

JP1 Version 11

**JP1/Integrated Management - Manager
Configuration Guide**

3021-3-A08-30(E)

Notices

■ Relevant program products

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

JP1/Integrated Management - Manager (for Windows):

P-2A2C-8EBL JP1/Integrated Management - Manager 11-50

The above product includes the following:

P-CC2A2C-9MBL JP1/Integrated Management - Manager 11-50 (for Windows Server 2016, Windows Server 2012, Windows Server 2008 R2)

P-CC2A2C-6HBL JP1/Integrated Management - View 11-50 (for Windows Server 2016, Windows 10, Windows 8.1, Windows 8, Windows Server 2012, Windows 7, Windows Server 2008 R2)

JP1/Integrated Management - Manager (for AIX):

P-1M2C-8EBL JP1/Integrated Management - Manager 11-50

The above product includes the following:

P-CC1M2C-9MBL JP1/Integrated Management - Manager 11-50 (for AIX)

P-CC2A2C-6HBL JP1/Integrated Management - View 11-50 (for Windows Server 2016, Windows 10, Windows 8.1, Windows 8, Windows Server 2012, Windows 7, Windows Server 2008 R2)

JP1/Integrated Management - Manager (for Linux):

P-812C-8EBL JP1/Integrated Management - Manager 11-50

The above product includes the following:

P-CC812C-9MBL JP1/Integrated Management - Manager 11-50 (for Linux 7, Linux 6 (x64), Oracle Linux 7, Oracle Linux 6 (x64), CentOS 7, CentOS 6 (x64))

P-CC9W2C-9MBL JP1/Integrated Management - Manager 11-50 (for SUSE Linux 12)

P-CC2A2C-6HBL JP1/Integrated Management - View 11-50 (for Windows Server 2016, Windows 10, Windows 8.1, Windows 8, Windows Server 2012, Windows 7, Windows Server 2008 R2)

■ Trademarks

HITACHI, HiRDB, JP1 are either trademarks or registered trademarks of Hitachi, Ltd. in Japan and other countries. Active Directory is either a registered trademark or a trademark of Microsoft Corporation in the United States and/or other countries.

IBM, AIX are trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide. Internet Explorer is either a registered trademark or trademark of Microsoft Corporation in the United States and/or other countries.

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

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

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

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

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

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

SUSE is a registered trademark or a trademark of SUSE LLC in the United States and other countries.

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

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

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

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

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

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

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

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

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

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

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

This product includes software developed by Andy Clark.

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

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

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



This product includes RSA BSAFE Cryptographic software of EMC Corporation.

■ Microsoft product name abbreviations

This manual uses the following abbreviations for Microsoft product names.

Abbreviation		Full name or meaning
Hyper-V		Microsoft ^(R) Windows Server ^(R) 2008 R2 Hyper-V ^(R)
		Microsoft ^(R) Windows Server ^(R) 2012 Hyper-V ^(R)
IE	Windows Internet Explorer	Windows ^(R) Internet Explorer ^(R)
SCVMM		Microsoft ^(R) System Center Virtual Machine Manager 2008
		Microsoft ^(R) System Center Virtual Machine Manager 2012
Windows 7		Microsoft ^(R) Windows ^(R) 7 Enterprise
		Microsoft ^(R) Windows ^(R) 7 Professional
		Microsoft ^(R) Windows ^(R) 7 Ultimate
Windows 8		Windows ^(R) 8 Enterprise
		Windows ^(R) 8 Pro
Windows 8.1		Windows ^(R) 8.1 Enterprise
		Windows ^(R) 8.1 Pro
Windows 10		Windows ^(R) 10 Enterprise 32-bit
		Windows ^(R) 10 Enterprise 64-bit
		Windows ^(R) 10 Home 32-bit
		Windows ^(R) 10 Home 64-bit
		Windows ^(R) 10 Pro 32-bit
		Windows ^(R) 10 Pro 64-bit
Windows Server 2008		Microsoft ^(R) Windows Server ^(R) 2008 Datacenter
		Microsoft ^(R) Windows Server ^(R) 2008 Enterprise
		Microsoft ^(R) Windows Server ^(R) 2008 Standard
Windows Server 2008 R2		Microsoft ^(R) Windows Server ^(R) 2008 R2 Datacenter

Abbreviation		Full name or meaning
		Microsoft ^(R) Windows Server ^(R) 2008 R2 Enterprise
		Microsoft ^(R) Windows Server ^(R) 2008 R2 Standard
Windows Server 2012	Windows Server 2012	Microsoft ^(R) Windows Server ^(R) 2012 Datacenter
		Microsoft ^(R) Windows Server ^(R) 2012 Standard
	Windows Server 2012 R2	Microsoft ^(R) Windows Server ^(R) 2012 R2 Datacenter
		Microsoft ^(R) Windows Server ^(R) 2012 R2 Standard
Windows Server 2016		Microsoft ^(R) Windows Server ^(R) 2016 Datacenter
		Microsoft ^(R) Windows Server ^(R) 2016 Standard

Windows is sometimes used generically, referring to Windows Server 2016, Windows 10, Windows 8.1, Windows 8, Windows Server 2012, Windows 7, and Windows Server 2008 R2.

■ Restrictions

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

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

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

■ Issued

Nov. 2017: 3021-3-A08-30(E)

■ Copyright

Copyright (C) 2016, 2017, Hitachi, Ltd.

Copyright (C) 2017, Hitachi Solutions, Ltd.

Summary of amendments

The following table lists changes in this manual (3021-3-A08-30(E)) and product changes related to this manual.

Changes	Location
A description was added to explain that the automated action definition file must be updated when JP1/IM - Manager is upgraded from versions earlier than 11-10.	<i>1.18.3(2), 2.17.5(3), 4.5.2</i>
A common exclusion-conditions group (extended) can now be set to exclude a collected JP1 event from automated-action execution.	<i>4.2.4(3), 4.2.4(3)(b)</i>
The maximum number of defined common exclusion-conditions groups (extended) was increased to 2,500.	<i>4.2.4(3)(b)</i>
Defined automated actions can now be enabled or disabled by using the Action Parameter Definitions window in JP1/IM - View or the <code>jcachange</code> command.	<i>4.5.2(1)</i>
Exclusion processing caused by common exclusion-conditions and update processing of common exclusion-conditions definition are now logged into history files.	<i>6.1.3(2), 7.1.3(2)</i>
For the procedure to link with JP1/Service Support, a step was added for cases where the incident registration mode is set to 3.	<i>9.1.1</i>

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

Preface

This manual explains how to set up JP1/Integrated Management - Manager and JP1/Integrated Management - View systems.

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

■ Intended readers

This manual is intended for personnel who use JP1/IM to create the infrastructure for managing open-platform systems. More specifically, it is intended for:

- System administrators who use JP1/IM to create systems that centrally monitor events occurring in the system
- Those who have knowledge of operating systems and applications

■ 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 (for Windows)

Chapter 6 describes the operation and environment configuration of JP1/IM - Manager in a cluster system for Windows.

7. Operation and Environment Configuration in a Cluster System (for UNIX)

Chapter 7 describes the operation and environment configuration of JP1/IM - Manager in a cluster system for UNIX.

8. Operation and Environment Configuration Depending on the Network Configuration

Chapter 8 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).

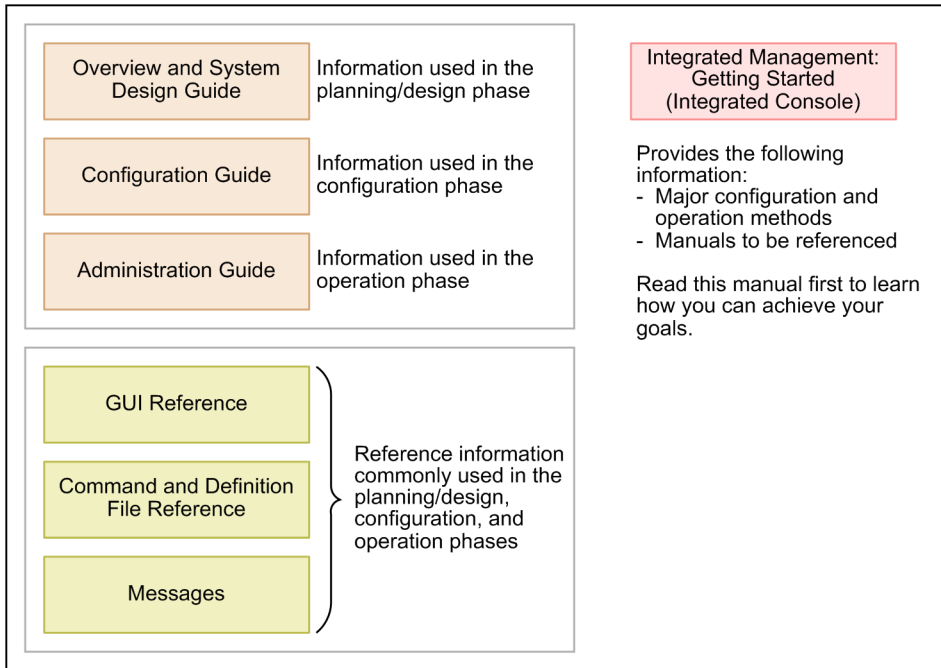
9. Settings for Linking to Other JP1 Products

Chapter 9 explains how to set up environments for linking JP1/IM to other JP1 products (such as JP1/IM - Service Support, JP1/IM - Navigation Platform, JP1/IM - Rule Operation, JP1/AJS, and JP1/PFM).

■ Manual suite

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

The following figure explains which phases the JP1/IM manuals provide information for.



■ Conventions: Diagrams

This manual uses the following conventions in diagrams:

• Computer (terminal)



• Computer



• Disk device, file



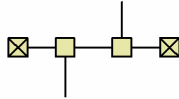
• Screen



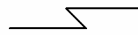
• WAN



• Network



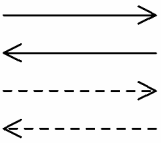
• Communication channel



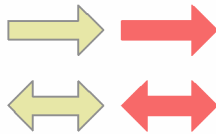
• Program



• Flow of control



• Flow of data



• Flow of process or task



• Error



The following table explains the text formatting conventions used in this manual:

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

The following table explains the symbols used in this manual:

Symbol	Convention
	In syntax explanations, a vertical bar separates multiple items, and has the meaning of OR. For example: A B C means A, or B, or C.
{ }	In syntax explanations, curly brackets indicate that only one of the enclosed items is to be selected. For example: { A B C } means only one of A, or B, or C.
[]	In syntax explanations, square brackets indicate that the enclosed item or items are optional. For example: [A] means that you can specify A or nothing. [B C] means that you can specify B, or C, or nothing.
. . .	In coding, an ellipsis (. . .) indicates that one or more lines of coding have been omitted. In syntax explanations, an ellipsis indicates that the immediately preceding item can be repeated as many times as necessary. For example: A, B, B, . . . means that, after you specify A, B, you can specify B as many times as necessary.
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: Installation folders for the Windows version of JP1/IM and JP1/Base

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

Product name	Installation folder	Default installation folder [#]
JP1/IM - View	<i>View-path</i>	<i>system-drive</i> : \Program Files\Hitachi\JP1CoView
JP1/IM - Manager	<i>Manager-path</i>	<i>system-drive</i> : \Program Files\Hitachi\JP1IMM
	<i>Console-path</i>	<i>system-drive</i> : \Program Files\Hitachi\JP1Cons
	<i>Scope-path</i>	<i>system-drive</i> : \Program Files\Hitachi\JP1Scope
JP1/Base	<i>Base-path</i>	<i>system-drive</i> : \Program Files\Hitachi\JP1Base

[#]: Represents the installation folder when the product is installed in the default location. The location represented by *system-drive*: \Program Files is determined at the time of installation by an OS environment variable, and might differ depending on the environment.

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

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

■ Conventions: Version numbers

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

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

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

■ Online manuals

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

The HTML manual has the same contents as this manual.

To view the HTML manual:

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

Note:

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

Contents

Notices 2

Summary of amendments 6

Preface 7

1	Installation and Setup (for Windows)	22
1.1	Installation and setup procedures (for Windows)	23
1.2	Preparations required before installation (for Windows)	25
1.2.1	Designing the JP1/IM setup details (for Windows)	25
1.2.2	Configuring the system environment (for Windows)	25
1.2.3	Installing the prerequisite program (for Windows)	25
1.3	Installing JP1/IM - Manager and JP1/IM - View (for Windows)	26
1.3.1	Installation procedure (for Windows)	26
1.3.2	Settings required immediately after installation (for Windows)	28
1.3.3	Notes about installing (for Windows)	29
1.4	Creating IM databases (for Windows)	31
1.4.1	Preparations for creating IM databases (for Windows)	31
1.4.2	Setting up the integrated monitoring database (for Windows)	32
1.4.3	Setting up the IM Configuration Management database (for Windows)	33
1.4.4	Settings for using the functions of IM Configuration Management (for Windows)	34
1.4.5	Updating IM databases (for Windows)	35
1.5	Setting the startup sequence for services (for Windows)	36
1.6	Setting up user authentication and user mapping (for Windows)	37
1.6.1	Specifying the authentication server (for Windows)	37
1.6.2	Registering JP1 users (for Windows)	38
1.6.3	Setting operation permissions for the JP1 users (for Windows)	38
1.6.4	Copying the primary authentication server settings (for Windows)	38
1.6.5	Setting user mapping (for Windows)	39
1.7	Specifying settings for handling JP1/Base failures (for Windows)	40
1.8	Setting the system hierarchy (when IM Configuration Management is used) (for Windows)	41
1.8.1	Using IM Configuration Management - View to set the system hierarchy (for Windows)	41
1.8.2	Using the export and import functions to set the system hierarchy (for Windows)	43
1.8.3	Settings for managing and monitoring a virtualization system configuration (for Windows)	43
1.9	Setting the system hierarchy (when IM Configuration Management is not used) (for Windows)	44
1.9.1	Setting the configuration definition information (for Windows)	44
1.9.2	Deleting the configuration definition information (for Windows)	45
1.9.3	Changing the configuration definition information (for Windows)	45
1.9.4	Notes about setting the configuration definition information (for Windows)	45

1.10	Setting up Event Service (for Windows)	47
1.11	Setting JP1 event forwarding when IM Configuration Management is used (for Windows)	48
1.12	Setting JP1 event forwarding when IM Configuration Management is not used (for Windows)	49
1.13	Collecting and distributing Event Service definition information when IM Configuration Management is used (for Windows)	50
1.14	Collecting and distributing Event Service definition information when IM Configuration Management is not used (for Windows)	51
1.15	Setting up a command execution environment (for Windows)	52
1.15.1	Setting up the command execution function for managed hosts (for Windows)	52
1.15.2	Setting up a client application execution environment (for Windows)	53
1.16	Specifying settings for using the source host name of Event Service in the FQDN format (for Windows)	54
1.16.1	Prerequisites (for Windows)	54
1.16.2	Setting method (for Windows)	54
1.16.3	Startup method (for Windows)	54
1.17	Specifying settings for monitoring logs on remotely monitored hosts (for Windows)	56
1.17.1	Configuring WMI (for Windows)	56
1.17.2	NetBIOS settings (NetBIOS over TCP/IP) (for Windows)	62
1.17.3	Configuring SSH (for Windows)	63
1.17.4	Specifying the size of log information that can be collected per monitoring interval (for Windows)	70
1.18	Setting up JP1/IM - Manager (for Windows)	71
1.18.1	Specifying settings for using the functions of Central Scope (for Windows)	71
1.18.2	Specifying settings for handling JP1/IM - Manager failures (for Windows)	71
1.18.3	Specifying settings for upgrading (for Windows)	74
1.19	Setting up JP1/IM - View (for Windows)	78
1.19.1	Specifying settings for handling JP1/IM - View failures (for Windows)	78
1.19.2	Customizing operation of JP1/IM - View (Central Console viewer and Central Scope viewer) (for Windows)	78
1.19.3	Setting up and customizing IM Configuration Management - View (for Windows)	79
1.19.4	Setting up JP1/IM - Rule Operation linkage (for Windows)	80
1.20	Saving manuals to a computer (for Windows)	82
1.21	Uninstallation (for Windows)	84
1.21.1	Uninstallation procedure (for Windows)	84
1.21.2	Notes on uninstallation (for Windows)	86
2	Installation and Setup (for UNIX)	87
2.1	Installation and setup procedures (for UNIX)	88
2.2	Preparations required before installation (for UNIX)	90
2.2.1	Designing the JP1/IM setup details (for UNIX)	90
2.2.2	Configuring the system environment (for UNIX)	90
2.2.3	Installing the prerequisite program (for UNIX)	90
2.3	Installing JP1/IM - Manager (for UNIX)	91
2.3.1	Installation procedure (for UNIX)	91

2.3.2	How to use the Hitachi Program Product Installer (for UNIX)	92
2.3.3	Settings required immediately after installation (for UNIX)	94
2.3.4	Notes about installing (for UNIX)	96
2.4	Creating IM databases (for UNIX)	97
2.4.1	Preparations for creating IM databases (for UNIX)	97
2.4.2	Setting up the integrated monitoring database (for UNIX)	98
2.4.3	Setting up the IM Configuration Management database (for UNIX)	99
2.4.4	Settings for using the functions of IM Configuration Management (for UNIX)	100
2.4.5	Updating IM databases (for UNIX)	101
2.5	Setting up user authentication and user mapping (for UNIX)	102
2.5.1	Specifying the authentication server (for UNIX)	103
2.5.2	Registering JP1 users (for UNIX)	103
2.5.3	Setting operation permissions for the JP1 users (for UNIX)	103
2.5.4	Copying the primary authentication server settings (for UNIX)	104
2.5.5	Setting user mapping (for UNIX)	104
2.6	Specifying settings for handling JP1/Base failures (for UNIX)	105
2.7	Setting the system hierarchy (when IM Configuration Management is used) (for UNIX)	106
2.7.1	Using IM Configuration Management - View to set the system hierarchy (for UNIX)	106
2.7.2	Using the export and import functions to set the system hierarchy (for UNIX)	108
2.7.3	Settings for managing and monitoring a virtualization system configuration (for UNIX)	108
2.8	Setting the system hierarchy (when IM Configuration Management is not used) (for UNIX)	109
2.8.1	Setting the configuration definition information (for UNIX)	109
2.8.2	Deleting the configuration definition information (for UNIX)	110
2.8.3	Changing the configuration definition information (for UNIX)	110
2.8.4	Notes about setting the configuration definition information (for UNIX)	110
2.9	Setting up Event Service (for UNIX)	112
2.10	Setting JP1 event forwarding when IM Configuration Management is used (for UNIX)	113
2.11	Setting JP1 event forwarding when IM Configuration Management is not used (for UNIX)	114
2.12	Collecting and distributing Event Service definition information when IM Configuration Management is used (for UNIX)	115
2.13	Collecting and distributing Event Service definition information when IM Configuration Management is not used (for UNIX)	116
2.14	Setting up a command execution environment (for UNIX)	117
2.14.1	Setting up the command execution function for managed hosts (for UNIX)	117
2.14.2	Setting up a client application execution environment (for UNIX)	118
2.15	Specifying settings for using the source host name of Event Service in the FQDN format (for UNIX)	119
2.15.1	Prerequisites (for UNIX)	119
2.15.2	Setting method (for UNIX)	119
2.15.3	Startup method (for UNIX)	119
2.16	Specifying settings for monitoring logs on remotely monitored hosts (for UNIX)	120
2.16.1	Configuring SSH (for UNIX)	120
2.16.2	Specifying the size of log information that can be collected per monitoring interval (for UNIX)	127

2.17	Setting up JP1/IM - Manager (for UNIX)	128
2.17.1	Executing the setup program (for UNIX)	128
2.17.2	Setting automatic startup and automatic stop (for UNIX)	128
2.17.3	Specifying settings for using the functions of Central Scope (for UNIX)	131
2.17.4	Specifying settings for handling JP1/IM - Manager failures (for UNIX)	131
2.17.5	Specifying settings for upgrading (for UNIX)	135
2.18	Saving manuals to a computer (for UNIX)	139
2.19	Uninstallation (for UNIX)	141
2.19.1	Uninstallation procedure (for UNIX)	141
2.19.2	Notes on uninstallation (for UNIX)	143
3	Using IM Configuration Management to Set the System Hierarchy	144
3.1	Registering hosts	145
3.1.1	Registering hosts	145
3.1.2	Registering remotely monitored hosts	145
3.1.3	Collecting information from hosts	147
3.1.4	Displaying host information	148
3.1.5	Changing the attributes of host information	148
3.1.6	Deleting hosts	149
3.2	Setting the system hierarchy	151
3.2.1	Collecting the system hierarchy	151
3.2.2	Displaying the system hierarchy	152
3.2.3	Verifying the system hierarchy	152
3.2.4	Editing the system hierarchy	153
3.2.5	Synchronizing the system hierarchy	159
3.3	Setting a virtualization system configuration	160
3.3.1	Using IM Configuration Management to manage a virtualization configuration	160
3.3.2	Collecting virtualization system configuration information	174
3.3.3	Using Central Scope to monitor a virtualization configuration	176
3.4	Setting business groups	178
3.4.1	Creating business groups	178
3.4.2	Adding hosts to business groups	184
3.4.3	Deleting hosts from business groups	184
3.4.4	Using Central Scope to monitor business groups	184
3.5	Setting the profiles	186
3.5.1	Setting the profiles on hosts in an agent configuration	186
3.5.2	Setting the profiles on hosts in a remote monitoring configuration	199
3.6	Importing and exporting the management information in IM Configuration Management	209
4	Setting Up Central Console	210
4.1	Settings for the operations to be performed during JP1/IM event acquisition	211
4.1.1	Displaying events by specifying the event acquisition range at login	211

4.2	Setting JP1 event filtering	213
4.2.1	Settings for view filters	213
4.2.2	Settings for event receiver filters	215
4.2.3	Settings for severe events filters	217
4.2.4	Settings for event acquisition filters	219
4.3	Setting monitoring of repeated events to be prevented	226
4.4	Setting the display colors of JP1 events	227
4.5	Setting automated actions	228
4.5.1	Setting up an execution environment for the automated action function	228
4.5.2	Setting the execution conditions and details of automated actions	228
4.5.3	Settings for monitoring the automated action execution status	230
4.5.4	Setting suppression of automated action execution	231
4.5.5	Setting email transmissions	231
4.6	Settings for generating correlation events	236
4.6.1	Setting startup of the correlation event generation function	236
4.6.2	Setting the size and number of correlation event generation history files	236
4.6.3	Setting startup options	237
4.6.4	Creating and applying a correlation event generation definition	238
4.7	Setting memo entries	239
4.8	Editing event guide information	240
4.8.1	How to edit event guide information	240
4.9	Setting JP1 event issuance during action status change	242
4.10	Adding program-specific attributes	243
4.11	Setting the display and specification of program-specific extended attributes	244
4.12	How to display user-specific event attributes	246
4.12.1	Creating the definition files	248
4.12.2	Enabling the definition files	250
4.13	Setting the severity changing function	251
4.13.1	Setting the severity changing function from the Severity Change Definition Settings window	251
4.13.2	Setting the severity changing function by using the severity changing definition file	252
4.14	Setting the display message change function	254
4.14.1	Configuring from the Display Message Change Definition Settings window	254
4.14.2	Configuring from the display message change definition file	256
4.14.3	Procedure for issuing events after display messages have been changed	256
4.15	Setting event source host mapping	258
4.16	Setting JP1/IM - View for each login user	261
4.16.1	Settings for JP1/IM - View	261
4.16.2	Procedure for specifying JP1/IM - View settings	262
4.17	Setting monitor startup for linked products	263
4.17.1	How to open monitor windows	263
4.17.2	Determining the window to be used for opening monitor windows	264

4.17.3	Creating the definition files	264
4.18	Setting the Tool Launcher window	266
4.18.1	Settings for opening the GUI of linked products from the Tool Launcher window	266
4.18.2	How to add new menus	266
4.18.3	Determining a window to be opened from the Tool Launcher window	267
4.18.4	Creating the definition files	267
4.18.5	Settings for opening the Web page of a linked product from the Tool Launcher window	270
4.19	Settings for using a Web-based JP1/IM - View	271
4.19.1	Installing an HTTP server	271
4.19.2	Setting up the HTTP server	271
4.19.3	Setting up a Web browser	272
4.19.4	Specifying display settings for the Java Console window	272
4.19.5	Setting timeout values for Web-based operation	272
4.19.6	Setting the URL of the web-based version of JP1/IM - View	273
4.20	Setting reference and operation restrictions on business groups	274
5	Setting Up Central Scope	276
5.1	Overview of the Central Scope environment setup	277
5.1.1	Before starting Central Scope environment setup	277
5.2	Registering host information	278
5.3	Using the GUI to create a monitoring tree	279
5.3.1	Opening the Monitoring Tree (Editing) window	279
5.3.2	Acquiring an existing monitoring tree	280
5.3.3	Generating a monitoring tree automatically	281
5.3.4	Customizing a monitoring tree	283
5.3.5	Saving a customized monitoring tree at the local host	292
5.3.6	Applying a customized monitoring tree to the manager	293
5.4	Using the GUI to create a Visual Monitoring window	294
5.4.1	Opening an edit window for the Visual Monitoring window	294
5.4.2	Acquiring an existing Visual Monitoring window	295
5.4.3	Customizing a Visual Monitoring window	295
5.4.4	Saving a customized Visual Monitoring window at the local host	299
5.4.5	Applying a customized Visual Monitoring window to the manager	299
5.4.6	Editing the list of Visual Monitoring windows and deleting Visual Monitoring windows	300
5.5	Editing the saved CSV file to create the Monitoring Tree window	302
5.6	Editing guide information	303
5.6.1	How to edit guide information	303
5.7	Setting up a Central Scope operating environment	306
5.7.1	Setting for the maximum number of status change events	306
5.7.2	Setting the completed-action linkage function	306
5.7.3	Settings for automatically deleting status change events when JP1 event handling is completed	307
5.7.4	Settings for initializing monitoring objects when JP1 events are received	307

