, click the **Yes** button.

(4) Moving monitoring nodes

You can move a monitoring node from one location to another in the monitoring tree.

This operation uses drag-and-drop or cut and paste operations.

(a) Using a drag-and-drop operation

1. Drag (left-click) a monitoring node and then drop it onto a monitoring group.

You can use the drag (left-click) operation in both the tree area and the details area. Perform the drop operation in the tree area.

(b) Using cut and paste operations

1. Select a monitoring node.
2. Cut the monitoring node.
 - From the right-click pop-up menu, choose **Cut**.
 - From the menu bar, choose **Edit**, and then **Cut**.
3. Select the destination monitoring group.
4. Paste the monitoring node.
 - From the right-click pop-up menu, choose **Paste**.
 - From the menu bar, choose **Edit**, and then **Paste**.

(5) Map display settings

You specify map display settings in order to display monitoring nodes in map format in the details area of the Monitoring Tree window.

To specify map display settings:

1. From the menu bar, choose **View** and then **Icon View**, or click .

The details area is enabled for map display settings.

2. Open the Background Image Settings window.

Use one of the following methods to display the Background Image Settings window:

- Right-click an empty space in the details area (with no monitoring node selected), and from the pop-up menu, choose **Background Image Settings** to display the Background Image Settings window.
 - Open a monitoring group's Properties window, and then on the **General** page, click the **Background Image Settings** button.
3. Select a background image.

In the Background Image Settings window, select the name of an image file that is to be used for the background image, and then click the **OK** button. The background image must be stored in the following folder in any of the three indicated file formats:

- Image file folder: *View-path*\image\map\
- Supported image file formats: JPEG, GIF, and PNG


You can also use a white background as is.

To use a white background, select `No background image` for the file.

When you make a selection, a configuration dialog box appears. Click the **Yes** button.

4. Drag-and-drop the monitoring node.

When background image setting has been completed, use the drag-and-drop operation to place the monitoring node at a desired location in the details area. To

refine the placement, either click  or from the menu bar, choose **View** and then **Set in Equal Intervals**. When a configuration dialog box appears, click the **Yes** button.

(6) **Setting the monitoring range**

To set the monitoring range by the JP1 resource group:

1. From the menu, choose **Options**, and then **Monitoring Range Settings**.

The monitoring range settings are enabled for the monitoring tree.

2. Open the Properties window for the monitoring node.

Select a monitoring node and then use one of the following methods to open the Properties window:

- Double-click (applicable only to monitoring objects).
- From the right-click pop-up menu, choose **Properties**.
- From the menu bar, choose **Edit**, and then **Properties**.

3. On the **General** page, specify the JP1 resource group.

Specify the JP1 resource group that is appropriate to the monitoring range.

4. Click the **OK** or **Apply** button.

(7) Settings for using visual icons

This subsection explains how to set visual icons to represent monitoring nodes. Visual icons are not provided by default. To use a visual icon, you must create an appropriate visual icon file in advance.

To specify settings for using visual icons:

1. From the menu bar, choose **Options**, and then **Visual Icon display**.

Enables display of visual icons.

2. Create a folder for storing visual icons.

Create the `visual` folder under the `View-path\image\` folder as shown below:

`View-path\image\visual`

3. In the folder created in step 2, store the image files that you have created for visual icons.

The supported formats and sizes of images are as follows:

- Image formats: JPEG, GIF, PNG
- Image size: Minimum 24 x 24 pixels, maximum 2,048 x 2,048 pixels

Select or create image files for visual icons taking into account that the background color will change depending on the status of the monitoring node.

The following table shows the colors used for the various monitoring node statuses.

Table 5-2: Colors used for monitoring node statuses

Monitoring node status	Color (RGB values)
Emergency	Red (255, 0, 0)
Alert	
Critical	
Error	Orange (255, 200, 0)
Warning	Yellow (255, 255, 0)
Debug	Light purple (255, 175, 175)

We recommend that you not use any of these colors in image files that you create.

4. Open the Properties window for the monitoring node.
Select a monitoring node and then use one of the following methods to open the Properties window:
 - Double-click (applicable only to monitoring objects).
 - From the right-click pop-up menu, choose **Properties**.
 - From the menu bar, choose **Edit**, and then **Properties**.
5. On the **General** page, click the **Change** button for **Visual Icon**.
The Visual Icon Selection window appears.
6. Select a visual icon.
In the Visual Icon Selection window, select the name of the image file that you want to use, and then click the **OK** button.
7. On the **General** page, click the **OK** or **Apply** button.

(8) Searching for a monitoring node

You can use this function to locate a particular monitoring node in a monitoring tree that has a complex hierarchical structure.

To search for a monitoring node:

1. Select a monitoring node.
The selected monitoring node and all its subordinate monitoring nodes become the target monitoring nodes.
2. Display the Search window.
 - From the right-click pop-up menu, choose **Search**.
 - Alternatively, from the menu bar, choose **Edit**, and then **Search**.
3. Enter a search condition and then click the **Search** button.
The monitoring nodes that satisfy your search condition are listed.
4. Double-click the monitoring node that you want to display.
If you double-click a monitoring node listed in the search results, the Monitoring Tree (Editing) window is displayed with that monitoring node selected.

5.3.5 Saving a customized monitoring tree at the local host

You can save as a CSV file at the local host a monitoring tree that was customized in the Monitoring Tree (Editing) window. You do this when you want to temporarily suspend the monitoring tree creation process or you want to save a backup of a monitoring tree.

5. Setting up Central Scope

To save a customized monitoring tree at the local host:

1. Choose **Save Tree**.

In the Monitoring Tree (Editing) window, from the menu bar, choose **File**, and then **Save Tree**.

2. Save the monitoring tree under a desired file name in any folder.

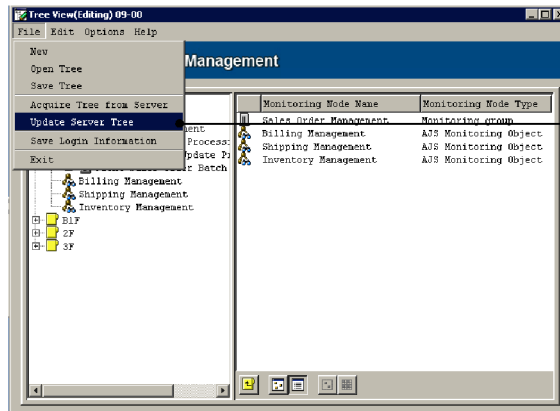
When the Save Tree window appears, specify a desired folder name and file name, and then save the monitoring tree.

5.3.6 Applying a customized monitoring tree to the manager

Once you have applied to the manager a monitoring tree that was customized in the Monitoring Tree (Editing) window, you can use it for system operation monitoring. If monitoring range settings were enabled for the monitoring tree in the Monitoring Tree (Editing) window, those settings also take effect at the manager.

The following figure shows the procedure for applying a monitoring tree to the manager.

Figure 5-10: Update Server Tree



1. Choose **Update Server Tree**.
2. Log in.
3. The server's monitoring tree is updated.

1. Choose **Update Server Tree**.

In the Monitoring Tree (Editing) window, from the menu bar, choose **File**, and then **Update Server Tree**.

A configuration dialog box appears. If you want to update, click the **Yes** button.

2. Log in to the server.

The Login window for logging in to JP1/IM - Manager (JP1/IM - Central Scope) is displayed.

Enter the JP1 user name and password. The JP1 user must belong to the

JP1_Console JP1 resource group and have JP1_Console_Admin permissions.

For the host to connect, enter the host name of the JP1/IM - Manager whose monitoring tree is to be updated.

3. The customized monitoring tree is applied to the server.

A dialog box is displayed while the processing is in progress. This dialog box closes when the processing is completed.

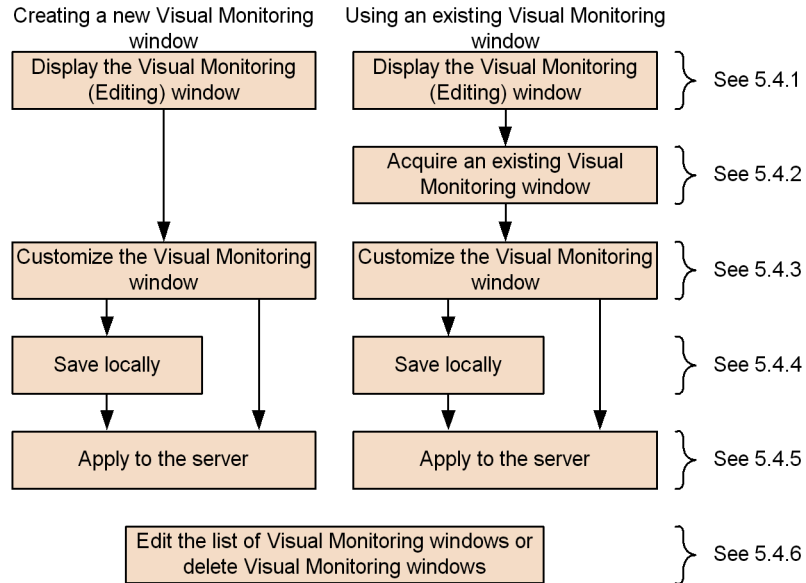
To check the applied monitoring tree, log in to JP1/IM - Manager (JP1/IM - Central Scope), and then check the Monitoring Tree window.

5.4 Using the GUI to create a Visual Monitoring window

This section explains how to use the GUI to create a Visual Monitoring window.

The following figure shows the procedure.

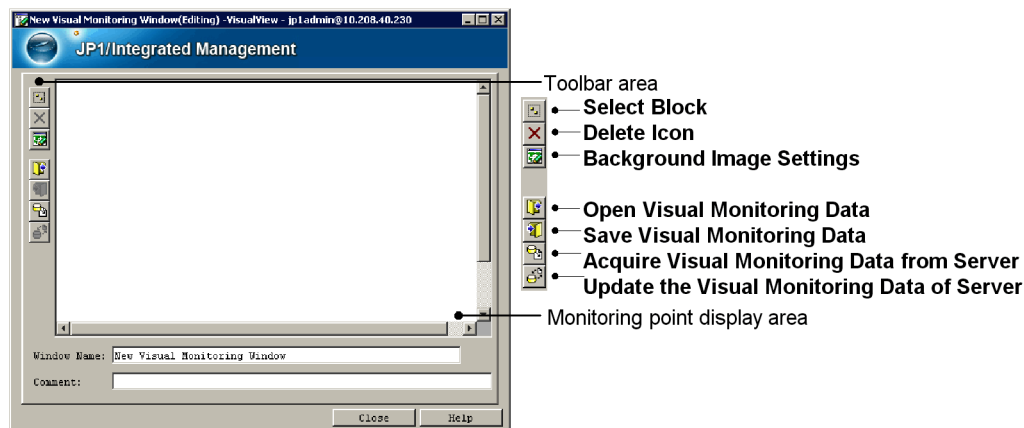
Figure 5-11: Procedure for using the GUI to create a Visual Monitoring window



5.4.1 Opening an edit window for the Visual Monitoring window

You use the Visual Monitoring (Editing) window to edit a Visual Monitoring window. You can open this window from the Monitoring Tree (Editing) window.

Figure 5-12: Visual Monitoring (Editing) window



To open an edit window for the Visual Monitoring window:

1. Open the Visual Monitoring (Editing) window.

Use the following method to open the window:

- In the Monitoring Tree (Editing) window, from the menu bar, choose **Edit**, and then **Create New Visual Monitoring Window**.


5.4.2 Acquiring an existing Visual Monitoring window

If you have already created and been using a Visual Monitoring window, you can connect to the manager and acquire the existing settings.

(1) Acquiring a Visual Monitoring window from the server

To acquire a Visual Monitoring window from the server:

1. Choose **Acquire Visual Monitoring Data from Server**.

In the Visual Monitoring (Editing) window, on the toolbar, click .

2. Log in to the server.

The Login window for logging in to JP1/IM - Manager (JP1/IM - Central Scope) is displayed.

Enter the JP1 user name and password. The JP1 user must belong to the JP1_Console JP1 resource group and have JP1_Console_Admin permissions.

For the host to connect, enter the host name of JP1/IM - Manager from which visual monitoring data is to be acquired.

3. Select the Visual Monitoring window to be acquired.


If login is successful, the Open Visual Monitoring Window window opens. Select the Visual Monitoring window whose settings are to be acquired, and then click the **OK** button.

If you have the settings (a CSV file) for a Visual Monitoring window that have been saved locally, you can also use those settings.

(2) Acquiring a Visual Monitoring window (CSV file) that has been saved locally

To acquire a Visual Monitoring window (CSV file) that has been saved locally:

1. Open the Open Visual Monitoring Data window.

In the Visual Monitoring (Editing) window, on the toolbar, click .

The Open Visual Monitoring Data window is displayed.

2. Specify the settings (CSV file) for the Visual Monitoring window.

Select the settings (CSV file) for the Visual Monitoring window that you want to use, and then click the **Open** button.

When a confirmation dialog box appears, click the **Yes** button.

5.4.3 Customizing a Visual Monitoring window

You can use the Visual Monitoring (Editing) window to customize an existing Visual Monitoring window as well as to create a new Visual Monitoring window. The following Visual Monitoring window operations are provided:

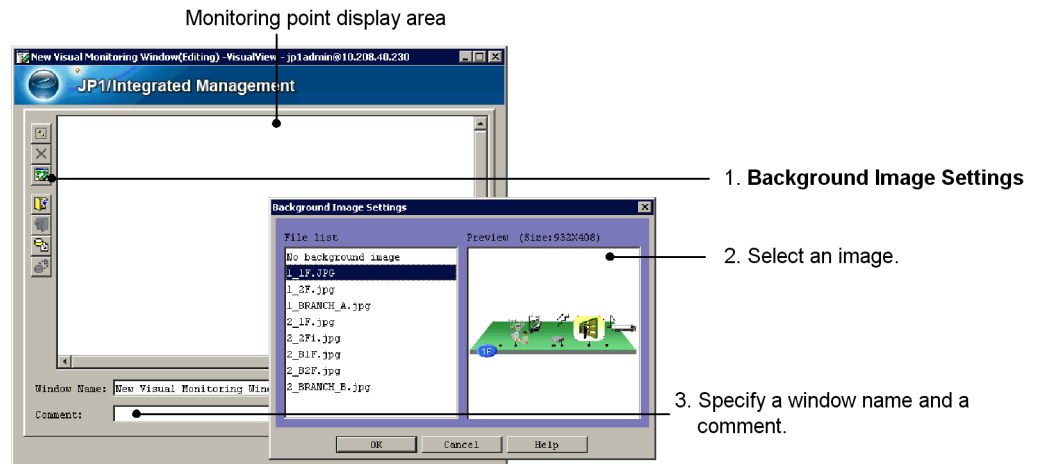
- Set a background image
- Add monitoring nodes
- Delete monitoring nodes
- Set attributes of monitoring nodes
- Change the monitoring status of monitoring nodes
- Search for monitoring nodes

(1) Setting a background image for a Visual Monitoring window

You can set a background image for a Visual Monitoring window. The background image must be stored in the following folder in any of the three indicated file formats:


- Image file folder: *View-path*\image\map\
• Supported image file formats: JPEG, GIF, and PNG

Figure 5-13: Setting the background image



1. Open the Background Image Settings window.

Use one of the following methods to display the Background Image Settings window:

- In the Visual Monitoring (Editing) window, on the toolbar, click .
- Right-click any empty area in the monitoring point display area (with no monitoring node selected), and from the pop-up menu, choose **Background Image Settings**.

2. Select a background image.

In the Background Image Settings window, select the name of an image file that is to be used for the background, and then click the **OK** button.

You can also use the Visual Monitoring window with a white background. In this case, select **No background image** for the file.

When you make a selection, a configuration dialog box appears. Click the **Yes** button.

3. Assign a name to the Visual Monitoring window.

Once you have chosen the background image, assign a name to the Visual Monitoring window.

In the **Window Name** field enter a name. In the **Comment** field enter an optional comment, such as an explanation of the monitoring purposes or an image description.

The window name is displayed on the title bar of the Visual Monitoring window, and the comment is displayed at the bottom of the background image.

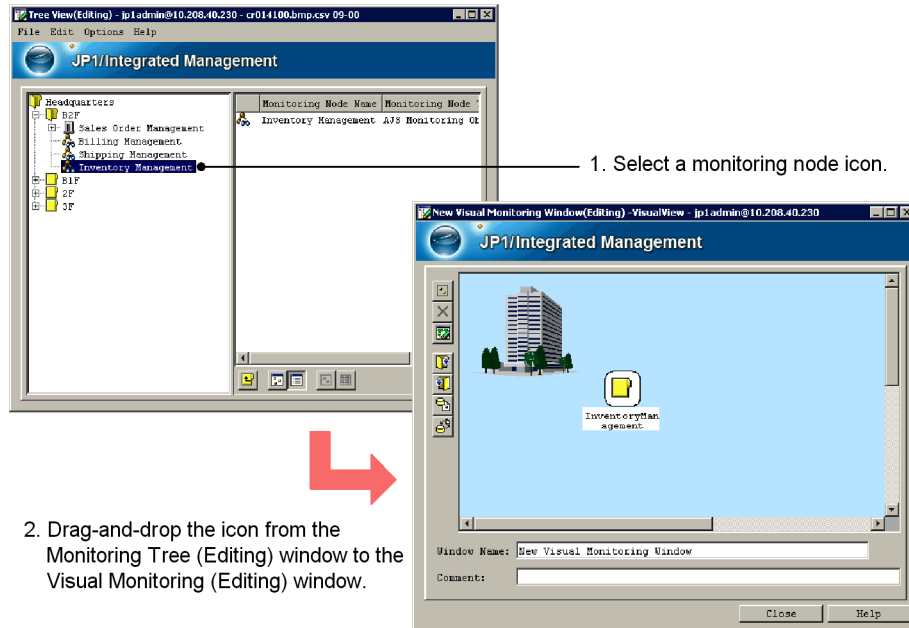
Hints on Visual Monitoring window operation

While a background image is selected in the monitoring point display area, you can scroll the background image by dragging the mouse.

(2) Adding monitoring nodes to a Visual Monitoring window

You can add monitoring nodes on the background image of a Visual Monitoring window. You do this by dragging monitoring node icons from the Monitoring Tree window and dropping them onto the Visual Monitoring window.

Figure 5-14: Adding monitoring nodes to a Visual Monitoring window



1. Select a monitoring node on the monitoring tree.
 In the Monitoring Tree (Editing) window, display and select the monitoring node that you want to monitor by using the Visual Monitoring window.
2. Drag-and-drop the monitoring node in the Visual Monitoring window.
 In the Monitoring Tree (Editing) window, drag (left-click) the monitoring node icon and drop it onto the Visual Monitoring (Editing) window.

In the case of a monitoring node icon added by the above method, the appropriate status color (such as red for failure) is displayed in the monitoring tree, thus reflecting

the monitoring node's status.

There will be a delay before information in the Monitoring Tree window takes effect on the Visual Monitoring window.

(3) *Deleting monitoring nodes from the Visual Monitoring window*


To delete monitoring nodes from the Visual Monitoring window:

1. Select a monitoring node icon and then delete it.

Use one of the methods described below. To delete multiple icons in a batch, use



to select multiple icons.

- Select an icon, and then in the Visual Monitoring (Editing) window, on the toolbar, click .
- Select an icon, and then from the right-click pop-up menu, choose **Delete Icon**.

When a configuration dialog box appears, click the **Yes** button.

(4) *Setting the attributes of monitoring nodes*

If you set the attributes of a monitoring node in the Visual Monitoring (Editing) window, the specified settings are applied to the corresponding monitoring node in the Monitoring Tree (Editing) window.

To set attributes for a monitoring node that has been placed in the Visual Monitoring (Editing) window:

1. Open the Properties window for the monitoring node.

Select a monitoring node and then use the following method to open the Properties window:

- From the right-click pop-up menu, choose **Properties**.

2. Specify the settings on the **General** page.

Specify the monitoring node name, icon to be used, visual icon to be used,^{#1} background image settings (monitoring groups only), monitoring status, and JP1 resource group.^{#2}

3. Specify the settings on the **Basic Information** page.

Specify basic information for the monitoring node.

4. Specify the settings on the **Status-Change Condition** page.

Specify the JP1 events that are to change the status of the monitoring node when those events are received by JP1/IM - Manager.

For details about the settings for status change conditions, 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*.

5. Specify the settings on the **Event-Issue Conditions** page.

Specify the status of the monitoring node that is to trigger issuance of a JP1 event.

If an automated action is to be executed based on the status of the monitoring node, specify the settings in **Event-Issue Conditions**, and then set an automated action for the JP1 event whose event ID is 00003FB0.

6. Click the **OK** or **Apply** button.

#1: Certain advance preparations are required in order to use visual icons. For details, see 5.3.4(7) *Settings for using visual icons*.

#2: You can set this item if the monitoring range setting is enabled for the monitoring tree.

For an example of property settings, see 5.3.4(2) *Setting the attributes of monitoring nodes*.

(5) Changing the monitoring status of monitoring nodes

If you change the monitoring status of a monitoring node in the Visual Monitoring (Editing) window, the change is applied to the corresponding monitoring node in the Monitoring Tree (Editing) window.

To change the monitoring status of a monitoring node placed in the Visual Monitoring (Editing) window:

1. Select a monitoring node.
2. From the right-click pop-up menu, choose **Change Monitoring Status** to change the monitoring node to a desired monitoring status.

A confirmation dialog box appears.

3. In the confirmation dialog box, click the **Yes** button.

(6) Searching for a monitoring node

You can use this function to locate a particular monitoring node in a monitoring tree that has a complex hierarchical structure.

To search for a monitoring node:

1. Select a monitoring node.

The selected monitoring node and its subordinate monitoring nodes become the target monitoring nodes.


2. Display the Search window.
From the right-click pop-up menu, choose **Search**.
3. Enter a search condition and then click the **Search** button.
The monitoring nodes that satisfy your search condition are listed.
4. Select the monitoring node that you want to monitor in the Visual Monitoring window from the displayed list, and then drag-and-drop it into the Visual Monitoring (Editing) window.

5.4.4 Saving a customized Visual Monitoring window at the local host

You can save as a CSV file at the local host a Visual Monitoring window that was customized in the Visual Monitoring (Editing) window. You do this when you want to temporarily suspend the Visual Monitoring window creation process, or you want to save a backup of a customized Visual Monitoring window.

To save a customized Visual Monitoring window at the local host:

1. Choose **Save Visual Monitoring Data**.

In the Visual Monitoring (Editing) window, on the toolbar, click .

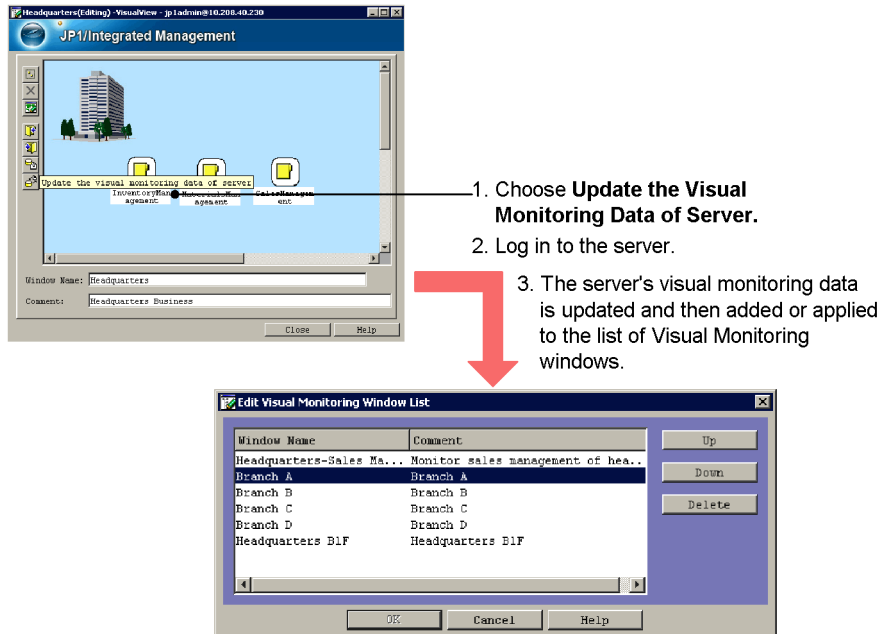
2. Save the Visual Monitoring window under a desired file name in any folder.

When the Save Visual Monitoring Data window appears, specify a desired folder name and file name, and then save the Visual Monitoring window.

5.4.5 Applying a customized Visual Monitoring window to the manager


Once you have applied to the manager a Visual Monitoring window that was customized in the Visual Monitoring (Editing) window, you can use it for system operation monitoring. The following figure shows the procedure for applying a customized Visual Monitoring window to the manager.

Figure 5-15: Updating a server's visual monitoring data



To apply a customized Visual Monitoring window to the manager:

1. Choose **Update the visual monitoring data of server**.

In the Visual Monitoring (Editing) window, on the toolbar, click .

When a configuration dialog box appears, click the **Yes** button.

2. Log in to the server.

The Login window for logging in to JP1/IM - Manager (JP1/IM - Central Scope) is displayed.

Enter the JP1 user name and password. The JP1 user must belong to the JP1_Console JP1 resource group and have JP1_Console_Admin permissions.

For the host to connect, enter the host name of JP1/IM - Manager.

3. The customized Visual Monitoring window is applied to the server.

A dialog box is displayed while the processing is in progress. This dialog box closes when the processing is completed. When the Visual Monitoring window has been applied to the manager, the Visual Monitoring window is added or applied to the list of visual windows.

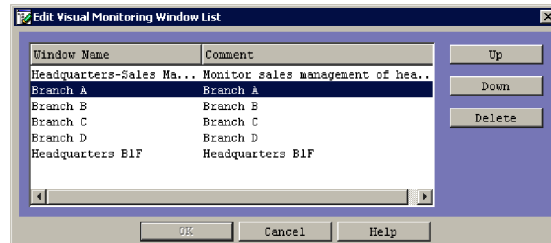
To check the applied Visual Monitoring window, log in to JP1/IM - Manager (JP1/

IM - Central Scope), and then check the Visual Monitoring window.

5.4.6 Editing the list of Visual Monitoring windows and deleting Visual Monitoring windows

This subsection explains how to use the Edit Visual Monitoring Window List window to edit the list of Visual Monitoring windows and to delete Visual Monitoring windows.

Figure 5-16: Editing the list of Visual Monitoring windows and deleting Visual Monitoring windows



1. Open the Edit Visual Monitoring Window List window.
2. Log in to the server.
3. Select a Visual Monitoring window and then click the **Up**, **End**, or **Delete** button.

To edit the list of Visual Monitoring windows and delete Visual Monitoring windows:

1. Open the Edit Visual Monitoring Window List window.

In the Monitoring Tree (Editing) window, from the menu bar, choose **Edit**, and then **Edit Visual Monitoring Window List**.

2. Log in to the server.

The Login window for logging in to JP1/IM - Manager (JP1/IM - Central Scope) is displayed.

Enter the JP1 user name and password. The JP1 user must belong to the JP1_Console JP1 resource group and have JP1_Console_Admin permissions.

For the host to connect, enter the host name of JP1/IM - Manager.

3. Select a Visual Monitoring window, and then move its position or delete it.

In the Edit Visual Monitoring Window List window, select the name of a Visual Monitoring window, and then click the **Up**, **Down**, or **Delete** button. At this point, only the display in the edit window has changed; the actual data at the server has not been changed. To cancel the change, click **Cancel**.