5.7.5	Setting the memory-resident status change condition function	308
5.7.6	Customizing the toolbar for the monitoring tree	308
5.7.7	Settings for suppressing the display of a monitoring node name and the icon margin	309
5.7.8	Settings of the status color of a monitoring node name and monitoring node	310
5.7.9	Settings for suppressing the movement of the icon of a monitoring node	312
5.8	Setting up for linked products	313
5.8.1	Setup for linkage with JP1/AJS	313
5.8.2	Setup for linkage with JP1/Cm2/SSO	314
5.8.3	Setup for linkage with JP1/PFM	316
5.8.4	Setup for linkage with HP NNM	317
5.8.5	Setup for linkage with JP1/Software Distribution	318
5.8.6	Setup for linkage with JP1/PAM	319
5.8.7	Setup for linkage with Cosminexus	319
5.8.8	Setup for linkage with HiRDB	320
5.8.9	Setup for linkage with JP1/ServerConductor	320
5.9	Examples of monitoring object creation	321
5.9.1	Example of creating system-monitoring objects (JP1/AJS jobnet monitoring)	321
5.9.2	Example of creating a general monitoring object (CPU monitoring by JP1/Cm2/SSO)	322
5.9.3	Example of creating a general monitoring object (HiRDB monitoring)	327
5.9.4	Example of creating a general monitoring object (Cosminexus resource monitoring by JP1/Cm2/SSO)	332
6	Operation and Environment Configuration in a Cluster System (for Windows)	338
6.1	Overview of cluster operation (for Windows)	339
6.1.1	Overview of a cluster system (for Windows)	339
6.1.2	Prerequisites for cluster operation (for Windows)	340
6.1.3	JP1/IM configuration in a cluster system (for Windows)	343
6.2	Environment setup procedure for cluster operation (for Windows)	346
6.3	Installing and setting up logical hosts (new installation and setup) (for Windows)	348
6.3.1	Newly installing JP1/Base and JP1/IM - Manager (for Windows)	348
6.3.2	Setting up the physical host environment during new installation (for Windows)	348
6.3.3	Setting up the logical host environment (primary node) during new installation (for Windows)	349
6.3.4	Copying the common definition information during new installation (for Windows)	354
6.3.5	Setting up the logical host environment (secondary node) during new installation (for Windows)	354
6.4	Registering into the cluster software during new installation and setup (for Windows)	359
6.4.1	Registering into the cluster software (for Windows)	359
6.4.2	Setting the resource start and stop sequence (for Windows)	360
6.5	Upgrade installation and setup of logical hosts (for Windows)	361
6.5.1	Upgrade installation of logical hosts (for Windows)	361
6.5.2	Setting up the physical host environment during upgrade installation (for Windows)	361
6.5.3	Setting up the logical host environment (primary node) during upgrade installation (for Windows)	362

6.5.4	Copying the common definition information during upgrade installation (for Windows)	363
6.6	Uninstalling logical hosts (for Windows)	364
6.6.1	Deleting logical hosts (for Windows)	364
6.6.2	Uninstalling JP1/IM - Manager and JP1/Base (for Windows)	366
6.7	Procedures for changing settings (for Windows)	367
6.7.1	Changing settings in files (for Windows)	367
6.7.2	Using commands to change settings (for Windows)	367
6.7.3	Updating IM databases in a cluster environment (for Windows)	368
6.8	Notes about cluster operation (for Windows)	370
6.9	Logical host operation and environment configuration in a non-cluster system (for Windows)	371
6.9.1	Evaluating the configuration for running logical hosts in a non-cluster system (for Windows)	371
6.9.2	Environment setup for running logical hosts in a non-cluster system (for Windows)	371
6.9.3	Notes about running logical hosts in a non-cluster system (for Windows)	372

7 Operation and Environment Configuration in a Cluster System (for UNIX) 373

7.1	Overview of cluster operation (for UNIX)	374
7.1.1	Overview of a cluster system (for UNIX)	374
7.1.2	Prerequisites for cluster operation (for UNIX)	374
7.1.3	JP1/IM configuration in a cluster system (for UNIX)	374
7.2	Environment setup procedure for cluster operation (for UNIX)	377
7.3	Installing and setting up logical hosts (new installation and setup) (for UNIX)	379
7.3.1	Newly installing JP1/Base and JP1/IM - Manager (for UNIX)	379
7.3.2	Setting up the physical host environment during new installation (for UNIX)	379
7.3.3	Setting up the logical host environment (primary node) during new installation (for UNIX)	380
7.3.4	Copying the common definition information during new installation (for UNIX)	383
7.3.5	Setting up the logical host environment (secondary node) during new installation (for UNIX)	384
7.4	Registering into the cluster software during new installation and setup (for UNIX)	387
7.4.1	Creating a script to be registered into the cluster software (for UNIX)	387
7.4.2	Setting the resource start and stop sequence (for UNIX)	389
7.5	Upgrade installation and setup of logical hosts (for UNIX)	390
7.5.1	Upgrade installation of logical hosts (for UNIX)	390
7.5.2	Setting up the physical host environment during upgrade installation (for UNIX)	390
7.5.3	Setting up the logical host environment (primary node) during upgrade installation (for UNIX)	391
7.5.4	Copying the common definition information during upgrade installation (for UNIX)	392
7.6	Uninstalling logical hosts (for UNIX)	393
7.6.1	Deleting logical hosts (for UNIX)	393
7.6.2	Uninstalling JP1/IM - Manager and JP1/Base (for UNIX)	395
7.7	Procedures for changing settings (for UNIX)	396
7.7.1	Changing settings in files (for UNIX)	396
7.7.2	Using commands to change settings (for UNIX)	396
7.7.3	Updating IM databases in a cluster environment (for UNIX)	397

7.8	Notes about cluster operation (for UNIX)	399
7.9	Logical host operation and environment configuration in a non-cluster system (for UNIX)	400
7.9.1	Evaluating the configuration for running logical hosts in a non-cluster system (for UNIX)	400
7.9.2	Environment setup for running logical hosts in a non-cluster system (for UNIX)	400
7.9.3	Notes about running logical hosts in a non-cluster system (for UNIX)	401

8 Operation and Environment Configuration Depending on the Network Configuration 402

8.1	Controlling communications by JP1/Base	403
8.2	Operating in multiple networks	404
8.2.1	Example 1 (non-cluster operation with JP1/IM - View connection)	404
8.2.2	Example 2 (non-cluster operation with command execution)	405
8.2.3	Example 3 (cluster operation with JP1/IM - View connection)	406
8.2.4	Example 4 (cluster operation with command execution)	407
8.3	Operating in a firewall environment	409
8.3.1	Basic information about firewalls	409
8.3.2	JP1/IM communication	414
8.4	Configuring encrypted communication	420
8.4.1	Newly using the communication encryption function	420
8.4.2	Changing configured certificates	424
8.4.3	Stopping using the communication encryption function	427
8.4.4	Configuring JP1/IM - Manager	429
8.4.5	Checking whether the communication encryption function has been configured correctly	430

9 Settings for Linking to Other JP1 Products 431

9.1	Linking to JP1/Service Support	432
9.1.1	Enabling calling the JP1/Service Support window	432
9.2	Linking to JP1/Navigation Platform	433
9.3	Linking to JP1/IM - Rule Operation	434
9.3.1	Settings for enabling the JP1/IM - Rule Operation linkage function	434
9.3.2	Settings for sending notifications to JP1/IM - Rule Operation	435
9.3.3	Settings for checking notifications on the Event Console window	435
9.4	Linking with JP1/AJS	436
9.4.1	Settings for launching a JP1/AJS window by monitor startup	436
9.4.2	Settings for launching a JP1/AJS window from the Tool Launcher window	436
9.4.3	Settings for displaying the monitor window from the event guide information	436
9.4.4	Settings for displaying the monitor window from an email sent by an automated action	436
9.5	Linking with JP1/PFM	437
9.5.1	Settings for launching a JP1/PFM window by monitor startup	437
9.5.2	Settings for launching a JP1/PFM window from the Tool Launcher window	437
9.5.3	Settings for displaying event-source-host performance reports	437

1

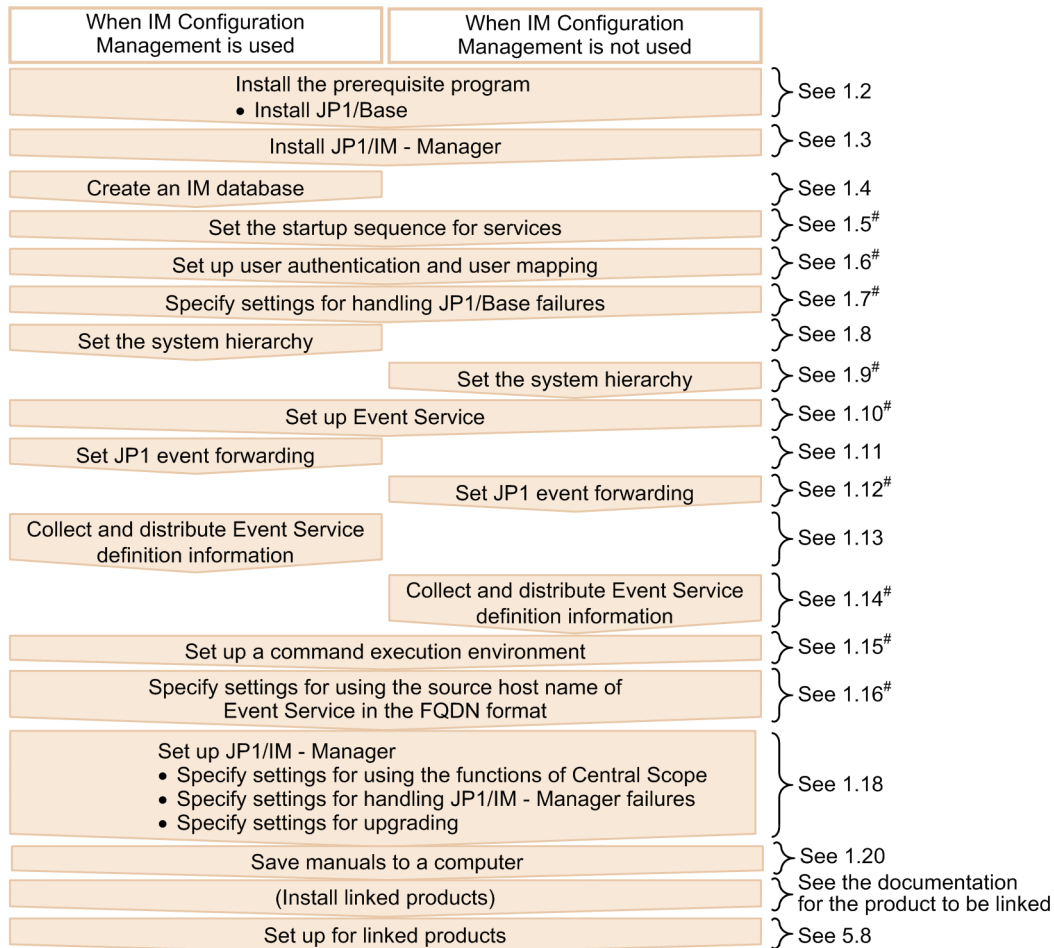
Installation and Setup (for Windows)

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

1.1 Installation and setup procedures (for Windows)

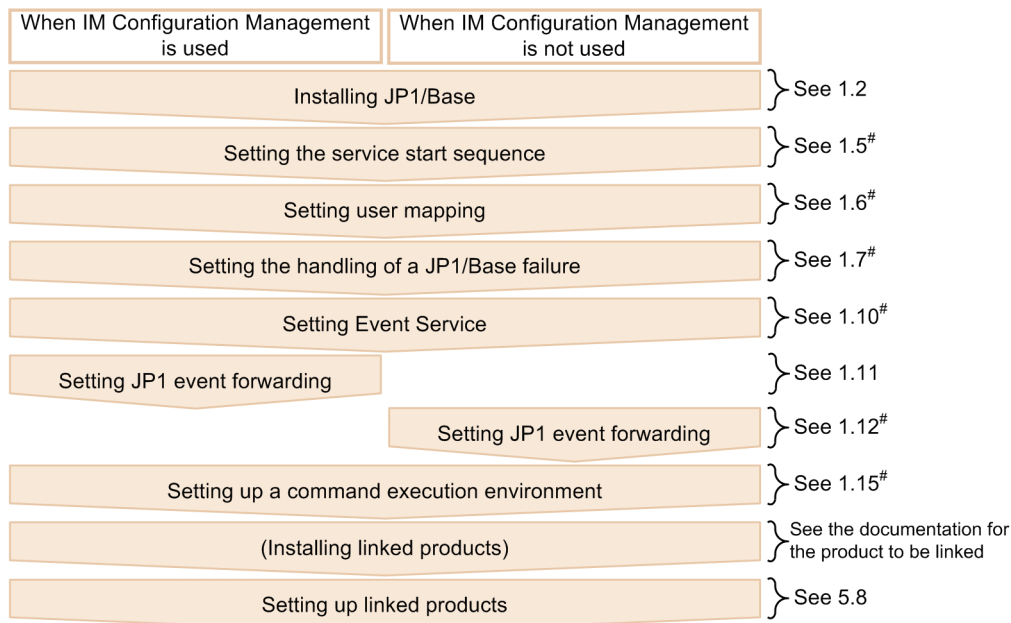
This section describes the procedure from the beginning of installation to the end of setup for a manager, an agent, a host to be monitored remotely, and a viewer. For details about the uninstallation procedure, see [1.21.1 Uninstallation procedure \(for Windows\)](#).

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



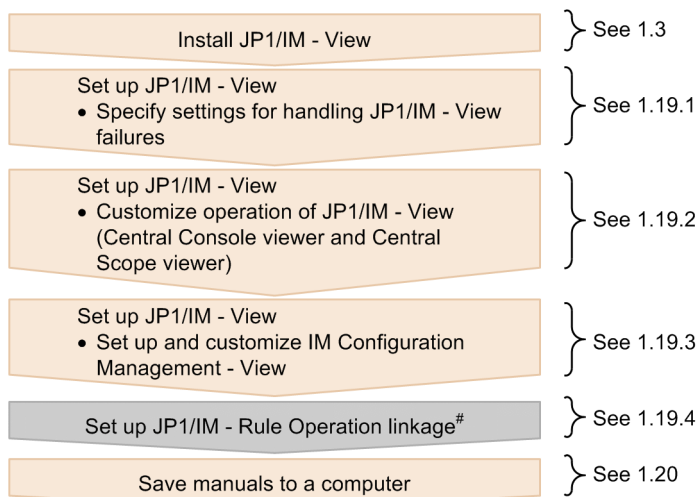
#: For details, see the *JP1/Base User's Guide*.

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



[#]: For details, see the *JP1/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*.

For details about the settings for monitoring logs on hosts that will be monitored remotely, see [1.17 Specifying settings for monitoring logs on remotely monitored hosts \(for Windows\)](#).

For details about the settings for using the communication encryption function that encrypts communication data, see [8.4 Configuring encrypted communication](#).

1.2 Preparations required before installation (for Windows)

1.2.1 Designing the JP1/IM setup details (for Windows)

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 *JP1/Integrated Management - Manager Overview and System Design Guide*.

1.2.2 Configuring the system environment (for Windows)

(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.
- A host name and IP address can be uniquely resolved.

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 (for Windows)

(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 *JP1/Integrated Management - Manager Overview and System Design Guide*. For details about how to install JP1/Base, see the *JP1/Base User's Guide*.

1.3 Installing JP1/IM - Manager and JP1/IM - View (for Windows)

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

1.3.1 Installation procedure (for Windows)

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

(1) How to install JP1/IM - Manager

To install:

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/IM-Manager service. If a JP1/IM - View is connected to the JP1/IM - Manager for which you want to perform an upgrade installation, the login user should log out from the JP1/IM - Manager.

2. Insert the distribution medium in the corresponding drive and start the installation.

Follow the instructions of the installer, which starts automatically.

Select the software you want to install, and then enter the following items:

- User information

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

- Installation folders

In an x64 environment, do not install JP1/IM under *system-drive*\Program Files\ (the Program Files folder without x86). Problems might occur during operation if JP1/IM is in the Program Files folder that contains 64-bit modules.

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

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}: The default installation folder is *system-drive* : \Program Files\Hitachi. In Windows, this value might be different depending on the environment because the value of *system-drive* : \Program Files is determined by the setting of an OS environment variable at the time of installation.

^{#2}: If a previous version of JP1/IM - Manager 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 must be a fixed disk.

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 [1.3.3 Notes about installing \(for Windows\)](#).

Important

- If you have upgraded JP1/IM - Manager in an environment in which IM databases have already been set up, use the `jimdbupdate` command to update the IM databases. If the IM databases have not been updated, a warning message is displayed when JP1/IM - Manager starts.
- You must specify a fixed disk as the drive for the JP1/IM - Manager installation folder. JP1/IM - Manager and JP1/IM - View must not be installed on a removable disk, network drive, or UNC path.

(2) How to install JP1/IM - View

To install:

1. Terminate all programs.

Before you start the installation, terminate all programs.

2. Insert the distribution medium in the corresponding drive and start the installation.

Follow the instructions of the installer, which starts automatically.

Select the software you want to install, and then enter the following items:

- User information

Enter this information only if you are performing a new installation.

- Installation folders

In an x64 environment, do not install JP1/IM under *system-drive*\Program Files\ (the Program Files folder that is not x86 compatible). Problems might occur during operation if JP1/IM is in the Program Files folder that contains 64-bit modules.

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

Table 1–2: Folders created during installation

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. In Windows, this value might be different depending on the environment because the value of *system-drive* : \Program Files is determined by the setting of an OS environment variable at the time of installation.

^{#2}: If an old version of JP1/IM - View was installed in a different folder, that installation folder is inherited and the default folder listed above is not created.

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

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 [1.3.3 Notes about installing \(for Windows\)](#).

Important

You must specify a fixed disk as the drive for the JP1/IM - View installation folder. 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 - View if it is installed anywhere other than on a fixed disk.

(3) 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 *JP1/Integrated Management - Manager Overview and System Design Guide*.

Remote installation using JP1/NETM/DM, JP1/IT Desktop Management 2 and Job Management Partner 1/Software Distribution

JP1/IM supports remote installation (software distribution) using JP1/NETM/DM, JP1/IT Desktop Management 2 and Job Management Partner 1/Software Distribution, and you can perform a new installation as well as an upgrade installation of JP1/IM. See JP1/NETM/DM, JP1/IT Desktop Management 2 or Job Management Partner 1/Software Distribution Manual for more information.

Be sure to use a JP1/NETM/DM 09-00 or later packager, a JP1/IT Desktop Management 2 packager or a Job Management Partner 1/Software Distribution 09-00 or later packager to package this software product. JP1/NETM/DM is sold only in Japan.

1.3.2 Settings required immediately after installation (for Windows)

If you will be changing the locale (system locale) after installation, you must set the appropriate encoding shown in the table below. Specify this setting in JP1/Base.

Table 1–3: Windows encoding

OS	Language	Encoding
Windows	Japanese	SJIS
	Chinese	GB18030
	English	C

(1) How to set the encoding

1. Edit `jplbs_param.conf`.

Use an editor to open the `Base-path\conf\jplbs_param.conf` file, set the encoding shown in the table above in the *encoding* part of `"LANG"="encoding"`.

2. Save the file, and then execute the following command with Administrator permissions:

```
Base-path\bin\jbssetcnf-Base-path\conf\jplbs_param.conf
```

3. Start or restart JP1/Base and JP1/IM - Manager.

The settings take effect when JP1/Base and JP1/IM - Manager start. If JP1/Base and JP1/IM - Manager are already running, restart JP1/Base and JP1/IM - Manager.



Note

Once you have set the encoding and started the operation, you can still use the steps above to change the encoding.

1.3.3 Notes about installing (for Windows)

- Relationship between products

JP1/IM - Manager requires JP1/Base. When you install 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 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 install JP1/IM - View, the startup type of the Hitachi Network Objectplaza Trace Monitor 2 service (Hitachi Network Objectplaza Trace Library) is set to Automatic, the service can start automatically when the system starts.

#: In Windows, this value might be different depending on the environment because the value of *system-drive*: \Program Files is determined by the setting of an OS environment variable at the time of installation.

- 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 *Appendix C. Port Numbers* in the *JP1/Integrated Management - Manager Overview and System Design Guide* are set. The port numbers are deleted during uninstallation.

#: In Windows, this value might be different depending on the environment because the value of *system-drive*: \Program Files is determined by the setting of an OS environment variable at the time of installation.

- 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 might be edited by the user, are not deleted. If you reinstall the program while these files remain in the system, the program might not function correctly. Therefore, if you reinstall JP1/IM - Manager or JP1/IM - View, be sure to restart the OS and use Windows Explorer to delete the folder in which JP1/IM - Manager or JP1/IM - View had been installed, and then reinstall the program.

- About downgrade installation

JP1/IM - Manager and JP1/IM - View do not support downgrade installation. If you want to downgrade a product that has been installed, uninstall the product, and then reinstall it.

1.4 Creating IM databases (for Windows)

You use IM databases to monitor events that occur in the system. The two types of IM databases are the integrated monitoring database and the IM Configuration Management database. The integrated monitoring database is used when Central Console is being used. The IM Configuration Management database is used with IM Configuration Management to manage the system hierarchy. For details about the functions available when the integrated monitoring database and the IM Configuration Management database are used, see *2.4 Functions provided by the IM database* in the *JP1/Integrated Management - Manager Overview and System Design Guide*.

During system configuration or after operations have started, you can create either or both the integrated monitoring database and the IM Configuration Management database.

The IM database must start before JP1/IM - Manager Service. See *3.1.1 In Windows* in the *JP1/Integrated Management - Manager Administration Guide* to use the startup control function to set it.

JP1 events obtained from the event database after the JP1/IM - Manager service has started are stored in the integrated monitoring database. For details, see *3.1.3(2) JP1 event control when using the integrated monitoring database* in the *JP1/Integrated Management - Manager Overview and System Design Guide*.

This section explains how to create an IM database.

1.4.1 Preparations for creating IM databases (for Windows)

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:

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

If JP1/IM - MO is being used and JP1/IM - Manager and JP1/IM - MO are located on separate hosts, you must add the item `IMDBHOSTNAME` in the setup information file. For details about the setup information file, see *Setup information file (jimdbsetupinfo.conf)* in *Chapter 2. Definition Files* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

2. Check the settings in the setup information file.

Make sure of the following:

- Network drives, Windows reserved device files, and paths containing symbolic links are not specified for `IMBENVDIR` and `IMBDDIR`.

3. Verify that the startup type of the Application Experience service is not disabled.

1.4.2 Setting up the integrated monitoring database (for Windows)

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 plan to use the integrated monitoring database, there is no need to perform this procedure.

The setup procedure differs depending on whether the IM Configuration Management database has already been set up. Apply the following procedures as appropriate depending on the case.

(1) When the IM Configuration Management database has been set up

The setup procedure differs depending on whether you stop JP1/IM-Manager Service. The following are the setup procedures for the two cases.

- To stop JP1/IM-Manager Service and set up the integrated monitoring database:
 1. Check if the IM database service (JP1/IM-Manager DB Server) is running.
 2. Stop the following services:
 - JP1/IM-Manager Service
 - If JP1/IM - MO is being used, the JP1/IM - Message Optimizer service of JP1/IM - MO at the connection source.
 3. Execute the `jcodbsetup` command to create an integrated monitoring database.
`jcodbsetup -s [-q]`
 4. Execute the `jcoimdef` command to enable the integrated monitoring database.
`jcoimdef -db ON`
 5. Start JP1/IM-Manager Service.
- To set up the integrated monitoring database without stopping JP1/IM-Manager Service:
 1. Execute the `jcoimdef` command to disable the IM Configuration Management service (`jcfmain`).
`jcoimdef -cf OFF`
 2. Restart JP1/IM-Manager Service.
 3. Check if the IM database service (JP1/IM-Manager DB Server) is running.
 4. Stop the following service:
 - If JP1/IM - MO is being used, the JP1/IM - Message Optimizer service of JP1/IM - MO at the connection source.
 5. Execute the `jcodbsetup` command to create an integrated monitoring database.
`jcodbsetup -s [-q]`
 6. Execute the `jcoimdef` command to enable the integrated monitoring database.
`jcoimdef -db ON`
 7. Execute the `jcoimdef` command to enable the IM Configuration Management service (`jcfmain`).
`jcoimdef -cf ON`
 8. Restart JP1/IM-Manager Service.

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

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

(2) When the IM Configuration Management database has not been set up

1. Stop the following service:

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

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

```
jcodbsetup -f setup-information-file-name [-q]
```

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

```
jcoimdef -db ON
```

4. Restart JP1/IM-Manager Service.

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

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

1.4.3 Setting up the IM Configuration Management database (for Windows)

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 plan to use the IM Configuration Management functions, there is no need to perform this procedure.

The setup procedure differs depending on whether the integrated monitoring database has already been set up. Apply the following procedures as appropriate depending on the case.

(1) When the integrated monitoring database has been set up

The setup procedure differs depending on whether you stop JP1/IM-Manager Service. The following are the setup procedures for the two cases.

- To stop JP1/IM-Manager Service and set up the IM Configuration Management database:

1. Check if the IM database service (JP1/IM-Manager DB Server) is running.

2. Stop the following services:

- JP1/IM-Manager Service
- If JP1/IM - MO is being used, the JP1/IM - Message Optimizer service of JP1/IM - MO at the connection source.

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

```
jcfdbsetup -s [-q]
```

- To set up the IM Configuration Management database without stopping the JP1/IM-Manager Service:
 1. Execute the `jcoimdef` command to disable the integrated monitoring database.


```
jcoimdef -db OFF
```
 2. Restart JP1/IM-Manager Service.
 3. Check if the IM database service (JP1/IM-Manager DB Server) is running.
 4. Stop the following service:
 - If JP1/IM - MO is being used, the JP1/IM - Message Optimizer service of JP1/IM - MO at the connection source.
 5. Execute the `jcfdbsetup` command to create an IM Configuration Management database.


```
jcfdbsetup -s [-q]
```
 6. Execute the `jcoimdef` command to enable the integrated monitoring database.


```
jcoimdef -db ON
```

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

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

(2) When the integrated monitoring database has not been set up

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


```
jcfdbsetup -f setup-information-file-name [-q]
```

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

1.4.4 Settings for using the functions of IM Configuration Management (for Windows)

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 *1.4.3 Setting up the IM Configuration Management database (for Windows)*, 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 (`jcmain`).


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

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

For details about the `jco_spm�_status` command, see *jco_spm�_status* in *Chapter 1. Commands* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

1.4.5 Updating IM databases (for Windows)

If you are using IM databases and you wish to upgrade JP1/Integrated Management or apply a corrected version of JP1/IM - Manager, you must first update the IM databases.

To update IM databases:

1. Check the following service statuses:

- The IM database service (JP1/IM - Manager DB Server) is running.
- JP1/IM-Manager Service is stopped.
- If JP1/IM - MO is being used, the JP1/IM - Message Optimizer service of JP1/IM - MO is stopped at the connection source.

2. Execute the `jimdbupdate` command to check if the IM databases have been updated.

- If the following message is output, perform step 5:
`KNAN11201-I The IM database service is the latest.`
- If the following message is output, perform the procedure beginning with step 3:
`KNAN11202-I The overwrite is necessary for the IM database.`
`KNAN11207-I An update of the table schema of an IM database service is required.`

3. Execute the `jimdbbackup` command to back up the IM databases:

```
jimdbbackup -o backup-file-name -m MAINT
```

4. Execute the `jimdbupdate` command to update the IM databases:

```
jimdbupdate -i
```

5. Start the following services:

- JP1/IM-Manager Service
- IM database service (JP1/IM - Manager DB Server)

Important

Do not restore into an IM database obtained after the `jimdbupdate` command has been executed any IM database backup data that was obtained before the `jimdbupdate` command was executed.

After you have executed the `jimdbupdate` command, execute the `jimdbbackup` command again to make a new backup.

1.5 Setting the startup sequence for services (for Windows)

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 *JP1/Base User's Guide*. For details about how to start the IM database, see *3.1 Starting JP1/IM - Manager* in the *JP1/Integrated Management - Manager Administration Guide*.

1.6 Setting up user authentication and user mapping (for Windows)

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 1–4: 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

[#]: Not required when automated actions are not performed or commands are not executed on managed hosts from JP1/IM - View.

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 1–5: 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
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).

1.6.1 Specifying the authentication server (for Windows)

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** tab.

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 *JP1/Base User's Guide*.

1.6.2 Registering JP1 users (for Windows)

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** tab, register the JP1 users and set their passwords.

1.6.3 Setting operation permissions for the JP1 users (for Windows)

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** tab, 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 *JP1/Integrated Management - Manager Overview and System Design Guide*.

1.6.4 Copying the primary authentication server settings (for Windows)

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.

1.6.5 Setting user mapping (for Windows)

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** tab.

2. Set the JP1 user names and host names.

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

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 *JP1/Base User's Guide*.

1.7 Specifying settings for handling JP1/Base failures (for Windows)

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 *JP1/Base User's Guide*.

JP1/Base also provides a 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 *JP1/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 *JP1/Base User's Guide*.

1.8 Setting the system hierarchy (when IM Configuration Management is used) (for Windows)

This section describes how to set the system hierarchy (IM configuration) when IM Configuration Management is used. For details about how to set the system hierarchy when IM Configuration Management is not used, see [1.9 Setting the system hierarchy \(when IM Configuration Management is not used\) \(for Windows\)](#).

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 and perform the following operations, the configuration definition information held in IM Configuration Management does not match that held in JP1/Base.

- Editing the configuration definition file of JP1/Base
- Executing the `jbsrt_distrib` command

Therefore, when you use IM Configuration Management we recommend that you use it to integrally manage your system hierarchy.

When you use JP1/Base functionality to distribute the definition of your system hierarchy, you need to obtain the system hierarchy to match the configuration definition information held in both IM Configuration Management and JP1/Base. If the system hierarchy is not obtained, operation will malfunction because of mismatched configuration definition information.

1.8.1 Using IM Configuration Management - View to set the system hierarchy (for Windows)

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 *JP1/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 *3.1.4 Displaying host information*.
 - For details about how to delete hosts, see *3.1.6 Deleting hosts*.
 - For details about how to change information about the registered hosts, see *3.1.5 Changing the attributes of host information*.
2. Add the host registered in IM Configuration Management to the system hierarchy and set the hierarchy between managers and agents.
 - For details about how to add hosts to a JP1/IM system, see *3.2.4(1)(a) Adding hosts*.
 - For details about how to set a hierarchy between managers and agents, see *3.2.4(1)(b) Moving hosts*.
 - For details about how to delete hosts from the JP1/IM system, see *3.2.4(1)(c) 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 *3.2.4(3) Applying a system hierarchy to a system managed by IM Configuration Management*.
 - 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 *3.2.5 Synchronizing the system hierarchy*.

(2) Editing an existing system hierarchy

Perform the following procedure to switch the method of setting configuration management information from the configuration management function provided by JP1/Base to IM Configuration Management.

To edit an existing system hierarchy:

1. In the IM Configuration Management window, read the existing configuration definitions of JP1/IM to obtain the system hierarchy.

The obtained configuration definitions are stored in the IM Configuration Management database. Hosts that have not been registered in IM Configuration Management are automatically registered in the database.
For details, see *3.2.1 Collecting the system hierarchy*.

2. In the Edit Host Properties window, check the registered host attributes, and edit the host names and host types as necessary.
For details, see [3.1.5 Changing the attributes of host information](#).
3. In the IM Configuration Management window, collect host information.
For details, see [3.1.3 Collecting information from hosts](#).
4. In the IM Configuration Management window, check the host information you have collected.
Host information includes lower-level host information, basic information, product information, and service information.
For details, see [3.1.4 Displaying host information](#).
5. In the IM Configuration Management window, check the system hierarchy and edit it as necessary.
When you edit the system hierarchy, make sure you apply the new hierarchy to the system.
For details, see [3.2.2 Displaying the system hierarchy](#), [3.2.4 Editing the system hierarchy](#), and [3.2.4\(3\) Applying a system hierarchy to a system managed by IM Configuration Management](#).
6. In the IM Configuration Management window, collect profile information.
The settings that are currently used by the services of agents and the configuration files stored in the agents are collected.
For details, see [3.5.1\(2\) Collecting profiles](#).
7. In the IM Configuration Management window, check the profile information and edit the configuration files as necessary.
When you edit configuration files, make sure you apply the edited information to agents. In addition, perform step 6 after you apply the new configuration files and check the profile information.
For details, see [3.5.1\(3\) Displaying profiles](#), [3.5.1\(5\) Editing configuration files](#), and [3.5.1\(6\) Applying edited information in configuration files](#).

1.8.2 Using the export and import functions to set the system hierarchy (for Windows)

When you use the export and import functions of IM Configuration Management, you can migrate the system configuration used in a test environment to a production environment. You can also migrate the system hierarchy (IM configuration) used before changes have been made to a new environment. For details about how to set the system hierarchy using the export and import functions, see [3.6 Importing and exporting the management information in IM Configuration Management](#).

1.8.3 Settings for managing and monitoring a virtualization system configuration (for Windows)

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 [3.3 Setting a virtualization system configuration](#).

1.9 Setting the system hierarchy (when IM Configuration Management is not used) (for Windows)

This section describes how to set the system hierarchy (IM configuration) when IM Configuration Management is not used. For details about the system hierarchy settings when IM Configuration Management is used, see [1.8 Setting the system hierarchy \(when IM Configuration Management is used\) \(for Windows\)](#).

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 JP1/Integrated Management - Manager Overview and System Design Guide](#).

1.9.1 Setting the configuration definition information (for Windows)

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.

For details about the configuration definition file, see [Configuration definition file \(`jbs_route.conf`\)](#) in [Chapter 2. Definition Files](#) in the manual [JP1/Integrated Management - Manager Command and Definition File Reference](#).

For details about the `jbsrt_distrib` command and the `jbsrt_sync` command, see the [JP1/Base User's Guide](#).

When you use IM Configuration Management, execute Collect IM Configuration from the IM Configuration Management window.

1.9.2 Deleting the configuration definition information (for Windows)

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. Then execute the `jbsrt_distrib` command at the highest manager.
For details about the `jbsrt_del` command, see the *JP1/Base User's Guide*.

1.9.3 Changing the configuration definition information (for Windows)

If you change the configuration definition information, follow the same procedure as in *1.9.1 Setting the configuration definition information (for Windows)*. 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 *1.9.2 Deleting the configuration definition information (for Windows)*.
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 *1.9.1 Setting the configuration definition information (for Windows)*.

1.9.4 Notes about setting the configuration definition information (for Windows)

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 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 *JP1/Base User's Guide*.

1.10 Setting up Event Service (for Windows)

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 *JP1/Base User's Guide*.

Important

Specify `keep-alive` for the communication type in the API settings file of the host on which JP1/IM Manager is running. If you specify `close` for the communication type, JP1/IM - Manager uses a temporary port every time it receives an event and temporary ports are insufficient.

1.11 Setting JP1 event forwarding when IM Configuration Management is used (for Windows)

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 *1.8 Setting the system hierarchy (when IM Configuration Management is used) (for Windows)*.

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 *3.5.1(5) Editing configuration files*.

1.12 Setting JP1 event forwarding when IM Configuration Management is not used (for Windows)

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 *1.9 Setting the system hierarchy (when IM Configuration Management is not used) (for Windows)*.

For details about the settings, see the chapter that provides details of the forwarding settings file in the *JP1/Base User's Guide*.

1.13 Collecting and distributing Event Service definition information when IM Configuration Management is used (for Windows)

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 batch collect and distribute Event Service definition information from and to multiple hosts on which JP1/Base version 9 or later 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
- Log-file trap startup 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 [3.5.1\(2\) 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 [3.5.1\(6\) Applying edited information in configuration files](#).

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

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.

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 *JP1/Base User's Guide*.

1.15 Setting up a command execution environment (for Windows)

This section describes how to set up a command execution environment for executing commands on managed hosts and for executing client applications.

1.15.1 Setting up the command execution function for managed hosts (for Windows)

This subsection describes how to set up a command execution environment for performing automated actions and for executing commands on managed hosts from the Execute Command window of JPI/IM - View.

1. 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
```

2. Creating an environment variable file

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

3. Defining host groups

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

4. Creating a command button definition file

If you want to execute a command from a command button, create a command button definition file.

To pass event information, set `true` in the `inev` parameter.

5. Creating a configuration file for converting information

When you pass event information for automated actions and command execution, if you want to convert specific ASCII characters in the event information to be passed to other types of characters, create a configuration file for converting information.

For details about when the settings of a command execution environment are enabled or how to create definition files, see the information in the locations described below.

About command execution environments

- `jcocmddef` command

See the chapter that describes commands in the *JPI/Base User's Guide*.

- Creation of an environment variable file

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

- Host group definition

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

- Creation of a command button definition file

See *Command button definition file (cmdbtn.conf)* in *Chapter 2. Definition Files* in the manual *JPI/Integrated Management - Manager Command and Definition File Reference*.

- Creation of a configuration file for converting information

See *Configuration file for converting information (event_info_replace.conf)* in *Chapter 2. Definition Files* in the manual *JPI/Integrated Management - Manager Command and Definition File Reference*.

1.15.2 Setting up a client application execution environment (for Windows)

This subsection describes how to set up a command execution environment for executing client applications from the Execute Command window of JPI/IM - View.

1. Creating a command button definition file

If you want to execute a client application from a command button, create a command button definition file.

To pass event information, set `true` in the `inev` parameter. In addition, set `client` in the `cmdtype` parameter.

2. Creating a configuration file for converting information

When you pass event information for automated actions and command execution, if you want to convert specific ASCII characters in the event information to be passed to other types of characters, create a configuration file for converting information.

For details about when the settings of a command execution environment are enabled or how to create definition files, see the information in the locations described below.

About command execution environments

- Creation of a command button definition file

See *Command button definition file (cmdbtn.conf)* in *Chapter 2. Definition Files* in the manual *JPI/Integrated Management - Manager Command and Definition File Reference*.

- Creation of a configuration file for converting information

See *Configuration file for converting information (event_info_replace.conf)* in *Chapter 2. Definition Files* in the manual *JPI/Integrated Management - Manager Command and Definition File Reference*.

1.16 Specifying settings for using the source host name of Event Service in the FQDN format (for Windows)

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.

1.16.1 Prerequisites (for Windows)

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.

1.16.2 Setting method (for Windows)

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 *JP1/Base User's Guide*:

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

For details about the `SpmSetSvcCon` command, see *SpmSetSvcCon (Windows only)* in *Chapter 1. Commands* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

1.16.3 Startup method (for Windows)

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.

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.

1.17 Specifying settings for monitoring logs on remotely monitored hosts (for Windows)

This section describes how to configure WMI, NetBIOS (NetBIOS over TCP/IP), and SSH to monitor the logs on remotely monitored hosts.

For details about the types of logs that can be collected from remotely monitored hosts and the remote communication methods, see *11.5.2 Managing the remote monitoring configuration* in the *JP1/Integrated Management - Manager Overview and System Design Guide*.

For details about how to register hosts that are to be monitored remotely in IM Configuration Management, see *3.1 Registering hosts*.



Note

You can collect the log information that is output on remotely monitored hosts while remote monitoring is stopped. Use the `START_OPTION` parameter in the remote log trap environment definition file (`jp1cf_remote_logtrap.conf`) to specify whether to collect the log information that is output while remote monitoring is stopped. This setting is enabled when JP1/IM - Manager is newly installed. If you upgraded JP1/IM - Manager from a version earlier than 11-01, this setting is disabled. Configure the remote log trap environment definition file as needed.

For details about the remote log trap environment definition file, see *Remote log trap environment definition file (jp1cf_remote_logtrap.conf)* in *Chapter 2. Definition Files* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

1.17.1 Configuring WMI (for Windows)

This subsection describes how to configure WMI.

WMI connections require the following:

- DCOM settings

DCOM must be configured on both the JP1/IM - Manager host and a host to be remotely monitored.

When you run a JP1/IM - Manager host in a cluster system, configure DCOM on both the executing node and the standby node.

- Firewall settings

Configure the firewall on a host to be remotely monitored as necessary.

When all the settings have been completed, check whether a connection can be established from the JP1/IM - Manager host to a remote host that will be monitored remotely.

Note:

- Log information cannot be collected if the startup status of Windows Management Instrumentation (service name `WinMgmt`) providing system management information in the OS on the monitored remote host is Disabled.
- Users accessing a remotely monitored host must be members of the Administrators group on that host.

(1) DCOM setting

The following describes how to configure DCOM on a JP1/IM - Manager host and a host to be monitored remotely.

(a) Configuring DCOM on a JP1/IM - Manager host

Configure DCOM on the JP1/IM - Manager host.

The procedure for configuring DCOM is described below.

Note that some steps in the procedure might differ depending on the OS environment on the remotely monitored host.

For example, If the OS of the remotely monitored host is Windows Server 2008, **Run** might not appear in the **Start** menu of Windows. If it does not appear, hold down the Windows logo key and press the R key to invoke **Run**.

1. From the Windows **Start** menu, choose **Run**.
2. Enter `dcomcnfg.exe` and then click the **OK** button.
The Component Services window appears.
3. Click **Component Services** and **Computers** to expand the tree.
4. Choose **My Computer**, and then from the right-click menu, choose **Properties**.
The My Computer Properties dialog box appears.
5. Choose the **Default Properties** tab, and then select **Enable Distributed COM on this computer**.
6. Click the **OK** button.
The My Computer Properties dialog box closes.
7. From the Windows **Start** menu, choose **Run**.
8. Enter `gpedit.msc`, and then click the **OK** button.
The Group Policy dialog box appears.
9. In the Group Policy dialog box, click **Computer Configuration**, **Administrative Templates**, and **System**. Then, expand the **User Profiles** node.
10. For **Do not forcefully unload the user registry at user logoff**, click **Enabled**.
11. Restart the machine.

(b) Configuring DCOM on a remote host to be monitored remotely

Configure DCOM on a host to be monitored remotely.

The procedure for configuring DCOM is described below.

Note that some steps in the procedure might differ depending on the OS on the host to be monitored remotely.

1. From the Windows **Start** menu, choose **Run**.
2. Enter `dcomcnfg.exe` and then click the **OK** button.
The Component Services window appears.
3. Click **Component Services** and **Computers** to expand the tree.

4. Choose **My Computer**, and then from the right-click menu, choose **Properties**.
The My Computer Properties dialog box appears.
5. Choose the **Default Properties** tab, and then select **Enable Distributed COM on this computer**.
6. Choose the **COM Security** tab, and then click the **Edit Limits** button for **Access Permissions**.
The Access Permission dialog box appears.
Check to see if the user who connects to the monitored host or the group to which the user belongs is displayed in **Group or user names**:
If it is not displayed, click the **Add...** button, and then add the user or the group to which the user belongs.
7. In the Select Users or Groups window, select the user who will connect to the host to be monitored or the group to which the user belongs.
Check to see if **Allow** is selected in **Remote Access**. If this option is not selected, select it.
8. Click the **OK** button.
The Access Permission dialog box closes.
9. Choose the **COM Security** tab, and then click the **Edit Limits** button for **Launch and Activation Permissions**.
The Launch and Activation Permissions dialog box appears.
In the Launch Permission dialog box, in the **Group or user names**: section, check to see if the user who will connect to the remote host to be monitored or the group to which the user belongs is displayed.
If the user or a group is not displayed, click the **Add...** button to add the user or the group to which the user belongs.
10. In the Select Users or Groups window, in the Launch and Activation Permissions dialog box, select the user who will connect to the host to be monitored remotely or the group to which the user belongs.
Check to see if **Allow** is selected for both **Remote Launch** and **Remote Activation**. If it is not selected, select it.
11. Click the **OK** button.
The My Computer Properties dialog box is displayed again.
12. Click the **OK** button.
The My Computer Properties dialog box closes.
13. Restart the machine.
This step is not needed if you have not changed the setting of **Enable Distributed COM on this computer**.

(2) Configuring the firewall

You need to configure the firewall when Windows Firewall is enabled.

In the Windows **Start** menu, click **Control Panel** and then **Windows Firewall** to check whether Windows Firewall is enabled.

To configure the firewall when Windows Firewall is enabled:

1. From the Windows **Start** menu, choose **Run**.
2. Enter `gpedit.msc` and then click the **OK** button.
The Group Policy Object Editor dialog box appears.

3. Click **Computer Configuration, Administrative Templates, Network, Network Connections, and Windows Firewall** to expand the tree.
4. Click **Standard Profile**[#], and then in the right-hand pane, from the right-click menu of **Windows Firewall: Allow inbound remote administration exception**, choose **Edit**.
The Windows Firewall: Allow inbound remote administration exception dialog box appears.
[#]: If the host machine is a domain environment, this will be Domain Profile.
5. Select the **Enabled** radio button in the Windows Firewall: Allow inbound remote administration exception dialog box.
6. Click the **OK** button.
The Windows Firewall: Allow inbound remote administration exception dialog box closes.

(3) WMI namespace setting

This subsection explains the procedure for setting the WMI namespace.

If the UAC security facility is enabled on the monitored host, set the WMI namespace security for the user itself or for a group to which the user belongs, except for the Users or Administrators group.

1. From the Windows **Start** menu, choose **Run**.
2. Enter `wmimgmt.msc` and then click the **OK** button.
The Windows Management Infrastructure (WMI) dialog box appears.
3. Choose **WMI Control (Local)**, and then from the right-click menu, choose **Properties**.
The WMI Control (Local) Properties dialog box appears.
4. Choose the **Security** tab, and then click **Root** and **CIMV2** to expand the tree.
5. Click the **Security** button.
The Security for ROOT\CIMV2 dialog box appears.
Check to see if the user who connects to the monitored host or the user's group is displayed in **Group or user names**. If it is not displayed, click the **Add** button, and then add the user or the group to which the user belongs.
6. In **Group or user names**, select the user who connects to the monitored host or the group to which the user belongs.
Check to see if **Allow** is selected for both **Enable Account** and **Remote Enable**. If it is not selected, select it.
7. Click the **OK** button.
The Security for ROOT\CIMV2 dialog box closes, and the WMI Control (Local) Properties dialog box is displayed again.
8. Click the **OK** button.
The WMI Control (Local) Properties dialog box closes.
9. In the Windows Management Infrastructure (WMI) dialog box, click **File**, and then **Exit** to close the dialog box.

(4) Setting up UAC

If you specify a local user who has Administrator permissions (except for the Administrator user who is created during OS installation) as the user in monitoring target setting, UAC will restrict the permission and connection will be made as an ordinary user.

Consequently, access might be refused and you might not be able to collect performance data. In this case, take one of the steps below.

(a) Specifying LocalAccountTokenFilterPolicy

You can specify the following settings only when the local host is not to be monitored:

```
reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v  
LocalAccountTokenFilterPolicy /t REG_DWORD /d 1 /f
```

To return to the original setting, execute the following command:

```
reg delete HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies  
\System /v LocalAccountTokenFilterPolicy /f
```

(b) Disabling UAC

Specify the following settings on the JP1/IM - Manager host and the monitored hosts.

- Setting the UAC setting slider to **Never notify**
 1. Select **Control Panel, User Accounts**, and then **Change User Account Control settings**.
 2. Set the slider on the left-hand side of the **User Account Control Settings** window to **Never notify**.
- Setting up local security policies
 1. Select **Control Panel, Administrative Tools**, and then **Local Security Policy**.
 2. Select **Security Settings, Local Policies**, and then **Security Options**.
 3. Disable **User Account Control: Run all administrators in Admin Approval Mode**.

(5) Checking WMI connections

Use the Windows tool `wbemtest.exe` to check whether the JP1/IM - Manager host and the host to be monitored remotely are connected.

The following procedure describes how to check WMI connections. Perform the procedure on the JP1/IM - Manager host.

1. At the command prompt, execute the following command:

```
runas /user:user-name wbemtest
```

The Windows Management Instrumentation Tester dialog box appears.

Note that for the user name, you need to enter the value specified in the **User name** box on the **IM Host Account** page in the System Common Settings window. If you are prompted to enter a password after a command is executed, specify the value set in the **Password** box on the **IM Host Account** page.

2. Click the **Connect** button.

The Connect window appears.

3. In **Namespace, User, Password**, and **Authority**, enter the appropriate information.

The following describes each item.

- **Namespace**

Enter `\\monitored-host-name\root\cimv2`.

Replace *monitored-host-name* with the name of the host that will actually be monitored.

- **User**

Enter the name of the user who will log on to the monitored remote host.

- **Password**

Enter the user's password.

- **Authority**

Enter `ntlmdomain:domain-name-of-monitored-host`. Leave this box blank if the remote host is a work group.

4. Click the **Connect** button.

If connection is established successfully, the Connect dialog box closes and all buttons are enabled in the Windows Management Instrumentation Tester dialog box.

If an error notification appears, check the item indicated by the error number. Causes of errors and the corresponding error numbers are given below.

An error might occur if you change settings while the tool (`wbemtest.exe`) is active and then re-establish the connection. In that case, restart the tool and check the connection.

- 0x8001011c

DCOM is not configured on the JP1/IM - Manager host.

- 0x80070005

One of the following is the probable cause of the error.

- DCOM is not configured on the JP1/IM - Manager host.

- DCOM is not configured on the host to be monitored remotely.

- The user name, password, or domain name for connecting to the host to be monitored remotely is incorrect.

- 0x80041003

No value is set in **Namespace** on the host to be monitored remotely.

- 0x80041008

The value specified in **Authority** does not begin with `ntlmdomain:.`

- 0x800706XX

One of the following is the probable cause of the error.

- The name of the host to be monitored remotely is incorrect.

- The host to be monitored remotely is not running.

- No firewall is configured on the host to be monitored remotely

- The password of the user who will log on to the host to be monitored remotely has expired.

5. Confirm that there is an event log whose log type is *System* or *Application* on the host to be monitored remotely, and then click the **Query** button. When the Query window appears, enter the next query, and then click the **Apply** button.

```
Select * From Win32_NTLogEvent Where ( Logfile='System' Or  
Logfile='Application' )
```

After you click the **Apply** button, check whether the execution results of the query appear in the Query Result window.

1.17.2 NetBIOS settings (NetBIOS over TCP/IP) (for Windows)

This subsection describes how to configure NetBIOS (NetBIOS over TCP/IP). After you configure NetBIOS, check whether you can read log files on monitored hosts from the JP1/IM - Manager host. If the log files on monitored hosts are in SEQ2 format, make sure that you can also read the backup files of the monitored log files.

(1) Configuring file sharing

Enable sharing of the folder containing the log files to be monitored on the remote host. Add the desired user names in the remote communication settings in the host information file on the monitored host and grant read permissions to the users. Note that if you allow file sharing to too few users, when log file trapping starts, the upper limit for the number of users who are granted file sharing is exceeded and an error might occur.

(2) Setting local security on the JP1/IM - Manager host

On the JP1/IM - Manager host, click **Administrative Tools, Local Security Policy, Security Settings, Local Policies, User Rights Assignment**, and then **Access this computer from the network**. In the properties window of **Access this computer from the network**, add the user name specified on the **IM Host Account** page in the System Common Settings window.

(3) Setting local security on the monitored host

On the host to be monitored remotely, click **Administrative Tools, Local Security Policy, Security Settings, Local Policies, User Rights Assignment**, and then **Access this computer from the network**. In the properties window of **Access this computer from the network**, add the user name specified in the remote communication settings in the host information file of the monitored host.

(4) Editing the registry

When monitored hosts are logical hosts and you monitor each host remotely by using multiple IP addresses or host names, set the registry on those monitored hosts. To do so, perform the following procedure.

1. Log on to the monitored host as an administrator.
2. Start the Registry Editor.
3. In the Registry Editor window, select the following key.
 - Key name
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanmanServer\Parameters
4. Add the registry value.
 - Name: DisableStrictNameChecking
 - Data type: REG_DWORD
 - Base: Hexadecimal
 - Value 1
5. Close the Registry Editor.
6. Restart the monitored host.

(5) Checking NetBIOS (NetBIOS over TCP/IP) connections

1. In Windows Explorer, in the **Address** box, enter `\\name-of-remotely-monitored-host`.
For *name-of-remotely-monitored-host*, enter the actual name you specified.
2. When the connection window appears, enter the user name and password for logging on to the remotely monitored host.
3. Check whether a NetBIOS connection is established with the host you want to monitor remotely.
4. In Windows Explorer, in the **Address** box, enter `\\name-of-remotely-monitored-host\path-for-folder-shared-in-(1)`.
For *name-of-remotely-monitored-host* and *path-for-folder-shared-in-(1)*, enter the actual host name and path you specified.
5. Check whether you can access *path-for-folder-shared-in-(1)*.

If access fails, check whether the procedure was performed correctly.

1.17.3 Configuring SSH (for Windows)

This subsection describes how to configure SSH when the JP1/IM - Manager host is running in a Windows environment. SSH uses public-key cryptography for authentication.

To establish SSH connections, you need to:

- Configure an SSH server
Configure an SSH server on a remotely monitored host.
- Create keys
Create keys on the monitored host in an UNIX environment.
- Place the private key on the JP1/IM - Manager host
Transfer the private key from the monitored host in an UNIX environment to the JP1/IM - Manager host.
- Place the public key on the monitored host
Place the public key on the remotely monitored host.
- Specify access permissions for monitored log files
If the monitored host is a UNIX host, specify access permissions for users who will be establishing SSH connections from the manager host to the monitored host.

Important

Do not write interactive commands such as `stty`, `tty`, `tset`, and `script` in the login script of the user who is permitted to establish SSH connections. If these commands must be written in the login script, create another user who is permitted to establish SSH connections for remote monitoring. Alternatively, change the login script of the user who is permitted to establish SSH connections so that these commands will not be executed.

(1) Configuring an SSH server

To configure an SSH server, follow the procedure below. OS settings and commands may vary depending on the OS version. For details, see the manual for each OS and the release notes for JP1/IM - Manager.

1. Log on to the remotely monitored host as a user with `root` privileges.
2. Open `sshd_config`.
For Linux, Solaris, or AIX: `/etc/ssh/sshd_config`
For HP-UX (IPF): `/opt/ssh/etc/sshd_config`
3. Set `yes` for `PubkeyAuthentication`^{#1}.
4. Set the following items^{#1, #2}.
 - If you are using OpenSSH on Solaris or the OS is not Solaris
Set `no` for `UseDNS`.
 - For Solaris
Set `no` for `LookupClientHostnames`.
5. Set `yes` for `PermitRootLogin`^{#1}.
Perform this step only when you are logged on as a user with `root` privileges to collect information.
6. Execute one of the following commands to restart the `sshd` service.
The following describes the command to be executed for each OS.
 - For Linux (Linux 6 example)
`/etc/rc.d/init.d/sshd restart`
 - For Solaris (Solaris 10 example)
`/usr/sbin/svcadm restart ssh`
 - For AIX (AIX 6.1 example)
`kill -HUP sshd-process-ID`
 - For HP-UX (HP-UX 11i V3 (IPF) example)
`/sbin/init.d/secsh stop; /sbin/init.d/secsh start`

#1

For details about the items to be set and how to set them in `sshd_config`, see the documentation for your SSH server.

#2

If you do not set these items, make sure that the monitored host can perform name resolution as follows.

- The monitored host can resolve the IP address of the manager host to the host name.
- The IP address resolved from the host name of the manager host matches the IP address of the manager host.

If you are using a DNS server for name resolution and the monitored host cannot connect to the DNS server, the startup of remote-monitoring log file traps or the collection of log files might be delayed. If a delay occurs, the startup of traps or the collection of log files might time out and fail. To prevent this problem, we recommend that you set `no` for `UseDNS` and `LookupClientHostnames`.

(2) Initially creating keys

Log on as a user who remotely monitors the target host in the UNIX environment and execute the `ssh-keygen` command to create keys. This procedure needs to be performed only the first time that you create keys.

You can choose the type of keys (RSA or DSA).

Before you start the procedure, make sure that only the owner of the keys has the write permission for the directory above the `.ssh` directory. If anyone other than the owner has the write permission for the higher-level directory, SSH connections fail.

1. Log on as a user who can remotely monitor the target host in an UNIX environment.
2. Execute the `ssh-keygen` command.
Enter the command as follows:
 - When creating RSA keys: `ssh-keygen -t rsa`
 - When creating DSA keys: `ssh-keygen -t dsa`
3. Determine the names of the file in which the private key will be stored and the directory that will hold the file.
The path and the file name must not contain multibyte characters. The default setting is `~/.ssh/id_rsa`.

4. Press the **Return** key twice.

When you are prompted to enter the passphrase for the private key, enter nothing and press the **Return** key. When you are prompted again, enter nothing and press the **Return** key again.

The following is an execution example of the `ssh-keygen -t rsa` command.