When the disabled **OK** button is enabled, click it. The list window is refreshed at this point. If you have clicked the **Delete** button, the data for the Visual Monitoring window is deleted from the server.

5.5 Using saved CSV files to create monitoring windows

You can use the locally saved CSV files to perform the following environment setup:

- Changing many monitoring nodes in batch mode by directly editing the saved CSV files
- Editing the stored CSV files

For details about the setup procedure, see the following:

Using the CSV files to create monitoring windows (Monitoring Tree window and Visual Monitoring window):

- Saving monitoring window settings as a CSV file
See *5.3.5 Saving a customized monitoring tree at the local host.*
See *5.4.4 Saving a customized Visual Monitoring window at the local host.*
- Creating monitoring windows from the CSV files
See *5.3.4 Customizing a monitoring tree.*
See *5.4.3 Customizing a Visual Monitoring window.*
- Details of the configuration file for monitoring tree
See *Configuration file for monitoring tree* in *2. Definition Files* in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference.*

5.6 Editing guide information

Guide information is displayed in the Guide window to provide the user with assistance in the event of a problem during system monitoring. If you display problem handling procedures as guide information, you can reduce the system administrator's workload at the initial stage of problem handling. You can also use the guide to provide information about monitoring nodes, such as the corresponding jobs and monitored targets.

You specify the information to be displayed as guide information in a guide information file located at the JP1/IM - Manager host.

This section explains how to edit guide information.

For details about the information to be provided as guide information and the guide function, see the following:

About the guide function and setting guide information:

- About the information to be provided as guide information and the guide function

See *4.7 Guide function* in the *Job Management Partner 1/Integrated Management - Manager Overview and System Design Guide*.

- 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*.

5.6.1 How to edit guide information

To edit guide information:

1. Edit the guide information file.

The guide information file is a TXT file. Open the file listed below with a text editor and then edit it.

Table 5-3: Correspondence between guide information files and language encodings supported by JP1/IM - Manager

OS	Guide information file to be edited
Windows	<i>Scope-path</i> \conf\jcs_guide.txt
	<i>shared-folder</i> \jp1scope\conf\jcs_guide.txt

OS	Guide information file to be edited
UNIX	/etc/opt/jp1scope/conf/jcs_guide.txt
	shared-directory/jp1scope/conf/jcs_guide.txt

2. Reload or restart JP1/IM - Manager to apply the guide information settings.

A guide information file is loaded when JP1/IM - Manager is reloaded or started. Do one of the following:

- Execute the `jco_spm�_reload` command to reload JP1/IM - Manager.
- Terminate JP1/IM - Manager and then restart it.

3. Make sure that the guide information has loaded successfully.

If the guide information file contains invalid information, an error occurs when JP1/IM - Manager loads the guide information file. Check the integrated trace log to make sure that the guide information file has loaded successfully.

Table 5-4: Folder/directory for the integrated trace log

OS	Integrated trace log
Windows	system-drive:\Program Files\HITACHI\HNTRLib2\spool\
UNIX	/var/opt/hitachi/HNTRLib2/spool/

When the guide information file has loaded successfully, the applicable message shown below is recorded in the integrated trace log; check to see if this message is recorded in the log:

- When JP1/IM - Manager was restarted:
KAVB7393-I The guide information definition was initialized successfully.
- When JP1/IM - Manager was reloaded:
KAVB7394-I The guide information definition was reloaded successfully.

If an error is detected in the guide information file, a message in the message number range of KAVB7377-W to KAVB7392-W is output to the integrated trace log. In the event of an error, check the error indicated by the message and then correct it. Then reload or restart JP1/IM - Manager.

5.7 Setting up a Central Scope operating environment

This section explains how to set up an operating environment for Central Scope.

5.7.1 Setting for the maximum number of status change events

A JP1 warning-level event can be issued when the number of monitoring object status change events exceeds a maximum value (which is 100).

The setting for whether such JP1 warning-level events are to be issued is enabled for a new installation. If the setting was disabled under an old version of JP1/IM - Manager or JP1/IM - Central Scope, it remains disabled. You should change the setting as appropriate to your operation.

To specify the settings for the maximum number of status change events:

1. Terminate JP1/IM - Manager.
2. Execute the `jbssetcnf` command using one of the following files as the argument as appropriate:

If JP1 events are to be issued when the maximum number of status change events exceeds the maximum value: `evhist_warn_event_on.conf`

If JP1 events are not to be issued when the maximum number of status change events exceeds the maximum value: `evhist_warn_event_off.conf`

When you execute the `jbssetcnf` command, the setting is applied to the JP1 common definition information.

For details about the `jbssetcnf` command, see the *Job Management Partner 1/ Base User's Guide*.

About the setting in the file:

For details about the setting in the file, 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*.

3. Start JP1/IM - Manager.

5.7.2 Setting the completed-action linkage function

The completed-action linkage function automatically changes the status of monitoring objects according to the JP1 event handling status.

This function simplifies Central Scope operations because it changes the status of monitoring objects according to the JP1 event handling status, thereby eliminating the need to change the status of monitoring groups manually.

In the case of a new installation, this setting is enabled. If the setting was disabled under an old version of JP1/IM - Manager or JP1/IM - Central Scope, it remains disabled. You should change the setting as appropriate to your operation.

To set the completed-action linkage function:

1. Terminate JP1/IM - Manager.
2. Execute the `jbssetcnf` command using one of the following files as the argument as appropriate:

To enable the completed-action linkage function: `action_complete_on.conf`

To disable the completed-action linkage function:
`action_complete_off.conf`

When you execute the `jbssetcnf` command, the setting is applied to the JP1 common definition information.

For details about the `jbssetcnf` command, see the *Job Management Partner 1/Base User's Guide*.

About the setting in the file:

For details about the setting in the file, 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. Start JP1/IM - Manager.

5.7.3 Settings for automatically deleting status change events when JP1 event handling is completed

To automatically delete the status change events of monitoring objects when JP1 event handling is completed:

1. Use one of the following methods to delete all status change events from the monitoring tree:
 - Use window operations from the Monitoring Tree window or use the `jcsostat` command to initialize all the monitoring nodes in the monitoring tree.
 - In the Monitoring Tree (Editing) window, choose **File**, and then **Update Server Tree** to update the monitoring tree.
 - Use the `jcsdbimport` command to update the monitoring tree.
2. Terminate JP1/IM - Manager.
3. Create a definition file for automatic delete mode of status change event.

About the settings in the file:

For details about the settings in the file, see *Definition file for automatic delete mode of status change event* in 2. *Definition Files* in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.

4. Execute the `jbssetcnf` command with the file created in step 3 specified as the argument.

When you execute the `jbssetcnf` command, the settings are applied to the JP1 common definition information.

For details about the `jbssetcnf` command, see the *Job Management Partner 1/Base User's Guide*.

5. Start JP1/IM - Manager.

5.7.4 Settings for initializing monitoring objects when JP1 events are received

To initialize monitoring objects when JP1 events are received:

1. Terminate JP1/IM - Manager.
2. Create a definition file for monitoring object initialization mode.

About the settings in the file:

For details about the settings in the file, see *Definition file for monitoring object initialization mode* in 2. *Definition Files* in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.

3. Execute the `jbssetcnf` command with the file created in step 2 specified as the argument.

When you execute the `jbssetcnf` command, the settings are applied to the JP1 common definition information.

For details about the `jbssetcnf` command, see the *Job Management Partner 1/Base User's Guide*.

4. Start JP1/IM - Manager.

5.7.5 Setting the memory-resident status change condition function

To set the function for making status change conditions resident in memory:

1. Terminate JP1/IM - Manager.
2. Create a definition file for on memory mode of status change condition.

About the settings in the file:

For details about the settings in the file, see *Definition file for on memory mode of status change condition* in 2. *Definition Files* in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.

3. Execute the `jbssetcnf` command with the file created in step 2 specified as the argument.

When you execute the `jbssetcnf` command, the settings are applied to the JP1 common definition information.

For details about the `jbssetcnf` command, see the *Job Management Partner 1/Base User's Guide*.

4. Start JP1/IM - Manager.

5.7.6 Customizing the toolbar for the monitoring tree

Your customized settings for the Monitoring Tree window take effect the next time you log in to JP1/IM - Manager (JP1/IM - Central Scope).

To customize the Monitoring Tree window and add programs (icons) to the toolbar:

1. Store a personalized icon in the following folder:

View-path\image\sovtool

2. Store the program that is to be started from your icon in any folder.
3. Edit the start program definition file (`!JP1_CS_APP0.conf`).

The start program definition file (`!JP1_CS_APP0.conf`) is stored in the following folder:

View-path\conf\sovtoolexec\en\

4. Edit the toolbar definition file (`!JP1_CS_FTOOL0.conf`).

The toolbar definition file (`!JP1_CS_FTOOL0.conf`) is stored in the following folder:

View-path\conf\sovtoolitem\en\

5. Edit the icon operation definition file (`!JP1_CS_FTREE0.conf`).

The icon operation definition file (`!JP1_CS_FTREE0.conf`) is stored in the following folder:

View-path\conf\sovtoolitem\en\

About customizing the Monitoring Tree window:

- About the start program definition file (!JP1_CS_APP0.conf)
See *Start program definition file (!JP1_CS_APP0.conf)* in 2. *Definition Files* in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.
- About the toolbar definition file (!JP1_CS_FTOOL0.conf)
See *Toolbar definition file (!JP1_CS_FTOOL0.conf)* in 2. *Definition Files* in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.
- About the icon operation definition file (!JP1_CS_FTREE0.conf)
See *Icon operation definition file (!JP1_CS_FTREE0.conf)* in 2. *Definition Files* in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.

5.8 Setting up for linked products

This section describes the setup for products that can be linked to Central Scope.

To simplify the linkage with each product, Central Scope provides functions for automatic generation of monitoring trees and of system-monitoring objects (for which the basic definition required for monitoring is predefined).

If you will use such system-monitoring objects to monitor specific products and will generate monitoring trees automatically, you should use the procedure explained in this section to set up the linked products.

This section assumes that the linked products have already been installed.

Overview of the setup for linking to a product

The following provides an overview of the setup procedure for linking to a specific product.

- Defining the system hierarchy

If you use IM Configuration Management, use IM Configuration Management - View to register the host that executes the linked product as a JP1/IM monitoring target.

If you do not use IM Configuration Management, execute the command to register the host that executes the linked product as a JP1/IM monitoring target.

- Enabling JP1 event issuance on the linked product (setting the linked product)

Because JP1/IM uses JP1 events to monitor systems, set each linked product to issue JP1 events.

- Setting SNMP trap conversion (setting JP1/Base)

If the linked product is HP NNM, it issues SNMP traps rather than JP1 events. In the case of such a product, you must set JP1/Base to convert the SNMP traps to JP1 events.

- Setting up the linkage program (setting the linked product)

If the linked product supports automatic generation of a monitoring tree, set up the function that collects definition information during automatic generation (linkage program) on the linked product.

5.8.1 Setup for linkage with JP1/AJS

(1) Setup for using system-monitoring objects for monitoring

To use a system-monitoring object of JP1/AJS, you must set JP1/AJS to issue JP1 events.

For details about the linkage setup, see the following manual:

- Description of JP1/AJS

See the chapter that describes use of JP1/IM for 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*.

(2) Setup for generating a monitoring tree automatically

JP1/AJS supports automatic monitoring tree generation. To enable the linkage for automatic generation, set up the linkage program.

For details about the linkage setup, see the following manual:

- Description of JP1/AJS

See the chapter that describes use of JP1/IM for 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*.

(a) For the JP1/AJS - Manager host

1. Setting up the linkage program for JP1/AJS

Execute the following command to enable collection of definition information from JP1/AJS when the monitoring tree is generated automatically:

```
ajs_adapter_setup -i (when enabling the linkage for automatic generation)
```

If the above setup is not completed, a JP1/AJS monitoring object is not created when an attempt is made to generate a monitoring tree automatically.

To release the linkage, execute the following command:

```
ajs_adapter_setup -u (when releasing the linkage for automatic generation)
```

(b) For the JP1/AJS - Agent host

There is no need to set up a linkage program at the JP1/AJS - Agent host. Once you complete the setup at the JP1/AJS - Manager, Central Scope extracts the job execution host and generates a monitoring tree automatically based on the jobnet definition that is collected during monitoring tree automatic generation.

5.8.2 Setup for linkage with JP1/PFM

(1) Setup for using system-monitoring objects for monitoring

To use a system-monitoring object of JP1/PFM, you must set JP1/PFM to issue JP1 events as described below. JP1/PFM supports automatic monitoring tree generation. To enable the linkage for automatic generation, set up the linkage program.

For details about the linkage setup, also see the following manual:

- Description of JP1/PFM

See the description of linkage with JP1/IM in the *Job Management Partner 1/ Performance Management User's Guide*.

(a) For the JP1/PFM - Manager host

To perform setup at the manager where JP1/PFM - Manager is installed:

1. Enable JP1 event issuance by JP1/PFM.

Set JP1/PFM to issue JP1 events by command execution actions in alarm definitions.

- If you remove an attribute from or set a non-default attribute value in the arguments of the `jpcimevt` command that issues JP1 events, the status of system-monitoring objects can no longer be monitored.
- If you clear the **Convert the alarm level to the severity level** check box, the status of system-monitoring objects can no longer be monitored.

(2) Setup for generating a monitoring tree automatically

JP1/PFM supports automatic monitoring tree generation. To enable the linkage for automatic generation, set up the linkage program.

For details about the linkage setup, also see the following manual:

- Description of JP1/PFM

See the description of linkage with JP1/IM in the *Job Management Partner 1/ Performance Management User's Guide*.

(a) For the JP1/PFM - Manager host

To perform setup at the manager where JP1/PFM - Manager is installed:

1. Setting up the linkage program for JP1/PFM

Execute the following command to enable collection of definition information from JP1/PFM when the monitoring tree is generated automatically:

```
jpcimsetup -i (when enabling the linkage for automatic generation)
```

If the above setup is not completed, a JP1/PFM monitoring object is not created when an attempt is made to generate a monitoring tree automatically.

To release the linkage, execute the following command:

```
jpcimsetup -u (when releasing the linkage for automatic generation)
```

5.8.3 Setup for linkage with HP NNM

This subsection describes the setup for linking with HP NNM version 8 or earlier. For details about the setup for linking with HP NNMi using 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*.

(1) Setup for using system-monitoring objects for monitoring

To link with HP NNM version 8 or earlier, you must convert SNMP traps issued by HP NNM to JP1 events so that the events can be monitored by Central Scope.

For details about the linkage setup, also see the following manual:

- Description of HP NNM version 8 or earlier
See the manual *HP OpenView Network Node Manager: Managing Your Network with HP OpenView Network Node Manager*.
- Description of conversion from SNMP traps to JP1 events
See the description of event conversion settings in the *Job Management Partner 1/Base User's Guide*.

(a) For the HP NNM host

To perform setup at the manager where HP NNM version 8 or earlier is installed:

1. Set the SNMP trap conversion function of JP1/Base.

To convert SNMP traps to JP1 events, set the SNMP trap conversion function of JP1/Base.

For details about how to set the SNMP trap conversion function, see the chapter that describes event conversion settings in the *Job Management Partner 1/Base User's Guide*.

The following is an overview of the setting procedure:

- Set the linkage between NNM and JP1/Base (execute `imevtgw_setup`).
 - Set the URL of NNM.
 - Set the JP1 event destination.
 - Set the filter definition file (`snmpfilter.conf`).
2. Edit the filter definition file for the SNMP trap conversion function of JP1/Base.
Add the contents of the sample file (`snmpfilter_im_sample.conf`) that contains settings for converting the SNMP traps handled by Central Scope to the filter definition file for the SNMP trap conversion function (`snmpfilter.conf`) of JP1/Base.

The file names are as follows:

- Filter definition file for the SNMP trap conversion function

In Windows:

Base-path\conf\evtgw\snmpfilter.conf

In UNIX:

/etc/opt/jplbase/conf/evtgw/snmpfilter.conf

- Sample file of Central Scope

In Windows:

Scope-path\conf\snmpfilter_im_sample.conf

In UNIX:

/etc/opt/jplscope/conf/snmpfilter_im_sample.conf

Notes:

- The plus sign (+) at the beginning of the sample file is a setting for loading SNMP trap variable binding to JP1 events. Do not remove it.
- There is a limit to the size of a filter definition file. In the filter definition file, add only definitions of SNMP traps that are to be monitored in your environment.

For details about the limitation on the size of a filter definition file, see the *Job Management Partner 1/Base User's Guide*.

5.8.4 Setup for linkage with JP1/Software Distribution

(1) Setup for using system-monitoring objects for monitoring

To use a system-monitoring object of JP1/Software Distribution, you must set JP1/Software Distribution to issue JP1 events.

For details about the linkage setup, also see the following manual:

- Description of JP1/Software Distribution

See the *Job Management Partner 1/Software Distribution Setup Guide, for Windows systems*.

(a) For the JP1/Software Distribution Manager host

To perform setup at the manager where JP1/Software Distribution Manager is installed:

1. Enable JP1 event issuance by JP1/Software Distribution.

Start the JP1/Software Distribution setup window, choose the Event Service

panel, and then select the **enable the event service** check box.

To link with Central Scope, select the **Report when the server is down** and **At error** check boxes.

5.8.5 Setup for linkage with JP1/PAM

(1) Setup for using system-monitoring objects for monitoring

To use a system-monitoring object of JP1/PAM, you must set JP1/PAM to issue JP1 events.

For details about the linkage setup, also see the following manual:

- Description of JP1/PAM

See the manual *Job Management Partner 1/Performance Management - Analysis Description, Operator's Guide and Reference*.

(a) For the JP1/PA - Manager host

To perform setup at the manager where JP1/PA - Manager is installed:

1. Enable JP1 event issuance by JP1/PAM.

Set the JP1 event issuance definition file (`pamjp1ev.conf`) for JP1/PAM as follows:

- File to be set

```
pamjp1ev.conf
```

- Settings

Specify `Y` for the settings as to whether to issue JP1 events (`jp1evt_flag`) and whether to issue each JP1 event (such as `metricNW`). For the settings as to whether to issue each JP1 event, specify `Y` for all events.

```
jp1evt_flag=Y
```

```
metricNW=Y
```

```
:
```

5.8.6 Setup for linkage with Cosminexus

(1) Setup for using system-monitoring objects for monitoring

To use a system-monitoring object of Cosminexus, you must specify the following settings at Cosminexus:

- JP1 event issuance settings

To use JP1/IM to monitor the Cosminexus system environment, you must set Cosminexus to issue JP1 events.

To display Cosminexus' operations management portal window from JP1/IM - View, you must set monitor startup using the Cosminexus-provided monitor startup command and settings file.

For details about the linkage setup, also see the following manual:

- Description of Cosminexus

See the *Cosminexus Simple Setup and Operation Guide*.

(2) Setup for generating a monitoring tree automatically

To link with Cosminexus for automatic monitoring tree generation, you must perform the following setup at Cosminexus:

- Setting up the adapter command

To use JP1/IM to collect information about the Cosminexus system environment, you must perform setup using the Cosminexus-provided adapter command (`mngsvr_adapter_setup`).

For details about the linkage setup, also see the following manual:

- Description of Cosminexus

See the *Cosminexus Simple Setup and Operation Guide*.

Note:

If you use JP1/IM to collect and monitor information about the Cosminexus system environment, note the following:

- If you will be generating a work-oriented tree by automatic generation, you must include in the JP1/IM system configuration the business server where the operations management server and J2EE server (J2EE application) are run.
- If you will be generating a server-oriented tree by automatic generation, you must include in the JP1/IM system configuration all operations management servers and business servers.

5.8.7 Setup for linkage with HiRDB

(1) Setup for using system-monitoring objects for monitoring

To use a system-monitoring object of HiRDB, you must set HiRDB to notify JP1/IM of events output by HiRDB as JP1 events.

For details about the linkage setup, also see the following manual:

- Description of HiRDB

Event notification to JP1/IM

See the manual *For Windows Systems HiRDB Version 8 Installation and Design Guide* or *For UNIX Systems HiRDB Version 8 Installation and Design Guide*.

Detailed settings for event notification to JP1/IM

See the manual *For Windows Systems HiRDB Version 8 System Definition* or *For UNIX Systems HiRDB Version 8 System Definition*.

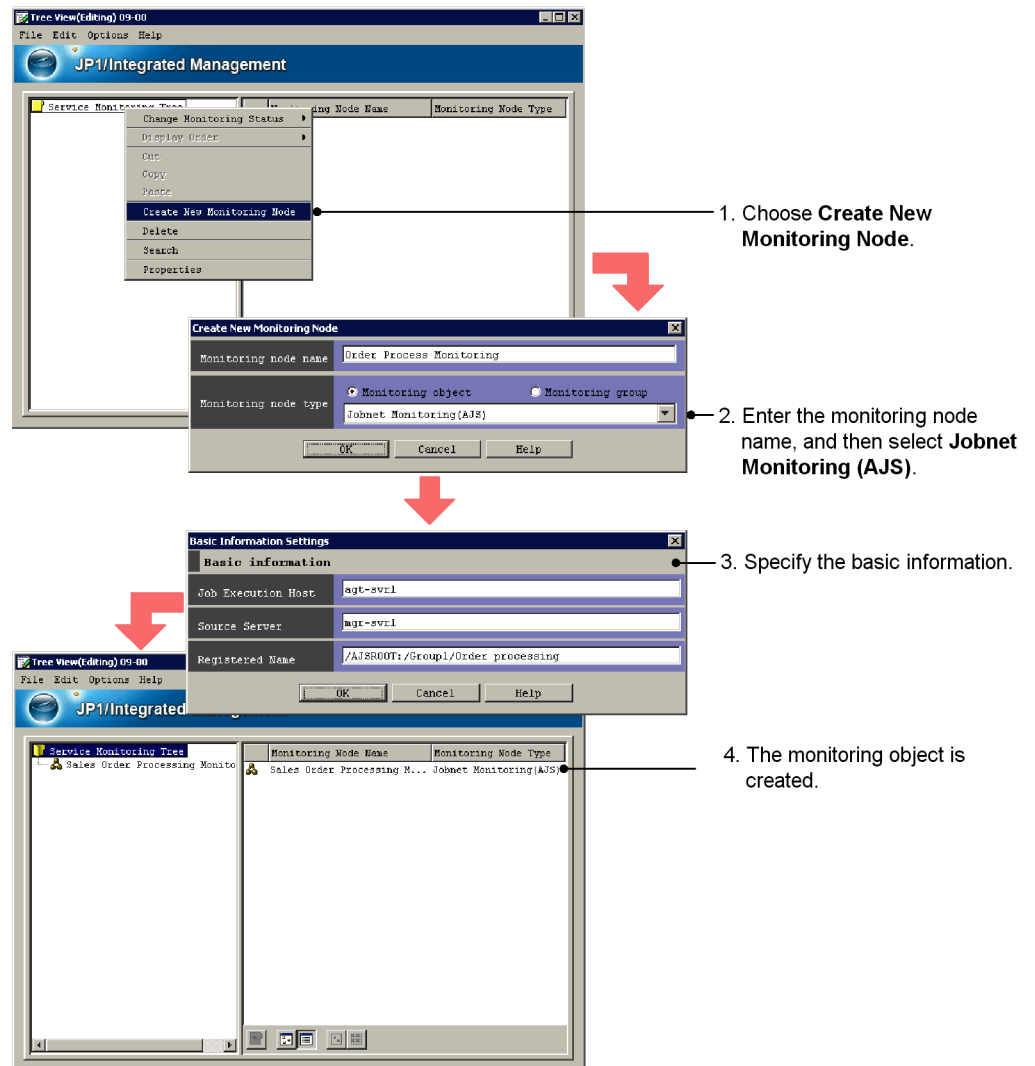
5.9 Examples of monitoring object creation

This section provides examples of manual creation of monitoring objects.

5.9.1 Example of creating system-monitoring objects (JP1/AJS jobnet monitoring)

This subsection presents an example of creating a system-monitoring object that monitors the execution status of JP1/AJS jobnet `AJSROOT:/Group1/Order_Processing`.

Figure 5-17: Example of creating a system-monitoring object



1. Open the Create New Monitoring Node window.

Use one of the following methods to open the window:

- Select a monitoring group, and then from the right-click pop-up menu, choose **Create New Monitoring Node**.
- Select a monitoring group, and then from the menu bar, choose **Edit**, then **Create New Monitoring Node**.

- To open the window from the details area, right-click with no monitoring node selected, and from the displayed pop-up menu, choose **Create New Monitoring Node**.

If there are no monitoring nodes, use the menu bar or the pop-up menu that is displayed by right-clicking in the monitoring tree area.

2. Enter a name for the monitoring node, and then select **Jobnet Monitoring (AJS)**.

Set the following items in the Create New Monitoring Node window:

- **Monitoring node name**

Specify any name.

- **Monitoring node type**

Select **Jobnet Monitoring (AJS)**.

3. Specify the basic information for the monitoring node.

In the Basic Information Settings window, specify the following information.

Table 5-5: Example of basic information for a monitoring node

Monitoring node attribute name	Attribute value to be entered (example)	Description
Job execution host	agt-svr1	Host where the job is executed. Enter the name of the JP1/AJS agent that is to execute the job.
Event-issuing server	mgr-svr1	Host that issues JP1 events. In JP1/AJS, enter the name of the JP1/AJS manager.
Registration name	AJSROOT:/Group/ Order_Processing	Enter a complete name in the format shown below; specification of job group names is optional: <i>scheduler-service-name:/job-group-name-1/ job-group-name-2/.../jobnet-name</i>

4. The monitoring object is created.

The monitoring object that monitors the execution status of the JP1/AJS jobnet AJSROOT:/Group/Order_Processing is created.

5.9.2 Example of creating a general-purpose monitoring object (HiRDB monitoring)

This subsection explains how to create and set up a monitoring object for monitoring HiRDB version 6. This example uses the message log events (JP1/SES event: 0x00010C03) that are output by HiRDB as the status change condition for the monitoring object.

Reference note:

HiRDB version 07-02 or later can issue JP1 events, not JP1/SES events (the output settings are required at HiRDB). In this case, use the system-monitoring object provided by Central Scope to create a monitoring object for HiRDB.

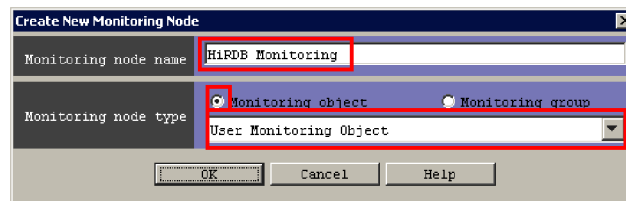
(1) Creating a monitoring object (HiRDB monitoring)

To create a monitoring object:

1. From the Monitoring Tree window, choose **Options**, and then **Edit Tree**.
The Monitoring Tree (Editing) window appears.
2. From the **File** menu, choose **Open Tree**.
Open the monitoring tree to which the monitoring object for HiRDB is to be added
3. In the tree area, select the location where the monitoring object for HiRDB is to be added.
4. From the **Edit** menu, choose **Create New Monitoring Node**.

The Create New Monitoring Node window appears.

Figure 5-18: Create New Monitoring Node window



The settings in the Create New Monitoring Node window are as follows.