```
[root@HOST]$ ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/home/ssh-user/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/ssh-user/.ssh/id_rsa.
Your public key has been saved in /home/ssh-user/.ssh/id_rsa.pub.
The key fingerprint is:
ax:xx:xx:xx:xx:bx:xx:xc:xx:xx:xx:xd:xd:xa:ed:xx root@HOST
```

5. Execute the `cat` command to add the public key file to the authentication key file.
6. Execute the `chmod` command to change the attribute of the authentication key file to 600.

The following is an execution example of the `cat` and `chmod` commands.

```
[ClientUser@TargetHost .ssh]$ cat id_rsa.pub >> authorized_keys
[ClientUser@TargetHost .ssh]$ chmod 600 authorized_keys
```

7. Configure `AuthorizedKeysFile` in `/etc/ssh/sshd_config`.

By default, `~/.ssh/authorized_keys` or `.ssh/authorized_keys` is set. If you change the path for the authentication key file created in step 6, check and, if necessary, revise the value of `AuthorizedKeysFile`. If you change any settings in `sshd_config`, restart the `sshd` service as a superuser.

Cautionary notes

- Manage private keys with the utmost care.

- The creation of keys (public key and a private key pair) does not depend on any environment or tool. You can create keys in any environment using any tool. However, after you create keys, you must place the private keys and public keys in the appropriate locations.

(3) Placing the private key on the JP1/IM - Manager host (when keys are initially created)

When the OS of the JP1/IM - Manager host is Windows, place the private key created as described in [1.17.3\(2\) Initially creating keys](#) on the JP1/IM - Manager host running Windows. The path for the location of the private key must not contain multibyte characters. This procedure needs to be performed only the first time that keys are created.

(4) Registering the location where the private key is placed

To register in the System Common Settings window the location on the JP1/IM - Manager host where the private key is placed:

1. In the IM Configuration Management window, from the menu bar, choose **Edit** and then **System Common Settings**. The System Common Settings window is displayed.
2. In the System Common Settings window, set the private key file path for SSH.

For details about the items displayed in the System Common Settings window, see [4.20 System Common Settings window](#) in the manual *JP1/Integrated Management - Manager GUI Reference*.

(5) Placing the public key on the host to be monitored remotely (when keys have already been created)

Place the public key created in [1.17.3\(2\) Initially creating keys](#) on the host to be monitored remotely. To do so, perform the procedure described below. Note that this procedure needs to be performed only when keys are created on another host and that host will be monitored remotely.

Before you start the procedure, make sure that only the owner of the keys has the write permission for the directory above the `.ssh` directory. If anyone other than the owner has the write permission for the higher-level directory, SSH connections fail.

1. Log on as a user who can remotely monitor the target host.
2. Navigate to the `.ssh` directory.
If the home directory of the user who performs remote monitoring does not contain the `.ssh` directory, create one. Set `700` as the attribute of the directory.
3. Execute the `scp` command to copy the public key file to the host to be monitored remotely.
Copy the public key file created as described in [1.17.3\(2\) Initially creating keys](#) to the monitored host. Copy the file to the `.ssh` directory in the home directory of the user who will perform remote monitoring.
4. Execute the `cat` command to add the contents of the public key file to the authentication key file.
5. Delete the copied public key file.
6. Execute the `chmod` command to change the attribute of the authentication key file to `600`.
7. Configure `AuthorizedKeysFile` in `/etc/ssh/sshd_config`.

By default, `~/.ssh/authorized_keys` or `./ssh/authorized_keys` is set. If you change the path for the authentication key file created in step 6, check and, if necessary, revise the value of `AuthorizedKeysFile`. If you change any settings in `sshd_config`, restart the `sshd` service as a superuser.

An execution example of the `scp` command, the `cat` command, and the `chmod` command is shown below. In this example, the host name of the host where keys are created as described in [1.17.3\(2\) Initially creating keys](#) is `IMHost`.

- Example of executing the commands:

```
[ClientUser@TargetHost ]$ cd .ssh
[ClientUser@TargetHost .ssh]$ scp
root@IMHost:/home/ssh-user/.ssh/id_rsa.pub ./
root@IMHost's password: Enter a password here.
id_rsa 100% 233 0.2KB/s 00:00
[ClientUser@TargetHost .ssh]$ cat id_rsa.pub >> authorized_keys
[ClientUser@TargetHost .ssh]$ rm id_rsa.pub
[ClientUser@TargetHost .ssh]$ chmod 600 authorized_keys
```

(6) Specifying access permissions for monitored log files

If the monitored host is a UNIX host, any user who will be establishing SSH connections from the manager host to the monitored host will need the following access permissions:

- Monitored log files
The user needs the read permission. If the monitored log files are in the SEQ2 format, the user also needs the read permission for the backup files of the monitored log files.
- Directory containing the monitored log files and all of its higher directories
The user needs the read permission and the execute permission. If the monitored log files are in the SEQ2 format, the user also needs the read permission and the write permission for the directory containing the backup files of the monitored log files and for all of its higher directories.

(7) Checking connections

When SSH client software is installed on the JP1/IM - Manager host in a Windows environment, use the private key placed on the host to verify that you can establish an SSH connection with the remote host that is monitored. In addition, when you establish an SSH connection, make sure that a password and passphrase do not need to be entered.

If an error occurs or you are prompted to enter a password and a passphrase, check whether the settings are specified correctly as described. Also check the settings of the OS to make sure that the OS will allow SSH connections.

Note that during remote monitoring, the following commands must be executable on the hosts that are to be monitored remotely. Make sure that the users that perform remote monitoring can execute these commands.

- `uname`
- `ls`
- `wc`
- `tail`
- `find`
- `grep`

- head

Use the following procedures to check whether these commands can be executed.

(a) Checking commands to be used for collection of host information

1. Log in to the monitored host as the user that was set on the **SSH** page in the System Common Settings window.
2. Execute the following command and then confirm that the return code is 0.

```
uname -s
```

(b) Checking commands to be used for collection of log files

1. Log in to the monitored host as the user that was set on the **SSH** page in the System Common Settings window.
2. Execute the following commands and then confirm that the return code is 0.

- `ls -ild monitored-log-file-path`

Example of executing the command:

```
ls -ild /var/log/messages
```

Example of execution result:

```
12345 -rw-r--r-- 1 root 100 Apr 12 13:00 2013 messages
```

- `ls path-to-directory-contains-monitored-log-file`

Example of executing the command:

```
ls /var/log/
```

Example of execution result:

```
messages
```

- (When the OS of the monitored host is AIX) `LC_CTYPE=C wc -l monitored-log-file-path`

Example of executing the command:

```
LC_CTYPE=C wc -l /var/log/messages
```

Example of execution result:

```
20 /var/log/messages
```

- (When the OS of the monitored host is not AIX) `wc -l monitored-log-file-path`

Example of executing the command:

```
wc -l /var/log/messages
```

Example of execution result:

```
20 /var/log/messages
```

- (When the OS of the monitored host is Solaris) `tail +any-line-number-of-monitored-file monitored-log-file-path | tail -maximum-collection-sizec`

Example of executing the command:

```
tail +19 /var/log/messages | tail -10241c
```

Example of execution result:

```
line num = 19
```

```
line num = 20
```

- (When the OS of the monitored host is not Solaris) `tail -n +any-line-number-of-monitored-file monitored-log-file-path | tail -c maximum-collection-size`

Example of executing the command:

```
tail -n +19 /var/log/messages | tail -c 10241
```

Example of execution result:

```
line num = 19
```

```
line num = 20
```

3. If the log file output format is SEQ2, execute the following command, in addition to the command in step 2, and check the results of the standard output:

- `find path-to-directory-containing-monitored-log-file -xdev -inum inode-of-backup-file-for-monitored-log-file`

Example of executing the command:

```
find /var/log/ -xdev -inum 12345
```

Example of standard output:

```
/var/log/messages.1
```

Verify that the path to the backup file of the monitored log file is output in the standard output.

To output the standard output to `stdout.txt` and the standard error output to `stderr.txt`, check the standard output by executing the command shown below.

Example of command:

```
find /var/log/ -xdev -inum 12345 1> stdout.txt 2> stderr.txt
```

(c) Checking commands to be used for application of predefined filters

1. Log in to the monitored host as the user that was set on the **SSH** page in the System Common Settings window.

2. Execute the following commands and then confirm that the return code is 0.

- (When the OS of the monitored host is Linux) `/bin/grep -E 'predefined-filter'`

Example of executing the command:

```
tail -n +19 /var/log/messages | /bin/grep -E 'filter' | tail -c 10241
```

Example of execution result:

```
line num = 19
```

```
line num = 20
```

- (When the OS of the monitored host is Solaris) `/usr/xpg4/bin/grep -E 'predefined-filter'`

Example of executing the command:

```
tail +19 /var/log/messages | /usr/xpg4/bin/grep -E 'filter' | tail -10241c
```

Example of execution result:

```
line num = 19
```

```
line num = 20
```

- (When the OS of the monitored host is not Linux and Solaris) `/usr/bin/grep -E 'predefined-filter'`

Example of executing the command:

```
tail -n +19 /var/log/messages | /usr/bin/grep -E 'filter' | tail -c 10241
```

Example of execution result:

```
line num = 19
```

```
line num = 20
```

- `head -n any-line-number-of-monitored-file`

Example of executing the command:

```
tail -n +19 /var/log/messages | head -n 20
```

Example of execution result:

```
line num = 19
```

```
line num = 20
```

1.17.4 Specifying the size of log information that can be collected per monitoring interval (for Windows)

In an environment in which the maximum size of log information that can be collected per monitoring interval is exceeded even when predefined filters are used, you can change the value that is initially set for the maximum size of log information that can be collected per monitoring interval.

To change the initial value:

1. Configure an execution environment for the remote-monitoring log file trap function and the remote-monitoring event log trap function.

Edit the remote log trap environment definition file (`jp1cf_remote_logtrap.conf`).

```
Manager-path\conf\imcf
```

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

```
jbssetcnf Manager-path\conf\imcf\jp1cf_remote_logtrap.conf
```

3. Restart JP1/IM - Manager.

The new settings take effect when JP1/IM - Manager is restarted.

About specifying the size of log information that can be collected per monitoring interval

- Remote log trap environment definition file (`jp1cf_remote_logtrap.conf`)

For details, see *Remote log trap environment definition file (jp1cf_remote_logtrap.conf)* in *Chapter 2. Definition Files* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

1.18 Setting up JP1/IM - Manager (for Windows)

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

The user who performs this setup must have Administrator permissions.

1.18.1 Specifying settings for using the functions of Central Scope (for Windows)

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 `Scope-path\bin\jcsdbsetup` command. Specify options as needed.

2. Enable Central Scope Service (`jcsmain`).

Execute `jcoimdef -s ON`.

3. Start 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 *Chapter 1. Commands* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

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

1.18.2 Specifying settings for handling JP1/IM - Manager failures (for Windows)

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 *10.3 Data that needs to be collected when a problem occurs* in the *JP1/Integrated Management - Manager Administration Guide*.

About the data collection tool

- About `jim_log.bat`

See *jim_log.bat* (Windows only) in Chapter 1. *Commands* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

In the event of a problem, you might need to obtain a memory dump and a crash dump. (This data can also be collected by using the data collection tool.) For details about how to configure output settings for memory dump and crash dump, see the release notes.

Important

- 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**.
- 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 (*jp1co_service.conf*) so that process restart is enabled:

```
Console-path\conf\jp1co_service.conf
```

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

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_spm�_reload
```

About process restart definition

- About the extended startup process definition file (*jp1co_service.conf*)
See *Extended startup process definition file (jp1co_service.conf)* in Chapter 2. *Definition Files* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

Note:

In a cluster system, do not enable process restart in the event of abnormal process termination. If JP1/IM - Manager fails, the process restart function might also be affected. If you want to restart processes in the event of abnormal process termination in a cluster system, use the cluster software (not JP1/IM - Manager) to control the restart.

(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 (*jp1co_param_v7.conf*):

```
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\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 Chapter 2. *Definition Files* in the manual *JP1/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. Use the `jco_spmd_reload` command to reload JP1/IM - Manager, or restart JP1/IM - Manager.

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

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



Important

In Windows (x64), if you execute a command in the `%WINDIR%\System32` folder, the redirection function of WOW64 redirects the command as a command in the `%WINDIR%\SysWow64` folder. If the command does not exist at the redirection destination, the command execution might fail. Be careful when you specify a command in the `%WINDIR%\System32` folder as the execution command.

About the health check function settings

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

See *Health check definition file (jcohc.conf)* in Chapter 2. *Definition Files* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

- About the `jcohctest` command

See *jcohctest* in Chapter 1. *Commands* in the manual *JP1/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 might 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 previous version of JP1/IM - Manager. Change the settings as appropriate to your operation.

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 *JP1/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 *Chapter 2. Definition Files* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

3. Start JP1/IM - Manager.

1.18.3 Specifying settings for upgrading (for Windows)

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

(1) 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.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 `jplcsverup.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 1–6: 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 *Chapter 1. Commands* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

(2) Updating the automated action definition file

If you have upgraded JP1/IM - Manager from version 11-10 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 11-10 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. Rename the file specified for the `-o` option of the `jcadefconv` command to `actdef.conf`, and then move the file to the correct location.

The path name (including the file name) of the correct location is shown below. Note that you do not need to perform this step if the file name that was specified for the `-o` option in step 2 is the path name including the file name shown below.

For a physical host: `Console-path\conf\action\actdef.conf`

For a logical host: `shared-folder\jp1cons\conf\action\actdef.conf`

4. Start JP1/IM - Manager.

- About the automated action function

See *Chapter 5. Command Execution by Automated Action* in the *JP1/Integrated Management - Manager Overview and System Design Guide*.

- About the `jcadefconv` command

See *jcadefconv* in *Chapter 1. Commands* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

(3) Displaying the source host

When you upgrade JP1/IM - Manager version 09-00 to 09-10, source hosts are not set in the file that defines which items are displayed for event conditions. As a result, even if you enable mapping for source hosts, the list box in the **Event conditions** section does not display **Source host** in the Action Parameter Detailed Definitions window. If you want to display **Source host** in the list box in the **Event conditions** section of the Action Parameter Detailed Definitions window, you need to add `E.JP1_SOURCEHOST` in the file that defines which items are displayed for event conditions.

For details about the Action Parameter Detailed Definitions window, see *2.33.1 Action Parameter Detailed Definitions window* in the manual *JP1/Integrated Management - Manager GUI Reference*.

For details about the file that defines which items are displayed for event conditions, see *File that defines which items are displayed for event conditions (attr_list.conf)* in *Chapter 2. Definition Files* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

(4) Specifying the event report output format

If you have upgraded from JP1/IM - Manager version 10-50 or earlier, the function for assigning one column to each program-specific extended attribute when event reports are output in CSV format is disabled. To specify whether this function is to be enabled, use the `PROGRAM_SPECIFIC_EX_ATTR_COLUMN` parameter in the environment definition file for event report output (`evtreport.conf`). This function is enabled when you perform a new installation. If necessary, configure the environment definition file for event report output.

For details about the environment definition file for event report output, see *Environment definition file for event report output (evtreport.conf)* in *Chapter 2. Definition Files* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

(5) Displaying the Start the process automatically when the log file trap service starts check box

If you have upgraded JP1/IM - Manager from version 11-01 or earlier, the **Start the process automatically when the log file trap service starts** check box is disabled (hidden).

You can use the `LOGFILETRAP_AUTO_START_CONTROL` parameter in the profile management environment definition file (`jp1cf_profile_manager.conf`) to specify the enable/disable setting for the **Start the process automatically when the log file trap service starts** check box. For details, see *Profile management environment definition file (jp1cf_profile_manager.conf)* in *Chapter 2. Definition Files* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

(6) Updated agent profile notification function

If you have upgraded JP1/IM - Manager from version 11-01 or earlier, the updated agent profile notification function is disabled.

You can use the `AGENT_PROFILE_UPDATE_NOTICE` parameter in the profile management environment definition file (`jp1cf_profile_manager.conf`) to specify the enable/disable setting for the updated agent profile notification function. For details, see *Profile management environment definition file (jp1cf_profile_manager.conf)* in *Chapter 2. Definition Files* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

(7) Setting for monitoring logs while remote monitoring is stopped

If you have upgraded JPI/IM - Manager from version 11-01 or earlier, the log data that is output while remote monitoring is stopped is set to be not collected.

You can use the `START_OPTION` parameter in the remote log trap environment definition file (`jplcf_remote_logtrap.conf`) to specify the setting for whether log data that is output while remote monitoring is stopped is to be collected. For details, see *Remote log trap environment definition file (jplcf_remote_logtrap.conf)* in *Chapter 2. Definition Files* in the manual *JPI/Integrated Management - Manager Command and Definition File Reference*.

1.19 Setting up JP1/IM - View (for Windows)

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

The user who performs this setup must have Administrator permissions.

1.19.1 Specifying settings for handling JP1/IM - View failures (for Windows)

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 *10.3 Data that needs to be collected when a problem occurs* in the *JP1/Integrated Management - Manager Administration Guide*.

About the data collection tool

- About `jcoview_log.bat`

See `jcoview_log.bat` (Windows only) in *Chapter 1. Commands* in the manual *JP1/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 `jcftthreadmp` command for collecting a thread dump in the event of a failure in IM Configuration Management - View. For details about the `jcftthreadmp` command, see `jcftthreadmp` (Windows only) in *Chapter 1. Commands* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

1.19.2 Customizing operation of JP1/IM - View (Central Console viewer and Central Scope viewer) (for Windows)

You can customize operation of JP1/IM - View (Central Console viewer and Central Scope viewer). To change the settings, edit the IM - View settings file (`tuning.conf`). The following are the items that you can specify for JP1/IM - View (Central Console viewer and Central Scope viewer).

- The number of connected-host log entries in the Login window
- Preventing the history of previously used JP1 login user names from appearing on the following item
 - User names in the Login window
- Whether the Tool Launcher window can start when the Event Console window opens
- Whether the List of Action Results window can start when the Event Console window opens
- Path to start the WWW browser that is used for opening monitor windows and Tool Launcher
- Whether to allow copying to the clipboard

- Preventing the names of JP1 users who are currently logged in from appearing in the Monitoring Tree window, Monitoring Tree (Editing) window, Visual Monitoring (Editing) window, Event Console window, List of Action Results window, and the Execute Command window

The settings specified below take effect only in the viewer in which you edit the IM - View settings file. The setting procedure is as follows:

1. Edit the following IM-View settings file (`tuning.conf`) by using a text editor.

`View-path\conf\tuning.conf`

2. Restart JP1/IM - View.

About customization of the IM-View settings file:

- About the IM-View settings file

Refer to: *IM-View settings file (tuning.conf)* in *Chapter 2. Definition Files* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*

1.19.3 Setting up and customizing IM Configuration Management - View (for Windows)

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

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

(1) Setting up IM Configuration Management - View

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 IM Configuration Management - View is created in the **Start** menu when you install JP1/IM - View.

To re-create the shortcut to IM Configuration Management - View after it has been deleted:

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 **All 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 *Chapter 1. Commands* in the manual *JP1/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.

(2) Customizing operation of IM Configuration Management - View

You can customize the operation of IM Configuration Management - View. To change settings, edit the operation definition file of the IM configuration management viewer (`jcfview.conf`). You can specify the following items for IM Configuration Management - View:

- The number of connected-host log entries displayed in the Login window for IM Configuration Management
- The number of connected-user log entries displayed in the Login window for IM Configuration Management
- Whether the window display settings history functionality can be used when the IM Configuration Management window, the Edit Agent Configuration window, the Edit Remote Monitoring Configuration window, or the Display/Edit Profiles window starts
- The server response timeout period
- Response timeout period when the system hierarchy is applied
- Preventing the names of JP1 users who are currently logged in from appearing in the IM Configuration Management window, Edit Agent Configuration window, Edit Remote Monitoring Configuration window, and the Display/Edit Profiles window

The settings specified below take effect only in the viewer in which you edit the operation definition file of the IM configuration management viewer. The setting procedure is as follows:

1. Edit the following operation definition file of the IM configuration management viewer (`jcfview.conf`) by using a text editor.

`View-path\conf\jcfview.conf`

2. Restart JP1/IM - View.

About customization of the operation definition file of the IM configuration management viewer:

- About the operation definition file of the IM configuration management viewer
Refer to: *Operation definition file for IM Configuration Management - View (jcfview.conf)* in *Chapter 2. Definition Files* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*

1.19.4 Setting up JP1/IM - Rule Operation linkage (for Windows)

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

The only task to be performed for setup is creation of shortcuts to JP1/IM - Rule Operation.

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 **All 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 **JP1_Integrated Management - View** (shortcut) registered in the **Start** menu, the shortcuts are not added.

1.20 Saving manuals to a computer (for Windows)

When you store HTML manuals to certain folders, you can access the manuals by clicking the **Help** button in a window.

To save HTML manuals to a computer:

1. Have ready the manual distribution medium provided as a standard item with each program product.
2. Store the target data from the manual distribution medium to JP1/IM - Manager and JP1/IM - View.
The target data is stored in the manual distribution medium. Store the target data in the destination folders of JP1/IM - Manager and JP1/IM - View (for each manual).

- Target data (HTML manual)
CSS file, all HTML files, and GRAPHICS folder
- Locations of data in the manual distribution medium (inserted in the drive of the Windows machine)

JP1/Integrated Management: Getting Started (Integrated Console)

Corresponding-drive\MAN\3021\03A0620D

JP1/Integrated Management - Manager Overview and System Design Guide

Corresponding-drive\MAN\3021\03A0720D

JP1/Integrated Management - Manager Configuration Guide

Corresponding-drive\MAN\3021\03A0820D

JP1/Integrated Management - Manager Administration Guide

Corresponding-drive\MAN\3021\03A0920D

JP1/Integrated Management - Manager GUI Reference

Corresponding-drive\MAN\3021\03A1020D

JP1/Integrated Management - Manager Command and Definition File Reference

Corresponding-drive\MAN\3021\03A1120D

JP1/Integrated Management - Manager Messages

Corresponding-drive\MAN\3021\03A1220D

- Locations to store the target data on the JP1/IM - Manager side:

JP1/Integrated Management: Getting Started (Integrated Console)

installation-folder\JP1Cons\www>manual\en\03A0600D

JP1/Integrated Management - Manager Overview and System Design Guide

installation-folder\JP1Cons\www>manual\en\03A0700D

JP1/Integrated Management - Manager Configuration Guide

installation-folder\JP1Cons\www>manual\en\03A0800D

JP1/Integrated Management - Manager Administration Guide

installation-folder\JP1Cons\www>manual\en\03A0900D

JP1/Integrated Management - Manager GUI Reference

installation-folder\JP1Cons\www>manual\en\03A1000D

JP1/Integrated Management - Manager Command and Definition File Reference

installation-folder\JP1Cons\www>manual\en\03A1100D

JP1/Integrated Management - Manager Messages

installation-folder\JP1Cons\www>manual\en\03A1200D

- Locations to store the target data on the JP1/IM - View side:

JP1/Integrated Management: Getting Started (Integrated Console)

installation-folder\JP1CoView\manual\en\03A0600D

JP1/Integrated Management - Manager Overview and System Design Guide

installation-folder\JP1CoView\manual\en\03A0700D

JP1/Integrated Management - Manager Configuration Guide

installation-folder\JP1CoView\manual\en\03A0800D

JP1/Integrated Management - Manager Administration Guide

installation-folder\JP1CoView\manual\en\03A0900D

JP1/Integrated Management - Manager GUI Reference

installation-folder\JP1CoView\manual\en\03A1000D

JP1/Integrated Management - Manager Command and Definition File Reference

installation-folder\JP1CoView\manual\en\03A1100D

JP1/Integrated Management - Manager Messages

installation-folder\JP1CoView\manual\en\03A1200D

Delete any existing HTML manuals in the JP1/IM - Manager and JP1/IM - View folders before storing the new ones.

1.21 Uninstallation (for Windows)

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

1.21.1 Uninstallation procedure (for Windows)

This subsection explains how to uninstall JP1/IM - Manager and JP1/IM - View. If you are using IM databases (integrated monitoring database and IM Configuration Management database), delete the IM databases before you uninstall JP1/IM - Manager.

(1) How to delete IM databases

If you will be deleting the IM databases to reconfigure the environment, first make a backup of the IM databases. For details about the backup method, see *1.2 Managing the databases* in the *JP1/Integrated Management - Manager Administration Guide*.

For details about the commands, see the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

To delete IM databases:

1. Stop JP1/IM - Manager.

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

2. To delete the integrated monitoring database or the IM Configuration Management database, check the status of the following services:

- For physical hosts

The IM database service (JP1/IM-Manager DB Server) is running.

- For physical hosts, when the integrated monitoring database or the IM Configuration Management database has been set up and the IM database is being used

The JP1/IM - Manager service (JP1/IM-Manager) is stopped.

- For logical hosts

The IM database (JP1/IM-Manager DB Server_ *logical-host-name*) on the logical host has started.

- For logical hosts, when the integrated monitoring database or the IM Configuration Management database has been set up and the IM database is being used

The JP1/IM - Manager service (JP1/IM-Manager_ *logical-host-name*) is stopped.

3. To disable the integrated monitoring database, execute the `jcoimdef` command:

```
jcoimdef -db OFF
```

The integrated monitoring database is disabled.

4. To delete the integrated monitoring database, execute the `jcodbunsetup` command:

```
jcodbunsetup
```

The integrated monitoring database is deleted.

5. To disable the IM Configuration Management database, execute the `jcoimdef` command:

```
jcoimdef -cf OFF
```

The IM Configuration Management service (`jcfmain`) is disabled.

6. To delete the IM Configuration Management database, execute the `jcfdbunsetup` command:

```
jcfdbunsetup
```

The IM Configuration Management database is deleted.

7. Delete the following files and folders on the physical host:

Files under *Manager-path*\data\imcf\imconfig

File and folders under *Manager-path*\data\imcf\profiles

8. Restart the machine.

(2) How to uninstall JP1/IM - Manager

To uninstall:

1. Terminate the programs.

Before you start the uninstallation procedure, terminate all programs.

Terminate JP1/IM - Manager Service. If a JP1/IM - View is connected to the JP1/IM - Manager which you want to uninstall, the login user should log out from the JP1/IM - Manager.

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, Programs and Features**, 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 might 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 had been installed.

(3) How to uninstall JP1/IM - View

To uninstall:

1. Terminate running programs.

Before you start the uninstallation procedure, terminate all programs.

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, Programs and Features**, 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 might have been edited by the user, are not deleted during uninstallation. To delete these files, use Windows Explorer to delete the folder in which JP1/IM - View had been installed.

1.21.2 Notes on uninstallation(for Windows)

- About Hitachi Network Objectplaza Trace Library (HNTRLib2)
 - When JP1/IM - View is uninstalled, Hitachi Network Objectplaza Trace Library (HNTRLib2) is also deleted unless other products use it.
- Settings in the Windows environment
 - 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.

#: In Windows, this value might be different depending on the environment because the value of *system-drive* : \Program Files is determined by the setting of an OS environment variable at the time of installation.

2

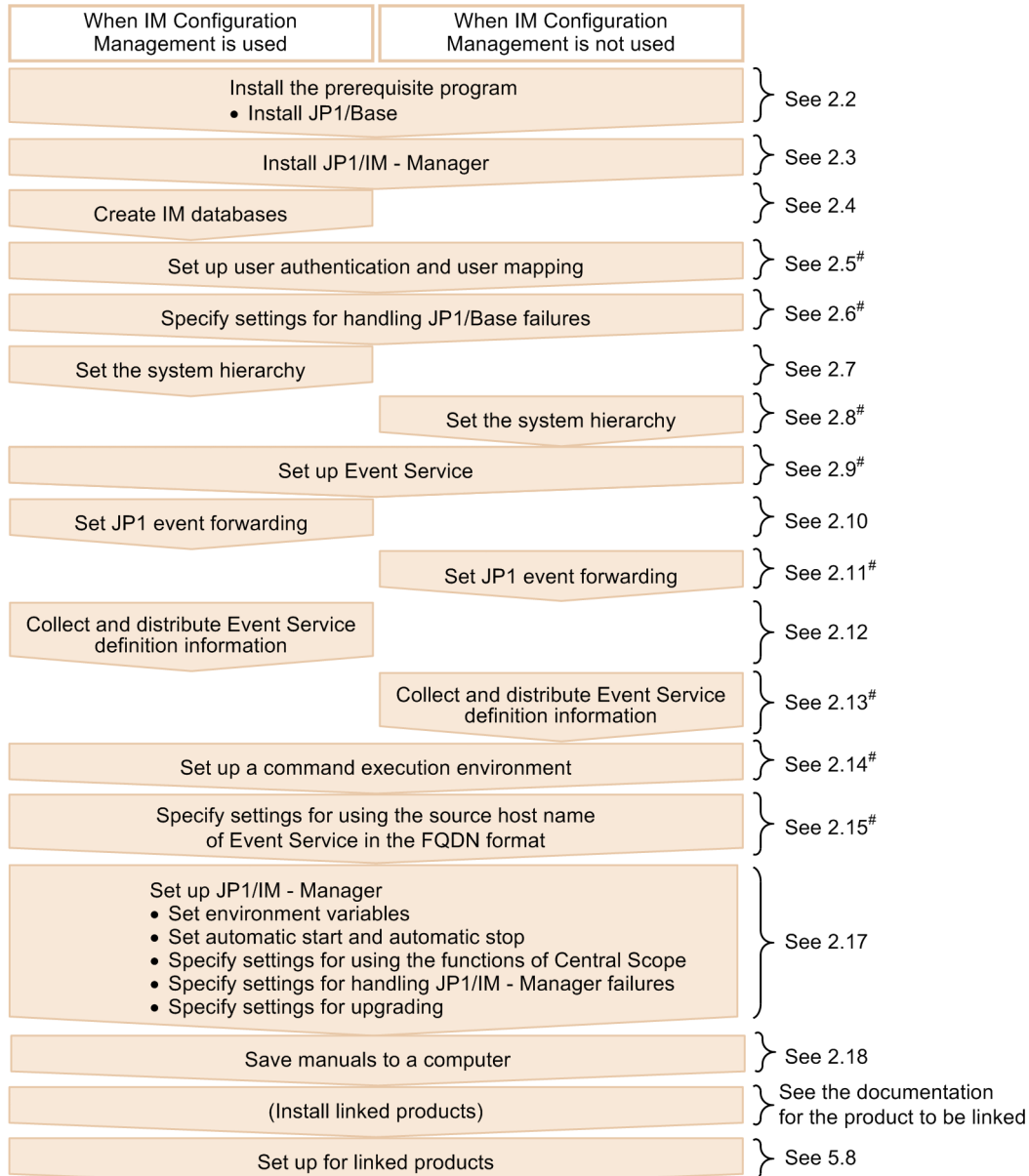
Installation and Setup (for UNIX)

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

2.1 Installation and setup procedures (for UNIX)

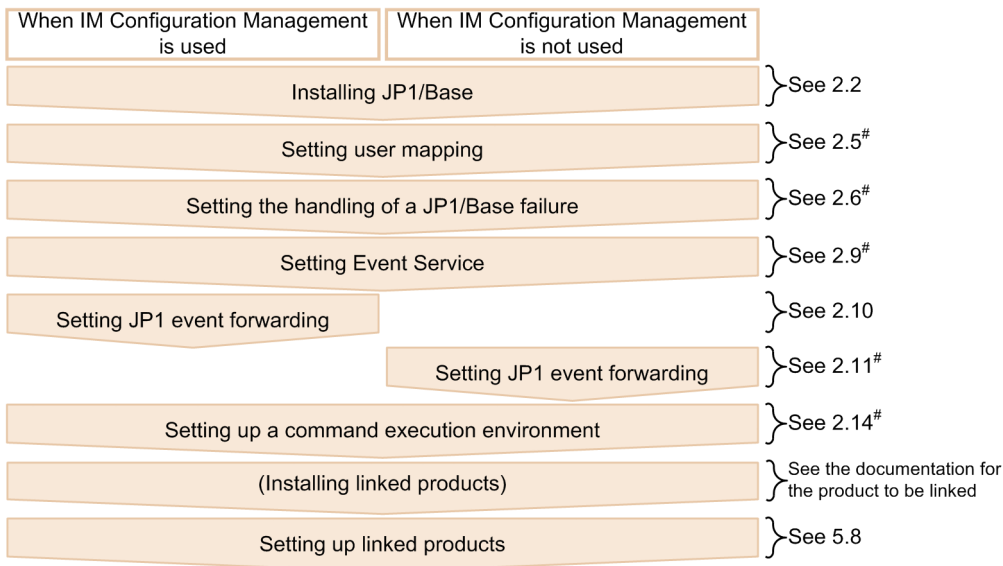
This section describes the procedure from the beginning of installation to the end of setup for a manager, an agent, and a host to be monitored remotely. For details about the uninstallation procedure, see [2.19.1 Uninstallation procedure \(for UNIX\)](#).

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



[#]: For details, see the *JP1/Base User's Guide*.

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



[#]: For details, see the *JP1/Base User's Guide*.

For details about the settings for monitoring logs on hosts that will be monitored remotely, see [2.16 Specifying settings for monitoring logs on remotely monitored hosts \(for UNIX\)](#).

For details about the settings for using the communication encryption function that encrypts communication data, see [8.4 Configuring encrypted communication](#).

2.2 Preparations required before installation (for UNIX)

2.2.1 Designing the JP1/IM setup details (for UNIX)

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 *JP1/Integrated Management - Manager Overview and System Design Guide*.

2.2.2 Configuring the system environment (for UNIX)

(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.
- The host name of the local host can be resolved with the IP address (IP address other than loopback address) in the connected LAN environment.

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 (for UNIX)

(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 *JP1/Integrated Management - Manager Overview and System Design Guide*. For details about how to install JP1/Base, see the *JP1/Base User's Guide*.

2.3 Installing JP1/IM - Manager (for UNIX)

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 (for UNIX)

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 \(for UNIX\)](#).

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
```

Important

If you have upgraded JP1/IM - Manager in an environment in which IM databases have already been set up, use the `jimdbupdate` command to update the IM databases. If the IM databases have not been updated, a warning message is displayed when JP1/IM - Manager starts.

(2) About the types of installation

Upgrade installation

If you are upgrading from a previous 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 *JP1/Integrated Management - Manager Overview and System Design Guide*.

Remote installation using JP1/NETM/DM, JP1/IT Desktop Management 2 and Job Management Partner 1/Software Distribution

JP1/IM supports remote installation (software distribution) using JP1/NETM/DM, JP1/IT Desktop Management 2 and Job Management Partner 1/Software Distribution, and you can perform a new installation as well as an upgrade installation of JP1/IM. See JP1/NETM/DM, JP1/IT Desktop Management 2 or Job Management Partner 1/Software Distribution Manual for more information.

Be sure to use a JP1/NETM/DM 09-00 or later packager, a JP1/IT Desktop Management 2 packager or a Job Management Partner 1/Software Distribution 09-00 or later packager to package this software product. JP1/NETM/DM is sold only in Japan.

2.3.2 How to use the Hitachi Program Product Installer (for UNIX)

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 in the drive.
2. Mount the distribution medium.

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

- In AIX

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

- In Linux

```
/bin/mount -r -o mode=0544 /dev/cdrom /mnt/cdrom
```

Note that the underlined distribution medium file system mount directory name depends on the environment.

3. Start the Hitachi Program Product Installer.

The directory and file names on the distribution medium might differ depending on the machine environment. Use the `ls` command to check the directory and file names, and then use the displayed names.

- In AIX

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

- In Linux

```
/mnt/cdrom/linux/setup /mnt/cdrom
```

Replace the underlined part with the actual distribution medium mount directory name.

Important

During installation, do not start Hitachi Program Product Installer by executing `/etc/hitachi_setup`.

4. Unmount the distribution medium.

After you finish the installation, unmount the distribution medium. For details about how to unmount a distribution medium, see the OS documentation.

- In AIX

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

- In Linux

```
/bin/umount /mnt/cdrom
```

Replace the underlined part with the actual distribution medium 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 Settings required immediately after installation (for UNIX)

Specify in a JP1/Base environment variable the *language encoding* in which JP1/IM - Manager runs. You must specify the language encoding in both the environment variable file and the common definitions. Effective with version 11-00, environment variables of JP1/IM (`jp1co_env.conf` file) are no longer used.

The language encoding in the environment variable file and common definitions must match on all local hosts. Additionally, use the character encoding of events in the JP1/SES format to unify the language environment of a system that monitors events in the JP1/SES format. This subsection describes how to set the language encoding in the environment variable file and common definitions.

(1) Setting the language encoding in the environment variable file

Using a text editor such as `vi`, open the `/etc/opt/jp1base/conf/jp1bs_env.conf` file and, following `LANG=` on the first line, set the appropriate value for the `LANG` environment variable based on the following table.

Table 2–1: Values that can be specified for `LANG` in the `jp1co_env.conf` file

OS	Language type	Encoding	Value of LANG environment variable ^{#3}
AIX	Japanese	SJIS	Ja_JP.IBM-932 or Ja_JP
		EUC	ja_JP.IBM-eucJP or ja_JP
		UTF-8 ^{#2}	JA_JP.UTF-8, JA_JP, or ja_JP.UTF-8
	English	C	C
	Chinese	GB18030	Zh_CN.GB18030
Linux	Japanese	SJIS ^{#1}	ja_JP.SJIS or ja_JP.sjis
		UTF-8 ^{#2}	ja_JP.UTF-8 or ja_JP.utf8
	English	C	C
	Chinese	GB18030	zh_CN.gb18030

#1

Applicable to SUSE Linux only.

#2

In UTF-8 encoding, two character codes are used to represent each of the following symbols:

Yen sign (\): 0x5C or 0xC2A5

Tilde (~): 0x7E or 0xE280BE

In JP1/IM - Manager, \ is represented by 0x5C and ~ is represented by 0x7E.

#3

Do not specify a `LANG` value that is not listed in the table. The value of `LANG` is case sensitive.

These definitions take effect the next time JP1/IM - Manager starts.

Important

When you select English as the language type, do not use multi-byte characters when you configure JP1/IM - Manager. If you do, JP1/IM - Manager handles the multi-byte characters as ASCII characters. As a result, JP1/IM - Manager might not operate normally.

(2) Checking the language environment settings of JP1/Base

1. Check the setting value in the `/etc/opt/jp1base/conf/jp1bs_env.conf` file.

Confirm that the value set after `LANG =` in the `jp1bs_env.conf` file matches the value set in [2.3.3\(1\) Setting the language encoding in the environment variable file](#).

For details about the `jp1bs_env.conf` file, see the *JP1/Base User's Guide*.

2. Check the setting value in the `/etc/opt/jp1base/jbs_start` file.

Confirm that the value set after `LANG =` in the `jbs_start` file matches the value set in [2.3.3\(1\) Setting the language encoding in the environment variable file](#).

For details about the `jbs_start` file, see the *JP1/Base User's Guide*.

Note

Once you have set the encoding and started the operation, you can still use the steps above to change the encoding.

For details about the language environment settings of JP1/Base, see the part that describes the language type settings in the *JP1/Base User's Guide*.

(3) Setting the language encoding in the common definitions

1. Edit the `jp1bs_param.conf` file.

Use a text editor to open the `/etc/opt/jp1base/conf/jp1bs_param.conf` file. After `LANG=`, set a value for the `LANG` environment variable based on the table below.

Table 2–2: Values that can be specified for `LANG` in the `jp1bs_param.conf` file

Language type	Code	LANG value
Japanese	Shift JIS code	SJIS
	EUC code	EUCJIS
	UTF-8 code	UTF-8
English		C
Chinese		GB18030

2. Stop JP1/IM - Manager.

3. Stop JP1/Base.

4. Execute the following command:

```
/opt/jp1base/bin/jbssetcnf /etc/opt/jp1base/conf/jp1bs_param.conf
```

If you need to change the environment variables of JP1/IM - Manager while Central Scope is running, perform the following procedure:

1. Use the `jcsdbexport` command to output the information stored in the monitoring object database to a local file.
2. Stop JP1/IM - Manager.
3. Change the language encoding used by JP1/IM - Manager when it runs and start JP1/IM - Manager.
4. Use the `jcsdbimport` command to apply the contents of the monitoring object database (output to the local file) to the monitoring object database of Central Scope.

If you do not perform the above procedure, the Monitoring Tree window and Visual Monitoring window will not be displayed correctly.

(4) Starting JP1/Base and JP1/IM - Manager

1. Start JP1/Base.
2. Start JP1/IM - Manager.

2.3.4 Notes about installing (for UNIX)

- Relationship between products
JP1/IM - Manager requires JP1/Base. When you install 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 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/Base, Hitachi Network Objectplaza Trace Library (HNTRLib2) is installed.
- Settings in the OS environment
 - During installation, the following information is set in the OS:
In the `services` file, the port numbers indicated in *Appendix C. Port Numbers* in the *JP1/Integrated Management - Manager Overview and System Design Guide* are set.
 - During uninstallation of JP1/IM - Manager, the port numbers indicated in *Appendix C. Port Numbers* in the *JP1/Integrated Management - Manager Overview and System Design Guide* are deleted.
- About downgrade installation
JP1/IM - Manager does not support downgrade installation. If you want to downgrade the product that has been installed, uninstall the product, and then reinstall it.

2.4 Creating IM databases (for UNIX)

You use IM databases to monitor events that occur in the system. The two types of IM databases are the integrated monitoring database and the IM Configuration Management database. The integrated monitoring database is used when Central Console is being used. The IM Configuration Management database is used with IM Configuration Management to manage the system hierarchy. For details about the functions available when the integrated monitoring database and the IM Configuration Management database are used, see *2.4 Functions provided by the IM database* in the *JP1/Integrated Management - Manager Overview and System Design Guide*.

During system configuration or after operations have started, you can create either or both the integrated monitoring database and the IM Configuration Management database.

JP1 events obtained from the event database after the JP1/IM - Manager service has started are stored in the integrated monitoring database. For details, see *3.1.3(2) JP1 event control when using the integrated monitoring database* in the *JP1/Integrated Management - Manager Overview and System Design Guide*.

This section explains how to create an IM database.

2.4.1 Preparations for creating IM databases (for UNIX)

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:

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

If JP1/IM - MO is being used and JP1/IM - Manager and JP1/IM - MO are located on separate hosts, you must add the item `IMDBHOSTNAME` in the setup information file. For details about the setup information file, see *Setup information file (jimdbsetupinfo.conf)* in *Chapter 2. Definition Files* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

2. Check the settings in the setup information file.

Make sure of the following:

- Permanently mounted directories are specified (that is, directories that might be unmounted are not specified) for `IMDBENVDIR` and `IMBDDIR`, and paths containing symbolic links are not specified for `IMDBENVDIR` and `IMBDDIR`.

2.4.2 Setting up the integrated monitoring database (for UNIX)

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

The setup procedure differs depending on whether the IM Configuration Management database has already been set up. Apply the following procedures as appropriate depending on the case.

(1) When the IM Configuration Management database has been set up

The setup procedure differs depending on whether you stop JP1/IM-Manager Service. The following are the setup procedures for the two cases.

- To stop JP1/IM-Manager Service and set up the integrated monitoring database:

1. Check if the IM database service (JP1/IM-Manager DB Server) is running.

2. Stop the following services:

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

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

```
jcodbsetup -s [-q]
```

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

```
jcoimdef -db ON
```

5. Start JP1/IM-Manager Service.

- To set up the integrated monitoring database without stopping JP1/IM-Manager Service:

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

```
jcoimdef -cf OFF
```

2. Restart JP1/IM-Manager Service.

3. Check if the IM database service (JP1/IM-Manager DB Server) is running.

4. Stop the following service:

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

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

```
jcodbsetup -s [-q]
```

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

```
jcoimdef -db ON
```

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

```
jcoimdef -cf ON
```

8. Restart JP1/IM-Manager Service.

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

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

(2) When the IM Configuration Management database has not been set up

1. Stop the following service:

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

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

```
jcodbsetup -f setup-information-file-name [-q]
```

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

```
jcoimdef -db ON
```

4. Restart JP1/IM-Manager Service.

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

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

2.4.3 Setting up the IM Configuration Management database (for UNIX)

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 plan to use the IM Configuration Management functions, there is no need to perform this procedure.

The setup procedure differs depending on whether the integrated monitoring database has already been set up. Apply the following procedures as appropriate depending on the case.

(1) When the integrated monitoring database has been set up

The setup procedure differs depending on whether you stop JP1/IM-Manager Service. The following are the setup procedures for the two cases.

- To stop JP1/IM-Manager Service and set up the IM Configuration Management database:

1. Check if the IM database service (JP1/IM-Manager DB Server) is running.

2. Stop the following services:

- JP1/IM-Manager Service
- If JP1/IM - MO is being used, the JP1/IM - Message Optimizer service of JP1/IM - MO at the connection source.

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

```
jcfdbsetup -s [-q]
```

- To set up the IM Configuration Management database without stopping the JP1/IM-Manager Service:
 1. Execute the `jcoimdef` command to disable the integrated monitoring database.


```
jcoimdef -db OFF
```
 2. Restart JP1/IM-Manager Service.
 3. Check if the IM database service (JP1/IM-Manager DB Server) is running.
 4. Stop the following service:
 - If JP1/IM - MO is being used, the JP1/IM - Message Optimizer service of JP1/IM - MO at the connection source.
 5. Execute the `jcfdbsetup` command to create an IM Configuration Management database.


```
jcfdbsetup -s [-q]
```
 6. Execute the `jcoimdef` command to enable the integrated monitoring database.


```
jcoimdef -db ON
```

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

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

(2) When the integrated monitoring database has not been set up

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


```
jcfdbsetup -f setup-information-file-name [-q]
```

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

2.4.4 Settings for using the functions of IM Configuration Management (for UNIX)

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 *2.4.3 Setting up the IM Configuration Management database (for UNIX)*, 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 (`jcmain`).


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

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

For details about the `jco_spm�_status` command, see *jco_spm�_status* in *Chapter 1. Commands* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

2.4.5 Updating IM databases (for UNIX)

If you are using IM databases and you wish to upgrade JP1/Integrated Management or apply a corrected version of JP1/IM - Manager, you must first update the IM databases.

To update IM databases:

1. Check the following service statuses:

- JP1/IM-Manager Service is stopped.
- If JP1/IM - MO is being used, the JP1/IM - Message Optimizer service of JP1/IM - MO is stopped at the connection source.

2. Execute the `jimdbupdate` command to check if the IM databases have been updated.

- If the following message is output, perform step 5:

```
KNAN11201-I The IM database service is the latest.
```

- If the following message is output, perform the procedure beginning with step 3:

```
KNAN11202-I The overwrite is necessary for the IM database.
```

```
KNAN11207-I An update of the table schema of an IM database service is required.
```

3. Execute the `jimdbbackup` command to back up the IM databases:

```
jimdbbackup -o backup-file-name -m MAINT
```

4. Execute the `jimdbupdate` command to update the IM databases:

```
jimdbupdate -i
```

5. Start JP1/IM - Manager.

Important

Do not restore into an IM database obtained after the `jimdbupdate` command has been executed any IM database backup data that was obtained before the `jimdbupdate` command was executed.

After you have executed the `jimdbupdate` command, execute the `jimdbbackup` command again to make a new backup.

2.5 Setting up user authentication and user mapping (for UNIX)

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 2–3: 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

#

Not required when automated actions are not performed or commands are not executed on managed hosts from JP1/IM - View.

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 2–4: 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
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).

2.5.1 Specifying the authentication server (for UNIX)

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/jbssetusrsvr 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 *JP1/Base User's Guide*.

2.5.2 Registering JP1 users (for UNIX)

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
```

2.5.3 Setting operation permissions for the JP1 users (for UNIX)

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 *JP1/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 *JP1/Integrated Management - Manager Overview and System Design Guide*.

2.5.4 Copying the primary authentication server settings (for UNIX)

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/jplbase/conf/user_acl` directory. These are text files. Use a method such as an ASCII transfer by FTP.

2.5.5 Setting user mapping (for UNIX)

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 (`jplBsUmap.conf`) to specify user mapping between JP1 users and OS users.

2. Execute the following user mapping definition command:

```
/opt/jplbase/bin/jbsmkumap
```

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 (`jplBsUmap.conf`) and the `jbsmkumap` command, see the description of the user management settings in the *JP1/Base User's Guide*.

2.6 Specifying settings for handling JP1/Base failures (for UNIX)

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 *JP1/Base User's Guide*.

2.7 Setting the system hierarchy (when IM Configuration Management is used) (for UNIX)

This section describes how to set the system hierarchy (IM configuration) when IM Configuration Management is used. For details about how to set the system hierarchy when IM Configuration Management is not used, see [2.8 Setting the system hierarchy \(when IM Configuration Management is not used\) \(for UNIX\)](#).

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 and perform the following operations, the configuration definition information held in IM Configuration Management does not match that held in JP1/Base.

- Editing the configuration definition file of JP1/Base
- Executing the `jbsrt_distrib` command

Therefore, when you use IM Configuration Management to manage your system hierarchy, we recommend that you use it to integrally manage your system hierarchy.

When you use JP1/Base functionality to distribute the definition of your system hierarchy, you need to obtain the system hierarchy. This will enable IM configuration Management to match the configuration definition information held in both IM Configuration Management and JP1/Base. If the system hierarchy is not obtained, operation will malfunction because of mismatched the configuration definition information.

2.7.1 Using IM Configuration Management - View to set the system hierarchy (for UNIX)

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 *JP1/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 *3.1.4 Displaying host information*.
 - For details about how to delete hosts, see *3.1.6 Deleting hosts*.
 - For details about how to change information about the registered hosts, see *3.1.5 Changing the attributes of host information*.
2. Add the host registered in IM Configuration Management to the system hierarchy and set the hierarchy between managers and agents.
 - For details about how to add hosts to a JP1/IM system, see *3.2.4(1)(a) Adding hosts*.
 - For details about how to delete hosts from the JP1/IM system, see *3.2.4(1)(c) Deleting hosts*.
 - For details about how to set a hierarchy between managers and agents, see *3.2.4(1)(b) 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 *3.2.4(3) Applying a system hierarchy to a system managed by IM Configuration Management*.
 - 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 *3.2.5 Synchronizing the system hierarchy*.

(2) Editing an existing system hierarchy

Perform the following procedure to switch the method of setting configuration management information from the configuration management function provided by JP1/Base to IM Configuration Management.

1. In the IM Configuration Management window, read the existing configuration definitions of JP1/IM to obtain the system hierarchy.

The obtained configuration definitions are stored in the IM Configuration Management database. Hosts that have not been registered in IM Configuration Management are automatically registered in the database.
For details, see *3.2.1 Collecting the system hierarchy*.

2. In the Edit Host Properties window, check the registered host attributes, and edit the host names and host types as necessary.
For details, see [3.1.5 Changing the attributes of host information](#).
3. In the IM Configuration Management window, collect host information.
For details, see [3.1.3 Collecting information from hosts](#).
4. In the IM Configuration Management window, check the host information you have collected.
Host information includes lower-level host information, basic information, product information, and service information.
For details, see [3.1.4 Displaying host information](#).
5. In the IM Configuration Management window, check the system hierarchy and edit it as necessary.
When you edit the system hierarchy, make sure you apply the new hierarchy to the system.
For details, see [3.2.2 Displaying the system hierarchy](#), [3.2.4 Editing the system hierarchy](#), and [3.2.4\(3\) Applying a system hierarchy to a system managed by IM Configuration Management](#).
6. In the IM Configuration Management window, collect profile information.
The settings that are currently used by the services of agents and the configuration files stored in the agents are collected.
For details, see [3.5.1\(2\) Collecting profiles](#).
7. In the IM Configuration Management window, check the profile information and edit the configuration files as necessary.
When you edit configuration files, make sure you apply the edited information to agents. In addition, perform step 6 after you apply the new configuration files and check the profile information.
For details, see [3.5.1\(3\) Displaying profiles](#), [3.5.1\(5\) Editing configuration files](#), and [3.5.1\(6\) Applying edited information in configuration files](#).

2.7.2 Using the export and import functions to set the system hierarchy (for UNIX)

When you use the export and import functions of IM Configuration Management, you can migrate the system configuration used in a test environment to a production environment. You can also migrate the system hierarchy (IM configuration) used before changes have been made to a new environment. For details about how to set the system hierarchy using the export and import functions, see [3.6 Importing and exporting the management information in IM Configuration Management](#).

2.7.3 Settings for managing and monitoring a virtualization system configuration (for UNIX)

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 [3.3 Setting a virtualization system configuration](#).

2.8 Setting the system hierarchy (when IM Configuration Management is not used) (for UNIX)

This section describes how to set the system hierarchy (IM configuration) when IM Configuration Management is not used. For details about the system hierarchy settings when IM Configuration Management is used, see [2.7 Setting the system hierarchy \(when IM Configuration Management is used\) \(for UNIX\)](#).

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 JP1/Integrated Management - Manager Overview and System Design Guide](#).

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

2.8.1 Setting the configuration definition information (for UNIX)

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.

For details about the configuration definition file, see [Configuration definition file \(`jbs_route.conf`\)](#) in [Chapter 2. Definition Files](#) in the manual [JP1/Integrated Management - Manager Command and Definition File Reference](#).

For details about the `jbsrt_distrib` command and the `jbsrt_sync` command, see the [JP1/Base User's Guide](#).

2.8.2 Deleting the configuration definition information (for UNIX)

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. Then execute the `jbsrt_distrib` command at the highest manager.
For details about the `jbsrt_del` command, see the *JP1/Base User's Guide*.

2.8.3 Changing the configuration definition information (for UNIX)

If you change the configuration definition information, follow the same procedure as in *2.8.1 Setting the configuration definition information (for UNIX)*. 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 *2.8.2 Deleting the configuration definition information (for UNIX)*.
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 *2.8.1 Setting the configuration definition information (for UNIX)*.

2.8.4 Notes about setting the configuration definition information (for UNIX)

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 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 *JP1/Base User's Guide*.

2.9 Setting up Event Service (for UNIX)

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 *JP1/Base User's Guide*.

Important

Specify `keep-alive` for the communication type in the API settings file of the host on which JP1/IM Manager is running. If you specify `close` for the communication type, because JP1/IM - Manager uses a temporary port every time it receives an event, temporary ports might be insufficient.

2.10 Setting JP1 event forwarding when IM Configuration Management is used (for UNIX)

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 [2.7 Setting the system hierarchy \(when IM Configuration Management is used\) \(for UNIX\)](#).

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 [3.5.1\(5\) Editing configuration files](#).

2.11 Setting JP1 event forwarding when IM Configuration Management is not used (for UNIX)

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 [2.8 Setting the system hierarchy \(when IM Configuration Management is not used\) \(for UNIX\)](#).

For details about the settings, see the chapter that provides details of the forwarding settings file in the *JP1/Base User's Guide*.

2.12 Collecting and distributing Event Service definition information when IM Configuration Management is used (for UNIX)

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 or later 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
- Log-file trap startup 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 [3.5.1\(2\) 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 [3.5.1\(6\) Applying edited information in configuration files](#).

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

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.

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 *JP1/Base User's Guide*.

2.14 Setting up a command execution environment (for UNIX)

This section describes how to set up a command execution environment for executing commands on managed hosts and for executing client applications.

2.14.1 Setting up the command execution function for managed hosts (for UNIX)

This subsection describes how to set up a command execution environment for performing automated actions and for executing commands on managed hosts from the Execute Command window of JPI/IM - View.

To set up a command execution environment:

1. 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/jplbase/bin/jcocmddef -execnum 3
```

2. Creating an environment variable file

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

3. Defining host groups

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

4. Creating a command button definition file

If you want to execute a command from a command button, create a command button definition file.