Table 5-6: Settings in the Create New Monitoring Node window

Item	Setting
Monitoring node name	Enter any name. We recommend that you assign a name that is easy to manage. This example enters HiRDB Monitoring.
Monitoring node type	Select the Monitoring object radio button, and select User Monitoring Object from the list box.

5. Click the **OK** button.

The monitoring object HiRDB Monitoring is added to the monitoring tree.

(2) Setting up the monitoring object (HiRDB monitoring)

(a) Setting the basic information for the monitoring object

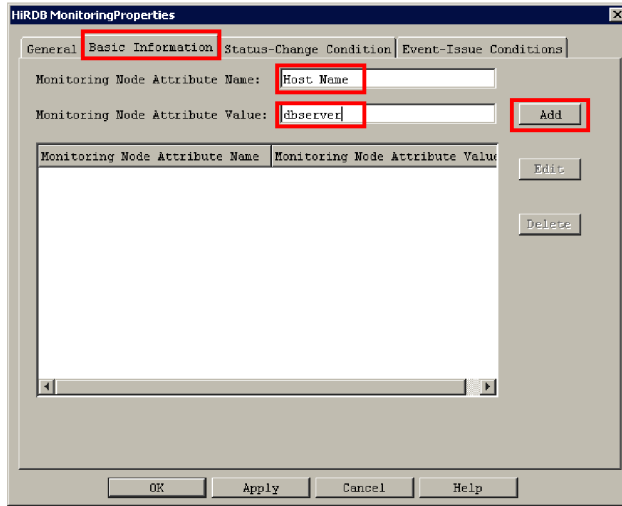
To set the basic information for the monitoring object:

1. Select the newly created monitoring object.
2. From the **Edit** menu, choose **Properties**.

The Properties window appears.

3. Choose the **Basic Information** page.

Figure 5-19: Basic Information page



The settings on the **Basic Information** page are as follows.

Table 5-7: Settings on the Basic Information page

Item	Setting
Monitoring node attribute name	Enter any name. We recommend that you assign a name that is easy to remember, such as a host name.
Monitoring node attribute value	Enter any value. This is the value for the name entered in Monitoring node attribute name . If you entered a host name in Monitoring node attribute name , enter a value such as the host name displayed by the <code>hostname</code> command, or a value that is easily associated with the product. This example enters <code>dbserver</code> as a value that is easily associated with HiRDB.

You can specify the monitoring node basic information specified here as the search

condition when you search for a monitoring node. The basic information has no effect on monitoring object status change.

4. Click the **Add** button.

The basic information is set for the monitoring object.

(b) Setting the status change condition for the monitoring object

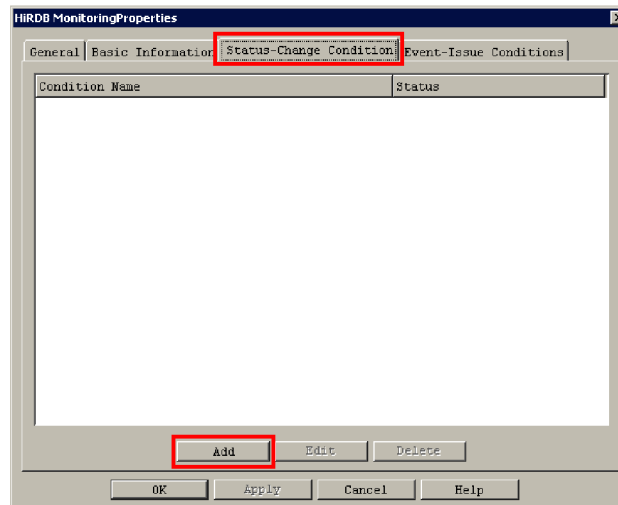
To set the status change condition for the monitoring object:

1. Select the newly created monitoring object.
2. From the **Edit** menu, choose **Properties**.

The Properties window appears.

3. Choose the **Status-Change Condition** page.

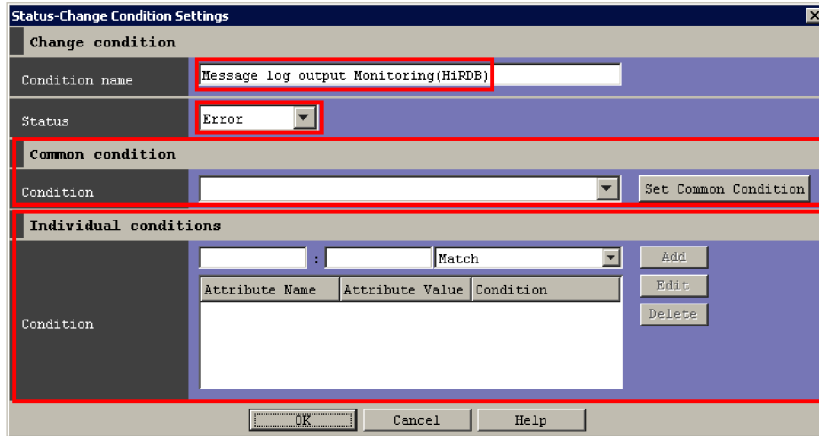
Figure 5-20: Status-Change Condition page



4. Click the **Add** button.

The Status-Change Condition Settings window appears.

Figure 5-21: Status-Change Condition Settings window



The settings in the Status-Change Condition Settings window are as follows.

Table 5-8: Settings in the Status-Change Condition Settings window

Item	Setting
Condition name	Specify a name for the condition.
Status	From the list box, select the status to which the monitoring object is to change when an event is received.
Common condition	Specify information needed to identify the event or the product that caused the event. The details are provided below.
Individual conditions	Specify information needed to identify the location where the event occurred. The details are provided below.

- After you have entered a condition name, status, common condition, and individual condition, click the **OK** button.

Specifying the common condition:

For the common condition, specify the information needed to identify the event or the product that caused the event.

To specify the common condition:

- Click the **Set Common Condition** button.
The Common Condition Settings window appears.

2. Click the **Add** button.

The Common Condition Detailed Settings window appears.

Figure 5-22: Common Condition Detailed Settings window

The settings in the Common Condition Detailed Settings window are as follows.

Table 5-9: Settings in the Common Condition Detailed Settings window

Item	Setting
Common condition name	Specify a name for the common condition.
Message	Specify the message for the JP1 event (in this example, a JP1/SES event). Specify this information if you want to monitor only a specific message. In the case of HiRDB, specify a JP1/SES event message that is issued by HiRDB. For example, if you enter <code>KFPS01222-I</code> and select Match prefix , you can monitor only the HiRDB log swap messages.
Event ID	Specify the event ID of the JP1 event (in this example a JP1/SES event) to be monitored. For a product that issues JP1/SES events such as HiRDB, specify the basic code of JP1/SES events (<code>00010C03</code>).

5. Setting up Central Scope

3. Click the **OK** button.

The Common Condition Settings window is displayed again.

4. Click the **Close** button.

The Status-Change Condition Settings window is displayed again.

5. Select the created common condition.

The created common condition is added to the list box. Select the created common condition.

Specifying the individual conditions:

In individual conditions, specify conditions needed to identify the location where the event occurred, such as the name of the host resulting in a failure.

To specify the individual conditions:

1. Enter the name and value of an attribute and then click the **Add** button.

The individual condition is added. Repeat this step as many times as there are individual conditions to be added.

The settings for individual conditions are as follows.

Table 5-10: Settings for individual conditions

Attribute name	Attribute value	Description
B . SOURCESERVER	dbserver	For the attribute name, enter B . SOURCESERVER to narrow down the source of the event (host) that is to be reported. For the attribute value, enter the name of the host where the HiRDB system manager is running.

Attribute name	Attribute value	Description
B . MESSAGE	<i>HiRDB-server-name</i>	<p>If product-specific message information is output as event information, use that message information for narrowing.</p> <p>This is because the message may contain information that identifies the location where the event occurred (such as a message log event issued by HiRDB).</p> <p>If you want to identify the location of the event on the basis of information in the message, enter B . MESSAGE as the attribute name and a keyword that can be narrowed down as the attribute value.</p> <p>For example, log swap messages of HiRDB contain a HiRDB server name. If you specify B . MESSAGE as the attribute name and <i>HiRDB-server-name</i> as the attribute value, and select Regular expression from the list box, you can monitor only those log swaps that occur at a specific HiRDB server.</p> <p>If you specify B . MESSAGE, make sure that no message that is not monitored satisfies the conditions.</p>

Note that detailed information for JP1/SES events cannot be specified in the status change conditions.

(c) Updating the edited monitoring tree

To update the edited monitoring tree in order to use it:

1. In the Monitoring Tree (Editing) window, from the **File** menu, choose **Update Server Tree**.

The HiRDB monitoring node is added to the monitoring object database of Central Scope.

Chapter

6. Operation and Environment Configuration in a Cluster System

JP1/IM - Manager supports operation in a cluster system. If you employ cluster operation in JP1/IM - Manager, processing can be inherited from the primary node to the secondary node in the event of a server failure, thereby achieving uninterrupted integrated system operations management.

This chapter describes cluster operation in JP1/IM - Manager and the setup procedure.

Before you use this function, make sure that your cluster software supports JP1/IM - Manager.

- 6.1 Overview of cluster operation
- 6.2 Environment setup for cluster operation (for Windows)
- 6.3 Environment setup for cluster operation (for UNIX)
- 6.4 Notes about cluster operation
- 6.5 Logical host operation and environment configuration in a non-cluster system

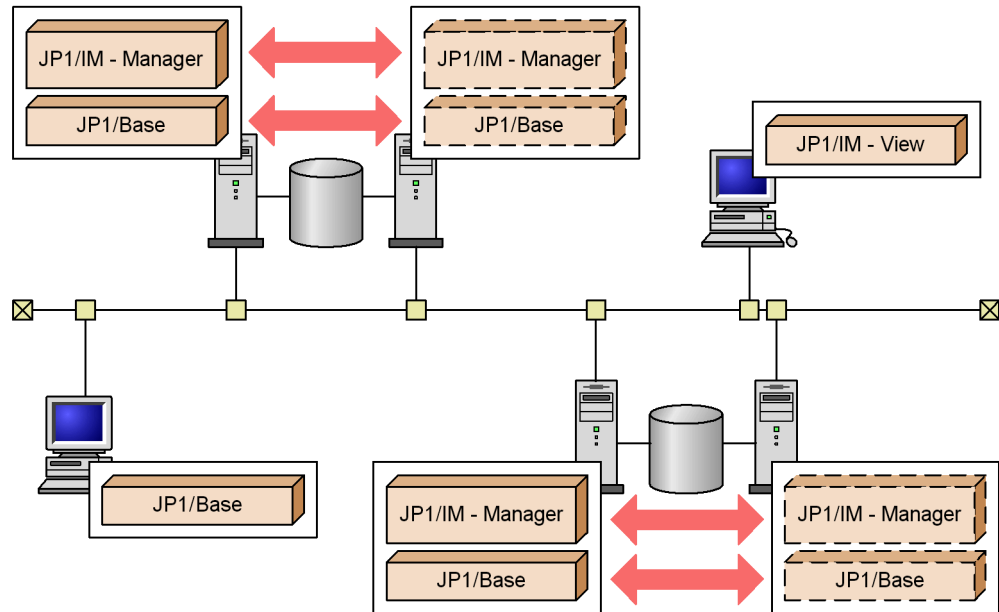
6.1 Overview of cluster operation

JP1/IM - Manager supports operation in a cluster system. If you employ cluster operation in JP1/IM - Manager, processing can be inherited from the primary node to the secondary node in the event of a server failure, thereby achieving uninterrupted system operations management.

Note that a cluster system is the same as what has been referred to as a *node switching system* in JP1 manuals.

To run JP1/IM - Manager in a cluster system, the following configuration is used.

Figure 6-1: Example of a JP1/IM configuration in a cluster system



This section describes JP1/IM - Manager operation in a cluster system, starting with an overview of cluster systems through an explanation of JP1/IM - Manager functions in a cluster system.

To apply cluster operation to JP1/IM - Manager, you must run both JP1/IM - Manager and JP1/Base in the same logical host environment.

For details about cluster operation in JP1/Base, see the description of settings for cluster system operation in the *Job Management Partner 1/Base User's Guide*.

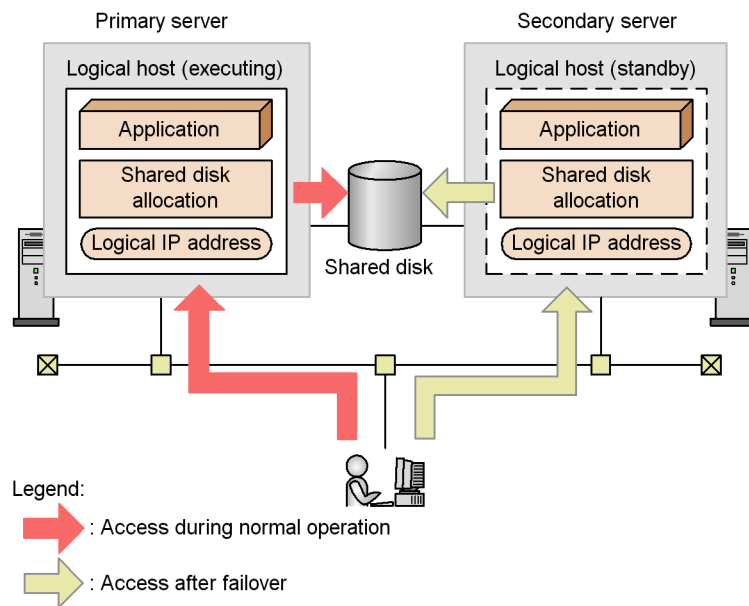
This section focuses on using a cluster system to achieve high availability (HA); it does not describe use of a cluster system for such purposes as evening out load distribution.

6.1.1 Overview of a cluster system

A cluster system consists of a primary server being used to execute processing and a secondary server that will inherit processing in the event of a failure. If a failure occurs, processing is transferred from the primary node to the secondary node to prevent interruption of jobs, thereby improving availability. Transferring processing in the event of a failure is called *failover*.

The software that controls the entire cluster system is called the *cluster software*. The cluster software monitors system operations and executes failover in the event of a failure in order to prevent interruption of jobs.

Figure 6-2: Access after failover during normal operation



To enable an application such as JP1/IM - Manager to perform failover, you must run the application on a *logical host*. A logical host is a logical server unit for failover that is controlled by the cluster software. The logical host uses a *logical host name* and has a *shared disk* and a *logical IP address* that can be inherited from the primary node to the secondary node. Applications that run on the logical host store data on the shared disk and use the logical IP address for communication so that they can execute failover without having to depend on the physical servers.

Running JP1/IM - Manager in the logical host environment of a cluster system is called *cluster operation*.

Reference note:

About the term *logical host*

This manual uses the term *logical host* to designate a failover unit. Some cluster software and applications use the term *group* or *package*. Check your cluster software manual for the corresponding term.

As opposed to the logical host that is the failover unit, a physical server is called a *physical host*. The host name used by the physical host (host name that is displayed when the `hostname` command is executed) is called a *physical host name*, and the IP address that corresponds to the physical host name is called the *physical IP address*. For the disk, a physical host uses the *local disk*. This disk is specific to the server and cannot be inherited to any other server.

6.1.2 Prerequisites for cluster operation

JP1/IM - Manager runs in a logical host environment in a cluster system and supports failover. The prerequisites for running JP1/IM - Manager in a logical host environment are the allocation and release of the shared disk and logical IP addresses, and normal control of operation monitoring by the cluster software.

Note:

Depending on the system configuration and environment configuration, the cluster software supported by JP1/IM - Manager may not always meet the prerequisites described here. Evaluate the system configuration and environment configuration so that the prerequisites are satisfied.

(1) Prerequisites for the logical host environment

When JP1/IM - Manager is to be run in a logical host environment, the prerequisites with respect to logical IP addresses and the shared disk that are described in the table below must be satisfied.

Table 6-1: Prerequisites for the logical host environment

Logical host component	Prerequisites
Shared disk	<ul style="list-style-type: none"> • A shared disk that can be inherited from the primary node to the secondary node must be available. • The shared disk must have been allocated before JP1 was started. • Allocation of the shared disk cannot be released during JP1 execution. • Release of the shared disk allocation must not occur until after JP1 has terminated. • The shared disk must be managed so that it will not be accessed illegally by multiple nodes. • Files must be protected by a method such as a file system with a journal function so that the files will not be deleted in the event of a system shutdown, etc. • The contents of files must be protected and inherited in the event of a failover. • Forced failover must be available in the event the shared disk is being used by a process at the time of a failover. • In the event of a failure on the shared disk, the cluster software must be able to manage the recovery procedure so that JP1 does not have to handle the recovery. If JP1 needs to be started or terminated as an extension of recovery processing, the cluster software must issue the startup or termination request to JP1.
Logical IP addresses	<ul style="list-style-type: none"> • Inheritable logical IP addresses must be available for communications. • It must be possible for a unique logical IP address to be obtained from the logical host name. • The logical IP addresses must be allocated before JP1 starts. • The logical IP addresses cannot be deleted during JP1 execution. • The correspondence between the logical host name and a logical IP address cannot change during JP1 execution. • The logical IP addresses must not be deleted until after JP1 has terminated. • In the event of a network failure, the cluster software must be able to manage the recovery procedure so that JP1 does not have to handle the recovery. If JP1 needs to be started or terminated as an extension of recovery processing, the cluster software must issue the startup or termination request to JP1.

If any the above conditions is not satisfied, problems such as the following may occur during JP1 operation:

- Data written by the primary node becomes corrupted during failover
Normal operation cannot be achieved due to problems with JP1, such as errors, data loss, or startup failure.
- Recovery processing is disabled due to a LAN board failure
JP1 cannot operate normally due to communication errors until the LAN boards are swapped or a failover to another server is achieved by a means such as the cluster software.

(2) Prerequisites for the physical host environment

In a cluster system where JP1/IM - Manager is run on a logical host, the physical host environment for each server must meet the prerequisites described below.

Table 6-2: Prerequisites for the physical host environment

Physical host component	Prerequisites
Server core	<ul style="list-style-type: none"> • The physical host environment must utilize a cluster configuration consisting of two or more server systems. • CPU performance must be high enough for processing to be executed. (For example, if multiple logical hosts are run concurrently, the CPU must be capable of handling the processing.) • There must be sufficient real memory for the processing that is to be executed. (For example, if multiple logical hosts are run concurrently, the size of the real memory must be adequate.)
Disk	<ul style="list-style-type: none"> • Files must be protected by a method such as a file system with the journal function so that files will not be lost in the event of a system shutdown.
Network	<ul style="list-style-type: none"> • It must be possible to establish communication using IP addresses that correspond to the physical host names (result of execution of the <code>hostname</code> command).[#] (It must not be possible for a program such as the cluster software to set a status that disables communication.) • Correspondence between host names and IP addresses cannot be changed during JP1 operation. (It must not be possible for programs, such as the cluster software and name server, to change the correspondence.) • In Windows, the LAN board corresponding to a host name must have priority in the network bind settings. (Priority cannot be given to any other LAN board, such as for heartbeat.)
OS, cluster software	<ul style="list-style-type: none"> • JP1 must support the cluster software and version being used. • All patches and service packs required by JP1 and the cluster software must have been installed. • Each server's environment must have been set up appropriately so that the same processing can be performed in the event of failover.

#

With some cluster software, the IP address corresponding to a physical host name (host name displayed by the `hostname` command) may not be usable for communication. In such a case, JP1 cannot be run in the physical host environment. Use JP1 only in the logical host environment.

(3) JP1's support range

When JP1 is run on a logical host in a cluster system, the range controlled by JP1 is

JP1 itself. Control of the logical host environment (shared disk and logical IP addresses) and the JP1 startup and termination timing depend on the control by the cluster software.

If the prerequisites for the logical host environment and physical host environment discussed above are not satisfied, or there are problems in the control of the logical host environment, there will be problems with the JP1 operations as well. In such a case, the problems must be dealt with by the OS and cluster software that controls the logical host environment.

6.1.3 JP1/IM configuration in a cluster system

To run JP1/IM - Manager in a cluster system, you must execute JP1/IM - Manager and JP1/Base under the control of the cluster software and be able to handle failovers. This subsection describes the configuration of JP1/IM in a cluster system.

(1) Overview of a JP1/IM configuration in a cluster operation system

Table 6-3: JP1/IM configuration in a cluster system

Product name	JP1/IM configuration in a cluster system
JP1/IM - View	<ul style="list-style-type: none"> • Use the logical IP address to connect from JP1/IM - View to JP1/IM - Manager. • Run JP1/IM - View itself in the physical host environment.
JP1/IM - Manager	<ul style="list-style-type: none"> • JP1/IM - Manager can be run in the logical host environment. • JP1/IM - Manager supports failover if it is registered in the cluster software. • To register JP1/IM - Manager into the cluster software, you need logical IP addresses and a shared disk resource. • Definition information is stored on the shared disk and is inherited during failover. • Multiple logical hosts can be executed by a single server. Therefore, JP1/IM - Manager can be run in a cluster system with an active-standby configuration as well as an active-active configuration. • Execute JP1/IM - Manager on the same logical host as for the required JP1/Base.

(2) File organization on the shared disk

The files described below are created on the shared disk when you set up JP1/IM - Manager in a logical host environment. These files are required in order to execute JP1/IM - Manager on a logical host.

(a) In Windows*Table 6-4: File organization on the shared disk (Windows)*

Function	Type of shared file	Folder name
Central Console	Definition file	<i>shared-folder\jplcons\conf\</i>
	Log file	<i>shared-folder\jplcons\log\</i>
	Temporary file	<i>shared-folder\jplcons\tmp\</i>
	History file [#]	<i>shared-folder\jplcons\operation\</i>
Central Scope	Definition file	<i>shared-folder\jplscope\conf\</i>
	Log file	<i>shared-folder\jplscope\log\</i>
	Temporary file	<i>shared-folder\jplscope\tmp\</i>
	Database	<i>shared-folder\jplscope\database\</i>
IM Configuration Management	Definition file	<i>shared-folder\JP1IMM\conf\imcf\</i>
	Log file	<i>shared-folder\JP1IMM\log\imcf\</i>
	Temporary file	<i>shared-folder\JP1IMM\tmp\</i>
	IM configuration data and profile data	<i>shared-folder\JP1IMM\data\imcf\</i>
IM database	Database	<i>user-specified-folder-on-shared-disk\imdb</i>

[#]: Event Generation Service processing is output as the history.

(b) In UNIX*Table 6-5: File organization on the shared disk (UNIX)*

Function	Type of shared file	Directory name
Central Console	Definition file	<i>shared-directory/jplcons/conf/</i>
	Log file	<i>shared-directory/jplcons/log/</i>
	Temporary file	<i>shared-directory/jplcons/tmp/</i>
	History file [#]	<i>shared-directory/jplcons/operation/</i>

Function	Type of shared file	Directory name
Central Scope	Definition file	<i>shared-directory/jp1scope/conf/</i>
	Log file	<i>shared-directory/jp1scope/log/</i>
	Temporary file	<i>shared-directory/jp1scope/tmp/</i>
	Database	<i>shared-directory/jp1scope/database/</i>
IM Configuration Management	Definition file	<i>shared-directory/jp1imm/conf/imcf/</i>
	Log file	<i>shared-directory/jp1imm/log/imcf/</i>
	Temporary file	<i>shared-directory/jp1imm/tmp/</i>
	IM configuration data and profile data	<i>shared-directory/jp1imm/data/imcf/</i>
IM database	Database	<i>user-specified-directory-on-shared-disk/imdb</i>

#: Event Generation Service processing is output as the history.

(3) Services and processes of JP1/IM - Manager

JP1/IM - Manager in a cluster operation system executes the services or processes of the logical host.

(a) In Windows

If you set up JP1/IM - Manager in the logical host environment, the services listed below are registered in Windows. To use these services, you must register them in the cluster software.

Table 6-6: Services of JP1/IM - Manager (Windows)

Displayed name	Service name
JP1/Console_ <i>logical-host-name</i>	JP1_Console_ <i>logical-host-name</i>
JP1/IM-Manager DB Cluster Service_ <i>logical-host-name</i> ^{#1}	HiRDBEmbeddedEdition_JM<n> ^{#2}

#1

Registered when IM databases are used.

#2

<n> is a number from 0 to 9; it is the value of LOGICALHOSTNUMBER in the cluster setup information file. For details, see *Cluster setup information file (jimdbclustersetupinfo.conf)* in 2. Definition Files in the manual *Job Management*

Partner 1/Integrated Management - Manager Command and Definition File Reference.

The *Displayed name* column indicates the name that is displayed by choosing **Control Panel, Administrative Tools**, and then **Services**. To use `net` commands (`net start` and `net stop`) to control the services from the cluster software, specify these names in the `net` commands.

The names in the *Service name* column are used to register services into the cluster software shown below. Specify these names as service names in MSCS or WSFC.

- In Windows Server 2003
MSCS (Microsoft(R) Cluster Service)
- In Windows Server 2008
WSFC (Windows Server(R) Failover Cluster)

(b) In UNIX

When you execute JP1/IM - Manager on the logical host, the process corresponding to the logical host is run.

The process name is the argument with the logical host name attached. For details about the process names, see *B. List of Processes* in the *Job Management Partner 1/Integrated Management - Manager Overview and System Design Guide*.

(4) Communication method

When you set up JP1/IM - Manager on the logical host, the communication method for JP1/IM - Manager is set to what is called the *IP binding method*. The IP binding method is applied to both logical and physical host environments.

The two types of communication methods are the *IP binding method* and the *ANY binding method*. These methods determine how the IP address used for communication is to be allocated (bound) by internal processing.

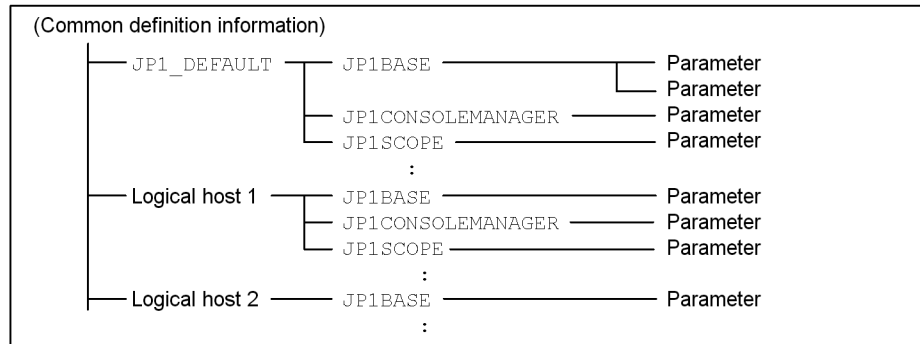
For details about the communication methods, see the descriptions of the JP1/Base communication methods in the *Job Management Partner 1/Base User's Guide*. JP1/IM - Manager uses the same communication methods as JP1/Base.

(5) Setting common definition information

When you set up JP1/IM - Manager on the logical host, settings for the logical host are set as common definition information.

The common definition information is managed by JP1/Base in the database that stores JP1 settings. The settings are stored in the format shown below on the local disk of each server.

Figure 6-3: Common definition information



The common definition information for the physical host (JP1_DEFAULT) is stored separately from the common definition information for the logical host. You use the `jbssetcnf` command to set the information for each physical and logical host, and you use the `jbsgetcnf` command to read the information.

The common definition information for the logical host must be the same for each server. When you perform setup or if you change the settings, copy the common definition information from the primary server where the settings are specified to the secondary server.

JP1/IM - Manager, JP1/Base, JP1/AJS, and JP1/Power Monitor (06-02 or later) use the common definition information to store the settings.

6.2 Environment setup for cluster operation (for Windows)

This section describes the environment setup for JP1/IM - Manager that supports cluster operation.

6.2.1 Environment setup procedure

The following figure shows the setup procedure.

Figure 6-4: Setup procedure (when upgrading the existing logical host environment)

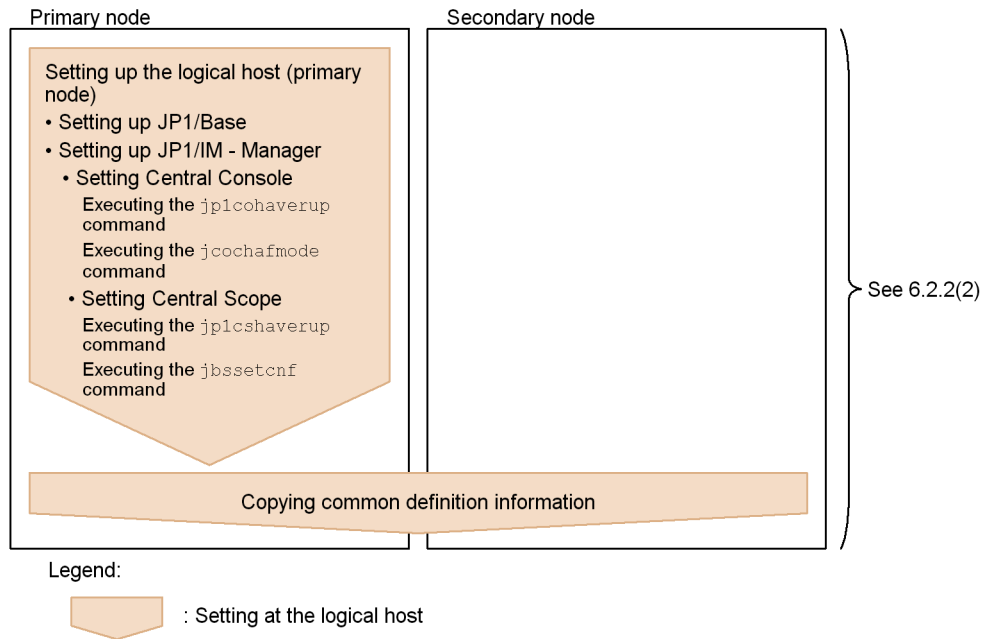
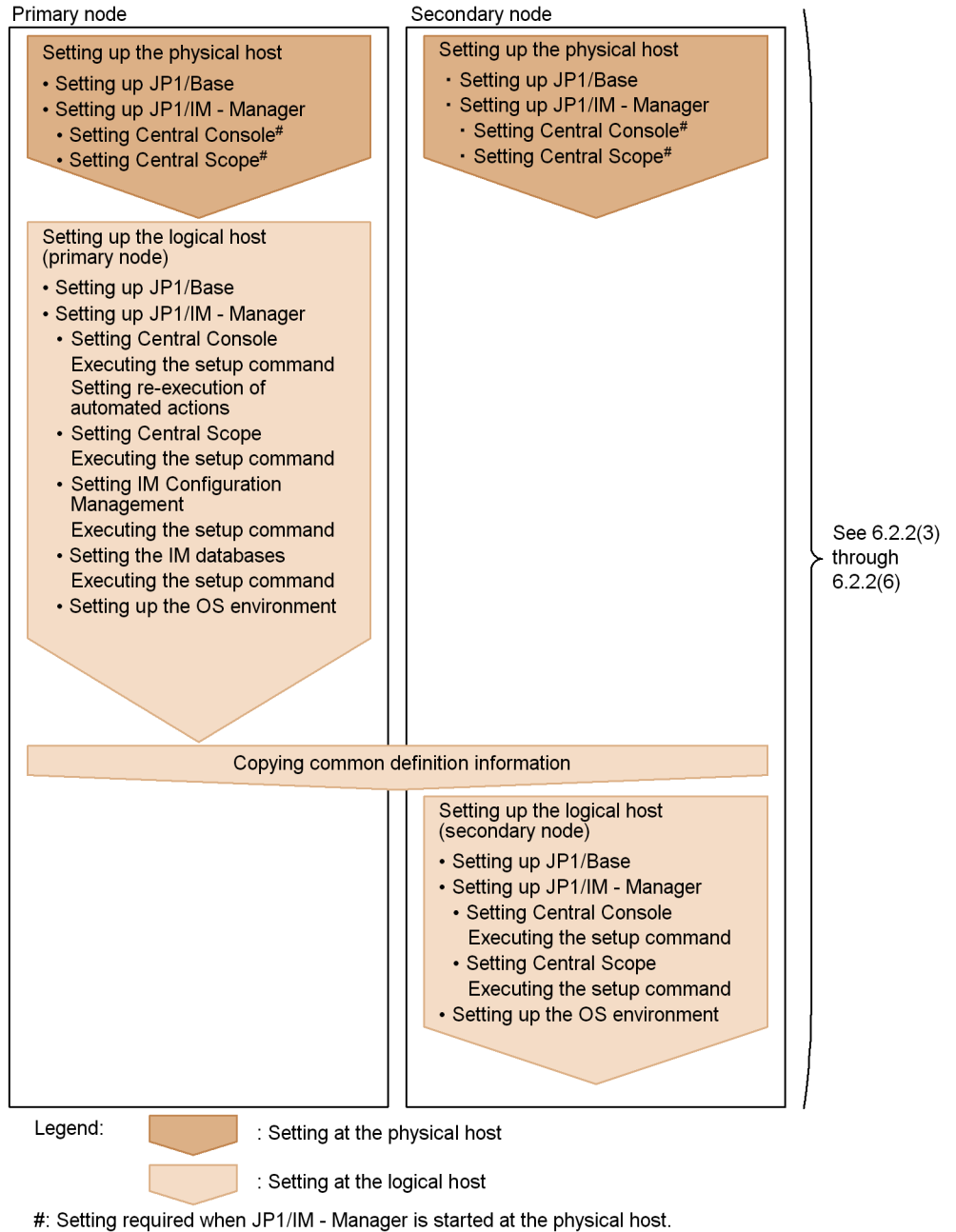


Figure 6-5: Setup procedure (when setting up a new environment)



6.2.2 Installing and setting up the logical host

This subsection describes the installation and setup of the logical host for JP1/IM - Manager. It also describes the setup of JP1/Base because JP1/Base must be set up on the same logical host.

Before you start the procedure, check the following information about the cluster system.

Table 6-7: Items to be checked before you install and set up the logical host (Windows)

Item to be checked	Description
Logical host name	Name of the logical host that executes JP1
Logical IP address	IP address that corresponds to the logical host name
Shared folder	Folder on the shared disk that stores a set of files for the JP1 execution environment on the logical host

Additionally, make sure that these items satisfy the prerequisites described in *6.1.2 Prerequisites for cluster operation*.

Once you have finished checking the above items, you are ready to start the installation and setup.

(1) Installing

Install JP1/IM - Manager and JP1/Base on the local disk of both the primary server and the secondary server. If you are upgrading, back up the settings and database before you start the installation (for the backup method, see the manual for the old version).

To install:

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

Use an installation folder and disk that have the same names on the primary server and the secondary server.

Do not install these programs on the shared disk.

(2) Setup during upgrading

If you are upgrading a logical host environment that has been set up under the previous version of JP1/IM - Manager, follow the setup procedure described below. If you are setting up a new environment, see *6.2.2(3) Setting up the physical host environment* through *6.2.2(6) Setting up the logical host (secondary node)*.

(a) Setting up the primary node

If you use the functions of Central Scope, steps 6 through 8 are required. If you do not use the functions of Central Scope, skip steps 6 through 8.

To set up the primary node:

1. Terminate JP1/IM - Manager.

Terminate the JP1/IM - Managers in both the physical and the logical host environments.

2. Set up a logical host environment for JP1/Base.

If you have upgraded JP1/Base, see the notes about installation and uninstallation in the *Job Management Partner 1/Base User's Guide* and then perform the setup. If you have not upgraded JP1/Base, there is no need to perform this setup.

3. Make sure that the shared disk is available.

4. Execute the `jplcohaberup` command.

```
jplcohaberup -h logical-host-name
```

5. If you want to change the location of the event acquisition filter to Event Base Service, execute the `jcochafmode` command.

```
jcochafmode -h logical-host-name
```

6. Check the available disk capacity.

To upgrade JP1/IM - Manager, you need as much free space on the hard disk as the disk capacity under *shared-folder*\JP1Scope\database\.

7. Execute the `jplcshaverup.bat` command.

```
jplcshaverup.bat -h logical-host-name -w work-folder
```

8. Execute the `jbssetcnf` command.

Whether the following functions are enabled or disabled depends on the settings in the old version of JP1/IM - Manager or Central Scope:

- Completed-action linkage function
- Monitoring of the maximum number of status change events

If these functions are currently disabled but you want to enable them, execute the `jbssetcnf` command using the files shown in the table below as arguments.

Table 6-8: Settings files for enabling the functions

File name	Description
action_complete_on.conf	File for enabling the completed-action linkage function

File name	Description
evhist_warn_event_on.conf	File for enabling the function for issuing JP1 events when the number of status change events for the monitoring object exceeds the maximum value (100).

9. Back up the common definition file.

```
jbsgetcnf -h logical-host-name >
common-definition-information-backup-file-name
```

(b) Setting up the secondary node

To set up the secondary node:

1. Terminate JP1/IM - Manager.
Terminate the JP1/IM - Managers in both the physical and the logical host environments.
2. Copy the common definition information backup file that was backed up at the primary node to the secondary node.
Use a method such as FTP.
3. Set the common definition information.

```
jbssetcnf common-definition-information-backup-file-name
```

(3) Setting up the physical host environment

At each server, set up the physical host environment for JP1/Base and JP1/IM - Manager.

To set up the physical host environment:

1. Set up the physical host environment for JP1/Base.
2. Set up the physical host environment for JP1/IM - Manager.

For details about how to set up JP1/Base, see the *Job Management Partner 1/Base User's Guide*.

The setup procedure for JP1/IM - Manager is the same as for non-cluster operation. See *1. Installation and Setup (for Windows)*. If you will not be using JP1/IM - Manager at the physical host, there is no need to perform this setup.

(4) Setting up the logical host environment (primary node)

(a) Preparations for setup

To prepare for setup:

1. Make sure that JP1 is stopped.

Make sure that the services of JP1/IM and JP1/Base are stopped on the physical host and all logical hosts.

2. Make sure that the shared disk is available.

(b) Setting up JP1/Base

To set up JP1/Base:

1. Set up the logical host for JP1/Base (primary node).

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

2. Set up a command execution environment for JP1/Base.

For details, see *1.16 Setting up a command execution environment*.

(c) Setting up JP1/IM - Manager

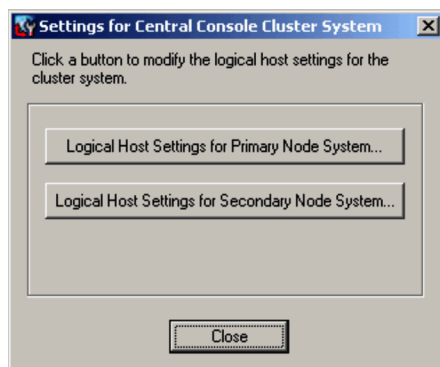
■ Setting JP1/IM - Manager (Central Console)

To set JP1/IM - Manager (Central Console):

1. Open the setup window for the logical host of JP1/IM - Manager (Central Console).

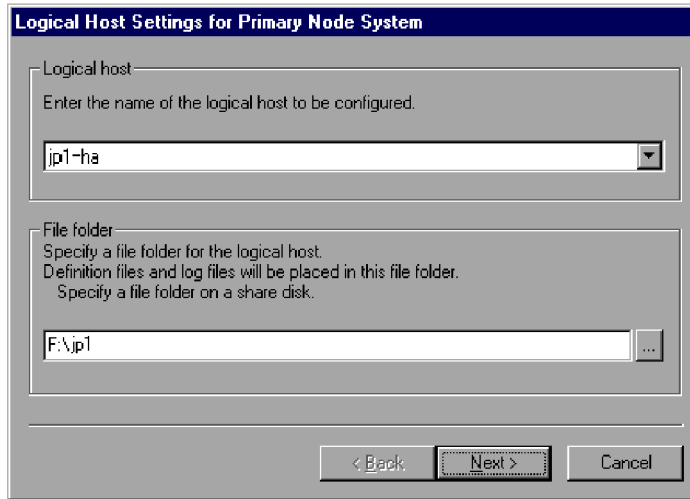
When you execute `Console-path\bin\jplcohasetup.exe`, the following window appears.

Figure 6-6: Window for setting the logical host (primary node)



2. Click the **Logical Host Settings for Primary Node System** button.
The following window appears.

Figure 6-7: Window for setting the logical host (primary node)



Specify the logical host name and file folder.

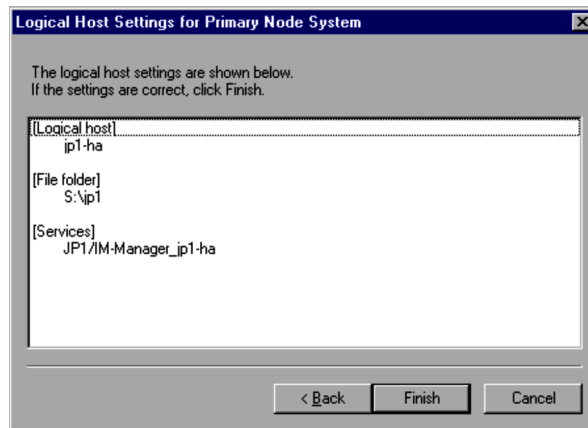
- Logical host name
The logical host names created in JP1/Base are displayed. Select the logical host name.
- File folder
Specify a folder on the shared disk. A set of JP1/IM - Manager files for the logical host is created under *specified-folder-name*\jp1cons\.

After you have specified the above information, click the **Next** button.

3. Check the settings.

The following window appears.

Figure 6-8: Window for setting the logical host (primary node)



Check the settings. If the settings are correct, click the **Finish** button.

To achieve correct failover operation, customize the environment settings for JP1/IM - Manager (Central Console) for the logical host.

4. Setting re-execution of automated actions.

Execute the following command to set re-execution of automated actions in the event of failover:

```
jcoimdef -r { EXE | OUTPUT | OFF } -h logical-host-name
```

Specifying EXE re-executes the actions whose status is **Wait**, **Send**, **Queue**, and **Running** in the event of failover; specifying OUTPUT outputs those actions to the actions list; specifying OFF executes no processing. Specify this setting according to your evaluation during the system design. This setting is optional.

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*.

■ Setting JP1/IM - Manager (Central Scope)

This subsection describes the setting procedure for using JP1/IM - Manager (Central Scope). The windows displayed for this setting are the same as for JP1/IM - Manager (Central Console) except for the title bar that displays Central Scope.

To set JP1/IM - Manager (Central Scope):

1. Open the window for setting the logical host for JP1/IM - Manager (Central Scope).

Execute `Scope-path\bin\jplcshasetup.exe`.

2. Click the **Logical Host Settings for Primary Node System** button.

In the Logical Host Settings for Primary Node System window, specify the logical host name and file folder.

- Logical host name

The logical host names created in JP1/Base are displayed. Select the logical host name.

- File folder

Specify a folder on the shared disk. A set of JP1/IM - Manager files for the logical host is created under the *specified-folder-name*\jp1scope\ folder.

After you have specified the above information, click the **Next** button.

3. Check the settings.

When the confirmation window appears, check the settings. If the settings are correct, click the **Finish** button.

■ Setting JP1/IM - Manager (IM Configuration Management)

This subsection describes the setting procedure for using JP1/IM - Manager (IM Configuration Management). The windows displayed for this setting are the same as for JP1/IM - Manager (Central Console) except for the title bar that displays Configuration Management.

To set JP1/IM - Manager (IM Configuration Management):

1. Open the window for setting the logical host for JP1/IM - Manager (IM Configuration Management).

Execute the *Manager-path*\bin\imcf\jp1cfhasetup.exe command.

2. Click the **Logical Host Settings for Secondary Node System** button.

In the Logical Host Settings for Secondary Node System window, specify the logical host name.

- Logical host name

Select the logical host that was set up at the primary server.

After you have specified the above information, click the **Next** button.

3. Check the settings.

When the confirmation window appears, check the settings. If the settings are correct, click the **Finish** button.

■ Setting JP1/IM - Manager (IM database)

This subsection describes the setting procedure for using JP1/IM - Manager (IM

database). You must create the IM databases in order to use the integrated monitoring database to manage JP1 events, and the IM Configuration Management database to manage the system hierarchy.

To set JP1/IM - Manager (IM database):

1. Edit the cluster setup information file.

Prepare a cluster setup information file that contains information about the size of the database area required for creating the IM databases and the database storage directory.

For details about the settings in the cluster setup information file, see *Cluster setup information file (jimdbclustersetupinfo.conf)* in 2. *Definition Files* in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.

2. Execute the `jcodbsetup` command to create an integrated monitoring database.


```
jcodbsetup -f cluster-setup-information-file-name -h logical-host-name
-c online [-q]
```

Use arguments to specify the cluster setup information file name, logical host name, setup type, and whether a message asking whether processing is to be continued is to be displayed.

- *cluster-setup-information-file-name* (-f option)

Specify the name of the cluster setup information file that was created in step 1.

- *logical-host-name* (-h option)

Specify the logical host name that was set up at the primary server.

- Setup type (-c option)

Specify the setup type (`online`) of the active host.

- Whether a message asking whether processing is to be continued is to be displayed (-q option)

If a message asking about execution of processing is not to be displayed after command execution, specify `-q`; if the message is to be displayed, do not specify `-q`.

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

3. Execute the `jcoimdef` command to enable the integrated monitoring database.


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

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*.

4. Execute the `jcfdbsetup` command to create an IM Configuration Management database.

```
jcfdbsetup -f cluster-setup-information-file-name -h logical-host-name  
-c online [-q]
```

Use arguments to specify the cluster setup information file name, logical host name, setup type, and whether a message asking whether processing is to be continued is to be displayed.

- *cluster-setup-information-file-name* (-f option)

Specify the name of the cluster setup information file that was created in step 1.

- *logical-host-name* (-h option)

Specify the logical host name that was set up at the primary server.

- Setup type (-c option)

Specify the setup type (`online`) of the active host.

- Whether a message asking whether processing is to be continued is to be displayed (-q option)

If a message asking about execution of processing is not to be displayed after command execution, specify `-q`; if the message is to be displayed, do not specify `-q`.

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

5. Execute the `jcoimdef` command to enable the IM Configuration Management database.

```
jcoimdef -cf ON -h logical-host-name
```

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*.

(d) Setting up an OS environment

In the event of an error, if the Dr. Watson dialog box and Microsoft error reporting dialog box are displayed, failover of JP1/IM - Manager may fail. Therefore, display of these dialog boxes must be suppressed.

■ **Setting Dr. Watson for Windows (for Windows Server 2003)**

To set Dr. Watson for Windows:

1. From the **Start** menu, choose **Run**.
2. In the text box, enter `drwtsn32` and then click the **OK** button.
The Dr. Watson for Windows dialog box appears.
3. Clear the **Visual Notification** check box.
4. Click the **OK** button.

■ **Suppressing Microsoft error reporting**

In Windows Server 2003:

1. In **Control Panel**, double-click **System**.
The System Properties dialog box appears.
2. On the **Advanced** page, click the **Error Reporting** button.
The Error Reporting dialog box appears.
3. Choose **Disable error reporting** and make sure that the **But notify me when critical errors occur** check box is not selected.
4. Click the **OK** button.

In Windows Server 2008:

1. In the **Run** text box, enter `wercn` and then click the **OK** button.
The Problem Reports and Solutions dialog box appears.
2. In the left-hand frame, click **Change settings**.
3. Choose **Advanced settings**.
4. In **Advanced settings for problem reporting**, choose **Off**, and then click the **OK** button.

Setup of the logical host at the primary server is now complete.

Make sure that the JP1/IM - Manager files for the logical host have been created on the shared disk and, if necessary, place the shared disk offline.

(5) Copying the common definition information

Copy the common definition information from the primary server to the secondary server.

The common definition information contains the settings needed to execute JP1/IM - Manager and JP1/Base on the logical host.

To copy the common definition information:

1. Back up the common definition information at the primary server.

At the primary node, execute the `jbsgetcnf` command to back up the common definition information.

```
jbsgetcnf -h logical-host-name >  
common-definition-information-backup-file-name
```

2. Copy the backup file from the primary server to the secondary server.

Use a method such as FTP.

3. Set the common definition information at the secondary server.

Use the backup file copied from the primary server to set the common definition information at the secondary server.

```
jbssetcnf common-definition-information-backup-file-name
```

Additionally, if you use the IM databases, the contents of the cluster setup information files at the primary and secondary servers must be identical. Copy the cluster setup information file that was used at the primary server to the secondary server. Store the copy in `Manager-path\conf\imdb\setup`.

(6) Setting up the logical host (secondary node)

(a) Preparations for setup

To prepare for setup:

1. Make sure that JP1 is stopped.

Make sure that all services of JP1/IM and JP1/Base are stopped on the physical host and all logical hosts.

Note that there is no need for the shared disk to be available for use at the secondary server.

(b) Setting up JP1/Base

To set up JP1/Base:

1. Set up the logical host (secondary node) for JP1/Base.

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

2. Set up a command execution environment for JP1/Base.

For details, see *1.16 Setting up a command execution environment*.

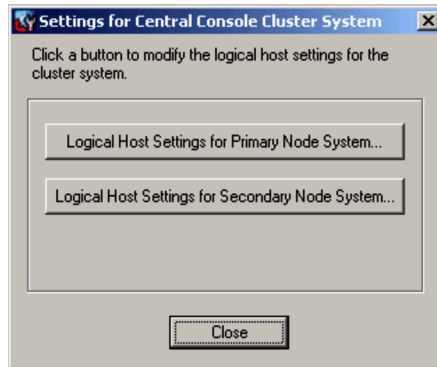
(c) Setting up JP1/IM - Manager**■ Setting JP1/IM - Manager (Central Console)**

To set JP1/IM - Manager (Central Console):

1. Open the setup window for the logical host of JP1/IM - Manager (Central Console).

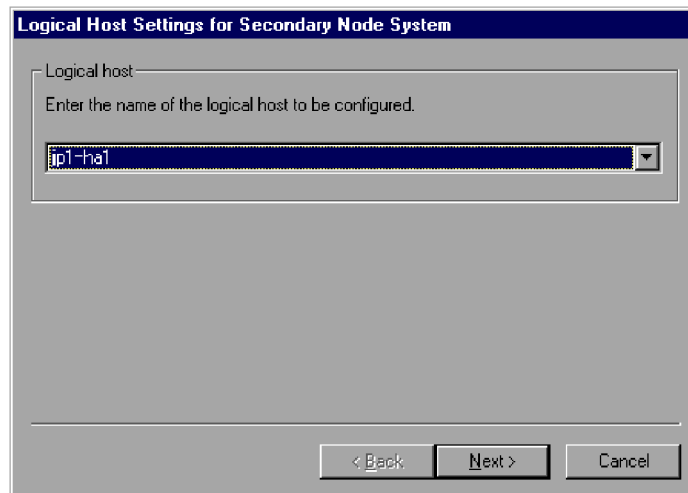
When you execute the *Console-path\bin\jp1cohasetup.exe* command, the following window appears.

Figure 6-9: Window for setting the logical host (secondary node)



2. Click the **Logical Host Settings for Secondary Node System** button. The following window appears.

Figure 6-10: Window for setting the logical host (secondary node)



Specify the logical host name.

- Logical host name

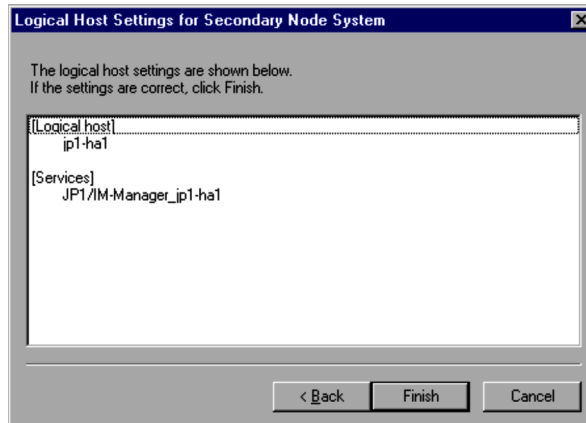
Select the logical host that was set up at the primary server.

After you have specified the above information, click the **Next** button.

3. Check the settings.

The following window appears.

Figure 6-11: Window for setting the logical host (secondary node)



Check the settings. If the settings are correct, click the **Finish** button.

■ Setting JP1/IM - Manager (Central Scope)

This subsection describes the setting procedure for using JP1/IM - Manager (Central Scope). The windows displayed for this setting are the same as for JP1/IM - Manager (Central Console) except for the title bar that displays Central Scope.

To set JP1/IM - Manager (Central Scope):

1. Open the window for setting the logical host for JP1/IM - Manager (Central Scope).

Execute the *Scope-path\bin\jp1cshasetup.exe* command.

2. Click the **Logical Host Settings for Secondary Node System** button.

In the Logical Host Settings for Secondary Node System window, specify the logical host name.

- Logical host name

Select the logical host that was set up at the primary server.

After you have specified the above information, click the **Next** button.

3. Check the settings.

When the confirmation window appears, check the settings. If the settings are correct, click the **Finish** button.

■ Setting JP1/IM - Manager (IM Configuration Management)

This subsection describes the setting procedure for using JP1/IM - Manager (IM Configuration Management). The windows displayed for this setting are the same as for JP1/IM - Manager (Central Console) except for the title bar that displays Configuration Management.

To set JP1/IM - Manager (IM Configuration Management):

1. Open the window for setting the logical host for JP1/IM - Manager (IM Configuration Management).

Execute the *Manager-path*\bin\imcf\jp1cfhsetup.exe command.

2. Click the **Logical Host Settings for Secondary Node System** button.

In the Logical Host Settings for Secondary Node System window, specify the logical host name.

- Logical host name

Select the logical host that was set up at the primary server.

After you have specified the above information, click the **Next** button.

3. Check the settings.

When the confirmation window appears, check the settings. If the settings are correct, click the **Finish** button.

■ Setting JP1/IM - Manager (IM database)

This subsection describes the setting procedure for using JP1/IM - Manager (IM database). You must create the IM databases in order to use the integrated monitoring database to manage JP1 events and the IM Configuration Management database to manage the system hierarchy.

To set JP1/IM - Manager (IM database):

1. Edit the cluster setup information file.

Prepare a cluster setup information file that contains information about the size of the database area required for creating the IM databases and the database storage directory. Check the contents of the cluster setup information file that was copied from the active host in 6.2.2(5) *Copying the common definition information*. The settings in the cluster setup information file must be the same as those specified at the primary node.

For details about the settings in the cluster setup information file, see *Cluster setup information file (jimdbclustersetupinfo.conf)* in 2. *Definition Files* in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.

2. Execute the `jcodbsetup` command to create an integrated monitoring database.
`jcodbsetup -f cluster-setup-information-file-name -h logical-host-name -c standby [-q]`

Use arguments to specify the cluster setup information file name, logical host name, setup type, and whether a message asking whether processing is to be continued is to be displayed.