To pass event information, set `true` in the `inev` parameter.

5. Creating a configuration file for converting information

When you pass event information for automated actions and command execution, if you want to convert specific ASCII characters in the event information to be passed to other types of characters, create a configuration file for converting information.

For details about when the settings of a command execution environment are enabled or how to create definition files, see the following.

About command execution environments

- `jcocmddef` command
See the chapter that describes commands in the *JPI/Base User's Guide*.
- Creation of an environment variable file
See *Environment variable file* in *Chapter 2. Definition Files* in the manual *JPI/Integrated Management - Manager Command and Definition File Reference*.
- Host group definition
See *Host group definition file* in *Chapter 2. Definition Files* in the manual *JPI/Integrated Management - Manager Command and Definition File Reference*.

- Creation of a command button definition file
See *Command button definition file (cmdbtn.conf)* in *Chapter 2. Definition Files* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.
- Creation of a configuration file for converting information
See *Configuration file for converting information (event_info_replace.conf)* in *Chapter 2. Definition Files* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

2.14.2 Setting up a client application execution environment (for UNIX)

This subsection describes how to set up a command execution environment for executing client applications from the Execute Command window of JP1/IM - View.

1. Creating a command button definition file

If you want to execute a client application from a command button, create a command button definition file.

To pass event information, set `true` in the `inev` parameter. In addition, set `client` in the `cmdtype` parameter.

2. Creating a configuration file for converting information

When you pass event information for automated actions and command execution, if you want to convert specific ASCII characters in the event information to be passed to other types of characters, create a configuration file for converting information.

For details about when the settings of a command execution environment are enabled or how to create definition files, see the following.

About command execution environments

- Creation of a command button definition file
See *Command button definition file (cmdbtn.conf)* in *Chapter 2. Definition Files* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.
- Creation of a configuration file for converting information
See *Configuration file for converting information (event_info_replace.conf)* in *Chapter 2. Definition Files* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

2.15 Specifying settings for using the source host name of Event Service in the FQDN format (for UNIX)

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.

2.15.1 Prerequisites (for UNIX)

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.

2.15.2 Setting method (for UNIX)

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/jp1cons  
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 *JP1/Base User's Guide*:

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

2.15.3 Startup method (for UNIX)

The startup method is the same as the normal startup method. For details, see *3.1.2 In UNIX* in the *JP1/Integrated Management - Manager Administration Guide*.

2.16 Specifying settings for monitoring logs on remotely monitored hosts (for UNIX)

This section describes how to configure SSH to monitor the logs on remotely monitored hosts.

For details about the types of logs that can be collected from remotely monitored hosts and the remote communication methods, see *11.5.2 Managing the remote monitoring configuration* in the *JP1/Integrated Management - Manager Overview and System Design Guide*.

For details about how to register hosts that are to be monitored remotely in IM Configuration Management, see *3.1 Registering hosts*.



Note

You can collect the log information that is output on remotely monitored hosts while remote monitoring is stopped. Use the `START_OPTION` parameter in the remote log trap environment definition file (`jp1cf_remote_logtrap.conf`) to specify whether to collect the log information that is output while remote monitoring is stopped. This setting is enabled when JP1/IM - Manager is newly installed. If you upgraded JP1/IM - Manager from a version earlier than 11-01, this setting is disabled. Configure the remote log trap environment definition file as needed.

For details about the remote log trap environment definition file, see *Remote log trap environment definition file (jp1cf_remote_logtrap.conf)* in *Chapter 2. Definition Files* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

2.16.1 Configuring SSH (for UNIX)

This subsection describes how to configure SSH when the JP1/IM - Manager host is running in a UNIX environment. SSH uses public-key cryptography for authentication.

To establish SSH connections, you need to:

- Configure an SSH server
Configure an SSH server on a remotely monitored host.
- Create keys
Create keys on the JP1/IM - Manager host in the UNIX environment.
- Place the public key on the monitored host
Place the public key on the remotely monitored host.
- Specify access permissions for monitored log files
If the monitored host is a UNIX host, specify access permissions for users who will be establishing SSH connections from the manager host to the monitored host.



Important

Do not write interactive commands such as `stty`, `tty`, `tset`, and `script` in the login script of the user who is permitted to establish SSH connections. If these commands must be written in the login script, create another user who is permitted to establish SSH connections for remote monitoring.

Alternatively, change the login script of the user who is permitted to establish SSH connections so that these commands will not be executed.

(1) Configuring an SSH server

To configure an SSH server, follow the procedure below. OS settings and commands may vary depending on the OS version. For details, see the manual for each OS and the release notes for JP1/IM - Manager.

1. Log on to the remotely monitored host as a user with `root` privileges.
2. Open `sshd_config`.
For Linux, Solaris, or AIX: `/etc/ssh/sshd_config`
For HP-UX (IPF): `/opt/ssh/etc/sshd_config`
3. Set `yes` for `PubkeyAuthentication`^{#1}.
4. Set the following items^{#1, #2}.
 - If you are using OpenSSH on Solaris or the OS is not Solaris
Set `no` for `UseDNS`.
 - For Solaris
Set `no` for `LookupClientHostnames`.
5. Set `yes` for `PermitRootLogin`^{#1}.
Perform this step only when you are logged on as a user with `root` privileges to collect information.
6. Execute one of following commands to restart the `sshd` service.
The following describes the command to be executed for each OS.
 - For Linux (Linux 6 example)
`/etc/rc.d/init.d/sshd restart`
 - For Solaris (Solaris 10 (SPARC) example)
`/usr/sbin/svcadm restart ssh`
 - For AIX (AIX 6.1 example)
`kill -HUP sshd-process-ID`
 - For HP-UX (HP-UX 11i V3 (IPF) example)
`/sbin/init.d/secsh stop; /sbin/init.d/secsh start`

#1

For details about the items to be set and how to set them in `sshd_config`, see the documentation for your SSH server.

#2

If you do not set these items, make sure that the monitored host can perform name resolution as follows.

- The monitored host can resolve the IP address of the manager host to the host name.
- The IP address resolved from the host name of the manager host matches the IP address of the manager host.

If you are using a DNS server for name resolution and the monitored host cannot connect to the DNS server, the startup of remote-monitoring log file traps or the collection of log files might be delayed. If a delay occurs, the

startup of traps or the collection of log files might time out and fail. To prevent this problem, we recommend that you set `no` for `UseDNS` and `LookupClientHostnames`.

(2) Initially creating keys

Log on to the JP1/IM - Manager host in the UNIX environment as a user with `root` privileges and execute the `ssh-keygen` command to create keys. This procedure needs to be performed only the first time you create keys.

You can choose the type of keys (RSA or DSA).

1. Log on as a user with `root` privileges.

2. Execute the `ssh-keygen` command.

Enter the command as follows:

- When creating RSA keys: `ssh-keygen -t rsa`
- When creating DSA keys: `ssh-keygen -t dsa`

3. Determine the names of the file in which the private key will be stored and the directory that will hold the file.

The path and the file name must not contain multibyte characters. The default setting is `~/.ssh/id_rsa`.

4. Press the **Return** key twice.

When you are prompted to enter the passphrase for the private key, enter nothing and press the **Return** key. When you are prompted again, enter nothing and press the **Return** key again.

The following is an execution example of the `ssh-keygen -t rsa` command.

```
[root@HOST]$ ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/home/ssh-user/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/ssh-user/.ssh/id_rsa.
Your public key has been saved in /home/ssh-user/.ssh/id_rsa.pub.
The key fingerprint is:
ax:xx:xx:xx:xx:bx:xx:xc:xx:xx:xx:xd:xd:xa:ed:xx root@HOST
```

Note:

- Manage private keys with the utmost care.
- The creation of keys (public key and a private key pair) does not depend on any environment or tool. You can create keys in any environment using any tool. However, after you create keys, you must place the private keys and public keys in the appropriate locations.

(3) Placing the public key on the host to be monitored remotely

Place the public key created as described in [2.16.1\(2\) Initially creating keys](#) on the remotely monitored host. To do so, perform the procedure described below.

Before you start the procedure, make sure that only the owner of the keys has the write permission for the directory above the `.ssh` directory. If anyone other than the owner has the write permission for the higher-level directory, SSH connections fail.

1. Log on as a user who can remotely monitor the target host.
2. Navigate to the `.ssh` directory.
If the home directory of the user who performs remote monitoring does not contain the `.ssh` directory, create one. Set `700` as the attribute of the directory.
3. Execute the `scp` command to copy the public key file to the host to be monitored remotely.
Copy the public key file created as described in [2.16.1\(2\) Initially creating keys](#) to the monitored host. Copy the file to the `.ssh` directory in the home directory of the user who will perform remote monitoring.
4. Execute the `cat` command to add the contents of the public key file to the authentication key file.
5. Delete the copied public key file.
6. Execute the `chmod` command to change the attribute of the authentication key file to `600`.
7. Configure `AuthorizedKeysFile` in `/etc/ssh/sshd_config`.
By default, `~/.ssh/authorized_keys` or `./ssh/authorized_keys` is set. If you change the path for the authentication key file created in step 6, check and, if necessary, revise the value of `AuthorizedKeysFile`. If you change any settings in `sshd_config`, restart the `sshd` service as a superuser.

An execution example of the `scp` command, the `cat` command, and the `chmod` command is shown below. In this example, the host name of the JP1/IM - Manager host where keys are created as described in [2.16.1\(2\) Initially creating keys](#) is `IMHost`.

- Example of executing the commands:

```
[ClientUser@TargetHost ]$ cd .ssh
[ClientUser@TargetHost .ssh]$ scp root@IMHost:/home/ssh-user/.ssh/
id_rsa.pub ./
root@IMHost's password: Enter a password here.
id_rsa.pub 100% 233 0.2KB/s 00:00
[ClientUser@TargetHost .ssh]$ cat id_rsa.pub >> authorized_keys
[ClientUser@TargetHost .ssh]$ rm id_rsa.pub
[ClientUser@TargetHost .ssh]$ chmod 600 authorized_keys
```

(4) Specifying access permissions for monitored log files

If the monitored host is a UNIX host, any user who will be establishing SSH connections from the manager host to the monitored host will need the following access permissions:

- Monitored log files
The user needs the read permission. If the monitored log files are in the SEQ2 format, the user also needs the read permission for the backup files of the monitored log files.
- Directory containing the monitored log files and all of its higher directories
The user needs the read permission and the execute permission. If the monitored log files are in the SEQ2 format, the user also needs the read permission and the write permission for the directory containing the backup files of the monitored log files and for all of its higher directories.

(5) Checking connections

The following procedure describes how to check if the JP1/IM - Manager host and the host to be monitored remotely can be connected.

1. Log on to the JP1/IM - Manager host as a user with `root` privileges.
2. Use the created private key and execute the `ssh` command for the remotely monitored host.

If a connection is successfully established without any prompt for an identity, SSH configuration is complete.

If an error occurs or you are prompted to enter a password and a passphrase, check whether the settings are specified correctly as described. Also check the settings of the OS to make sure that the OS will allow SSH connections.

An execution example of the `ssh` command for checking connections is shown below.

In this example, the host name of the JP1/IM - Manager host is `IMHost`. The host name of the monitored host is `TargetHost`, and the name of the user performing remote monitoring is `ssh-user`.

- Example of executing the commands:

```
[root@IMHost]$ /usr/bin/ssh -i /home/ssh-user/.ssh/id_rsa -p 22 ssh-  
user@TargetHost  
The authenticity of host 'TargetHost (xxx.xxx.xxx.xxx)' can't be  
established.  
RSA key fingerprint is xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx.  
Are you sure you want to continue connecting (yes/no)? yes  
Warning: Permanently added 'TargetHost,xxx.xxx.xxx.xxx' (RSA) to the list of  
known hosts.  
Last login: Mon Mar 23 17:17:52 2011 from xxx.xxx.xxx.xxx  
[ssh-user@TargetHost ~]$ exit  
logout  
Connection to TargetHost closed.  
[root@IMHost]$
```

Note that during remote monitoring, the following commands must be executable on the hosts that are to be monitored remotely. Make sure that the users that perform remote monitoring can execute these commands.

- `uname`
- `ls`
- `wc`
- `tail`
- `find`
- `grep`
- `head`

Use the following procedure to check whether these commands can be executed.

(a) Checking commands to be used for collection of host information

1. Log in to the monitored host as the user that was set on the **SSH** page in the System Common Settings window.

2. Execute the following command and then confirm that the return code is 0.

```
uname -s
```

(b) Checking commands to be used for collection of log files

1. Log in to the monitored host as the user that was set on the **SSH** page in the System Common Settings window.

2. Execute the following commands and then confirm that the return code is 0.

- `ls -ild monitored-log-file-path`

Example of executing the command:

```
ls -ild /var/log/messages
```

Example of execution result:

```
12345 -rw-r--r-- 1 root root 100 April 12 13:00 2013 messages
```

- `ls path-to-directory-contains-monitored-log-file`

Example of executing the command:

```
ls /var/log/
```

Example of execution result:

```
messages
```

- (When the OS of the monitored host is AIX) `LC_CTYPE=C wc -l monitored-log-file-path`

Example of executing the command:

```
LC_CTYPE=C wc -l /var/log/messages
```

Example of execution result:

```
20 /var/log/messages
```

- (When the OS of the monitored host is not AIX) `wc -l monitored-log-file-path`

Example of executing the command:

```
wc -l /var/log/messages
```

Example of execution result:

```
20 /var/log/messages
```

- (When the OS of the monitored host is Solaris) `tail +any-line-number-of-monitored-file monitored-log-file-path | tail -maximum-collection-sizec`

Example of executing the command:

```
tail +19 /var/log/messages | tail -10241c
```

Example of execution result:

```
line num = 19
```

```
line num = 20
```

- (When the OS of the monitored host is not Solaris) `tail -n +any-line-number-of-monitored-file monitored-log-file-path | tail -c maximum-collection-size`

Example of executing the command:

```
tail -n +19 /var/log/messages | tail -c 10241
```

Example of execution result:

```
line num = 19
```

```
line num = 20
```

3. If the log file output format is SEQ2, execute the following command, in addition to the command in step 2, and check the results of the standard output:

- `find path-to-directory-containing-monitored-log-file -xdev -inum inode-of-backup-file-for-monitored-log-file`

Example of executing the command:

```
find /var/log/ -xdev -inum 12345
```

Example of standard output:

```
/var/log/messages.1
```

Verify that the path to the backup file of the monitored log file is output in the standard output.

To output the standard output to `stdout.txt` and the standard error output to `stderr.txt`, check the standard output by executing the command show below.

Example of command:

```
find /var/log/ -xdev -inum 12345 1> stdout.txt 2> stderr.txt
```

(c) Checking commands to be used for application of predefined filters

1. Log in to the monitored host as the user that was set on the **SSH** page in the System Common Settings window.

2. Execute the following commands and then confirm that the return code is 0.

- (When the OS of the monitored host is Linux) `/bin/grep -E 'predefined-filter'`

Example of executing the command:

```
tail -n +19 /var/log/messages | /bin/grep -E 'filter' | tail -c 10241
```

Example of execution result:

```
line num = 19
```

```
line num = 20
```

- (When the OS of the monitored host is Solaris) `/usr/xpg4/bin/grep -E 'predefined-filter'`

Example of executing the command:

```
tail +19 /var/log/messages | /usr/xpg4/bin/grep -E 'filter' | tail -10241c
```

Example of execution result:

```
line num = 19
```

```
line num = 20
```

- (When the OS of the monitored host is not Linux and Solaris) `/usr/bin/grep -E 'predefined-filter'`

Example of executing the command:

```
tail -n +19 /var/log/messages | /usr/bin/grep -E 'filter' | tail -c 10241
```

Example of execution result:

```
line num = 19
```

```
line num = 20
```

- `head -n any-line-number-of-monitored-file`

Example of executing the command:

```
tail -n +19 /var/log/messages | head -n 20
```

Example of execution result:

```
line num = 19
```

```
line num = 20
```

2.16.2 Specifying the size of log information that can be collected per monitoring interval (for UNIX)

In an environment in which the maximum size of log information that can be collected per monitoring interval is exceeded even when predefined filters are used, you can change the value that is initially set for the maximum size of log information that can be collected per monitoring interval.

To change the initial value:

1. Configure an execution environment for the remote-monitoring log file trap function and the remote-monitoring event log trap function.

Edit the remote-monitoring log file trap environment definition file (`jp1cf_remote_logtrap.conf`).
`/etc/opt/jp1imm/conf/imcf/jp1cf_remote_logtrap.conf`

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

```
/opt/jp1base/bin/jbssetcnf /etc/opt/jp1imm/conf/imcf/  
jp1cf_remote_logtrap.conf
```

3. Restart JP1/IM - Manager.

The new settings take effect when JP1/IM - Manager is restarted.

About specifying the size of log information that can be collected per monitoring interval

- Remote-monitoring log file trap environment definition file (`jp1cf_remote_logtrap.conf`)

For details, see *Remote log trap environment definition file (`jp1cf_remote_logtrap.conf`)* in *Chapter 2. Definition Files* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

2.17 Setting up JP1/IM - Manager (for UNIX)

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 (for UNIX)

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

1. Execute the setup program.
 - `/opt/jplcons/bin/jplcc_setup`
 - `/opt/jplscope/bin/jplcs_setup`
 - `/opt/jplimm/bin/imcf/jplcf_setup`

Depending on the installation status, execution of the setup program might 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 (for UNIX)

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

In the automatic startup and automatic stop scripts, `C` is set for the `LANG` environment variable by default. If you want to change the language for the output messages when the scripts are executed, edit the line of the `LANG` environment variable in the scripts.

(1) In Linux

To set automatic startup and automatic stop:

1. Copy the automatic startup and automatic stop scripts.

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

(a) Notes about automatic startup of services

In a Linux environment, when the automatic startup and automatic stop of JP1/IM - Manager are enabled but you want to start or stop JP1/IM - Manager manually, execute the commands listed below. To check the status (started or stopped) of JP1/IM - Manager processes, you can use the `jco_spmc_status` command. When the IM database is used, you can use the `jimdbstatus` command to check the operation status of the IM database.

- Starting JP1/IM - Manager

Physical hosts:

```
systemctl start jp1_cons.service
```

Logical hosts:

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

- Stopping JP1/IM - Manager

Physical hosts:

```
systemctl stop jp1_cons.service
```

Logical hosts:

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

Even when automatic startup and stop is set to enabled, JP1/IM - Manager does not stop automatically after it is started or stopped by using a command other than the `systemctl` command, for example, by using the `jco_start` or `jco_start.cluster` command to start, or the `jco_stop` or `jco_stop.cluster` command to stop. (In such a case, automatic startup and stop remains enabled although the stop script does not start when the system stops.)

To allow JP1/IM - Manager to stop automatically when the system stops, start it again by using the `systemctl` command. To know whether JP1/IM - Manager will stop automatically, execute the following commands to check whether `active` is returned.

Physical hosts:

```
systemctl is-active jp1_cons.service
```

Logical hosts:

```
systemctl is-active jp1_cons_logical-host-name.service
```

(b) Notes about syslog

If automatic startup and automatic stop have not been configured^{#1} in a Linux system on which the `systemd` package has been installed and an attempt is made to start or stop the system, the message shown below is output to `syslog`.

Even though this message is output, automatic startup and automatic stop are not performed, because they have not been configured. You can use the `jco_spmc_status` command to check the status of JP1/IM-Manager Service.

- Message that is output to `syslog`^{#2}

At startup: `systemd: Started JP1/Integrated Management - Manager Service.`

#1

Automatic startup and automatic stop have not been configured means that the following files do not exist:

```
/etc/opt/jp1cons/jco_start
```

```
/etc/opt/jp1cons/jco_stop
```

#2

When automatic startup and automatic stop are performed on a logical host in a non-cluster system, the service name specified in `Description` in the automated startup script and the automated stop script that has been created for the logical host are displayed in the message.

Example:

At startup: `systemd: Started JP1/Integrated Management - Manager logical-host-name Service.`

(2) In AIX

To set automatic startup and automatic stop:

1. Copy the automatic startup and automatic stop scripts.

```
# cd /etc/opt/jplcons
# 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. Set up the IM database and then use `mkitab` to add entries 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
pe01:234:wait:/var/opt/jplimm/dbms/JM0/etc/pdpwon_e
pd01:234:respawn:env LIBPATH=/var/opt/jplimm/dbms/JM0/lib LC_MESSAGES=C
var/opt/jplimm/dbms/JM0/lib/servers/pdprcd /var/opt/jplimm/dbms/JM0
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`, `pe01`, `pd01`, and `jplcons`.

Note that the order of the entries in the `/etc/inittab` file changes when you execute the `jimdbupdate` command. If you specify the automatic startup settings before setting up the IM database and execute the `jimdbupdate` command, the entries must be specified in the order of `hntr2mon` (Hitachi Network Objectplaza Trace Library (HNTRLib2)), `jplbase`, `pe01`, `pd01`, 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`

```
:
testΔ-xΔ/etc/opt/jplcons/jco_stopΔ&&Δ/etc/opt/jplcons/jco_stop
testΔ-xΔ/etc/opt/jplbase/jbs_stopΔ&&Δ/etc/opt/jplbase/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 `exit 0` at the end of the `/etc/rc.shutdown` script:

The automatic startup and stop scripts are now enabled.

2.17.3 Specifying settings for using the functions of Central Scope (for UNIX)

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 *Chapter 1. Commands* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

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

2.17.4 Specifying settings for handling JP1/IM - Manager failures (for UNIX)

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 *10.3 Data that needs to be collected when a problem occurs* in the *JP1/Integrated Management - Manager Administration Guide*.

About the data collection tool

- About `jim_log.sh`

See `jim_log.sh (UNIX only)` in *Chapter 1. Commands* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

In the event of a problem, you might need 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, edit the scripts to set an acceptable value as shown below.

- The following example limits the size to 8,388,608 blocks:

```
ulimit -c 8388608
```

Important

If the setting is commented out or a value other than `unlimited` is set, you might not be able to investigate problems because no dump or a limited core dump will be output in case of core dump output events such as a segmentation failure in a JP1/IM - Manager process, a bus failure, or the execution of the `jcogencore` command.

(b) Setting the kernel parameters regarding core dump (Linux only)

When the output destination for a core dump file and the name of the core dump file are changed from the default settings in the kernel parameters of Linux (`kernel.core_pattern`), the data collection tool might not be able to acquire the core dump file when the tool is executed. To prevent this problem, we recommend that you do not change the settings of the Linux kernel parameters (`kernel.core_pattern`).

The data collection tool acquires files with file names beginning with `core` from the following default output directories.

- For physical hosts: `/var/opt/jp1cons/log/`
- For logical hosts: `shared-directory/jp1cons/log/`

If you have changed the settings of `kernel.core_pattern`, you need to perform the following before you execute the data collection tool.

- When the output directory for a core dump file is changed
Make a copy of the core dump file in the default output directory.
- When the file name of a core dump file is changed
Change the file name of the core dump file to a name beginning with `core`.

(c) Setting ABRT for core dump files (Linux only)

In a Linux with Automatic Bug Reporting Tool (ABRT) installed, ABRT can be configured to allow limited processes, OS user accounts, or user groups to generate core dump files. In such a case, you cannot investigate problems because a core dump file might not be generated in case of core dump output events such as a segmentation failure in a JP1/IM - Manager process, a bus failure, or the execution of the `jcogencore` command.

Depending on your operation, you should change the ABRT settings to ensure that processes or OS user accounts or user groups that run JP1/IM - Manager are allowed to generate core dump files. For details, see the documentation for your Linux.

(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 (`jplco_service.conf`) 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_spmd_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 Chapter 2. *Definition Files* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

Note:

In a cluster system, do not enable process restart in the event of abnormal process termination. If JP1/IM - Manager fails, the process restart function might also be affected. If you want to restart processes in the event of an abnormal process termination in a cluster system, use the cluster software (not JP1/IM - Manager) to control the restart.

(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 (`jplco_param_v7.conf`):

```
/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 *Chapter 2. Definition Files* in the manual *JP1/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. Use the `jco_spmd_reload` command to reload JP1/IM - Manager, or restart JP1/IM - Manager.
3. If you specified the notification command, execute the `jcohctest` command to check the notification command's execution validity.
Execute the `jcohctest` command to determine whether the command specified in `COMMAND` executes correctly. If the operation is not valid, check and, if necessary, revise the specification.

About the health check function settings

- About the health check definition file (`jcohc.conf`)
See *Health check definition file (jcohc.conf)* in *Chapter 2. Definition Files* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.
- About the `jcohctest` command
See *jcohctest* in *Chapter 1. Commands* in the manual *JP1/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 might 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 previous version of JP1/IM - Manager. 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 *JP1/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 *Chapter 2. Definition Files* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

3. Start JP1/IM - Manager.

2.17.5 Specifying settings for upgrading (for UNIX)

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 had been using an event acquisition filter (for compatibility) with a previous version of JP1/IM - Manager, you can use the `jcochafmode` command to change the location of the event acquisition filter from the Event Console Service to the Event Base Service. 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.

Important

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 *JP1/Integrated Management - Manager Overview and System Design Guide*.
 - About the `jcochafmode` command
See *jcochafmode (UNIX only)* in *Chapter 1. Commands* in the manual *JP1/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` 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/jp1scope/database/jcsdb/
```

3. Execute the `jp1csverup` 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 2–5: 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` command

See *jp1csverup (UNIX only)* in *Chapter 1. Commands* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

(3) Updating the automated action definition file

If you have upgraded JP1/IM - Manager from version 11-10 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 11-10 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. Rename the file specified for the `-o` option of the `jcadefconv` command to `actdef.conf`, and then move the file to the correct location.

The path name (including the file name) of the correct location is shown below. Note that you do not need to perform this step if the file name that was specified for the `-o` option in step 2 is the path name including the file name shown below.

For a physical host: `/etc/opt/jp1cons/conf/action/actdef.conf`

For a logical host: `shared-directory/jp1cons/conf/action/actdef.conf`

4. Start JP1/IM - Manager.

- About the automated action function

See *Chapter 5. Command Execution by Automated Action* in the *JP1/Integrated Management - Manager Overview and System Design Guide*.

- About the `jscadefconv` command

See `jscadefconv` in *Chapter 1. Commands* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

(4) Displaying the source host

When you upgrade JP1/IM - Manager version 09-00 to 09-10, source hosts are not set in the file that defines which items are displayed for event conditions. As a result, even if you enable mapping for source hosts, the list box in the **Event conditions** section does not display **Source host** in the Action Parameter Detailed Definitions window. If you want to display **Source host** in the list box in the **Event conditions** section in the Action Parameter Detailed Definitions window, you need to add `E.JP1_SOURCEHOST` in the file that defines which items are displayed for event conditions.

For details about the Action Parameter Detailed Definitions window, see *2.33.1 Action Parameter Detailed Definitions window* in the manual *JP1/Integrated Management - Manager GUI Reference*.

For details about the file that defines which items are displayed for event conditions, see *File that defines which items are displayed for event conditions (attr_list.conf)* in *Chapter 2. Definition Files* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

(5) Specifying the event report output format

If you have upgraded from JP1/IM - Manager version 10-50 or earlier, the function for assigning one column to each program-specific extended attribute when event reports are output in CSV format is disabled. To specify whether this function is to be enabled, use the `PROGRAM_SPECIFIC_EX_ATTR_COLUMN` parameter in the environment definition file for event report output (`evtreport.conf`). This function is enabled when you perform a new installation. If necessary, configure the environment definition file for event report output.

For details about the environment definition file for event report output, see *Environment definition file for event report output (evtreport.conf)* in *Chapter 2. Definition Files* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

(6) Displaying the Start the process automatically when the log file trap service starts check box

If you have upgraded JP1/IM - Manager from version 11-01 or earlier, the **Start the process automatically when the log file trap service starts** check box is disabled (hidden).

You can use the `LOGFILETRAP_AUTO_START_CONTROL` parameter in the profile management environment definition file (`jp1cf_profile_manager.conf`) to specify the enable/disable setting for the **Start the process automatically when the log file trap service starts** check box. For details, see *Profile management environment definition file (jp1cf_profile_manager.conf)* in *Chapter 2. Definition Files* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

(7) Updated agent profile notification function

If you have upgraded JP1/IM - Manager from version 11-01 or earlier, the updated agent profile notification function is disabled.

You can use the `AGENT_PROFILE_UPDATE_NOTICE` parameter in the profile management environment definition file (`jp1cf_profile_manager.conf`) to specify the enable/disable setting for the updated agent profile notification function. For details, see *Profile management environment definition file (jp1cf_profile_manager.conf)* in *Chapter 2. Definition Files* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

(8) Setting for monitoring logs while remote monitoring is stopped

If you have upgraded JP1/IM - Manager from version 11-01 or earlier, the log data that is output while remote monitoring is stopped is set to be not collected.

You can use the `START_OPTION` parameter in the remote log trap environment definition file (`jp1cf_remote_logtrap.conf`) to specify the setting for whether log data that is output while remote monitoring is stopped is to be collected. For details, see *Remote log trap environment definition file (jp1cf_remote_logtrap.conf)* in *Chapter 2. Definition Files* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

2.18 Saving manuals to a computer (for UNIX)

When you store HTML manuals to certain directories, you can access the manuals by clicking the **Help** button in each window.

To save HTML manuals to a computer:

1. Have ready the manual distribution medium provided as a standard item with each program product.
2. Store the target data from the manual distribution medium to JP1/IM - Manager.

The target data is stored in the manual distribution medium. Store the target data in the destination folders of JP1/IM - Manager (for each manual).

- Target data (HTML manuals)
CSS file, all HTML files, and GRAPHICS directory
- Locations of the target data in the manual distribution medium (when the medium is inserted in the drive of the UNIX machine)

JP1/Integrated Management: Getting Started (Integrated Console)

mount-point-of-manual-distribution-medium/MAN/3021/03A0620D

JP1/Integrated Management - Manager Overview and System Design Guide

mount-point-of-manual-distribution-medium/MAN/3021/03A0720D

JP1/Integrated Management - Manager Configuration Guide

mount-point-of-manual-distribution-medium/MAN/3021/03A0820D

JP1/Integrated Management - Manager Administration Guide

mount-point-of-manual-distribution-medium/MAN/3021/03A0920D

JP1/Integrated Management - Manager GUI Reference

mount-point-of-manual-distribution-medium/MAN/3021/03A1020D

JP1/Integrated Management - Manager Command and Definition File Reference

mount-point-of-manual-distribution-medium/MAN/3021/03A1120D

JP1/Integrated Management - Manager Messages

mount-point-of-manual-distribution-medium/MAN/3021/03A1220D

- Locations to store the target data on the JP1/IM - Manager side:

JP1/Integrated Management: Getting Started (Integrated Console)

/opt/jp1cons/www/manual/en/03A0600D

JP1/Integrated Management - Manager Overview and System Design Guide

/opt/jp1cons/www/manual/en/03A0700D

JP1/Integrated Management - Manager Configuration Guide

/opt/jp1cons/www/manual/en/03A0800D

JP1/Integrated Management - Manager Administration Guide

/opt/jp1cons/www/manual/en/03A0900D

JP1/Integrated Management - Manager GUI Reference

/opt/jp1cons/www/manual/en/03A1000D

JP1/Integrated Management - Manager Command and Definition File Reference

/opt/jp1cons/www/manual/en/03A1100D

JP1/Integrated Management - Manager Messages

/opt/jp1cons/www/manual/en/03A1200D

When you transfer files using FTP, set the mode for file transfer to binary.

Delete any existing HTML manuals in the JP1/IM - Manager and JP1/IM - View folders before storing the new ones.

2.19 Uninstallation (for UNIX)

This section describes how to uninstall JP1/IM - Manager. Note that the uninstallation procedure must be performed by a user with root privileges.

2.19.1 Uninstallation procedure (for UNIX)

This subsection explains how to uninstall JP1/IM - Manager. If you are using IM databases (integrated monitoring database and IM Configuration Management database), delete the IM databases before you uninstall JP1/IM - Manager.

(1) How to delete IM databases

If you will be deleting the IM databases to reconfigure the environment, first make a backup of the IM databases. For details about the backup method, see *1.2 Managing the databases* in the *JP1/Integrated Management - Manager Administration Guide*.

For details about the commands, see the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

To delete IM databases:

1. Stop JP1/IM - Manager.

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

2. To delete the integrated monitoring database or the IM Configuration Management database, check the status of the following services:

- For physical hosts
The IM database service (JP1/IM-Manager DB Server) is running.
- For physical hosts, when the integrated monitoring database or the IM Configuration Management database has been set up and the IM database is being used
The JP1/IM - Manager service (JP1/IM-Manager) is stopped.
- For logical hosts
The IM database (JP1 / IM-Manager DB Server_ *logical-host-name*) on the logical host has started.
- For logical hosts, when the integrated monitoring database or the IM Configuration Management database has been set up and the IM database is being used
The JP1/IM - Manager service (JP1 / IM-Manager_ *logical-host-name*) is stopped.

3. To delete the integrated monitoring database, execute the `jcoimdef` command:

```
jcoimdef -db OFF
```

The integrated monitoring database is disabled.

4. To delete the integrated monitoring database, execute the `jcodbunsetup` command:

```
jcodbunsetup
```

The integrated monitoring database is deleted.

5. To delete the IM Configuration Management database, execute the `jcoimdef` command:

```
jcoimdef -cf OFF
```

The IM Configuration Management service (`jcfdmain`) is disabled.

6. To delete the IM Configuration Management database, execute the `jcfdbunsetup` command:

```
jcfdbunsetup
```

The IM Configuration Management database is deleted.

7. Delete the following files and folders on the physical host:

Files under `/var/opt/jplimm/data/imcf/imconfig`

Files and folders under `/var/opt/jplimm/data/imcf/profiles`

8. Restart the machine.

(2) 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 all programs that require JP1/IM - Manager. 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 might remain. Check the following directories and manually delete any user files:

- `/opt/jplimm/`
- `/var/opt/jplimm/`
- `/etc/opt/jplcons/`
- `/opt/jplcons/`
- `/var/opt/jplcons/`
- `/etc/opt/jplscope/`
- `/opt/jplscope/`
- `/var/opt/jplscope/`

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/jplimm_inst{1|2|3|4|5}.log`

2.19.2 Notes on uninstallation (for UNIX)

- Setting in the OS environment
 - When JP1/IM - Manager is uninstalled, the port numbers set in the `services` file are deleted. For the specific port numbers, see *Appendix C Port Numbers* in the *JP1/Integrated Management - Manager Overview and System Design Guide*.

3

Using IM Configuration Management to Set the System Hierarchy

This chapter describes how to use IM Configuration Management to set the system hierarchy (IM configuration).

3.1 Registering hosts

To register hosts into IM Configuration Management, you need to operate IM Configuration Management - View. This section provides notes on registering hosts or changing attributes contained in host information. For details about the procedure of registering hosts into IM Configuration Management, see [3.1.1 Registering hosts](#).

- You need to specify the names of the hosts managed by the manager.
- A host name can consist of only one-byte alphanumeric characters and symbols (hyphen (-), period (.)).
- On hosts that will be monitored remotely, the settings for allowing logs to be monitored must be completed in JP1/IM - Manager.
- For host names, specify the host names that are registered in the `hosts` file or on the DNS server, or the host names defined in `jp1hosts` or `jp1hosts2`. If you perform remote monitoring, specify the host names that are registered in the `hosts` file or on the DNS server because the settings defined in `jp1hosts` or `jp1hosts2` are not referenced.
- If you use aliases to define hosts, do not assign multiple aliases to one host. If you do, the aliases are treated as different hosts despite indicating the same host.
- Do not enter an IP address or an alias as a host name that is to be registered into the system hierarchy.
- When you perform agent monitoring, the host name registered in IM Configuration Management must match the event server name of JP1/Base on the registered host. Similarly, the format (short name format or FQDN format) of the host name must also match that of the event server name. For details about how to register hosts using FQDNs, see [12.3.11 System configuration for managing monitored hosts with host names in FQDN format](#) in the *JP1/Integrated Management - Manager Overview and System Design Guide*. For details about how to change event server names, see the description about specifying event servers in systems using DNS in the *JP1/Base User's Guide*.

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:
 - On the **Host List** page, in the tree area, select **Host List**. From the menu bar, choose **Edit**, and then **Register Host**.
 - On the **Host List** page, in the tree area, select and right-click **Host List** to display a pop-up menu. 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 *JP1/Integrated Management - Manager GUI Reference*.
4. Click the **OK** button.

3.1.2 Registering remotely monitored hosts

To register remotely monitored hosts, you must configure communication for remote connection. The required communication settings depend on the operating systems on the manager host and the monitored hosts.

There are two ways to specify communication settings. One is to specify communication settings common to all systems, and the other is to specify communication settings for each monitored host. If you use the method for specifying communication settings common to all systems and you specify these settings in the System Common Settings window, you can reduce the number of items that need to be specified for each monitored host in the Remote Monitoring Settings window.

To register remotely monitored hosts:

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:

- On the **Host List** page, in the tree area, select **Host List**. From the menu bar, choose **Edit**, and then **Register Host**.
- On the **Host List** page, in the tree area, select and right-click **Host List** to display a pop-up menu. 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 *JPI/Integrated Management - Manager GUI Reference*.

4. If the manager host is running Windows, specify the IM host account on the **IM Host Account** page in the System Common Settings window.

In the IM Configuration Management window, from the menu bar, choose **Edit** and then **System Common Settings** to display the System Common Settings window.

In the System Common Settings window, on the **IM Host Account** page, specify the IM host account.

For details about the items displayed in the System Common Settings window, see *4.20 System Common Settings window* in the manual *JPI/Integrated Management - Manager GUI Reference*.

5. If the operating system of the monitored host is Window, configure WMI/NetBIOS.

To specify communication settings common to all systems, specify the settings described in both (a) and (b) below; to specify communication settings individually for each monitored host, specify the settings described in (b) below.

(a) Settings common to all systems

In the IM Configuration Management window, from the menu bar, choose **Edit** and then **System Common Settings** to display the System Common Settings window. In the System Common Settings window, on the **WMI/NetBIOS** page, specify the WMI/NetBIOS settings.

For details about the items displayed in the System Common Settings window, see *4.20 System Common Settings window* in the manual *JPI/Integrated Management - Manager GUI Reference*.

(b) Settings for each monitored host

In the Register Host window, click the **Setup** button for **Remote communication settings** to display the Remote Monitoring Settings window. In this window, specify WMI/NetBIOS settings in **Remote communication type**.

If you are specifying communication settings for each monitored host, in the Remote Monitoring Settings window, select **Individual** in **Setting method**.

If you are specifying communication settings common to all systems, in the Remote Monitoring Settings window, select **Common** in **Setting method**.

For details about the items that are displayed in the Remote Monitoring Settings window, see *4.7 Remote Monitoring Settings window* in the manual *JPI/Integrated Management - Manager GUI Reference*.

6. If the operating system of the monitored host is UNIX, configure SSH.

To specify communication settings for all systems, configure the settings described in (a) and (b) below. To specify communication settings for each monitored host, configure the settings described in (b).

(a) Settings common to all systems

In the IM Configuration Management window, from the menu bar, choose **Edit** and then **System Common Settings** to display the System Common Settings window. In the System Common Settings window, on the **SSH** page, specify the SSH settings.

For details about the items displayed in the System Common Settings window, see *4.20 System Common Settings window* in the manual *JP1/Integrated Management - Manager GUI Reference*.

(b) Settings for each monitored host

Click the **Setup** button for **Remote monitoring settings** to display the Remote Monitoring Settings window. In the Remote Monitoring Settings window, select **SSH** in **Remote communication type**.

If you are specifying communication settings for each monitored host, in the Remote Monitoring Settings window, select **Individual** for **Setting method**.

If you are specifying communication settings for all systems, in the Remote Monitoring Settings window, select **Common** for **Setting method**.

For details about the items displayed in the Remote Monitoring Settings window, see *4.7 Remote Monitoring Settings window* in the manual *JP1/Integrated Management - Manager GUI Reference*.

7. Click the **OK** button

3.1.3 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. For this reason, all unapplied profiles in JP1/Base stored on the server will be deleted.

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. On the **Host List** page or the **IM Configuration** page, in the tree area, select 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. If host information is collected while a remote-monitoring log file trap or remote-monitoring event log trap is running on the selected host, the host

information is collected based on the your response to the confirmation message. If host information is to be collected but no information can be obtained from the monitored host, remote monitoring stops. Similarly, if the OS name differs from the one that had been collected previously, remote monitoring stops.

In the case of multiple hosts, you can check the execution results in the Execution Results window.

Because JP1/Base cannot be installed on hosts running VMware ESX or Hitachi Compute Blade logical partitioning feature, choosing **Collect Host Information** on such hosts results in an error. For a remote host whose host information contains the remote communication type, until the remote host is registered in the system hierarchy (IM configuration), the manager attempts to collect host information from JP1/Base as well as from the remote host.

This means that if you choose **Collect Host Information** for a host on which JP1/Base is not installed and which is not registered in the system hierarchy (IM configuration), a warning is output because the manager cannot connect to JP1/Base on the target host.

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.

3.1.4 Displaying host information

The procedure for displaying information about the hosts that have been registered in the IM Configuration Management database is shown below. If you want to display host information other than basic information, host information must be collected in advance. For details about how to collect host information, see [3.1.3 Collecting information from hosts](#).

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 *JP1/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.

3.1.5 Changing the attributes of host information

To change the attributes of 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. On the **Host List** page, in the tree area, select 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 *4.4 Edit Host Properties window* in the manual *JP1/Integrated Management - Manager GUI Reference*.
5. To change the attributes of host information for remotely monitored hosts, use either of the following methods to change the communication settings for remote connection:
 - Changing the remote monitoring settings for specific remotely monitored hosts
In the **Remote communication settings** section, click the **Setup** button to display the Remote Monitoring Settings window.
For details about the items displayed in the Remote Monitoring Settings window, see *4.7 Remote Monitoring Settings window* in the manual *JP1/Integrated Management - Manager GUI Reference*.
 - Changing the remote monitoring settings that are saved and managed as system common settings
In the IM Configuration Management window, from the menu bar, choose **Edit** and then **System Common Settings**. The System Common Settings window appears.
For details about the items displayed in the System Common Settings window, see *4.20 System Common Settings window* in the manual *JP1/Integrated Management - Manager GUI Reference*.

As the communication method for remote monitoring, use WMI/NetBIOS (NetBIOS over TCP/IP) connection for Windows and SSH connection for UNIX.
6. Click the **OK** button.

When you change the host name of a host in an agent configuration, the host name also changes in the system hierarchy displayed on the **IM Configuration** page in the IM Configuration Management window. When this occurs, the system hierarchy is displayed in gray in the tree area on the **IM Configuration** page.

If you change the name of an actual host, change it in the IM Configuration Management database.

If you change host names, collect the information for the hosts again. For details about how to collect host information, see *3.1.3 Collecting information from hosts*.

When you change the host name of a host in an agent configuration, apply the new agent configuration. For details about how to apply an agent configuration, see *3.2.4(3) Applying a system hierarchy to a system managed by IM Configuration Management*.

3.1.6 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. On the **Host List** page, in the tree area, select 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.

3.2 Setting the system hierarchy

This section describes how to set a system hierarchy (IM configuration) to be managed by IM Configuration Management when you configure a JP1/IM system.

3.2.1 Collecting the system hierarchy

To collect the system hierarchy (IM configuration):

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. On the **Host List** page or the **IM Configuration** page, from the menu bar, choose **Operation**, and 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 (agent configuration) does not match the configuration definition information stored in 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 is displayed.

Clicking the **Yes** button deletes the configuration definition information stored in the IM Configuration Management database, and the agent configuration becomes undefined. As a result, the system hierarchy is displayed in gray in the tree area of the **IM Configuration** page. 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.

- For an agent configuration, if the system hierarchy is displayed in gray in the tree area of the **IM Configuration** page, check and, if necessary, revise the configuration definition information (agent configuration) and then apply the agent configuration to the system. For details about how to apply the agent configuration, see [3.2.4\(3\) Applying a system hierarchy to a system managed by IM Configuration Management](#).

3.2.2 Displaying the system hierarchy

You can view the system hierarchy (IM configuration) on the **IM Configuration** page in the IM Configuration Management window. This subsection describes how to display 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 *JP1/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. On the **Host List** page or the **IM Configuration** page, from the menu bar, choose **Operation**, and 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 (agent configuration) held by JP1/Base installed on the manager running IM Configuration Management does not match the configuration definition information stored in the IM Configuration Management database, the icon of the selected host in the tree area of the **IM Configuration** page in the IM Configuration Management window indicates an error.

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 on the host is before version 9, JP1/Base does not support verification of system hierarchies (IM configurations). In such cases, the host icon in the tree area of the **IM Configuration** page in the IM Configuration Management window indicates an undetermined configuration.

If JP1/Base on the manager does not have configuration definition information or the configuration definition information of JP1/Base does not match the configuration definition information stored in the IM Configuration Management database, verification by the manager results in an error and the processing is canceled. As a result, the system hierarchy is displayed in gray in the tree area of the **IM Configuration** page.

3.2.4 Editing the system hierarchy

Perform the following procedure to change a system hierarchy (IM configuration).

1. Use IM Configuration Management - View to edit an agent configuration or a remote monitoring configuration.
2. Obtain update rights.
3. Apply the new system hierarchy to the system.
4. Cancel update rights.

See below for details.

(1) Using IM Configuration Management - View to edit an agent configuration or a remote monitoring configuration

The following describes how to edit an agent configuration or a remote monitoring configuration.

You can change an agent configuration by adding, moving, and deleting hosts. You can change a remote monitoring configuration by adding and deleting hosts.

Use the following windows to edit an agent configuration or a remote monitoring configuration.

Editing an agent configuration

Use the Edit Agent Configuration window. For details about the Edit Agent Configuration window, see *4.6 Edit Agent Configuration window* in the manual *JPI/Integrated Management - Manager GUI Reference*.

Editing a remote monitoring configuration

Use the Edit Remote Monitoring Configuration window. For details about the Edit Remote Monitoring Configuration window, see *4.8 Edit Remote Monitoring Configuration window* in the manual *JPI/Integrated Management - Manager GUI Reference*.

(a) 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. Display the editing window.

When editing an agent configuration

In the IM Configuration Management window, from the menu bar, choose **Edit**, and then **Edit Agent Configuration** to display the Edit Agent Configuration window.

When editing a remote monitoring configuration

In the IM Configuration Management window, from the menu bar, choose **Edit**, and then **Edit Remote Monitoring Configuration** to display the Edit Remote Monitoring Configuration window.

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 editing window, in the **Host List** section, select the host to be added and drag it to the tree area.

- In the editing window, from the menu bar, choose **Edit**, and 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 editing window, right-click on the host to be added (icon) to display a pop-up menu. From the pop-up menu, 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 Select Hosts window, see *4.5 Select Hosts window* in the manual *JP1/Integrated Management - Manager GUI Reference*.

(b) Moving hosts

The following describes how to move hosts in an agent configuration to set the hierarchy of a manager and agents. You cannot move hosts in a remote monitoring configuration.

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. To move an agent host, from the menu bar, choose **Edit**, and then **Edit Agent Configuration**.
The Edit Agent Configuration window appears.
3. In the Edit Agent Configuration window, in the tree area, select the host to be moved, and use one of the following methods to move the host:
 - Drag the host to the desired level in the tree area.
 - From the menu bar, choose **Edit**, and then **Cut**. In the tree area, select the host under which you want to move the target host. From the menu bar, choose **Edit**, and then **Paste**.
 - In the tree area, right-click to display a pop-up menu. From the pop-up menu, choose **Cut**. In the tree area, select the host under which you want to move the target host. Right-click again to display a pop-up menu, and 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 *JP1/Integrated Management - Manager Overview and System Design Guide*.

(c) 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. Display the editing window.

When editing an agent configuration

From the menu bar, choose **Edit**, and then **Edit Agent Configuration** to display the Edit Agent Configuration window.

When editing a remote monitoring configuration

From the menu bar, choose **Edit**, and then **Edit Remote Monitoring Configuration** to display the Edit Remote Monitoring Configuration window.

3. In the editing window, in the tree area, select the host to be deleted, and then use one of the following methods to delete the host:

- In the tree area, select the host to be deleted and drag it to the **Host List** section.
- From the menu bar, choose **Edit**, and then **Delete Host**.
- In the tree area, right-click to display a pop-up menu. From the pop-up menu, 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.

When you delete a host from an agent configuration and apply the new agent configuration to the system, the profile lists of JP1/Base stored on the manager are cleared, and the manager obtains the profile trees active on the agents again. As a result, all the unapplied profiles stored on the manager are deleted. Also, when you delete a host from a remote monitoring configuration and apply the new remote monitoring configuration to the system, all the remote monitoring profiles are deleted.

After you delete a host from a system hierarchy, before you apply the new system hierarchy to the system, change the event transfer settings of the deleted host in the profile so that JP1 events will not be transferred. If you do not change the settings, the configuration information retained by the deleted agent remains in the profile managed by IM Configuration Management after the new system hierarchy is applied. As a result, the JP1 events generated on the deleted agent continue to be sent to the higher-level host.

Use either of the following methods to stop the transfer of JP1 events from the deleted agent.

1. Before you apply the new system hierarchy, in the event transfer configuration file in the profiles managed by IM Configuration Management, change the settings related to the transfer of JP1 events so that JP1 events will not be transferred (for example, by inserting a comment).
2. Before you change a system hierarchy or after you apply the new system hierarchy, execute the `jbsrt_del` command on the deleted agent.

If the method for applying the system hierarchy is the batch distribution method (with deleted configurations), the system hierarchy is deleted and then is applied. For details about methods for applying the system hierarchy, see *6.2.6 Applying the system hierarchy* in the *JP1/Integrated Management - Manager Overview and System Design Guide*.

(d) Replacing hosts

To replace hosts:

1. In the IM Configuration Management window, click the **Host List** tab or the **IM Configuration** tab.
The **Host List** page or the **IM Configuration** page is displayed.

2. Display the editing window.

When editing an agent configuration

From the menu bar, choose **Edit**, and then **Edit Agent Configuration** to display the Edit Agent Configuration window.

When editing a remote monitoring configuration

From the menu bar, choose **Edit**, and then **Edit Remote Monitoring Configuration** to display the Edit Remote Monitoring Configuration window.

3. In the editing window, in the tree area, select the host to be replaced, and then use either of the following methods to display the Exchange Hosts dialog box:
 - From the menu bar, choose **Edit**, and then **Exchange Hosts**.

- In the tree area, right-click to display a pop-up menu. From the pop-up menu, choose **Exchange Hosts**.

The selected host appears in the **Host before the exchange** box in the Exchange Hosts dialog box.

4. In the Exchange Hosts dialog box, in the **Host after the exchange** box, enter the host that replaces the selected host. The host selected in step 3 is replaced by the host specified in step 4.

(e) Setting a site manager

The following describes how to set a host as a site manager.

■ Settings on the integrated manager host

1. In the IM Configuration Management window, click the **Host List** tab or the **IM Configuration** tab. The **Host List** page or the **IM Configuration** page is displayed.
2. From the menu bar, choose **Edit**, and then **Edit Agent Configuration**. The Edit Agent Configuration window appears.
3. In the tree area, select the host you want to set as a site manager.
4. Use either of the following methods to set the host as a site manager:
 - In the Edit Agent Configuration window, from the menu bar, choose **Edit**, and then **Base Manager Settings**.
 - In the Edit Agent Configuration window, in the tree area, right-click to display a pop-up menu. From the pop-up menu, choose **Base Manager Settings**.