- *cluster-setup-information-file-name* (-f option)
Specify the name of the cluster setup information file that was created in step 1.
- *logical-host-name* (-h option)
Specify the logical host name that was set up at the primary server.
- Setup type (-c option)
Specify the setup type (`standby`) of the standby host.
- Whether a message asking whether processing is to be continued is to be displayed (-q option)
If a message asking about execution of processing is not to be displayed after command execution, specify `-q`; if the message is to be displayed, do not specify `-q`.

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

3. Execute the `jcoimdef` command to enable the integrated monitoring database.
`jcoimdef -db ON -h logical-host-name`

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

4. Execute the `jcfdbsetup` command to create an IM Configuration Management database.
`jcfdbsetup -f setup-information-file-name -h logical-host-name -c standby [-q]`

Use arguments to specify the cluster setup information file name, logical host name, setup type, and whether a message asking whether processing is to be

continued is to be displayed.

- *cluster-setup-information-file-name* (-f option)
Specify the name of the cluster setup information file that was created in step 1.
- *logical-host-name* (-h option)
Specify the logical host name that was set up at the primary server.
- Setup type (-c option)
Specify the setup type (*standby*) of the active host.
- Whether a message asking whether processing is to be continued is to be displayed (-q option)
If a message asking about execution of processing is not to be displayed after command execution, specify -q; if the message is to be displayed, do not specify -q.

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

5. Execute the `jcoimdef` command to enable the IM Configuration Management database.

```
jcoimdef -cf ON -h logical-host-name
```

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*.

(d) Setting up an OS environment

If the Dr. Watson dialog box or the Microsoft error reporting dialog box is displayed when an error occurs, failover of JP1/IM - Manager may fail. Therefore, display of these dialog boxes must be suppressed.

■ Setting Dr. Watson for Windows (for Windows Server 2003)

To set Dr. Watson for Windows:

1. From the **Start** menu, choose **Run**.
2. In the text box, enter `drwtsn32` and then click the **OK** button.
The Dr. Watson for Windows dialog box appears.
3. Clear the **Visual Notification** check box.
4. Click the **OK** button.

■ Suppressing Microsoft error reporting

In Windows Server 2003:

1. In **Control Panel**, double-click **System**.
The System Properties dialog box appears.
2. On the **Advanced** page, click the **Error Reporting** button.
The Error Reporting dialog box appears.
3. Choose **Disable error reporting** and make sure that the **But notify me when critical errors occur** check box is not selected.
4. Click the **OK** button.

In Windows Server 2008:

1. In the **Run** text box, enter `wercn` and then click the **OK** button.
The Problem Reports and Solutions dialog box appears.
2. In the left-hand frame, click **Change settings**.
3. Choose **Advanced settings**.
4. In **Advanced settings for problem reporting**, choose **Off**, and then click the **OK** button.

Setup of the secondary node is now complete.

6.2.3 Registering into the cluster software (for Windows)

To apply cluster operation to JP1/IM - Manager, you must register JP1/IM - Manager and JP1/Base on the logical host into the cluster software, and then set them to be started and terminated by the cluster software.

The following table shows the settings for JP1/IM - Manager that are to be registered in the cluster software.

Table 6-9: Settings to be registered into the cluster software (Windows)

No.	Name	Service name	Dependencies
1	JP1/Base Event <i>logical-host-name</i>	JP1_Base_Event <i>logical-host-name</i>	IP address resource Physical disk resource
2	JP1/Base_ <i>logical-host-name</i>	JP1_Base_ <i>logical-host-name</i>	Cluster resource of No. 1
3	JP1/IM-Manager DB Cluster Service_ <i>logical-host-name</i> ^{#1}	HiRDBClusterService_JM<n> ^{#2}	Cluster resources of Nos. 1 and 2
4	JP1/IM - Manager_ <i>logical-host-name</i>	JP1_Console_ <i>logical-host-name</i>	Cluster resources of Nos. 1, 2, and 3 ^{#3}

#1

Registered in the cluster software only when the IM databases are used.

#2

<n> is a number from 0 to 9; it is the value specified in LOGICALHOSTNUMBER in the cluster setup information file. For details, see *Cluster setup information file (jimdbclustersetupinfo.conf)* in 2. *Definition Files* in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.

#3

If you do not use the IM databases, remove the cluster resource of No.3 from the dependencies.

(1) Registering into the cluster software

(a) In MSCS (Microsoft Cluster Service) or WSFC (Windows Server Failover Cluster)

Register the services of JP1/IM - Manager and JP1/Base as MSCS or WSFC resources. Set each resource as described below. Bold type indicates an MSCS setting item. For details about how to set WSFC, see the WSFC manual.

- For **Resource Types**, register as **Generic Service**.
- Set **Name**, **Dependencies**, and **Service name** as shown in the table. The name is used to display the service, and the service name is used to specify the service that is controlled from MSCS.
- Do not set **Start parameters** and **Registry Replication**.
- Set the **Advanced** page for properties according to whether failover is to occur in the event of a JP1/IM - Manager failure.

For example, to set failover to occur in the event of a JP1/IM - Manager failure, select the **Restart** and **Affect the group** check boxes and specify **Threshold** for the restart retry count; use 3 (times) as a guideline for the value to be specified.

(b) When registering the service start and stop commands

Register into the cluster software JP1/IM - Manager and the JP1/Base services to be started and stopped. For example, specify the settings so that the services shown in the *Name* column in the table above will be started and stopped by the `net` command.

To check the operation of JP1/IM - Manager and JP1/Base, use the following commands:

- `jco_spmd_status`

Use this command to check the operation of JP1/IM - Manager (except the IM

databases).

- `jimdbstatus`

Use this command to check the operation of the IM databases (when the IM databases are used).

- `jbs_spmd_status`

Use this command to check the operation of JP1/Base.

- `jevstat`

Use this command to check the operation of JP1/Base Event Service.

For details about how to use these commands, see 6.3.3 *Registering into the cluster software (for UNIX)*.

(2) Setting the resource start and stop sequence

To execute JP1/IM - Manager and JP1/Base on the logical host, the shared disk and logical IP address must be available for use.

Set the start and stop sequence or dependencies in such a manner that they are controlled by the cluster software as shown below.

- When the logical host starts

1. Allocate the shared disk and logical IP addresses, and make them available for use.
2. Start JP1/Base and JP1/IM - Manager, in this order.

- When the logical host terminates

1. Terminate JP1/IM - Manager and JP1/Base, in this order.
2. Release the allocation of the shared disk and logical IP addresses.

6.2.4 Procedures for changing settings

If you change the settings at the primary server after you have started operation in the cluster system, you must apply the changes to the secondary server so that the system is synchronized. If the system is not synchronized, secondary server operation may not match primary server operation in the event of a failover.

Change settings at both the primary and the secondary servers in the following cases.

(1) Changing settings in files

If you have edited the files listed below and used the `jbssetcnf` command to apply the settings, you must copy the common definition information from the primary server to the secondary server:

- Automated action environment definition file (`action.conf.update`)

- Communication environment definition file (`console.conf.update`)
- Settings file for the maximum number of status change events (`evhist_warn_event_xxx.conf`)
- Settings file for completed-action linkage function (`action_complete_xxx.conf`)
- Definition file for automatic delete mode of status change event
- Definition file for monitoring object initialization mode
- Automatic backup and recovery settings file for monitoring object database (`auto_dbbackup_xxx.conf`)
- Correlation event generation environment definition file
- Definition file for on memory mode of status change condition

Copy the common definition information using the setup procedure described in 6.2.2(5) *Copying the common definition information*.

The common definition information contains settings for JP1/Base, JP1/IM - Manager, JP1/AJS, and JP1/Power Monitor (06-02 or later). If these products have been set up on the logical host, the settings are also copied.

(2) Using commands to change settings

If you have used the `jcocmddef` or `jcochafmode` command to change settings, you must also specify the same settings at the primary and secondary servers.

- When the `jcochafmode` command was executed

If you have changed the location of the event acquisition filter by specifying the `-h` option, you must copy the common definition information from the primary server to the secondary server.

Copy the common definition information using the setup procedure described in 6.2.2(5) *Copying the common definition information*.

- When the `jcocmddef` command was executed

If you have changed the settings at the primary server by specifying the `-host` option, you must also specify the same settings at the secondary server. You can execute the `jcocmddef` command even when the shared disk is not mounted.

6.2.5 Deleting the IM databases and logical host

This subsection explains how to delete the logical host. When you delete the logical host, you must delete it at both the primary server and the secondary server.

If you use the IM databases (integrated monitoring database and IM Configuration Management database), you must delete them also (either before or after deleting the

logical host).

(1) **Deleting the IM databases**

This procedure is applicable when the IM databases (integrated monitoring database and IM Configuration Management database) are used.

If you are deleting the IM databases in order to reconfigure the environment, back up the databases beforehand. For details about the backup method, see *1.2 Managing the databases* in the *Job Management Partner 1/Integrated Management - Manager Administration Guide*.

To delete the IM databases:

1. Terminate JP1/IM - Manager.

Terminate all JP1/IM - Managers in both the physical and the logical host environments.

2. Execute the `jcodbunsetup` command to delete the integrated monitoring database.

```
jcodbunsetup -h logical-host-name -c {online|standby} [-q]
```

Use arguments to specify the logical host name, unsetup type, and whether a message asking whether processing is to be continued is to be displayed.

- *logical-host-name* (-h option)

Specify the logical host name that was set up at the primary server.

- Unsetup type (-c option)

To delete the integrated monitoring database at the active host, specify `online`; to delete the integrated monitoring database at the standby host, specify `standby`.

- Whether a message asking whether processing is to be continued is to be displayed (-q option)

If a message asking about execution of processing is not to be displayed after command execution, specify `-q`; if the message is to be displayed, do not specify `-q`.

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

3. Execute the `jcfdbunsetup` command to delete the IM Configuration Management database.

```
jcfdbunsetup -h logical-host-name -c {online|standby} [-q]
```

Use arguments to specify the logical host name, unsetup type, and whether a

message asking whether processing is to be continued is to be displayed.

- *logical-host-name* (-h option)
Specify the logical host name that was set up at the primary server.
- Unsetup type (-c option)
To delete the IM Configuration Management database at the active host, specify `online`; to delete the IM Configuration Management database at the standby host, specify `standby`.
- Whether a message asking whether processing is to be continued is to be displayed (-q option)
If a message asking about execution of processing is not to be displayed after command execution, specify -q; if the message is to be displayed, do not specify -q.

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

(2) Deleting the logical host

To delete a logical host in Windows, use the `jp1bshasetup.exe` command of JP1/Base.

To delete the logical host:

1. Execute the `jp1bshasetup.exe` command.
2. In the Settings for Base Node Switching System window, click the **Delete Logical Host** button.
3. Select the name of the logical host that you want to delete.
4. Click the **Next** button.
5. Check the deletion details and then click the **Finish** button.

The logical host is now deleted. Note that when you delete the logical host, JP1/Base, JP1/IM - Manager, JP1/AJS, and JP1/Power Monitor (06-02 or later) are all deleted in batch mode.

Shared files and shared folders on the shared disk are not deleted; you must delete them manually.

6.3 Environment setup for cluster operation (for UNIX)

This section describes the environment setup for JP1/IM - Manager that supports cluster operation.

6.3.1 Environment setup procedure

The following figure shows the setup procedure.

Figure 6-12: Setup procedure (when upgrading the existing logical host environment)

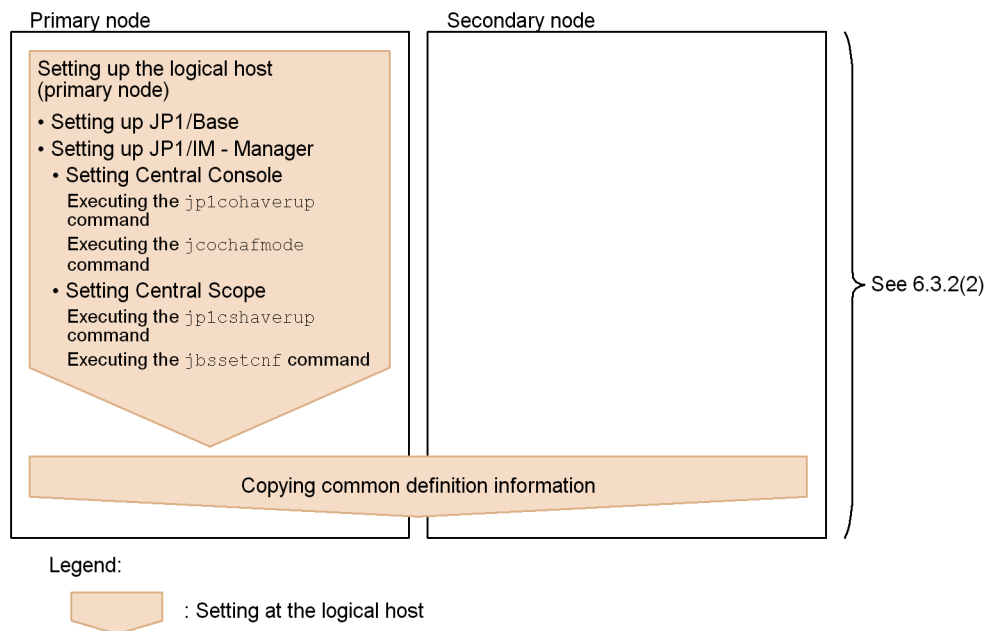
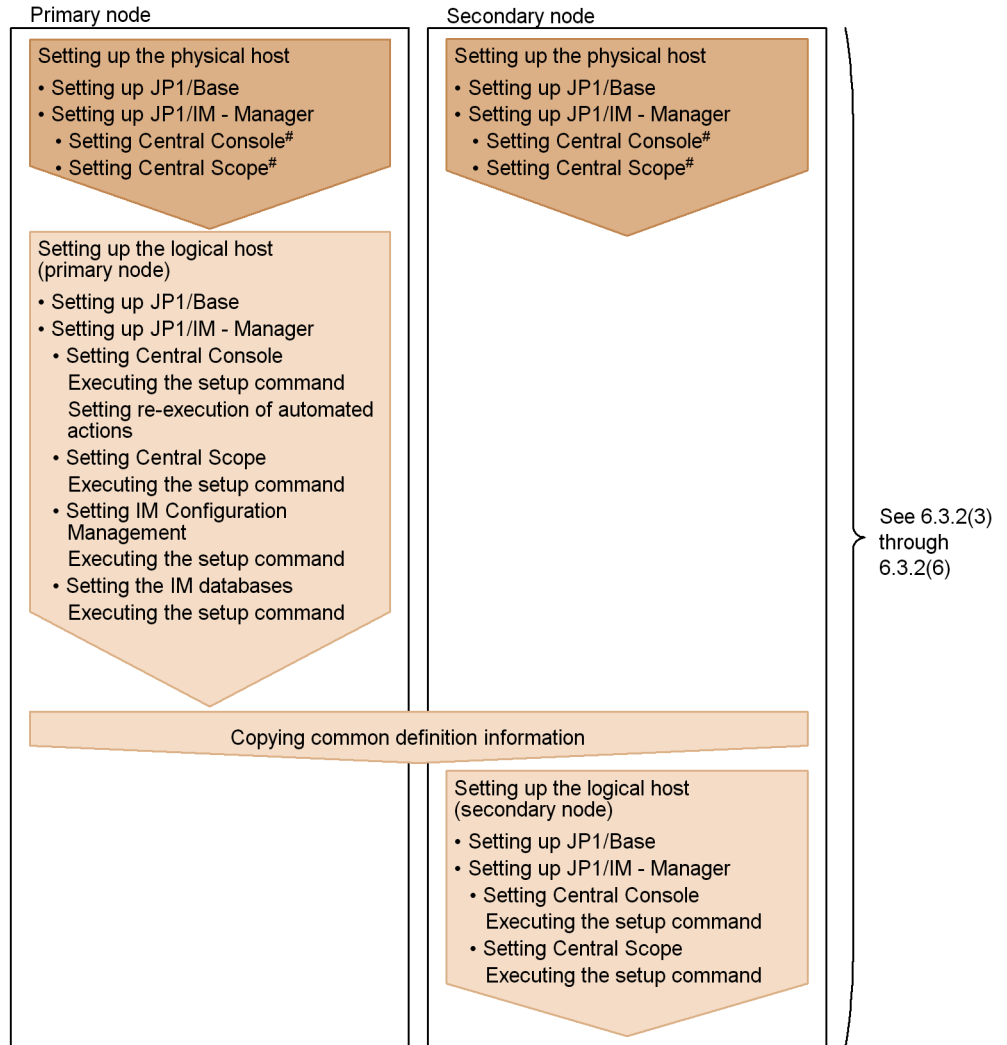


Figure 6-13: Setup procedure (when setting up a new environment)



Legend:

- : Setting at the physical host
- : Setting at the logical host

#: Setting required when JP1/IM - Manager is started at the physical host.

6.3.2 Installing and setting up the logical host

This subsection describes the installation and setup of the logical host for JP1/IM -

Manager. It also describes the setup of JP1/Base because JP1/Base must be set up on the same logical host.

Before you start the procedure, check the following information about the cluster system.

Table 6-10: Items to be checked before you install and set up the logical host (UNIX)

Item to be checked	Description
Logical host name	Name of the logical host that executes JP1
Logical IP address	IP address that corresponds to the logical host name
Shared folder	Folder on the shared disk that stores a set of files for the JP1 execution environment on the logical host

Additionally, make sure that these items satisfy the prerequisites described in *6.1.2 Prerequisites for cluster operation*.

Once you have finished checking the above items, you are ready to start the installation and setup.

(1) Installing

Install JP1/IM - Manager and JP1/Base on the local disk of both the primary server and the secondary server. If you are upgrading, back up the settings and database before you start the installation (for the backup method, see the manual for the old version).

To install:

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

Do not install these programs on the shared disk.

(2) Setup during upgrading

If you are upgrading the logical host environment, follow the setup procedure described below. If you are setting up a new environment, see *6.3.2(3) Setting up the physical host environment* through *6.3.2(6) Setting up the logical host (secondary node)*.

(a) Setting up the primary node

If you use the functions of Central Scope, steps 6 through 8 are required. If you do not use the functions of Central Scope, skip steps 6 through 8.

To set up the primary node:

1. Terminate JP1/IM - Manager.

Terminate the JP1/IM - Managers in both the physical and the logical host environments.

2. Set up a logical host environment for JP1/Base.

If you have upgraded JP1/Base, see the notes about installation and uninstallation in the *Job Management Partner 1/Base User's Guide* and then perform the setup. If you have not upgraded JP1/Base, there is no need to perform this setup.

3. Make sure that the shared disk is available.

4. Execute the `jplcohaberup` command.

```
/opt/jplcons/bin/jplcohaberup -h logical-host-name
```

5. If you want to change the location of the event acquisition filter to Event Base Service, execute the `jcochafmode` command.

```
/opt/jplcons/bin/jcochafmode -h logical-host-name
```

6. Check the available disk capacity.

To upgrade JP1/IM - Manager, you need as much free space on the hard disk as the disk capacity under `/var/opt/jplscope/database/`.

7. Execute the `jplcshaverup` command.

```
/opt/jplscope/bin/jplcshaverup -h logical-host-name -w  
work-directory
```

8. Execute the `jbssetcnf` command.

Whether the following functions are enabled or disabled depends on the settings in the old version of JP1/IM - Manager or Central Scope:

- Completed-action linkage function
- Monitoring of the maximum number of status change events

If these functions are currently disabled but you want to enable them, execute the `jbssetcnf` command using the files shown in the table below as arguments.

Table 6-11: Settings files for enabling the functions

File name	Description
<code>action_complete_on.conf</code>	File for enabling the completed-action linkage function
<code>evhist_warn_event_on.conf</code>	File for enabling the function for issuing JP1 events when the number of status change events for the monitoring object exceeds the maximum value (100).

1. Back up the common definition file.

```
/opt/jplbase/bin/jbsgetcnf -h logical-host-name >  
common-definition-information-backup-file-name
```

(b) Setting up the secondary node

To set up the secondary node:

1. Terminate JP1/IM - Manager.

Terminate the JP1/IM - Managers in both the physical and the logical host environments.

2. Copy the common definition information backup file that was backed up at the primary node to the secondary node.

Use a method such as FTP.

3. Set the common definition information.

```
/opt/jplbase/bin/jbssetcnf  
common-definition-information-backup-file-name
```

(3) Setting up the physical host environment

At each server, set up the physical host environment for JP1/Base and JP1/IM - Manager.

To set up the physical host environment:

1. Set up the physical host environment for JP1/Base.
2. Set up the physical host environment for JP1/IM - Manager.

For details about how to set up JP1/Base, see the *Job Management Partner 1/Base User's Guide*.

The setup procedure for JP1/IM - Manager is the same as for non-cluster operation. See 2. *Installation and Setup (for UNIX)*. If you will not be using JP1/IM - Manager at the physical host, there is no need to perform this setup.

(4) Setting up the logical host environment (primary node)

(a) Preparations for setup

To prepare for setup:

1. Make sure that JP1 is stopped.

Make sure that the processes of JP1/IM and JP1/Base are stopped on the physical host and all logical hosts.

2. Make sure that the shared disk is available.

Execute the `mount` command to make sure that the shared disk is mounted.

(b) Setting up JP1/Base

To set up JP1/Base:

1. Set up the logical host for JP1/Base (primary node).

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

2. Set up a command execution environment for JP1/Base.

For details, see 2.15 *Setting up a command execution environment*.

(c) Setting up JP1/IM - Manager**■ Setting JP1/IM - Manager (Central Console)**

To set JP1/IM - Manager (Central Console):

1. Execute the setup command for the logical host of JP1/IM - Manager (Central Console).

```
/opt/jp1cons/bin/jp1cc_setup_cluster -h logical-host-name -d shared-directory-name
```

Specify the logical host name and shared directory name using arguments.

- *logical-host-name* (-h option)

Specify the logical host name that was set in JP1/Base.

- *shared-directory-name* (-d option)

Specify a directory on the shared disk.

The *specified-directory-name*/jp1cons/ directory is created and a set of JP1/IM - Manager (Central Console) files for the logical host is created.

For details about the command, see *jp1cc_setup_cluster (UNIX only)* in 1. *Commands* in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.

To achieve correct failover operation, customize the environment settings for JP1/IM - Manager for the logical host.

2. Setting re-execution of automated actions.

Execute the following command to set re-execution of automated actions in the event of failover:

```
/opt/jp1cons/bin/jcoimdef -r { EXE | OUTPUT | OFF } -h logical-host-name
```

Specifying EXE re-executes the actions whose status is **Wait**, **Send**, **Queue**, and **Running** in the event of failover; specifying OUTPUT outputs those actions to the

actions list; specifying `OFF` executes no processing. Specify this setting according to your evaluation during the system design. This setting is optional.

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*.

■ Setting JP1/IM - Manager (Central Scope)

1. Execute the setup command for the logical host of JP1/IM - Manager (Central Scope).

```
/opt/jp1scope/bin/jp1cs_setup_cluster -h logical-host-name -d shared-directory-name
```

Specify the logical host name and shared directory name using arguments.

- *logical-host-name* (-h option)

Specify the logical host name that was set in JP1/Base.

- *shared-directory-name* (-d option)

Specify a directory on the shared disk.

The *specified-directory-name/jp1scope/* directory is created and a set of JP1/IM - Manager (Central Scope) files for the logical host is created.

For details about the command, see *jp1cs_setup_cluster (UNIX only)* in *1. Commands* in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.

■ Setting JP1/IM - Manager (IM Configuration Management)

To specify settings for using JP1/IM - Manager (IM Configuration Management):

1. Execute the setup command for the logical host of JP1/IM - Manager (IM Configuration Management).

```
/opt/jp1imm/bin/imcf/jp1cf_setup_cluster -h logical-host-name -d shared-directory-name
```

Specify the logical host name and shared directory name using arguments.

- *logical-host-name* (-h option)

Specify the logical host name that was set in JP1/Base.

- *shared-directory-name* (-d option)

Specify a directory on the shared disk.

When you execute `jp1cf_setup_cluster`, the following directories are created:

- *shared-directory*/jp1imm/conf/imcf
- *shared-directory*/jp1imm/tmp
- *shared-directory*/jp1imm/log/imcf
- *shared-directory*/jp1imm/data/imcf

For details about the command, see *jp1cf_setup_cluster (UNIX only)* in 1. *Commands* in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.

■ Setting JP1/IM - Manager (IM database)

This subsection describes the setting procedure for using JP1/IM - Manager (IM databases). You must create the IM databases in order to use the integrated monitoring database to manage JP1 events and the IM Configuration Management database to manage the system hierarchy.

To set JP1/IM - Manager (IM database):

1. Edit the cluster setup information file.

Prepare a cluster setup information file that contains information about the size of the database area required for creating the IM databases and the database storage directory.

For details about the settings in the cluster setup information file, see *Cluster setup information file (jimdbclustersetupinfo.conf)* in 2. *Definition Files* in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.

2. Execute the `jcodbsetup` command to create an integrated monitoring database.


```
jcodbsetup -f cluster-setup-information-file-name -h logical-host-name
-c online [-q]
```

Use arguments to specify the cluster setup information file name, logical host name, setup type, and whether a message asking whether processing is to be continued is to be displayed.

- *cluster-setup-information-file-name* (-f option)

Specify the name of the cluster setup information file that was created in step 1.

- *logical-host-name* (-h option)

Specify the logical host name that was set up at the primary server.

- Setup type (-c option)

Specify the setup type (`online`) of the active host.

- Whether a message asking whether processing is to be continued is to be displayed (-q option)

If a message asking about execution of processing is not to be displayed after command execution, specify -q; if the message is to be displayed, do not specify -q.

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

3. Execute the `jcoimdef` command to enable the integrated monitoring database.
`jcoimdef -db ON -h logical-host-name`

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*.

4. Execute the `jcfdbssetup` command to create an IM Configuration Management database.

```
jcfdbssetup -f cluster-setup-information-file-name -h logical-host-name  
-c online [-q]
```

Use arguments to specify the cluster setup information file name, logical host name, setup type, and whether a message asking whether processing is to be continued is to be displayed.

- `cluster-setup-information-file-name` (-f option)

Specify the name of the cluster setup information file that was created in step 1.

- `logical-host-name` (-h option)

Specify the logical host name that was set up at the primary server.

- Setup type (-c option)

Specify the setup type (`online`) of the active host.

- Whether a message asking whether processing is to be continued is to be displayed (-q option)

If a message asking about execution of processing is not to be displayed after command execution, specify -q; if the message is to be displayed, do not specify -q.

For details about the `jcfdbssetup` command, see `jcfdbssetup` in *1. Commands* in

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

- Execute the `jcoimdef` command to enable the IM Configuration Management database.

```
jcoimdef -cf ON -h logical-host-name
```

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*.

Setup of the logical host at the primary server is now complete.

Make sure that the JP1/IM - Manager files for the logical host have been created on the shared disk and, if necessary, unmount the shared disk.

(5) Copying the common definition information

Copy the common definition information from the primary server to the secondary server.

The common definition information contains the settings needed to execute JP1/IM - Manager and JP1/Base on the logical host.

To copy the common definition information:

- Back up the common definition information at the primary server.

At the primary node, execute the `jbsgetcnf` command to back up the common definition information.

```
/opt/jplbase/bin/jbsgetcnf -h logical-host-name >
common-definition-information-backup-file-name
```

- Copy the backup file from the primary server to the secondary server.

Use a method such as FTP.

- Set the common definition information at the secondary server.

Use the backup file copied from the primary server to set the common definition information at the secondary server.

```
/opt/jplbase/bin/jbssetcnf
common-definition-information-backup-file-name
```

Additionally, if you use the IM databases, the contents of the cluster setup information files at the primary and secondary servers must be identical. Copy the cluster setup information file that was used at the primary server to the secondary server. Store the copy in `/etc/opt/jplimm/conf/imdb/setup/`.

(6) Setting up the logical host (secondary node)

(a) Preparations for setup

To prepare for setup:

1. Make sure that JP1 is stopped.

Make sure that all processes of JP1/IM and JP1/Base are stopped on the physical host and all logical hosts.

Note that there is no need for the shared disk to be available for use at the secondary server.

(b) Setting up JP1/Base

To set up JP1/Base:

1. Set up the logical host (secondary node) for JP1/Base.

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

2. Set up a command execution environment for JP1/Base.

For details, see *2.15 Setting up a command execution environment*.

(c) Setting up JP1/IM - Manager

■ Setting JP1/IM - Manager (Central Console)

To set JP1/IM - Manager (Central Console):

1. Execute the setup command for the logical host of JP1/IM - Manager (Central Console).

```
/opt/jplcons/bin/jplcc_setup_cluster -h logical-host-name
```

Specify the logical host name by using an argument.

- *logical-host-name* (-h option)

Specify the logical host name that was set up at the primary server.

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

■ Setting JP1/IM - Manager (Central Scope)

To set JP1/IM - Manager (Central Scope):

1. Execute the setup command for the logical host of JP1/IM - Manager (Central Scope).

```
/opt/jplscope/bin/jplcs_setup_cluster -h logical-host-name
```

Specify the logical host name by using an argument.

- *logical-host-name* (-h option)

Specify the logical host name that was set up at the primary server.

For details about the command, see *jp1cs_setup_cluster (UNIX only)* in *1. Commands* in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.

Setup of the secondary node is now complete.

■ Setting JP1/IM - Manager (IM Configuration Management)

To specify settings for using JP1/IM - Manager (IM Configuration Management):

1. Execute the setup command for the logical host of JP1/IM - Manager (IM Configuration Management).

```
/opt/jp1imm/bin/imcf/jp1cf_setup_cluster -h logical-host-name
```

Specify the logical host name by using an argument.

- *logical-host-name* (-h option)

Specify the logical host name that was set in JP1/Base.

When you execute *jp1cf_setup_cluster*, the following directories are created:

- *shared-directory*/jp1imm/conf/imcf
- *shared-directory*/jp1imm/tmp
- *shared-directory*/jp1imm/log/imcf
- *shared-directory*/jp1imm/data/imcf

For details about the command, see *jp1cf_setup_cluster (UNIX only)* in *1. Commands* in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.

■ Setting JP1/IM - Manager (IM database)

This subsection describes the setting procedure for using JP1/IM - Manager (IM database). You must create the IM databases in order to use the integrated monitoring database to manage JP1 events and the IM Configuration Management database to manage the system hierarchy.

To set JP1/IM - Manager (IM database):

1. Edit the cluster setup information file.

Prepare a cluster setup information file that contains information about the size of the database area required for creating the IM databases and the database storage

directory. Check the contents of the cluster setup information file that was copied from the active host in 6.3.2(5) *Copying the common definition information*. The settings in the cluster setup information file must be the same as those specified at the primary node.

For details about the settings in the cluster setup information file, see *Cluster setup information file (jimdbclustersetupinfo.conf)* in 2. *Definition Files* in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.

2. Execute the `jcodbsetup` command to create an integrated monitoring database.


```
jcodbsetup -f cluster-setup-information-file-name -h logical-host-name
-c standby [-q]
```

Use arguments to specify the cluster setup information file name, logical host name, setup type, and whether a message asking whether processing is to be continued is to be displayed.

- *cluster-setup-information-file-name* (-f option)

Specify the name of the cluster setup information file that was created in step 1.

- *logical-host-name* (-h option)

Specify the logical host name that was set up at the primary server.

- Setup type (-c option)

Specify the setup type (`standby`) of the standby host.

- Whether a message asking whether processing is to be continued is to be displayed (-q option)

If a message asking about execution of processing is not to be displayed after command execution, specify `-q`; if the message is to be displayed, do not specify `-q`.

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

3. Execute the `jcoimdef` command to enable the integrated monitoring database.


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

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

4. Execute the `jcfdbssetup` command to create an IM Configuration Management database.

```
jcfdbsetup -f cluster-setup-information-file-name -h logical-host-name
-c standby [-q]
```

Use arguments to specify the cluster setup information file name, logical host name, setup type, and whether a message asking whether processing is to be continued is to be displayed.

- *cluster-setup-information-file-name* (-f option)
Specify the name of the cluster setup information file that was created in step 1.
- *logical-host-name* (-h option)
Specify the logical host name that was set up at the primary server.
- Setup type (-c option)
Specify the setup type (*standby*) of the standby host.
- Whether a message asking whether processing is to be continued is to be displayed (-q option)
If a message asking about execution of processing is not to be displayed after command execution, specify -q; if the message is to be displayed, do not specify -q.

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

5. Execute the `jcoimdef` command to enable the IM Configuration Management database.

```
jcoimdef -cf ON -h logical-host-name
```

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*.

6.3.3 Registering into the cluster software (for UNIX)

To apply cluster operation to JP1/IM - Manager, you must register JP1/IM - Manager and JP1/Base on the logical host into the cluster software, and then set them to be started and terminated by the cluster software.

(1) Creating a script to be registered into the cluster software

When you use UNIX cluster software, you normally use a method such as a script to create a tool to control applications, and then register the script into the cluster software. In general, such a script must provide the start, stop, operation monitoring, and forced termination functions.

This subsection describes the JP1/IM - Manager information that is needed to design a script. You use this information to create a script that controls JP1/IM - Manager according to the cluster software specifications, and then you register the script into the cluster software.

Table 6-12: Detailed information for script design in cluster registration

Function to be registered	Description
Start	<p>Starts JP1/IM - Manager.</p> <ul style="list-style-type: none"> • Command to be used <code>jco_start.cluster logical-host-name</code> • Start command termination timing The start command waits for JP1/IM - Manager to start before it terminates itself. However if the startup processing is not completed within the timeout period (60 seconds is the default) due to some problem, the command terminates without completing the startup processing. In such a case, the command terminates with the startup processing still underway (the command does not cancel the startup processing). • Check the start command result The script should determine the result of starting JP1/IM - Manager by the operation monitoring method described below. Normally, the result is determined by the cluster software's operation monitoring. The return value of the start command is 0 (normal termination) or 1 (argument error); therefore, the result cannot be determined from the return value.
Stop	<p>Terminates JP1/IM - Manager.</p> <ul style="list-style-type: none"> • Command to be used <code>jco_stop.cluster logical-host-name</code> • Stop command termination timing The stop command waits for JP1/IM - Manager to terminate before it terminates itself. However if the stop processing is not completed within the timeout period (60 seconds is the default) due to some problem, the command terminates without completing the stop processing. In such a case, the command terminates with the stop processing still underway (the command does not cancel the stop processing). • Check the stop command result The script should determine the result of terminating JP1/IM - Manager by the operation monitoring method described below. The return value of the stop command is 0 (normal termination) or 1 (argument error); therefore, the result cannot be determined from the return value. <p>We recommend that you execute the forced termination command described below after the stop command has terminated. This enables you to terminate the process and prevent a failover error even in the event of a problem.</p>

Function to be registered	Description
JP1/IM - Manager operation monitoring ^{#1}	<p>Monitors normal operation of JP1/IM - Manager.</p> <ul style="list-style-type: none"> Command to be used <code>jco_spmc_status -h logical-host-name</code> <p>To determine whether JP1/IM - Manager is running normally, check the return value of the <code>jco_spmc_status</code> command. This command determines the status from the operating status of each process.</p> <p>Some cluster software does not provide the operation monitoring function. If there is no need to perform failover in the event of a JP1/IM - Manager failure, do not register this function.</p> <ul style="list-style-type: none"> Check the operation monitoring result <p>The following explains how to interpret the return value:</p> <p>Return value = 0 (all running): JP1/IM - Manager is running normally.</p> <p>Return value = 1 (error): An unrecoverable error occurred. Treat this as a failure.</p> <p><i>Note:</i> If you were to execute the <code>jco_spmc_status</code> command at the secondary server whose shared disk is offline, the return value will be 1 because the shared disk is not available.</p> <p>Return value = 4 (partially stopped): Some JP1/IM - Manager processes are stopped due to a problem. Treat this as a failure.</p> <p>Return value = 8 (all stopped): All JP1/IM - Manager processes are stopped due to a problem. Treat this as a failure.</p> <p>Return value = 12 (retriable error): While the <code>jco_spmc_status</code> was checking the operating status, an error that can be recovered by retries has occurred. Retry checking the operating status as many times as specified.</p>

Function to be registered	Description
IM database operation status checking ^{#2}	<p>Checks to see if the IM databases are running normally.</p> <ul style="list-style-type: none"> Command to be used <code>jimdbstatus -h <i>logical-host-name</i></code> <p>To determine the operating status, check the return value of the <code>jimdbstatus</code> command.</p> <ul style="list-style-type: none"> Check the operating status result The following explains how to interpret the return value: Return value = 0: Running Return value = 1: The <code>jimdbstatus</code> command terminated abnormally. Return value = 4: Start or stop processing is underway. Return value = 8: Stopped (IM database is in restart-interrupted status and is unstable) Return value = 12: Stopped (stopped normally) Return value = 16: Not running (only the Windows service control program is running; IM database core is not running) Return value = 20: Installed HiRDB has not been set up. Return values 1 and 4 are subject to retries. Return values 8 and above indicate an error and are subject to failover.
Forced termination	<p>Forcibly terminates JP1/IM - Manager and releases the current resources.</p> <ul style="list-style-type: none"> Command to be used <code>jco_killall.cluster <i>logical-host-name</i></code> <p>The <code>jco_killall.cluster</code> command forcibly terminates each process without performing JP1/IM - Manager termination processing.</p> <p><i>Note:</i> Before you execute forced termination, use the stop command to terminate JP1/IM - Manager.</p>

#1

The commands used for JP1 operations related to operation checking are the same between UNIX and Windows, but the operations are different.

Windows operations differ from UNIX operations due to their association with Windows service control. In Windows, when some of the processes terminate, the JP1 process management terminates each process automatically and places the service in stopped status. Treat service stop as an error or detect an error when a command such as `jco_spmc_status` returns a value of 8.

#2

Executed when the IM databases are used.

Reference note:

About JP1 restart

When a JP1 failure is detected in a cluster operation system, restart of JP1 may be retried at the same server before failover to the secondary server is executed.

In such a case, do not perform restart using JP1 process management.

The cluster software attempts restart after detection of the JP1 failure.

Depending on the nature of the failure, JP1's restart function may be affected and normal operation may not be achieved. To restart JP1 successfully, use the cluster software to restart JP1.

(2) Setting the resource start and stop sequence

To execute JP1/IM - Manager and JP1/Base on the logical host, the shared disk and logical IP addresses must be available for use.

Set the start and stop sequence or resource dependencies in such a manner that they are controlled by the cluster software as shown below.

- When the logical host starts
 1. Allocate the shared disk and logical IP addresses, and make them available for use.
 2. Start JP1/Base and JP1/IM - Manager, in this order.
- When the logical host terminates
 1. Terminate JP1/IM - Manager and JP1/Base, in this order.
 2. Release the allocation of the shared disk and logical IP addresses.

6.3.4 Procedures for changing settings

If you change the settings at the primary server after you have started operation in the cluster system, you must apply the changes to the secondary server so that the system is synchronized. If the system is not synchronized, secondary server operation may not match primary server operation in the event of a failover.

Change settings at both the primary and the secondary servers in the following cases.

(1) Changing settings in files

If you have edited the files listed below and used the `jbssetcnf` command to apply the settings, you must copy the common definition information from the primary server to the secondary server:

- Automated action environment definition file (`action.conf.update`)
- Communication environment definition file (`console.conf.update`)
- Settings file for the maximum number of status change events

(evhist_warn_event_xxx.conf)

- Settings file for completed-action linkage function (action_complete_xxx.conf)
- Definition file for automatic delete mode of status change event
- Definition file for monitoring object initialization mode
- Automatic backup and recovery settings file for monitoring object database (auto_dbbackup_xxx.conf)
- Correlation event generation environment definition file
- Definition file for on memory mode of status change condition

Copy the common definition information using the setup procedure described in 6.3.2(5) *Copying the common definition information*.

The common definition information contains settings for JP1/Base, JP1/IM - Manager, JP1/AJS, and JP1/Power Monitor (06-02 or later). If these products have been set up on the logical host, the settings are also copied.

(2) Using commands to change settings

If you have used the `jcocmddef` or `jcochafmode` command to change settings, you must also specify the same settings at the primary and secondary servers.

- When the `jcochafmode` command was executed

If you have changed the location of the event acquisition filter by specifying the `-h` option, you must copy the common definition information from the primary server to the secondary server.

Copy the common definition information using the setup procedure described in 6.3.2(5) *Copying the common definition information*.

- When the `jcocmddef` command was executed

If you have changed the settings at the primary server by specifying the `-host` option, you must also specify the same settings at the secondary server. You can execute the `jcocmddef` command even when the shared disk is not mounted.

6.3.5 Deleting the IM databases and logical host

This subsection explains how to delete the logical host. When you delete the logical host, you must delete it at both the primary server and the secondary server.

If you use the IM databases (integrated monitoring database and IM Configuration Management database), you must delete them also (either before or after deleting the logical host).

(1) Deleting the IM databases

This procedure is applicable when the IM databases (integrated monitoring database and IM Configuration Management database) are used.

If you are deleting the IM databases in order to reconfigure the environment, back up the databases beforehand. For details about the backup method, see *1.2 Managing the databases* in the *Job Management Partner 1/Integrated Management - Manager Administration Guide*.

To delete the IM databases:

1. Terminate JP1/IM - Manager.

Terminate all JP1/IM - Managers in both the physical and the logical host environments.

2. Execute the `jcodbunsetup` command to delete the integrated monitoring database.

```
jcodbunsetup -h logical-host-name -c {online|standby} [-q]
```

Use arguments to specify the logical host name, unsetup type, and whether a message asking whether processing is to be continued is to be displayed.

- *logical-host-name* (-h option)

Specify the logical host name that was set up at the primary server.

- Unsetup type (-c option)

To delete the integrated monitoring database at the active host, specify `online`; to delete the integrated monitoring database at the standby host, specify `standby`.

- Whether a message asking whether processing is to be continued is to be displayed (-q option)

If a message asking about execution of processing is not to be displayed after command execution, specify `-q`; if the message is to be displayed, do not specify `-q`.

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

3. Execute the `jcfdbunsetup` command to delete the IM Configuration Management database.

```
jcfdbunsetup -h logical-host-name -c {online|standby} [-q]
```

Use arguments to specify the logical host name, unsetup type, and whether a message asking whether processing is to be continued is to be displayed.

- *logical-host-name* (-h option)
Specify the logical host name that was set up at the primary server.
- Unsetup type (-c option)
To delete the IM Configuration Management database at the active host, specify `online`; to delete the IM Configuration Management database at the standby host, specify `standby`.
- Whether a message asking whether processing is to be continued is to be displayed (-q option)
If a message asking about execution of processing is not to be displayed after command execution, specify `-q`; if the message is to be displayed, do not specify `-q`.
For details about the `jcfdbunsetup` command, see *jcfdbunsetup* in *1. Commands* in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.

(2) Deleting the logical host

To delete a logical host in UNIX, use the `jbsunsetcnf` command of JP1/Base. Execute the following command:

```
/opt/jp1base/bin/jbsunsetcnf -i -h logical-host-name
```

For details about the `jbsunsetcnf` command, see the *Job Management Partner 1/Base User's Guide*.

The logical host is now deleted. Note that when you delete the logical host, JP1/Base, JP1/IM - Manager, JP1/AJS, and JP1/Power Monitor (06-02 or later) are all deleted in batch mode.

Shared files and shared directories on the shared disk are not deleted; you must delete them manually.

6.4 Notes about cluster operation

- If you run multiple logical hosts concurrently in the cluster system, you need as many system resources as there are logical hosts running concurrently.
- Web-based JP1/IM - View does not support cluster systems; you must use JP1/IM - View.
- Before you set up JP1/IM - Manager in the cluster system, make sure that JP1/IM - Manager on the physical host has terminated. If you set up the cluster system while JP1/IM - Manager is running on the physical host, the logical host services will no longer function correctly. In such a case, restart the server to recover the system.
- When you set the user authentication server and register users on the logical host, make sure that you use the host at the primary node. Also make sure when you register users that you have already started the logical host services.
- If server switching occurs at the user authentication server due to node switching during login processing, a communication failure occurs on JP1/IM - Manager. The error is recovered after the switching is completed.

If the problem is in the JP1/IM - Manager operation, you can avoid the problem by placing the user authentication server outside the cluster system.

- In the case of Windows, specify in the `jbsgetcnf` command used to back up the primary node definitions exactly the same case-sensitive logical host name that was specified when the logical host was defined.

If you specify the wrong name by mistake, you must delete the logical host and then specify the settings again.

- If you do not use IM Configuration Management but distribute configuration definition information in the cluster system, create the configuration definition file under the following name:

In Windows:

shared-folder\jplbase\conf\route\jbs_route.conf

In UNIX:

shared-directory/jplbase/conf/route/jbs_route.conf

6.5 Logical host operation and environment configuration in a non-cluster system

This section provides an overview of the configuration and operation of logical hosts that do not employ failover.

Non-failover logical hosts can also be set up and run using the same procedure as for logical hosts running in a normal cluster system.

6.5.1 Evaluating the configuration for running logical hosts in a non-cluster system

If you start JP1/IM - Manager on multiple logical hosts, each JP1/IM - Manager uses system resources (such as memory, disk, processes, and semaphores). You must estimate the resource requirements based on the number of JP1/IM - Managers that will run concurrently.

Alternatively, you can adjust the number of JP1/IM - Managers that will run concurrently as appropriate for the desired level of system performance. If there are not enough resources to run multiple JP1/IM - Managers concurrently, normal system operation will not be achieved. As a guideline, you should not allow more than two or three logical hosts to run concurrently.

For details about how to estimate the memory and disk capacity requirements, see the Release Notes for JP1/IM - Manager.

6.5.2 Environment setup for running logical hosts in a non-cluster system

This subsection explains how to run JP1/IM - Manager in a non-failover logical host environment without having to link with cluster software.

(1) *Preparing for a logical host environment*

To create a logical host environment, provide the disk area and IP address for the logical host.

- Disk area for a logical host

Create directories on the local disk for storing files that are used exclusively by the JP1/IM - Manager on the logical host; make sure that these are separate directories from the directories used by JP1 on the physical host and other logical hosts.

- IP address for the logical host

Use the OS to assign an IP address to be used by the JP1/IM - Manager on the logical host.

This IP address may be a real IP or an alias IP, but it must be uniquely identifiable from the logical host name.

The prerequisites are the same as for cluster system operation. However, conditions such as inheritance between servers are not applicable because the operation does not involve failover.

Where they appear in this chapter (*6. Operation and Environment Configuration in a Cluster System*), replace the shared disk and logical IP address with the disk area and IP address for the logical host that were allocated above.

- Estimating the performance

When you estimate the performance, evaluate the system operation in terms of the following:

- Evaluate whether sufficient resources to run multiple JP1/IM - Managers in the system can be allocated. If there are not enough resources, the system may not run correctly or may not achieve an acceptable level of performance.

(2) Setting up JP1 in the logical host environment

Set up JP1 in the logical host environment using the same procedure as for the primary server in the cluster system. In the cluster system, this setup has to be performed for both servers involved in failover. For a non-failover logical host, you need to set up only the one server that will be running.

(3) Setting automatic startup and automatic termination in the logical host environment

The settings for automatic startup and automatic termination are not made in the logical host environment in the case of JP1 setup. To perform automatic startup and automatic termination in the logical host environment, see *2.17.2 Setting automatic startup and automatic stop*.

6.5.3 Logical host operation in the non-cluster system

The operation methods for running a non-failover logical host, such as JP1/IM - Manager operation, backup, and recovery, are the same as for logical hosts that run in a cluster system, except for the failover operations associated with cluster software.

(1) Startup and termination

Start the JP1 products on the logical host in the following order:

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

If you use the IM databases, start the JP1 products in the following order:

1. JP1/Base

2. IM databases
3. JP1/IM - Manager

Stop the JP1 products on the logical host in the following order:

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

If you use the IM databases, stop the JP1 products in the following order:

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

(2) Example of setting automatic startup and automatic termination

If you will be starting and stopping JP1 services automatically for the logical host at the times of system startup and termination, you must specify the settings as described below. The setting method depends on the OS supported by JP1/IM - Manager. This subsection describes the setting method for each OS.

(a) In a Windows environment

To set automatic startup and automatic termination:

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

```
storage-destination: Base-path\conf\boot\JP1SVPRM.DAT
```

```
[Jp1BaseEvent_logical-host-name]
```

```
Name=JP1/BaseEvent_logical-host-name
```

```
ServiceName=JP1_Base_Event logical-host-name
```

```
[Jp1Base_logical-host-name]
```

```
Name=JP1/Base_logical-host-name
```

```
ServiceName=JP1_Base_logical-host-name
```

```
StopCommand=jbs_spm�_stop.exe -h logical-host-name
```

```
[Jp1IM-Manager DB_logical-host-name]
```

```
Name=JP1/IM-Manager DB Server_logical-host-name
```

```
ServiceName=HiRDBEmbeddedEdition_JMn
```

```
StopCommand=Manager-path\bin\imdb\jimdbstop.exe -h  
logical-host-name
```

```
[Jp1IM-Manager_logical-host-name]
```

```
Name=JP1/IM-Manager_logical-host-name
```

```
ServiceName=JP1_Console_logical-host-name
```

```
StopCommand=jco_spmd_stop.exe -h logical-host-name
```

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

The command specified in the StopCommand parameter is executed when shutdown is performed from JP1/Power Monitor.

(b) In a Solaris environment

To set automatic startup and automatic termination:

1. Create an automatic startup script and an automatic termination script for the logical host.

```
storage-destination:/etc/init.d/jpl_service_cluster
```

Example of automatic startup and automatic termination scripts:

```
#!/bin/sh

## Set Environment-variables
PATH=/sbin:/bin:/usr/bin:/opt/jplbase/bin:/opt/jplcons/bin
export PATH
JP1_HOSTNAME=logical-host-name
export JP1_HOSTNAME

case $1 in
start_msg)
echo "Start JP1 Service $JP1_HOSTNAME"
;;

stop_msg)
echo "Stop JP1 Service $JP1_HOSTNAME"
;;

'start')
if [ -x /etc/opt/jplbase/jbs_start.cluster ]
then
/etc/opt/jplbase/jbs_start.cluster
fi
if [ -x /etc/opt/jplcons/jco_start.cluster ]
then
/etc/opt/jplcons/jco_start.cluster
fi
;;

'stop')
if [ -x /etc/opt/jplcons/jco_stop.cluster ]
then
```

```

/etc/opt/jplcons/jco_stop.cluster
fi
if [ -x /etc/opt/jplbase/jbs_stop.cluster ]
then
/etc/opt/jplbase/jbs_stop.cluster
fi
;;

esac

exit 0

```

2. Set a link to the scripts created in step 1.

Startup script

Execute the following command to set the link:

```
ln -s /etc/init.d/jpl_service_cluster /etc/rc2.d/
S**_JP1_SERVICE
```

The larger the value of ** in a start script, the later the script is executed.

Termination script

Execute the following command to set the link:

```
ln -s /etc/init.d/jpl_service_cluster /etc/rc0.d/
K**_JP1_SERVICE
```

The larger the value of ** in a termination script, the later the script is executed.

In general, set the program that is started first to be stopped last.

(c) In an AIX environment

To set automatic startup and automatic termination:

1. Use the `mkitab` command to add the following code in the `/etc/inittab` file:

```
# mkitab -i hntsr2mon "jplbase:2:wait:/etc/opt/jplbase/
jbs_start.cluster logical-host-name"
# mkitab -i jplbase "jplcons:2:wait:/etc/opt/jplcons/
jco_start.cluster logical-host-name"
```

This code executes JP1 service startup processing when the system starts.

2. Following the entries for products that require JP1/Base and JP1/IM - Manager in `/etc/rc.shutdown`, use a text editor to add the following code:

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

```

jplbase/jbs_stop.cluster logical-host-name
test -x /opt/hitachi/HNTRLib2/etc/D002stop &&
/opt/hitachi/HNTRLib2/etc/D002stop

```

This code executes JP1 service stop processing when the system terminates.

(d) Settings for performing automatic startup and automatic termination on both physical and logical hosts

To perform automatic startup and automatic termination on both physical and logical hosts, you must specify the settings described below in addition to the automatic startup and termination settings for the logical host.

The setting method depends on the OS. This subsection describes the setting method for each OS.

In a Windows environment:

Startup control executes startup and termination processing sequentially in the order specified in the start sequence definition file (JP1SVPRM.DAT). To change the start sequence of physical and logical hosts, define the startup and termination of physical and logical hosts in the desired sequence in the start sequence definition file (JP1SVPRM.DAT).

In a Solaris environment:

The sequence of automatic startup and automatic termination is determined by the value of ** in the expressions S** and K** in the automatic startup and termination scripts. The greater the value of **, the later the processing is executed. A symbolic link to the automatic startup and termination scripts for the physical host is created automatically during installation. To perform automatic startup and termination also for the physical host, rename the symbolic link that is created for the logical host, and then adjust the startup and termination sequence for both physical and logical hosts.

Automatic startup and automatic termination scripts for a physical host are already provided. The following table provides a list of the symbolic links to automatic startup and automatic termination scripts for a physical host.

Table 6-13: List of symbolic links to automatic startup and automatic termination scripts for a physical host

OS name	Startup script	Termination script
Solaris	/etc/rc2.d/S99_JP1_20_CONS	/etc/rc0.d/K01_JP1_80_CONS

Adjust the start sequence for the physical and logical hosts according to the relationship between the numeric value of ** in the expressions S** and K** in the above list, and the numeric value of ** in the expressions S** and K** in the symbolic link in the automatic startup and termination scripts for the logical

host.

For example, to start the logical host first, set a value that is less than 99 (for Solaris) in ** in the expression S** that is the name of the symbolic link to the automatic start script for a logical host.

In an AIX environment:

To perform automatic startup and termination of a physical host, you must add settings. For details about the settings to be added, see *2.17.2 Setting automatic startup and automatic stop*.

(3) Logical host operation on JP1

When you execute commands on the JP1 created on the logical host, specify the logical host name explicitly in the same manner as with a logical host that is run in a cluster system.

(4) Inheriting the logical host

The logical host in a non-cluster system environment does not support failover because the management information on the shared disk is not inherited. Do not run a logical host in such a manner that the logical host IP is inherited among multiple hosts.

Chapter

7. Operation and Environment Configuration Depending on the Network Configuration

This chapter describes the operation and environment configuration depending on the network configuration.

In the case of a configuration in which the JP1/IM - Manager host is connected to multiple networks, or a firewall is used, you must evaluate the setup and operation of JP1/IM - Manager and JP1/Base depending on the network configuration.

- 7.1 Controlling communications by JP1/Base
- 7.2 Operating in multiple networks
- 7.3 Operating in a firewall environment

7.1 Controlling communications by JP1/Base

JP1/IM - Manager runs in accordance with the communication settings of JP1/Base, which is a prerequisite for JP1/IM - Manager.

For example, the JP1/Base communication control functions are used for the communication settings for multiple LANs (configuration in which multiple networks are connected) and the communication method (such as an IP binding method for cluster systems).

For details about the communication method and settings, see the following information in the *Job Management Partner 1/Base User's Guide*:

- JP1/Base communication method in the *Overview* chapter
- *JP1/Base Communication Settings Depending on the Network Configuration* chapter

7.2 Operating in multiple networks

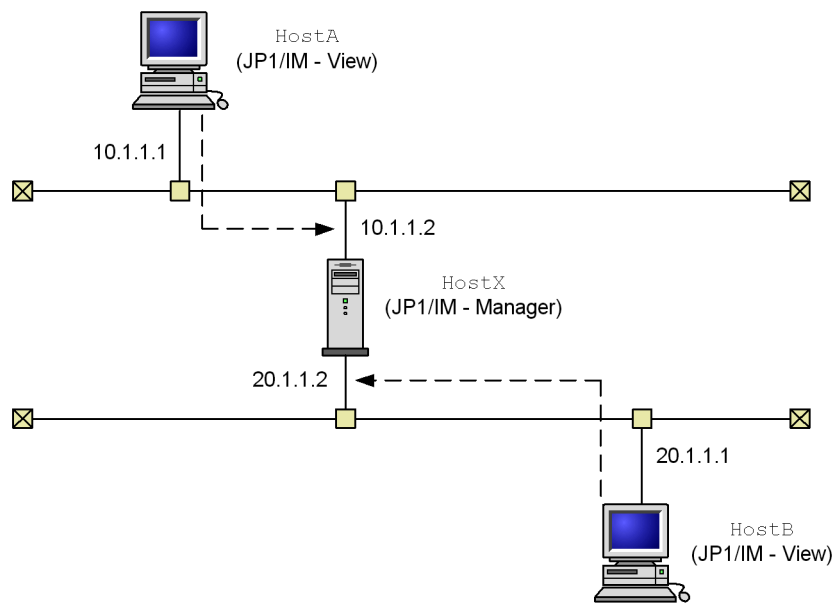
This section describes examples of system configurations that use multiple LANs (configurations in which multiple networks are connected), and the required communication settings based on the configuration examples.

The settings for multiple LANs are the same as in JP1/Base. If you specify the settings in JP1/Base, JP1/IM - Manager runs according to the specified settings.

7.2.1 Example 1 (non-cluster operation with JP1/IM - View connection)

In this example, although cluster operation is not employed, the manager is connected to two LANs that cannot be mutually routed, and JP1/IM - View is connected from each LAN.

Figure 7-1: Connecting JP1/IM - View in a multi-LAN environment (non-cluster operation)



The following tables show the settings for each host.

Table 7-1: Settings for HostX (JP1/IM - Manager)

Host name	Binding method [#]	jp1host setting [#]
HostX	send ANY, receive ANY	--
	send ANY, receive IP	10.1.1.2, 20.1.1.2

Legend:

--: Setting is not required

#: Can be connected with either settings.

You can achieve normal operation without having to change the JP1/Base communication settings (when cluster operation is not employed, the ANY binding methods can be used for both send and receive operations).

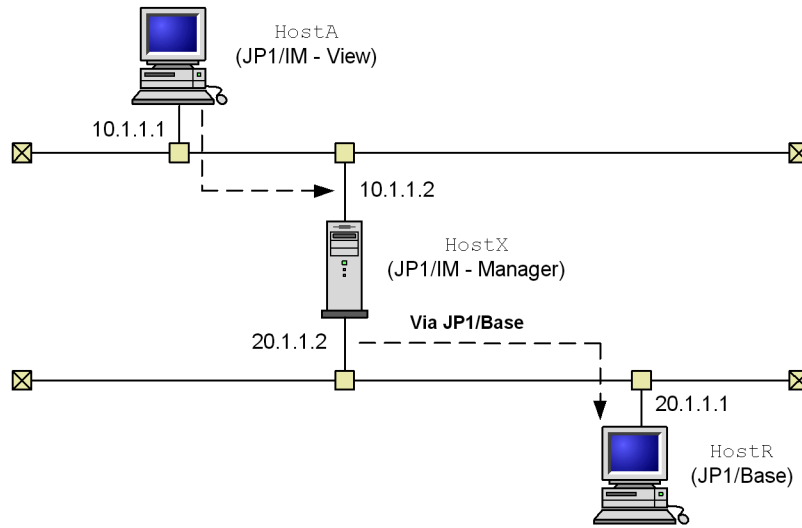
Table 7-2: Settings for HostA and HostB (JP1/IM - View)

Host name	Host to connect	Other conditions
HostA	HostX	Conversion from host name HostX to 10.1.1.2 must be possible.
HostB	HostX	Conversion from host name HostX to 20.1.1.2 must be possible.

7.2.2 Example 2 (non-cluster operation with command execution)

In this example, although cluster operation is not employed, the manager is connected to two LANs that cannot be mutually routed, one of the LANs is used to connect from JP1/IM - View to the manager, and the other LAN is used to execute commands at the other host.

Figure 7-2: Command execution in a multi-LAN environment (non-cluster operation)



The following tables show the settings for each host.

Table 7-3: Settings for HostX (JP1/IM - Manager)

Host name	Binding method#	jp1host setting#
HostX	send ANY, receive ANY	--
	send ANY, receive IP	10.1.1.2, 20.1.1.2

Legend:

--: Setting is not required

#: Can be connected with either settings.

You can achieve normal operation without having to change the JP1/Base communication settings (when cluster operation is not employed, the ANY binding methods can be used for both send and receive operations).

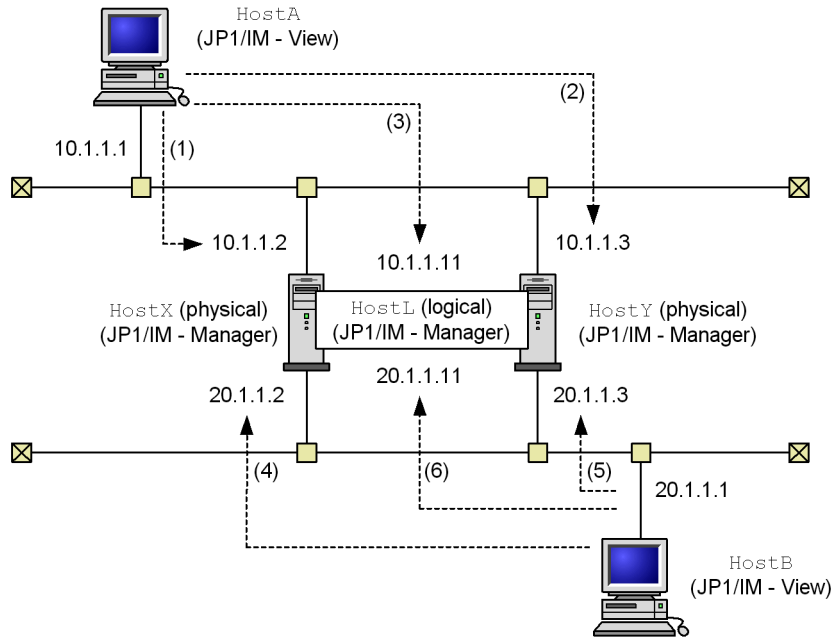
Table 7-4: Settings for HostA (JP1/IM - View)

Host name	Host to connect	Other conditions
HostA	HostX	Conversion from host name HostX to 10.1.1.2 must be possible.

7.2.3 Example 3 (cluster operation with JP1/IM - View connection)

In this example, the manager is run in a cluster operation system, and is connected to two LANs that cannot be mutually routed, and JP1/IM - View is connected from each LAN.

Figure 7-3: Connecting JP1/IM - View in a multi-LAN environment (cluster operation)



The following tables show the settings for each host.

Table 7-5: Settings for HostX, HostY, and HostL (JP1/IM - Manager)

Host name	Binding method	jp1host setting
HostX (physical host)	send ANY, receive IP	10.1.1.2, 20.1.1.2
HostY (physical host)	send ANY, receive IP	10.1.1.3, 20.1.1.3
HostL (logical host)	send ANY, receive IP	10.1.1.11, 20.1.1.11

Note that you need JP1/Base communication settings. For details of the settings, see the chapter that describes JP1/Base communication settings depending on the network configuration in the *Job Management Partner 1/Base User's Guide*.

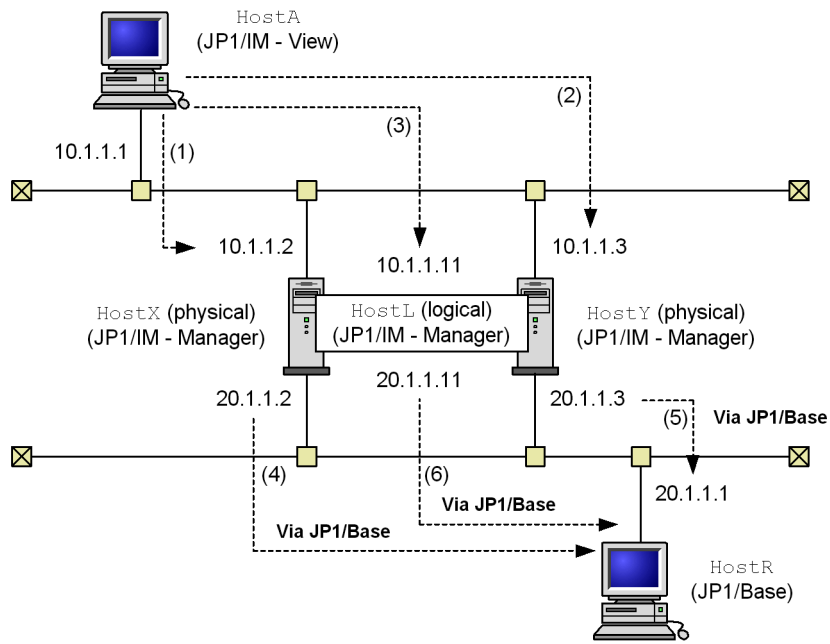
Table 7-6: Settings for HostA (JP1/IM - View)

Host name	Host to connect	Other conditions	Correspondence to number in parentheses in figure
HostA	HostX	Conversion from host name HostX to 10.1.1.2 must be possible.	1
	HostY	Conversion from host name HostY to 10.1.1.3 must be possible.	2
	HostL	Conversion from host name HostL to 10.1.1.11 must be possible.	3
HostB	HostX	Conversion from host name HostX to 20.1.1.1 must be possible.	4
	HostY	Conversion from host name HostY to 20.1.1.2 must be possible.	5
	HostL	Conversion from host name HostL to 20.1.1.11 must be possible.	6

7.2.4 Example 4 (cluster operation with command execution)

In this example, the manager is run in a cluster operation system, and is connected to two LANs that cannot be mutually routed, one of the LANs is used to connect to JP1/IM - View, and the other LAN is used to execute commands on the other host.

Figure 7-4: Command execution in a multi-LAN environment (cluster operation)



The following tables show the settings for each host.

Table 7-7: Settings for HostX, HostY, and HostL (JP1/IM - Manager)

Host name	Binding method	jp1host setting
HostX (physical host)	send ANY, receive IP	10.1.1.2, 20.1.1.2
HostY (physical host)	send ANY, receive IP	10.1.1.3, 20.1.1.3
HostL (logical host)	send ANY, receive IP	10.1.1.11, 20.1.1.11

Note that you need JP1/Base communication settings. For details of the settings, see the chapter that describes JP1/Base communication settings depending on the network configuration in the *Job Management Partner 1/Base User's Guide*.

Table 7-8: Settings for HostA (JP1/IM - View)

Host name	Host to connect	Other conditions	Correspondence to number in parentheses in figure
HostA	HostX	Conversion from host name HostX to 10.1.1.2 must be possible.	1, 4
	HostY	Conversion from host name HostY to 10.1.1.3 must be possible.	2, 5
	HostL	Conversion from host name HostL to 10.1.1.11 must be possible.	3, 6

7.3 Operating in a firewall environment

This section describes JP1/IM operation in a network environment that contains a firewall. JP1/IM supports system configurations with firewalls.

7.3.1 Basic information about firewalls

Before describing the operation in a firewall environment, this subsection provides basic information about firewalls.

If you run JP1 in a network environment that includes a firewall, you must evaluate support of two of the firewall functions:

- Packet filtering (access permissions)

With packet filtering, only required communications are permitted and unauthorized communications are blocked.

- NAT (address translation)

With NAT, an IP address is converted in order to connect to a network that has a different address; connection cannot be made directly. In addition, the machine used to convert the IP address is hidden from the outside.

To evaluate support of these functions and to set up an environment, you must understand the method used by the firewall to control communications.

Note:

The information provided here constitutes a simple overview intended to acquaint you with the basics of firewalls and does not provide sufficient detail for you to evaluate and set up an actual firewall. When you install a firewall, consult the firewall documentation as well as appropriate security documentation to evaluate and set up an environment.

(1) Packet filtering

The packet filtering function filters through the firewall the applications that can be used. It checks each communication packet that attempts to pass through the firewall and discards packets that do not satisfy the specified passage conditions, thereby blocking unauthorized communications from passing through the firewall. Only applications that are specified in the passage conditions can be used.

JP1/IM supports packet filtering.

(a) Setting packet filtering

To set packet filtering:

1. Check the communication method, such as the port numbers used by applications.

Check the port numbers, IP addresses, and passage directions that are set as the firewall passage conditions.

In the case of JP1/IM, check the communication method by referencing the information provided in this chapter and in *C. Port Numbers* in the *Job Management Partner 1/Integrated Management - Manager Overview and System Design Guide*.

2. Set the passage conditions for the firewall.

Initially, you should prohibit all passage, then set passage conditions so that only specific applications can communicate through the firewall.

In the case of JP1/IM, set the JP1/IM communications checked in step 1 to pass the firewall.

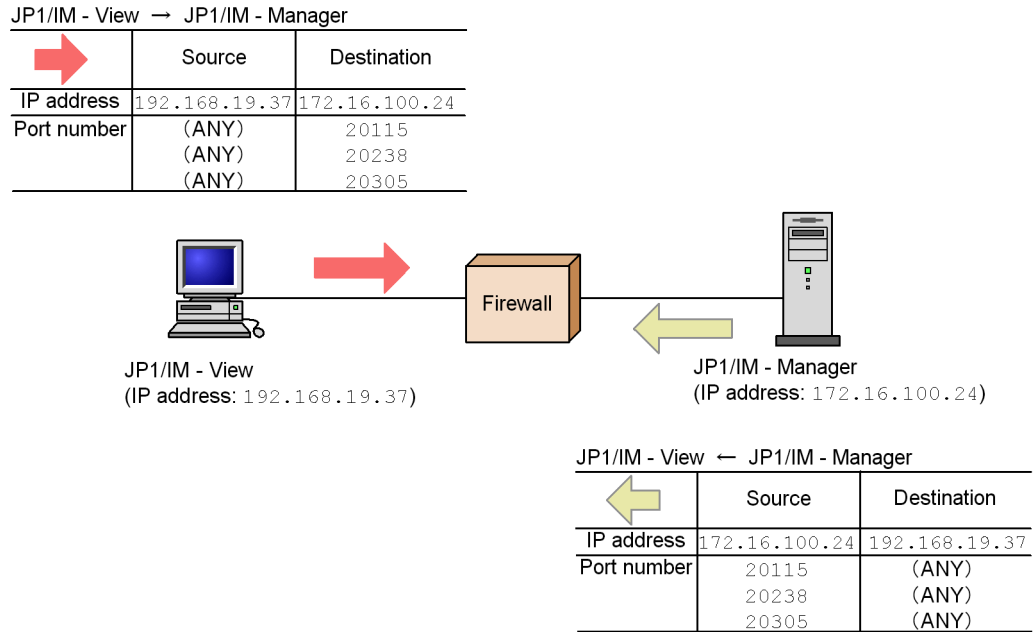
(b) Example of settings for JP1/IM

This subsection describes the settings for packet filtering using an example of an environment in which there is a firewall between JP1/IM - View and JP1/IM - Manager.

■ Example: Connecting JP1/IM - View to JP1/IM - Manager via a firewall

- The IP address of the JP1/IM - View machine is 192.168.19.37.
- The IP address of the JP1/IM - Manager machine is 172.16.100.24.
- The port numbers are JP1's default port numbers.

Figure 7-5: Example of setting packet filtering



1. Check JP1's communication method.

First, check JP1's communication method, which is required for setting packet filtering. According to the information provided in *Appendix C.2 Direction of communication through a firewall* in the *Job Management Partner 1/Integrated Management - Manager Overview and System Design Guide*, the port numbers used by JP1/IM are described as shown in the table below.

Table 7-9: Firewall passage directions

No.	Service name	Port number	Firewall passage direction
1	jp1imevtcon	20115/tcp	JP1/IM - View → JP1/IM - Manager (JP1/IM - Central Console)
2	jp1imcmda	20238/tcp	JP1/IM - View → JP1/IM - Manager (JP1/IM - Central Console) JP1/IM - Manager (JP1/IM - Central Console) → JP1/Base ^{#1}
3	jp1imcss	20305/tcp	JP1/IM - View → JP1/IM - Manager (JP1/IM - Central Scope)

No.	Service name	Port number	Firewall passage direction
4	jp1imegs	20383/tcp	There is no need to set a firewall because communication is performed only within the machine where JP1/IM - Manager is installed.
5	jp1rmregistry	20380/tcp	JP1/IM - View → JP1/IM - Rule Operation
6	jp1rmobject	20381/tcp	
7	http	80/tcp ^{#2}	Web-based JP1/IM - View (Web browser) → HTTP server
8	jp1imcf	20702/tcp	JP1/IM - View → JP1/IM - Manager (IM Configuration Management)

#1: This is the manager's JP1/Base.

#2: This may depend on the HTTP server settings.

This table assumes the following communication method:

- *Service name* and *Port number* columns

These are the service names and port numbers used by JP1 for communication. According to this table, port number 20115 (service name `jp1imevtcon`), port number 20238 (service name `jp1imcmda`), and port number 20305 (service name `jp1imcss`) are used, and TCP is used as the communication protocol for communication between JP1/IM - View and JP1/IM - Manager.

- *Firewall passage direction* column

This column shows the direction of communication when connection begins (at the time connection is established). The direction for establishing connection is required in order to limit the firewall passage direction. For example, in No. 1 in this table, connection is permitted from JP1/IM - View to JP1/IM - Manager (JP1/IM - Central Console).

- Other

Although it is not specified in the table, based on the information provided in the table and the TCP communication specifications, the following is true:

Because TCP is a bi-directional communications protocol, it involves two-way communications (JP1/IM - View to JP1/IM - Manager and JP1/IM - Manager to JP1/IM - View). In the source and destination packets of TCP communications, the source IP address and destination IP address are switched.

2. Set packet filtering.

Based on the direction of communication between JP1/IM - View and JP1/IM - Manager, set packet filtering in such a manner that only communications in the correct direction can pass through the firewall.

The passage conditions for packet filtering are as follows:

Example: Filtering condition: For JP1/IM - View and JP1/IM - Manager

Table 7-10: Passage conditions for packet filtering

No.	Source address	Destination address	Protocol	Source port	Destination port	Control
1	192.168.19.37	172.16.100.24	TCP	(ANY)	20115	accept
2	192.168.19.37	172.16.100.24	TCP	(ANY)	20238	accept
3	192.168.19.37	172.16.100.24	TCP	(ANY)	20305	accept
4	172.16.100.24	192.168.19.37	TCP	20115	(ANY)	accept
5	172.16.100.24	192.168.19.37	TCP	20238	(ANY)	accept
6	172.16.100.24	192.168.19.37	TCP	20305	(ANY)	accept
7	(ANY)	(ANY)	(ANY)	(ANY)	(ANY)	reject

This table shows the conditions for checking packets and the control to be applied when the conditions are satisfied.

The *Control* column specifies whether the firewall permits (*accept*) or blocks (*reject*) the passage of packets. (*ANY*) means that any available port number assigned by the OS is to be used.

Set packet filtering for a firewall according to the filtering conditions shown in this table.

Note that the detailed setting method depends on the firewall; see your firewall documentation.

(2) NAT (address translation)

NAT (Network Address Translator) is a function for translating between private IP addresses and global IP addresses. By translating addresses, you can hide the private addresses from the outside, thereby improving internal machine security. NAT may be provided as a router function as well as a firewall function.

JP1 supports only static-mode NAT (method for translating addresses according to predefined rules).

(a) Setting NAT

To set NAT:

1. Check the IP addresses to be used.

First, check the IP addresses used by the applications. It is simple if a machine uses only one IP address. If there are multiple network adapters (using multiple IP addresses), or a logical IP address is used in a cluster system, the IP addresses to be used depend on the application.

In the case of JP1/IM, the IP addresses to be used depend on the settings, such as when communication settings are specified in JP1/Base, or a logical IP address is used for cluster operation.

2. Evaluate and set the address translation rules.

After you have checked the IP addresses used by the applications, determine the IP addresses obtained after translation.

Once you have determined rules for address change, set them in NAT.

(b) Example of settings for JP1/IM

This subsection describes the NAT settings based on an example of an environment in which there is a firewall between JP1/IM - View and JP1/IM - Manager.

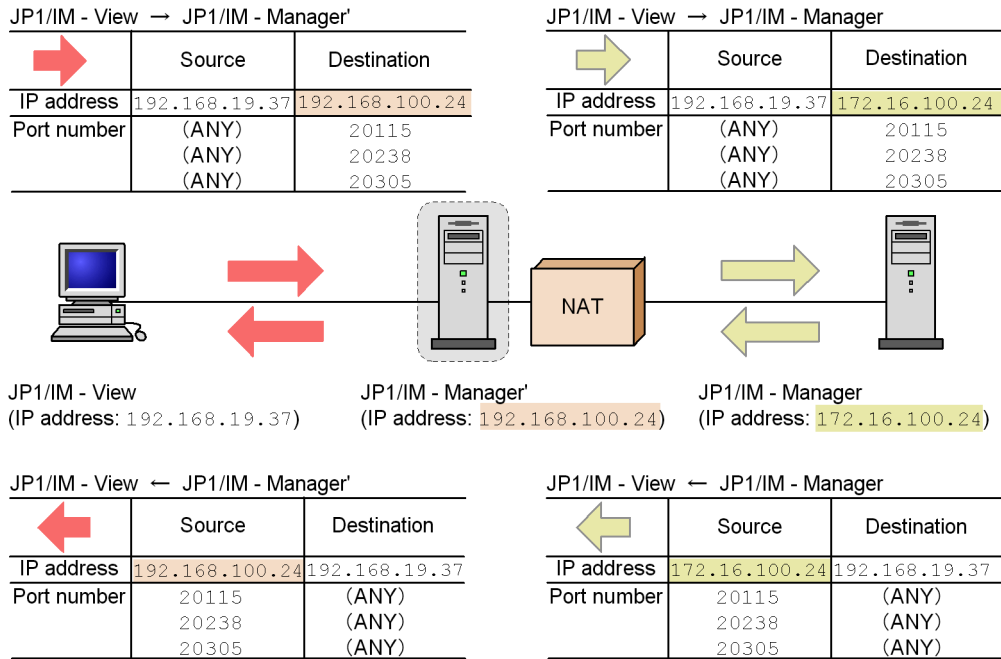
- Example: Connecting from JP1/IM - View to JP1/IM - Manager whose address has been translated

- The IP address of the JP1/IM - View machine is 192.168.19.37.
- The IP address of the JP1/IM - Manager machine is 172.16.100.24.

The IP address of this JP1/IM - Manager is translated to 192.168.100.24.

JP1/IM - View connects to 192.168.100.24 that is obtained after address translation.

Figure 7-6: Example of NAT settings



Note: This is an example of address translation by NAT. Other translation methods are also available.

To set NAT:

1. Check the IP address to be used.

First, check the IP addresses used by JP1, which is required in order to set NAT.

This example uses the IP address that corresponds to the host name (result of hostname).

2. Evaluate and set the address translation rule.

Define the translation rule in such a manner that the IP address of the JP1/IM - Manager machine is translated from 172.16.100.24 to 192.168.100.24 by NAT.

Example: Address translation rule: Translating from 172.16.100.24 to 192.168.100.24

Table 7-11: Address translation rule

No.	Source address	Destination address	Source address (translated)	Destination address (translated)
1	(ANY)	192.168.100.24	(ANY)	172.16.100.24
2	172.16.100.24	(ANY)	192.168.100.24	(ANY)

This table shows the correspondence between the source packet and the (translated) packet obtained after address translation.

Define this address translation rule in the NAT settings for the firewall.

Note that the detailed setting method depends on the firewall and router; see your product documentation.

JP1/IM - View accesses the address obtained after address translation (192.168.100.24), not the actual address of the JP1/IM - Manager machine (172.16.100.24).

Therefore, to JP1/IM - View, it appears that access is to the JP1/IM - Manager host whose address is 192.168.100.24.

(3) Communication settings for a JP1 that is run in a firewall environment

If you run JP1 in a network environment that includes a firewall, consider setting the JP1 communication method to the IP binding method and the effects of multi-LAN connection settings.

To run JP1 in a firewall environment, you must set IP address and port number conditions in packet filtering and NAT as discussed above.

The IP addresses used by JP1 must be clear. Therefore, the IP binding method that determines JP1's IP addresses by the JP1 settings is suitable.

For example, in a configuration in which the server that executes JP1 is connected to multiple LANs or in a cluster system configuration, the IP address to be used may be determined by the OS, resulting in an unintended IP address. In such a case, if you set JP1's communication method to the IP binding method, the IP address specified in the JP1 environment settings is always used for communication.

7.3.2 JP1/IM communication

This subsection describes support of port numbers, IP addresses, and address translation (NAT) with respect to JP1/IM communication.

The information provided here applies to both JP1/IM and JP1/Base communications, because JP1/IM uses the functions of JP1/Base as the prerequisite product.

(1) Port numbers

(a) Port numbers

For details about the port numbers used by JP1/IM and JP1/Base and the firewall passage direction (direction in which connection is established), see the following:

- Port numbers of JP1/Base: Description of port numbers in the *Job Management Partner 1/Base User's Guide*
- Port numbers of JP1/IM: C. *Port Numbers* in the *Job Management Partner 1/Integrated Management - Manager Overview and System Design Guide*

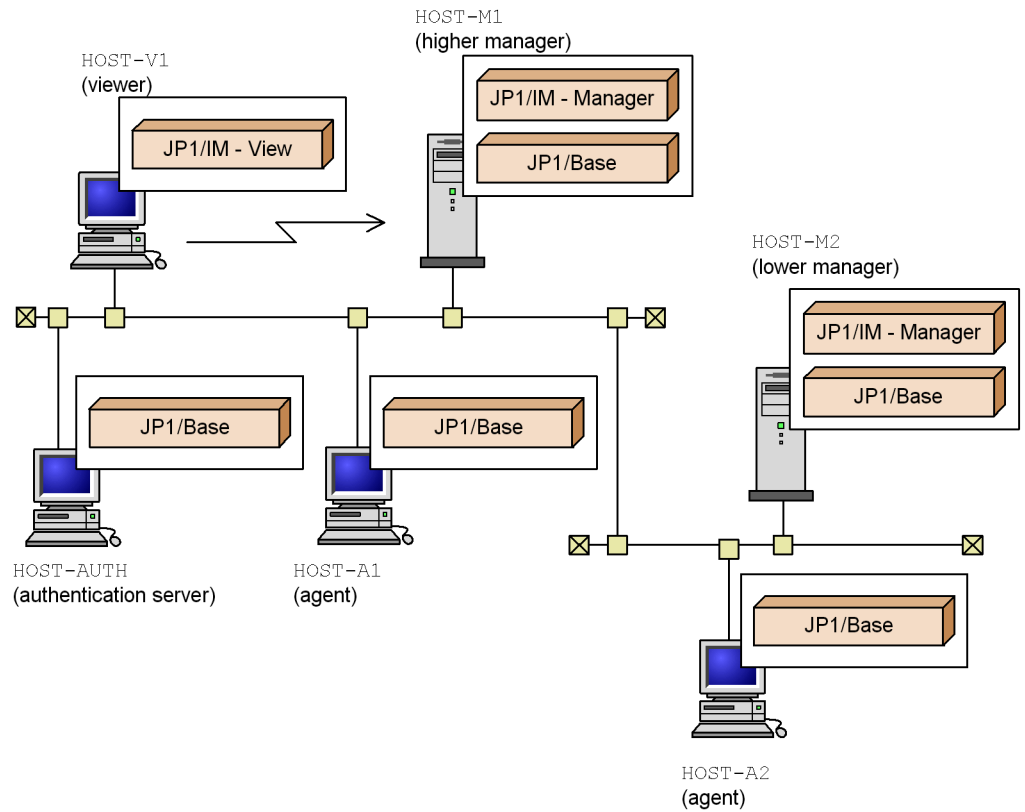
(b) Example of system configuration and communication

This subsection describes the port numbers to be used and the firewall passage direction (direction in which connection is established) based on an example system configuration.

Note:

If you use JP1 on the firewall host, set communications within the same host in such a manner that all ports used by JP1 can be passed. This is because ports are used between JP1 processes.

Figure 7-7: System configuration (example)



To set JP1/IM communication:

1. Connect to HOST-M1 by JP1/IM - View of HOST-V.
2. Position HOST-M2 under HOST-M1.
3. Install HOST-A1 as an agent under HOST-M1, and install HOST-A2 as an agent under HOST-M2.
4. Set the authentication server on HOST-M1 to HOST-AUTH.

■ Authentication server and communication between managers and agents

Manager or agent (JP1/Base)	Passage direction	Authentication server (JP1/Base)
(ANY)	→	20240/tcp (jp1bsuser)

This table applies to communication between each host and HOST-AUTH in the example system configuration.

■ Communication between viewer and manager

JP1/IM - View	Passage direction	Manager (JP1/IM and JP1/Base)
(ANY)	→	20115/tcp (jplimevtcon) 20238/tcp (jplimcnda) 20305/tcp (jplimcss) ^{#1} 20380/tcp (jplrmregistry) ^{#2} 20381/tcp (jplrmobject) ^{#2} 20702/tcp (jplimcf) ^{#3}

#1: The port of jplimcss is used only when JP1/IM - Manager (JP1/IM - Central Scope) is used.

#2: This port is used only when JP1/IM - Rule Operation is used.

#3: The port of jplimcf is used only when JP1/IM - Manager (JP1/IM - Configuration) is used.

This applies to communication between HOST-V1 and HOST-M1 in the example system configuration.

If a Web-based JP1/IM - View is used on HOST-V1, the settings are as shown below.

Web-based JP1/IM - View (Web browser)	Passage direction	Manager (HTTP server and JP1/IM - Manager)
(ANY)	→	80/tcp [#] 20115/tcp (jplimevtcon)

#: Used when a Web browser accesses the HTTP server. This may be different depending on the HTTP server settings.

■ Communication between JP1/IM - View and agent

There is no communication between JP1/IM - View and agent (JP1/Base).

■ Communication between the higher manager and the lower manager

Higher manager (JP1/IM and JP1/Base)	Passage direction	Lower manager (JP1/IM and JP1/Base)
(ANY)	→	20098/tcp (jplimevt) 20099/tcp (jplimevtapi) 20237/tcp (jplimrt) 20239/tcp (jplimcmdc) 20306/tcp (jplbsplugin)
20098/tcp (jplimevt) 20239/tcp (jplimcmdc)	←	(ANY)

This table applies to communication between HOST-M1 and HOST-M2 in the example system configuration.

This example assumes that event forwarding occurs only from the lower manager to the higher manager, and communication execution occurs only from the higher manager to the lower manager.

■ Communication between managers and agents

Manager (JP1/IM and JP1/Base)	Passage direction	Agent (JP1/Base)
(ANY)	→	20098/tcp (jplimevt) 20099/tcp (jplimevtapi) 20237/tcp (jplimrt) 20239/tcp (jplimcmdc) 20306/tcp (jplbsplugin)
20098/tcp (jplimev) 20239/tcp (jplimcmdc)	←	(ANY)

This table applies to communications between HOST-M1 and HOST-A1 and HOST-A2, and between HOST-M2 and HOST-A2.

When JP1/SES events are used:

If JP1/SES-format JP1 events are used, the following settings are also required:

- Define a port number by the service name JP1AutoJob (in Windows) or jesrd (in UNIX).
- Set the firewall in such a manner that the defined port number is used for bi-directional communication between JP1/Base and the products that use JP1/SES events.

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

(2) IP addresses

This subsection describes the IP addresses that are used by JP1/IM and JP1/Base.

If you use IP addresses for filtering or perform address translation (NAT), specify the IP addresses described here.

JP1/IM uses the functions of the JP1/Base required product to control the communication method.

For details about the settings, see the chapter that describes the JP1/Base communication settings depending on the network in the *Job Management Partner 1/Base User's Guide*.

(a) For a normal system

This subsection describes the IP addresses that are used when a logical host has not been set up in a normal non-cluster system.

- Receiver's IP address (when the receiver uses ANY binding)

JP1 services use this IP address to accept connection.

Use the IP address that corresponds to the host name (result of `hostname` command execution).

- Sender's IP address (when the sender uses ANY binding)

This IP address is used to connect to JP1 services.

JP1 issues a connection request (executes the `connect` function) without specifying its own IP address. In this case, depending on the OS specifications, the IP address corresponding to the target is assigned by the OS. In general, the assigned IP address corresponds to the NIC that is used when packets are sent to the target IP address. For details, check the TCP/IP control specifications of the OS.

(b) For a cluster system

If a logical host environment is set up in a cluster system, unlike in a normal system, the following IP addresses are used:

- Receiver's IP address (when the receiver uses IP binding)

JP1 services use this IP address to accept connection.

A physical host environment uses the IP address that corresponds to the physical host name (result of `hostname` command execution). A logical host environment uses the logical IP address that corresponds to the logical host name.

- Sender's IP address (when the sender uses IP binding)

This IP address is used to connect to JP1 services.

A physical host environment uses the IP address that corresponds to the physical host name (result of `hostname` command execution). A logical host environment uses the logical IP address that corresponds to the logical host name.

(c) Notes about customizing the communication settings

The information provided in 7.3.2(2)(a) *For a normal system* and 7.3.2(2)(b) *For a cluster system* constitutes the standard communication settings when JP1 has just been set up. If you have customized multi-LAN connection settings such as by defining `jplhosts` in JP1/Base, operation is determined by the combination of the receiver's and the sender's communication methods (ANY and IP binding methods).

If you have customized the settings so that the receiver uses IP binding and the sender uses ANY binding, the receiver's operation is as discussed in 7.3.2(2)(b) *For a cluster system*, while the sender's operation is as discussed in 7.3.2(2)(a) *For a normal system*.

Note that if you have set the `jplhosts` information, definition in the `hosts` file is not referenced regarding the host name and IP address defined in the `jplhosts` information.

For example, suppose that the `jplhosts` information is defined as follows:

```
hostA 100.0.0.10 200.0.0.10
```

Also suppose that the `hosts` file contains the following definition:

```
100.0.0.10 hostA hostB
200.0.0.10 hostC
```

The `hosts` file is not referenced regarding `hostA` and IP addresses `100.0.0.10` and `200.0.0.10`. Therefore, if the configuration definition file contains `hostB` and `hostC` that are not defined in the `jplhosts` information, the system configuration cannot be defined.

(3) Support of address translation (NAT)

JP1/IM supports static-mode address translation (NAT).

Specify settings in NAT so that the IP addresses used by JP1/IM can be translated correctly.

Chapter

8. Settings for Linking to Other Integrated Management Products

This chapter describes the environment setup for linking JP1/IM to other integrated management products.

8.1 Linking to JP1/IM - Rule Operation

8.1 Linking to JP1/IM - Rule Operation

To link to JP1/IM - Rule Operation, you must specify the following settings:

- Settings for enabling the JP1/IM - Rule Operation linkage function
- Settings for sending notifications to JP1/IM - Rule Operation
- Settings for checking notifications on the Event Console window

8.1.1 Settings for enabling the JP1/IM - Rule Operation linkage function

This subsection explains how to specify settings to enable the JP1/IM - Rule Operation linkage function. You can perform the steps described below in any order. You can also perform the procedure in a single operation by specifying multiple arguments.

To enable the JP1/IM - Rule Operation linkage function:

1. Enable the JP1/IM - Rule Operation linkage function.

Execute the following command:

```
jcoimdef -rule ON
```

2. Specify the JP1/IM - Rule Operation host.

Execute the following command:

```
jcoimdef -rulehost JP1/IM-Rule-Operation-host-name
```

3. Specify the JP1 user who is to be notified of any event that results in issuance of a rule startup request to JP1/IM - Rule Operation.

Execute the following command:

```
jcoimdef -ruleuser JP1-user-name
```

If you have enabled or disabled the JP1/IM - Rule Operation linkage function while JP1/IM - Manager was running by executing the `jcoimdef` command with the `-rule` option specified, you must restart JP1/IM - Manager. You must also restart the JP1/IM - View that is connected.

You must execute the `jcoimdef` command with the `-i` option specified or the `jco_spmc_reload` command in either of the following situations: You changed the JP1/IM - Rule Operation host while JP1/IM - Manager was running by executing the `jcoimdef` command with the `-rulehost` option specified, or you specified the JP1 user who is to be notified of an event that results in issuance of a rule startup request to JP1/IM - Rule Operation by executing the `jcoimdef` command with the `-ruleuser` option specified. There is no need to restart the JP1/IM - View that is connected.

About the settings for enabling the JP1/IM - Rule Operation linkage function:

- About the `jcoimdef` command

See `jcoimdef` in *1. Commands* in the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference*.

8.1.2 Settings for sending notifications to JP1/IM - Rule Operation

Notification to JP1/IM - Rule Operation is achieved by using automated actions. The procedure is the same as for regular automated actions except for the execution settings described below. For details, see *4.3 Setting automated actions*.

- When using the GUI to specify settings

In the Action Parameter Detailed Definitions window, in **Action Definition**, select **Rule**.

- When using the definition file to specify settings

In the automated action definition file (`actdef.conf`), specify `<RULE>` for `action` in the automated action definition parameter. Do not specify the items `u=user-name`, `e=environment-variable-file-name`, and `d=execution-host-name|group-name`.

About the settings for sending notifications to JP1/IM - Rule Operation:

- 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*

- 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*

Note:

To stop sending notifications to JP1/IM - Rule Operation, delete the actions that specify the notifications to JP1/IM - Rule Operation from the automated action definition.

Even when the JP1/IM - Rule Operation linkage function is disabled by the `jcoimdef` command with the `-rule` option specified, an action that specifies notification to JP1/IM - Rule Operation will continue to execute as a normal automated action.

8.1.3 Settings for checking notifications on the Event Console window

To check the notification for automatic login in the Event Console window, you must specify settings so that **Action type** is displayed in the Event Console window.

To set the Event Console window to display **Action type**:

1. In JP1/IM - View, log in to the JP1/IM - Manager (JP1/IM - Central Console) for which the JP1/IM - Rule Operation linkage function is enabled.

The Event Console window appears.

2. From the menu bar, choose **Options**, and then **Preferences**.

The Preferences window appears.

3. From **Available items**, select **Action type**, and then click the -> button to move to **Display items & order**.

4. Click the **OK** button.

About the notification checking settings in the Event Console window:

- About the Preferences window

See 2.16 Preferences window in the manual Job Management Partner 1/ Integrated Management - Manager GUI Reference.

Index

A

abbreviations defined iii
abnormal process termination, restart settings in event of 38
acquiring existing Visual Monitoring window 201
action status change, setting JP1 event issuance during 152
adding

- monitoring nodes to monitoring tree 188
- monitoring nodes to Visual Monitoring window 204

address translation 314

- support of 323

alias name 174
applying

- customized monitoring tree to manager 198
- customized Visual Monitoring window to manager 207

authentication server, specifying 16, 64
automated action definition file, updating 43, 92
automated actions

- setting 139
- setting details of 140
- setting execution conditions of 140
- setting suppression of execution 143
- setting up execution environment for 139
- settings for monitoring execution status of 142

automatic generation of monitoring tree 184
automatic startup, setting 84
automatic stop, setting 84

C

Central Console, setting up 123
Central Scope

- before starting environment setup for 178
- environment setup for 178
- executing upgrade command 42, 91

registering host information 179
setting up 177
setting up for linked products 218
setting up operating environment for 213
settings for using functions of 36, 86
clipboard, whether data can be copied to 163
cluster operation 239

- changing settings in 268, 289
- environment setup for (UNIX) 272
- environment setup for (Windows) 248
- JP1's support range 242
- JP1/IM configuration in 243
- notes about 293
- prerequisites for 240

cluster software 239

- creating script to be registered into 285
- registering into (UNIX) 285
- registering into (Windows) 266, 267

cluster system

- environment setup 248, 272
- installing and setting up logical host 250, 273
- JP1/IM configuration in 243
- logical host 239
- operation and environment configuration in 237
- overview of using 238, 239

command execution, setting up environment for 32, 80
common definition information, setting 246
communication method 246
communications, controlling by JP1/Base 302
completed-action linkage, setting 213
configuration definition information

- changing 25, 73
- deleting 25, 73
- notes about setting 25, 74
- setting 24, 72

configuration files

- applying edited information in 110

- editing 108
 - console.html 175
 - consolidated display of repeated events 162
 - conventions
 - abbreviations iii
 - diagrams x
 - fonts and symbols x
 - KB, MB, GB and TB xiii
 - mathematical expressions xii
 - version numbers xiii
 - correlation event generation
 - creating and applying definition of 146
 - history files, setting size and number of 144
 - setting 144
 - setting startup of 144
 - setting startup options 146
 - Cosminexus, setup for linkage with 223
 - crash dump output settings 37
 - CSV files to create monitoring windows, using 210
 - customizing
 - monitoring tree 186
 - toolbar for monitoring tree 216
 - Visual Monitoring window 202
- D**
- data, preparations for collecting 36, 87
 - definition files
 - creating 156, 165, 169
 - enabling 159
 - deleting monitoring nodes 193
 - diagram conventions x
- E**
- editing
 - event guide information 149
 - guide information 211
 - list of Visual Monitoring windows 209
 - environment setup
 - for cluster operation (UNIX) 272
 - for cluster operation (Windows) 248
 - procedure (UNIX) 272
 - procedure (Windows) 248
 - event acquisition filter
 - changing location of 41, 90
 - setting (for compatibility) 135
 - setting common exclusion conditions 136
 - setting only one 132
 - setting, by switching filter conditions 134
 - settings for 132
 - event guide information, editing 149
 - event receiver filter
 - changing 130
 - creating new 128
 - deleting 130
 - settings for 128
 - Event Service
 - setting 27, 75
 - settings for using source host name of, in FQDN format 34, 82
 - Event Service definition information, collecting and distributing 31, 79
- F**
- failover 239
 - failure, preparations for collecting data in event of 36, 87
 - filters, setting 125
 - firewall
 - basic information about 310
 - communication settings for JPI that is run in 317
 - environment, operating in 310
 - filtering through 310
 - font conventions x
 - FQDN format, settings for using source host name of Event Service in 34, 82
- G**
- GB meaning xiii
 - general-purpose monitoring objects, example of creating 228
 - GUI
 - using to create monitoring tree 180
 - using to create Visual Monitoring window 200
 - guide information, editing 211

H

- health check function, setting 40, 89
 - HiRDB
 - example of creating general-purpose monitoring objects 228
 - setup for linkage with 224
 - Hitachi Program Product Installer
 - starting 54
 - using 54
 - hosts
 - registering 94
 - registering information of 179
 - HP NNM, setup for linkage with 221
 - HTTP server
 - installing 174
 - setting up 174
- I**
- IM Configuration Management
 - importing and exporting management information in 113
 - setting system hierarchy by using 93
 - setting using export and import functions of 22, 70
 - setting virtualization system configuration 115
 - settings for using functions of 13, 62
 - IM Configuration Management - View
 - setting up 45
 - setting using 20, 68
 - IM Configuration Management database, setting 12, 61
 - IM databases
 - creating 10, 59
 - deleting 269, 290
 - installation
 - designing setup details 4, 52
 - notes about 8, 57
 - preparations required before 4, 52
 - procedure 2, 5, 50, 53
 - types of 7, 53
 - installing
 - HTTP server 174
 - JP1/IM - Manager 5, 53

JP1/IM - View 5

- prerequisite program 4, 52
- integrated monitoring database, setting 10, 59
- IP addresses 322
 - support of 317

J

- Java Console window, specifying display settings for 175
- JP1 events
 - displaying attributes of user specific 153
 - editing guide information of 149
 - setting Event Service 27, 75
 - setting filters for 125
 - setting forwarding of 29, 77
 - setting issuance of, during action status change 152
 - setting to issue, in event of abnormal process termination 39, 88
 - settings for operations to be performed during acquisition of 124
- JP1 users
 - registering 16, 64
 - setting operation permissions for 16, 64
- JP1/AJS
 - example of creating system-monitoring objects 226
 - setup for linkage with 218
- JP1/Base
 - collecting and distributing Event Service definition information 31, 79
 - controlling communications by 302
 - copying primary authentication server settings 17, 65
 - installing 4, 52
 - registering JP1 users 16, 64
 - setting JP1 event forwarding 29, 77
 - setting operation permissions for JP1 users 16, 64
 - setting startup sequence for services 14
 - setting up command execution environment 32, 80
 - setting user authentication 15, 63
 - setting user mapping 15, 63

- settings for handling failures 19, 67
 - specifying authentication server 16, 64
- JP1/IM
- Central Scope environment setup 178
 - communication 317
 - controlling communications by JP1/Base 302
 - creating IM database 10, 59
 - installation and setup procedures 2, 50
 - installing (UNIX) 49, 53
 - installing (Windows) 1, 5
 - linking to JP1/IM - Rule Operation 326
 - notes about cluster operation 293
 - operating in firewall environment 310
 - operating in multiple networks 303
 - operation and environment configuration depending on network configuration 301
 - operation and environment configuration in cluster system 237
 - overview of cluster operation 238
 - preparations required before installing 4, 52
 - registering host information 179
 - setting automated actions 139
 - setting correlation event generation 144
 - setting monitor startup for linked products 164
 - setting Tool Launcher window 167
 - setting up (UNIX) 49
 - setting up (Windows) 1
 - setting up Central Console 123
 - setting up Central Scope 177
 - setting up Central Scope operating environment 213
 - setting up JP1/IM - Manager 36, 84
 - setting up JP1/IM - View 45
 - settings for linking to other integrated management products 325
- JP1/IM - Manager
- executing setup program after installing 84
 - installing 5, 53
 - services and processes of 245
 - setting automatic startup of 84
 - setting automatic stop of 84
 - setting up 36, 84
 - settings during upgrade installation of 41, 90
 - settings for handling failures 36, 86
- JP1/IM - Rule Operation
- linking to 326
 - settings 326
 - settings for enabling linkage function of 326
 - settings for linking 46
 - settings for sending notifications to 327
- JP1/IM - View
- customizing operation of 163
 - installing 5
 - setting up 45
 - setting, for login user 161
 - settings for handling failures 45
 - settings for using Web-based 174
- JP1/PAM, setup for linkage with 223
- JP1/PFM, setup for linkage with 219
- JP1/Software Distribution
- remote installation using 7, 53
 - setup for linkage with 222
- jp1cohasetup.exe 253
- jp1cshasetup.exe 255
- K**
- KB meaning xiii
- L**
- linked products
- setting monitor startup for 164
 - setting up for 218
- List of Action Results window, whether to start when Event Console window starts 163
- logical host 239
- common definition information 246
 - deleting 269, 290
 - installing and setting up 250, 273
 - prerequisites for environment of 240
- logical IP address 239, 241
- login information, saving 181
- Login window, number of connection-target host entries in 163
- M**
- map display settings 194

- mathematical expression conventions xii
 - MB meaning xiii
 - memory dump output settings 37
 - memory entries, setting 148
 - monitor startup, setting 164
 - monitor windows
 - determining window to be used for opening 165
 - opening 164
 - monitoring nodes
 - adding 188, 204
 - changing monitoring status of 206
 - deleting 193, 205
 - moving 194
 - searching for 197, 206
 - setting attributes of 190, 205
 - monitoring object database, automatic backup and recovery settings for 40, 89
 - monitoring objects, examples of creating 226
 - monitoring tree
 - acquiring existing 183
 - acquiring, from server 183
 - acquiring, stored locally 183
 - applying customized 198
 - creating, by using GUI 180
 - customizing 186
 - customizing toolbar for 216
 - generating automatically 184
 - opening editing window 180
 - saving customized 197
 - searching for monitoring nodes in 197
 - setting monitoring range 195
 - setting up for linked products 218
 - settings for using visual icons 196
 - Monitoring Tree (Editing) window, opening 180
 - monitoring windows, using saved CSV files to create 210
 - moving monitoring nodes 194
 - multi-LAN environment
 - command execution (cluster operation) 307
 - command execution (non-cluster operation) 304
 - JP1/IM - View connection (cluster operation) 306
 - JP1/IM - View connection (non-cluster operation) 303
- N**
- NAT 314
 - support of 323
 - networks
 - operating in firewall environment 310
 - operating in multiple 303
 - operation and environment configuration depending on 301
 - non-cluster system
 - environment setup for running logical hosts in 294
 - evaluating configuration for running logical hosts in 294
 - logical host operation and environment configuration in 294
 - logical host operation in 295
 - notes about
 - cluster operation 293
 - installing and uninstalling 8, 57
 - number of events to acquire
 - at updating 161
 - per search 161
- O**
- opening edit window for Visual Monitoring window 200
 - OS environment, configuring 4, 52
- P**
- packet filtering 310
 - physical host 240
 - prerequisites for environment of 242
 - port numbers 318
 - changing 174
 - support of 317
 - prerequisite program, installing 4, 52
 - primary authentication server, copying settings for 17, 65
 - procedure
 - installation 5, 53

- uninstallation 7, 56
- profiles
 - collecting 104
 - collecting list of 106
 - displaying 107
- R**
- refresh interval 161
- regular expressions, setting 139
- remote installation 7, 53
- repeated events, consolidated display of 162
- resource start and stop sequence, setting 268, 289
- S**
- saving
 - customized monitoring tree at local host 197
 - customized Visual Monitoring window at local host 207
- script to be registered into cluster software, creating 285
- setting
 - abnormal process termination, restart settings in event of 87
 - attributes of monitoring nodes 190
 - automated actions 139
 - automatic startup 84
 - automatic stop 84
 - Central Console 123
 - Central Scope 177
 - Central Scope operating environment 213
 - cluster operating environment (UNIX) 272
 - cluster operating environment (Windows) 248
 - command execution environment 32, 80
 - completed-action linkage function 213
 - correlation event generation 144
 - environment 248, 272
 - Event Service 27, 75
 - execution conditions and details of automated actions 140
 - execution environment for automated action function 139
 - health check function 40, 89
 - host information 179
 - JP1 event filtering 125
 - JP1 event forwarding 29, 77
 - JP1 event issuance during action status change 152
 - JP1/IM - View for login user 161
 - JP1/IM - View operation 163
 - maximum number of status change events 213
 - memo entries 148
 - memory-resident status change condition function 215
 - monitor startup for linked products 164
 - monitoring range 195
 - number of connection-target host entries in Login window 163
 - start path of Web browser 163
 - startup sequence for services 14
 - system hierarchy (when IM Configuration Management is not used) 24, 72
 - system hierarchy (when IM Configuration Management is used) 20, 68
 - Tool Launcher window 167
 - whether data can be copied to clipboard 163
 - whether to start List of Action Results window when Event Console window starts 163
 - whether to start Tool Launcher window when Event Console window starts 163
- settings for
 - automatic backup and recovery for monitoring object database 40, 89
 - changing location of event acquisition filter 41, 90
 - deleting status change events when JP1 event handling is completed 214
 - event acquisition filters 132
 - event receiver filters 128
 - handling JP1/Base failures 19, 67
 - handling JP1/IM - Manager failures 36, 86
 - handling JP1/IM - View failures 45
 - initializing monitoring objects when JP1 events are received 215
 - issuing JP1 events in event of abnormal process termination 39, 88

- linking to other integrated management products 325
- operations to be performed during JP1/IM event acquisition 124
- restarting process in event of abnormal termination 38, 87
- severe events filters 130
- user authentication 15, 63
- user mapping 15, 63
- using functions of Central Scope 36, 86
- using visual icons 196
- using Web-based JP1/IM - View 174
- view filters 125

setup

- designing details of JP1/IM 4, 52
- IM Configuration Management - View 45
- JP1/IM - Manager 36, 84
- JP1/IM - Rule Operation linkage 46
- JP1/IM - View 45
- linked products 218
- procedure 2, 50

setup program, executing 84

severe events filters, setting 130

severity changing function, setting 160

shared disk 239, 241

- file organization on 243

start path of Web browser that is used when Tool Launcher window and monitor windows are called 163

startup sequence for services, setting 14

status change events, setting for maximum number 213

symbol conventions x

syntax conventions xi

system configurations using multiple LANs 303

system environment, configuring 4, 52

system hierarchy

- setting 93
- setting (when IM Configuration Management is not used) 24, 72
- setting (when IM Configuration Management is used) 20, 68

system-monitoring objects, example of creating 226

T

TB meaning xiii

timeout values for Web-based operation, setting 175

Tool Launcher window

- adding new menus 168
- determining window to be opened from 168
- setting 167
- settings for opening GUI of linked products from 167
- settings for opening Web page of linked products from 172
- whether to start, when Event Console window starts 163

tuning.conf 163

U

uninstallation

- notes about 8, 57
- procedure 7, 56

upgrade installation

- changing location of event acquisition filter 41, 90
- settings during 41, 90

user authentication, setting 15, 63

user mapping, setting 15, 17, 63, 65

user-specific event attributes, displaying 153

V

version information, displaying 56

version number conventions xiii

view filters

- changing 127
- creating new 125
- deleting 128
- settings for 125

virtualization system configuration

- setting 115
- settings for managing and monitoring 23, 71

visual icons, settings for using 196

Visual Monitoring window

- acquiring existing 201
- acquiring, from server 201
- adding monitoring nodes to 204

Index

- applying customized 207
- customizing 202
- deleting 209
- deleting monitoring nodes from 205
- opening edit window for 200
- saving customized 207
- setting background image for 202
- that has been saved locally, acquiring 202
- using GUI to create 200

W

- Web browser, setting up 174
- Web-based JP1/IM - View, settings for using 174

Reader's Comment Form

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

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

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

(For Hitachi use)