■ Settings on the site manager host

1. In the IM Configuration Management window, click the **Host List** tab or the **IM Configuration** tab. The **Host List** page or the **IM Configuration** page is displayed.
2. From the menu bar, choose **Edit**, and then **Edit Agent Configuration**. The Edit Agent Configuration window appears.
3. In the Edit Agent Configuration window, in the tree area, select the host you want to set as a site manager.
4. Use either of the following methods to set the host as a site manager:
 - In the Edit Agent Configuration window, from the menu bar, choose **Edit**, and then **Base Manager Settings**.
 - In the Edit Agent Configuration window, in the tree area, right-click to display a pop-up menu. From the pop-up menu, choose **Base Manager Settings**.

(f) Removing a site manager

The following describes how to release the setting of a host as a site manager.

■ Settings on the integrated manager host

1. In the IM Configuration Management window, click the **Host List** tab or the **IM Configuration** tab. The **Host List** page or the **IM Configuration** page is displayed.
2. From the menu bar, choose **Edit**, and then **Edit Agent Configuration**. The Edit Agent Configuration window appears.

3. In the tree area, select the host you want to remove as a site manager.
4. Use either of the following methods to release the settings:
 - In the Edit Agent Configuration window, from the menu bar, choose **Edit**, and then **Release Base Manager Settings**.
 - In the Edit Agent Configuration window, in the tree area, right-click to display a pop-up menu. From the pop-up menu, choose **Release Base Manager Settings**.

■ Settings on the site manager host

1. In the IM Configuration Management window, click the **Host List** tab or the **IM Configuration** tab. The **Host List** page or the **IM Configuration** page is displayed.
2. From the menu bar, choose **Edit**, and then **Edit Agent Configuration**. The Edit Agent Configuration window appears.
3. In the Edit Agent Configuration window, in the tree area, select the host you want to remove as a site manager.
4. Use either of the following methods to remove the host as a site manager:
 - In the Edit Agent Configuration window, from the menu bar, choose **Edit**, and then **Release Base Manager Settings**.
 - In the Edit Agent Configuration window, in the tree area, right-click to display a pop-up menu. From the pop-up menu, choose **Release Base Manager Settings**.

(2) Obtaining update rights

The following describes how to obtain update rights.

When editing an agent configuration

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

When editing a remote monitoring configuration

In the Edit Remote Monitoring Configuration window, select the **Acquire update right** check box.

With update rights, you can now apply the new system hierarchy (IM configuration) to the system. Note that while you are editing a system hierarchy with the **Acquire update right** check box selected, other users are not able to apply their system hierarchies.

(3) Applying a system hierarchy to a system managed by IM Configuration Management

To apply the system hierarchy to the system that is managed by IM Configuration Management: If you want to apply an agent configuration to the system, JP1/Base must be running on all the agents in the agent configuration and all the agents to be deleted.

When editing an agent configuration

In the Edit Agent Configuration window, from the menu bar, choose **Operation**, and then **Apply Agent Configuration**.

The configuration definition information edited in the Edit Agent Configuration window is distributed to the manager and agents.

When editing a remote monitoring configuration

In the Edit Remote Monitoring Configuration window, from the menu bar, choose **Operation**, and then **Apply Remote Monitoring Configuration**.

The configuration is updated with the configuration definition information edited in the Edit Remote Monitoring Configuration window.

Because remote monitoring configurations are managed by the integrated manager or site managers, the configuration definition information is not distributed to managed hosts.

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 applying the system hierarchy fails, see *10.5.1(36) Actions to take when IM Configuration Management fails to apply the system hierarchy* in the *JP1/Integrated Management - Manager Administration Guide* and apply the system hierarchy again. If application fails again, all the host icons in the tree area of the **IM Configuration** page indicate an error.

If a new remote monitoring configuration is applied but a new agent configuration is not applied, the system hierarchies are displayed in gray in the tree area of the **IM Configuration** page. When you apply a remote monitoring configuration, make sure that you apply the new agent configuration.

When you use a site manager to manage agents or remotely managed hosts, perform the following procedure to apply an agent configuration or a remote monitoring configuration.

1. On the site manager, open the configuration editing window. From the menu bar, choose **Operation**, and then **Apply Agent Configuration** or **Apply Remote Monitoring Configuration**.
2. On the integrated manager, open the configuration editing window. From the menu bar, choose **Operation**, and then **Apply Agent Configuration** or **Apply Remote Monitoring Configuration**.
3. On the integrated manager, open the IM Configuration Management window. From the menu bar, choose **Operation**, and then **Synchronize IM Configuration**.
4. On the site manager, open the IM Configuration Management window. From the menu bar, choose **Operation**, and then **Collect IM Configuration**.

If you want to change the agent configuration or the remote monitoring configuration managed by a site manager, perform the following procedure.

1. On the site manager, open the configuration editing window. From the menu bar, choose **Operation**, and then **Apply Agent Configuration** or **Apply Remote Monitoring Configuration**.
2. On the integrated manager, open the IM Configuration Management window. From the menu bar, choose **Operation**, and then **Synchronize IM Configuration**.
3. On the site manager, open the IM Configuration Management window. From the menu bar, choose **Operation**, and then **Collect IM Configuration**.

However, this step is not necessary if you did not choose **Apply Agent Configuration** in step 1.

If you do not perform the above procedure, the configuration definition information held by JP1/Base on the site manager host does not match the configuration definition information stored in the IM Configuration Management database. In such cases, the system hierarchy is displayed in gray in the tree area in the IM Configuration Management window when you choose **Operation** from the menu bar and then **Verify IM Configuration** or you restart the JP1/IM - Manager service.

If the method for applying the system hierarchy is the batch distribution method (with deleted configurations) and **Apply Agent Configuration** is run on the site manager, events are no longer forwarded because the system hierarchy held by the site manager is deleted and then is applied.

If you want the site manager to apply the new IM configuration after the integrated manager applies the new IM configuration, perform the following procedure.

1. On the integrated manager, open the IM Configuration Management window. From the menu bar, choose **Operation**, and then **Synchronize IM Configuration**.
2. On the site manager, execute the `jevreload` command.
3. On the site manager, open the IM Configuration Management window. From the menu bar, choose **Operation**, and then **Collect IM Configuration**.

The supported methods for applying agent configurations include the batch distribution method (with deleted configurations) and the batch distribution method (without deleted configurations). For details about the methods for applying the system hierarchy, see *6.2.6 Applying the system hierarchy* in the *JP1/Integrated Management - Manager Overview and System Design Guide*.

(4) Canceling update rights

Perform the following procedure to cancel update rights.

When editing an agent configuration

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

When editing a remote monitoring configuration

In the Edit Remote Monitoring Configuration window, clear the **Acquire update right** check box.

Other users will now be able to apply their system hierarchies.

3.2.5 Synchronizing the system hierarchy

To synchronize a system hierarchy (IM configuration) between the integrated manager and site managers:

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 a virtualization system configuration

This section describes the procedure for using IM Configuration Management to set the virtualization system configuration during JP1/IM system configuration.

3.3.1 Using IM Configuration Management to manage a virtualization configuration

This subsection describes the settings for using IM Configuration Management to manage a virtualization configuration.

(1) Prerequisites for managing a virtualization configuration

The followings are the prerequisites for managing a virtualization configuration.

(a) Conditions for a manageable virtualization configuration

When you manage a KVM, you can manage the virtualization system configuration without virtualization environment management software. To manage virtualization software other than KVM, one of the following virtualization environment managers must be installed on the virtualization system management host.

- vCenter
- JP1/SC/CM
- SCVMM
- HCSM

The following table describes the requirements for using the above virtualization environment managers. The table after that gives the requirements for KVM.

Table 3–1: Requirements for virtualization environment management software

Virtualization environment management software	Requirements for the manager	Requirements for the virtualization system management host	Requirements for the VMM host on which the guest OS is running	Requirements for the guest OS
vCenter	The user ID and the password of the account for accessing the vCenter host to which the manager connects are registered in IM Configuration Management.	The manager can communicate with the host on which vCenter is running.	VMware ESX has been installed.	VMware Tools are installed on the guest OSs running on VMware ESX hosts, and IP addresses and host names are assigned to the guest OSs.
JP1/SC/CM	None.	The manager can communicate with JP1/Base on the host on which JP1/SC/CM is running.	Hitachi Compute Blade logical partitioning feature has been installed.	IP addresses and host names are assigned to the guest OSs managed by Hitachi Compute Blade logical partitioning feature.
SCVMM	<ul style="list-style-type: none">• The domain name of the SCVMM host to which the manager connects, the names of users with administrator	<ul style="list-style-type: none">• The OS on the host on which SCVMM is running is Windows Server 2012 or Windows Server 2008 R2.	Hyper-V or vCenter has been installed.	Hyper-V Integrated Services is installed on the guest OSs running on Hyper-V hosts, and IP addresses and host names are assigned to the guest OSs.

Virtualization environment management software	Requirements for the manager	Requirements for the virtualization system management host	Requirements for the VMM host on which the guest OS is running	Requirements for the guest OS
	<ul style="list-style-type: none"> privileges in the domain, and the passwords of such users are registered in IM Configuration Management. The SCVMM management console is installed on the manager.^{#1, #2} The version of the SCVMM management console matches the version of the SCVMM on the collection-target virtualization system management host. 	<ul style="list-style-type: none"> The SCVMM management console that is installed on the manager can communicate with the SCVMM that is installed on the virtualization system management host. The version of SCVMM matches the virtualization system management hosts that are specified as collection targets by a specific manager. 		
HCSM	<ul style="list-style-type: none"> The user name, the password, and the port number of the HCSM host to which the manager connects are registered in IM Configuration Management. HTTP communication can be used with the above user name, password, and port number on the HCSM host to which the manager connects. 	None.	<ul style="list-style-type: none"> HCSM manages the chassis and blade on which Hitachi Compute Blade logical partitioning feature is running. HCSM manages the host whose virtualization system configuration is to be collected. 	IP addresses and host names are assigned to the guest OSs managed by Hitachi Compute Blade logical partitioning feature.

#1: Do not install different versions of SCVMM management console on the same manager.

#2: Check prerequisite OSs for installing the SCVMM management console beforehand.

Table 3–2: Requirements for KVM

Requirements for the manager	Requirements for the VMM host on the virtual host	Requirements for the guest OS
<ul style="list-style-type: none"> The OS user ID, the password of the private key, and port number of the KVM host to which the manager connects are registered in IM Configuration Management. The manager can connect to the KVM host to which the manager wants to connect with SSH based on the information registered in IM Configuration Management. The OS user registered in IM Configuration Management has root privileges. 	The public key required for SSH connection with the manager has been distributed.	<ul style="list-style-type: none"> IP addresses and host names are assigned to the guest OSs managed by KVM. The guest OSs managed by KVM can resolve the IP address and host name of the local host. The host names of the guest OSs managed by KVM are the same as the host identification names defined by KVM.[#] If the host names of the guest OSs are changed, the host identification names defined by KVM are also redefined as the same names.

#: When you collect the virtualization configuration information of KVM, collect the host identification name (called a domain name in KVM) displayed in `IdName` when the `virsh list` command is executed, defined by KVM as the host name of a virtual host.

For details, see *6.3 Virtualization configuration management* in the *JP1/Integrated Management - Manager Overview and System Design Guide*.

(b) Conditions of JP1/Base for managing a virtualization configuration

Make sure that the following settings of JP1/Base satisfy the prerequisites for managing a virtualization configuration.

- JP1 permission levels

Use either of the following JP1 permission levels when using IM Configuration Management to manage a virtualization configuration.

- JP1_CF_Admin
- JP1_CF_Manager

When you use IM Configuration Management - View to apply a virtualization system configuration to Central Scope, the JP1 user who logs on to IM Configuration Management - View must have the following permissions:

- JP1 resource group: JP1_Console
- JP1 permission level: JP1_Console_Admin

- Requirements for registering hosts

- When you register host names you obtain from the virtualization configuration information in IM Configuration Management without change, check whether the name of the event server of JP1/Base running on the hosts to be registered satisfies the following requirements:
 - When you register short host names in IM Configuration Management, the name of the event server of JP1/Base running on the hosts to be registered is a short name.
 - When you register FQDN host names in IM Configuration Management, the name of the event server of JP1/Base running on the hosts to be registered is an FQDN.
- If the host names obtained from the virtualization configuration information differ from the host names you want to register in IM Configuration Management, use the Register Host window to register the hosts with the host names you want registered in IM Configuration Management.

(2) Setting virtualization configuration information

Use one of the following methods to specify information about the virtual hosts that are to be added to the JP1/IM system:

(a) Using the Register Host window to register virtual hosts

Invoke the Register Host window from the IM Configuration Management window to register new virtual hosts.

1. In the IM Configuration Management window, click the **Host List** tab to display the **Host List** page.
2. Use either of the following methods to display the Register Host window:
 - In the tree area, select **Host List**. From the menu bar, choose **Edit**, and then **Register Host**.
 - In the tree area, right-click **Host List** to display a pop-up menu and then choose **Register Host**.
3. In the Register Host window, enter information in the blank boxes to register a new host.
In the **Host type** section, select **Physical host** or **Virtual host** from the drop-down list.

When you select **Physical host** in the **Host type** section

In the Virtual Manager Settings window, in the **Virtual Manager Type** section, from the top drop-down list, select the name of virtualization management software installed on the host.

When you select **Virtual host** in the **Host type** section

In the **VMM host** box, specify the name of the host on which virtualization software is installed.

In the **Virtual Manager Type** box, specify the name of the virtualization management software that manages the host.

(b) Collecting virtualization configuration information on the virtualization system management host

Collect virtualization configuration information on the virtualization system management host and set the virtualization configuration information of the managed host in IM Configuration Management.

For details about how to collect virtualization configuration information on the virtualization system management host, see [3.3.2 Collecting virtualization system configuration information](#).

(3) Adding virtual hosts to the system hierarchy

Use IM Configuration Management - View to add the virtual hosts in [3.3.1\(2\) Setting virtualization configuration information](#) to the system hierarchy (IM configuration). For details about how to add hosts to the JP1/IM system configuration, see [3.2.4 Editing the system hierarchy](#).

(4) Applying the system hierarchy to the system

Use IM Configuration Management - View to apply the system hierarchy (IM configuration) that was set in [3.3.1\(3\) Adding virtual hosts to the system hierarchy](#) to the system. For details about how to apply a system hierarchy to a system, see [3.2.4\(3\) Applying a system hierarchy to a system managed by IM Configuration Management](#).

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.

(5) Installing certificates

When you collect virtualization configuration information from hosts running vCenter and VMware ESX, you can choose between using SSL (https) and not using SSL (http).

When the manager uses SSL to communicate with vCenter or VMware ESX, the certificate for the vCenter host or the VMware ESX host must be installed on the manager running JP1/IM - Manager. Install a certificate for each vCenter or VMware ESX host that the manager communicates with.

The following provides an overview of installing a vCenter host or a VMware ESX host certificate. For details, see the vCenter or 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. To obtain an SSL certificate from vCenter, use Internet Explorer. This subsection describes both methods.

■ Using Internet Explorer

If you are using Internet Explorer to obtain SSL certificates from VMware ESX or vCenter, see Internet Explorer's Help.

■ 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 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*.

Note: If you want to install a certificate for a logical host, replace `..\..\..\` with `shared-directory\JP1IMM`.

For *certificate-file-name*, specify the name of the certificate file (including the path) that was obtained in 3.3.1(5) (a) *Obtaining certificates*. For *host-name*, specify the name of the vCenter host or the VMware ESX host from which the certificate is to be obtained.

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 to 4 for each vCenter host or VMware ESX host.

■ 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 host-name -keystore /var/opt/jplimm/data/imcf/vmware.keystore
```

Note: If you want to install a certificate for a logical host, replace `/var/opt/jplimm` with `shared-directory/jplimm`.

For *certificate-file-name*, specify the name of the certificate file (including the path) that was obtained in 3.3.1(5) (a) *Obtaining certificates*.

For *host-name*, specify the name of the vCenter host or the VMware ESX host from which the certificate is to be obtained.

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 to 4 for each vCenter host or VMware ESX host.

(c) Deleting certificates from IM Configuration Management

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 host-name -keystore ..\..\..\data\imcf\vmware.keystore
```

Note: If you want to delete the certificate for a logical host, replace `..\..\..\` with *shared-directory*\JP1IMM.
For *host-name*, specify the name of the vCenter host or the VMware ESX host from which the certificate you want to delete was obtained.
3. Enter the password that was specified in *3.3.1(5)(b) Installing certificates in IM Configuration Management*.
The specified vCenter host or VMware ESX host certificate 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 host-name -keystore /var/opt/jplimm/data/imcf/vmware.keystore
```

Note: If you want to delete the certificate for a logical host, replace `/var/opt/jplimm` with *shared-directory*/`jplimm`.
For *host-name*, specify the name of the vCenter host or the VMware ESX host from which the certificate you want to delete was obtained.
3. Enter the password that was specified in *3.3.1(5)(b) Installing certificates in IM Configuration Management*.
The certificate for the specified vCenter host or VMware ESX host is deleted from IM Configuration Management.

(6) 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.

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. Note, however, that the procedure might differ depending on the version of VMware ESX. 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
```

(7) Changing the communication type for vCenter

The `jcfcolvmvc` command enables you to communicate with vCenter using a VMware Infrastructure SDK interface in order to obtain virtualization configuration information. The virtualization configuration collection function that works for vCenter hosts via the IM Configuration Management window operates in the same way.

By default, only communication using SSL (https) is permitted.

The following provides an overview of how to change the communication type permitted by VMware Infrastructure SDK. Note, however, that the procedure might differ depending on the version of vCenter. For details, see the vCenter documentation.

1. Log on to the vCenter host as a user with Administrator permissions.
2. Navigate to `C:\Documents and Settings\All Users\Application Data\VMware\VMware VirtualCenter`.
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="5">
  <_type>vim.ProxyService.LocalServiceSpec</_type>
  <accessMode>httpsWithRedirect</accessMode>
```

```
<port>8085</port>
<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 methods, specify `httpAndHttps`.

5. Use the command line or the Services window to restart vCenter Service.

(8) Setting up an SSH connection with the host started by KVM (in Windows)

This subsection describes how to configure SSH when the JP1/IM - Manager host is running in a Windows environment. SSH uses public-key cryptography for authentication.

To establish SSH connections, you need to:

- Configure an SSH server
Configure an SSH server on the host on which KVM has been installed.
- Create keys
Create keys on the host on which KVM has been installed.
- Place the private key on the JP1/IM - Manager host
Transfer the private key from the host on which KVM has been installed to the JP1/IM - Manager host.
- Place the public key on the monitored host
Place the public key on the host on which KVM has been installed.

Important

Do not use interactive commands such as `stty`, `tty`, `tset`, and `script` in the login script of the user who is permitted to establish SSH connections. If you must use these commands in the login script, create another user who is permitted to establish SSH connections for the host on which KVM has been installed. Alternatively, change the login script of the user who is permitted to establish SSH connections so that these commands will not be executed.

(a) Configuring an SSH server

To configure an SSH server:

1. Log on to the host on which KVM has been installed as a user with `root` privileges.
2. Open `/etc/ssh/sshd_config`.
3. Set `yes` for `PubkeyAuthentication`^{#1}.
4. Set `no` for `UseDNS`^{#1, #2}.
5. Set `yes` for `PermitRootLogin`^{#1}.

6. Execute the following command to restart the `sshd` service.

```
/etc/rc.d/init.d/sshd restart
```

Note that these commands might differ depending on the version of the OS. For details, see the documentation of the applicable OS.

#1

For details about the items to be set and how to set them in `sshd_config`, see the documentation for your SSH server.

#2

If you do not set these items, make sure that the host on which KVM has been installed can perform name resolution as follows.

- The host can resolve the IP address of the manager host to the manager host name.
- The IP address resolved from the host name of the manager host matches the IP address of the manager host.

If you are using a DNS server for name resolution and the host on which KVM has been installed cannot connect to the DNS server, the collection of virtualization configuration information from KVM might be delayed. If a delay occurs, startup or collection might time out and fail. To prevent this problem, we recommend that you set `no` for `UseDNS` and `LookupClientHostnames`.

(b) Initially creating keys

Log on to the host on which KVM has been installed as a user who collects virtualization configuration information from KVM and execute the `ssh-keygen` command to create keys. You only need to do this the first time that you create keys.

You can choose the type of keys (RSA or DSA).

Before you start the procedure, make sure that only the owner of the keys has write permission for the directory above the `.ssh` directory. If anyone other than the owner has write permission for the higher-level directory, SSH connections will fail.

1. Log on to the host on which KVM has been installed as a user who can collect virtualization configuration information from KVM.

2. Execute the `ssh-keygen` command.

Enter the command as follows:

- When creating RSA keys: `ssh-keygen -t rsa`
- When creating DSA keys: `ssh-keygen -t dsa`

3. Determine the name of the file in which the private key will be stored and the directory that will hold the file.

The path and the file name must not contain multibyte characters. The default setting is `~/ .ssh/id_rsa`.

4. Press the **Return** key twice.

When you are prompted to enter the passphrase for the private key, enter nothing and press the **Return** key. When you are prompted again, enter nothing and press the **Return** key again.

The following is an example of executing the `ssh-keygen -t rsa` command.

```
[root@HOST]$ ssh-keygen -t rsa
```

```
Generating public/private rsa key pair.
```

```
Enter file in which to save the key (/home/ssh-user/.ssh/id_rsa):
```

```
Enter passphrase (empty for no passphrase):
```



```
Enter same passphrase again:
Your identification has been saved in /home/ssh-user/.ssh/id_rsa.
Your public key has been saved in /home/ssh-user/.ssh/id_rsa.pub.
The key fingerprint is:
ax:xx:xx:xx:xx:bx:xx:xc:xx:xx:xx:xd:xd:xa:ed:xx root@HOST
```

5. Execute the `cat` command to add the public key file to the authentication key file.
6. Execute the `chmod` command to change the attribute of the authentication key file to 600.

The following is an example of executing the `cat` and `chmod` commands.

```
[ClientUser@TargetHost .ssh]$ cat id_rsa.pub >> authorized_keys
[ClientUser@TargetHost .ssh]$ chmod 600 authorized_keys
```

7. Configure `AuthorizedKeysFile` in `/etc/ssh/sshd_config`.

By default, `~/.ssh/authorized_keys` or `.ssh/authorized_keys` is set. If you change the path for the authentication key file created in step 6, check and, if necessary, revise the value of `AuthorizedKeysFile`. If you change any settings in `sshd_config`, restart the `sshd` service as a superuser.

Cautionary notes

- Manage private keys with the utmost care.
- The creation of keys (public key and a private key pair) does not depend on any environment or tool. You can create keys in any environment using any tool. However, after you create keys, you must place the private keys and public keys in the appropriate locations.

(c) Placing the private key on the JP1/IM - Manager host (when keys are initially created)

When the OS of the JP1/IM - Manager host is Windows, place the private key created as described in [3.3.1\(8\)\(b\) Initially creating keys](#) on the JP1/IM - Manager host running Windows. The path for the location of the private key must not contain multibyte characters. This only needs to be done the first time that keys are created.

(d) Placing the public key on the host on which KVM has been installed (when keys have already been created)

Place the public key created in [3.3.1\(8\)\(b\) Initially creating keys](#) on the host on which KVM has been installed. To do so, follow the procedure below. Note that this only needs to be done when keys were created on another host.

Before you start the procedure, make sure that only the owner of the keys has write permission for the directory above the `.ssh` directory. If anyone other than the owner has write permission for the higher-level directory, SSH connections will fail.

1. Log on to the host on which KVM has been installed as a user who can collect virtualization configuration information from KVM.
2. Navigate to the `.ssh` directory.
If the home directory of the user who collects virtualization configuration information from KVM does not contain the `.ssh` directory, create one. Set 700 as the attribute of the directory.
3. Execute the `scp` command to copy the public key file to the host on which KVM has been installed.

Copy the public key file created as described in [3.3.1\(8\)\(b\) Initially creating keys](#) to the monitored host. Copy the file to the `.ssh` directory in the home directory of the user who will collect virtualization configuration information from KVM.

4. Execute the `cat` command to add the contents of the public key file to the authentication key file.

5. Delete the copied public key file.

6. Execute the `chmod` command to change the attribute of the authentication key file to `600`.

7. Configure `AuthorizedKeysFile` in `/etc/ssh/sshd_config`.

By default, `~/.ssh/authorized_keys` or `.ssh/authorized_keys` is set. If you change the path for the authentication key file created in step 6, check and, if necessary, revise the value of `AuthorizedKeysFile`. If you change any settings in `sshd_config`, restart the `sshd` service as a superuser.

An example of executing the `scp`, `cat`, and `chmod` commands is shown below. In this example, the host name of the host where keys are created as described in [3.3.1\(8\)\(b\) Initially creating keys](#) is `IMHost`.

- Example of executing the commands:

```
[ClientUser@TargetHost ]$ cd .ssh
[ClientUser@TargetHost .ssh]$ scp
root@IMHost:/home/ssh-user/.ssh/id_rsa.pub ./
root@IMHost's password: Enter a password here.
id_rsa 100% 233 0.2KB/s 00:00
[ClientUser@TargetHost .ssh]$ cat id_rsa.pub >> authorized_keys
[ClientUser@TargetHost .ssh]$ rm id_rsa.pub
[ClientUser@TargetHost .ssh]$ chmod 600 authorized_keys
```

(e) Checking connections

When SSH client software is installed on the JP1/IM - Manager host in a Windows environment, use the private key placed on the host as described in [3.3.1\(8\)\(c\) Placing the private key on the JP1/IM - Manager host \(when keys are initially created\)](#) and check whether you can establish an SSH connection with the host on which KVM has been installed. In addition, when you establish an SSH connection, make sure that a password and passphrase do not need to be entered.

If an error occurs or you are prompted to enter a password and a passphrase, check whether the settings are specified correctly as described. Also check the settings of the OS to make sure that the OS will allow SSH connections.

Note that when virtualization configuration information from KVM is collected, the following commands must be executable on the hosts on which KVM has been installed. Make sure that the users that collect virtualization configuration information from KVM can execute these commands. If these commands cannot be executed, make sure that KVM has been installed correctly and that the command path has been set correctly.

- `virsh version`
- `virsh list --all`

(9) Setting up an SSH connection with the host started by KVM (in UNIX)

This subsection describes how to configure SSH when the JP1/IM - Manager host is running in a UNIX environment. SSH uses public-key cryptography for authentication.

To establish SSH connections, you need to:

- Configure an SSH server
Configure an SSH server on the host on which KVM has been installed.
- Create keys
Create keys on the JP1/IM - Manager host in a UNIX environment.
- Place the public key on the monitored host
Place the public key on the host on which KVM has been installed.

Important

Do not use interactive commands such as `stty`, `tty`, `tset`, and `script` in the login script of the user who is permitted to establish SSH connections. If you must use these commands in the login script, create another user who is permitted to establish SSH connections for collecting virtualization configuration information from KVM. Alternatively, change the login script of the user who is permitted to establish SSH connections so that these commands will not be executed.

(a) Configuring an SSH server

To configure an SSH server:

1. Log on to the host on which KVM has been installed as a user with `root` privileges.
2. Open `/etc/ssh/sshd_config`.
3. Set `yes` for `PubkeyAuthentication`^{#1}.
4. Set `no` for `UseDNS`^{#1, #2}.
5. Set `yes` for `PermitRootLogin`^{#1}.
6. Execute the following command to restart the `sshd` service.

```
/etc/rc.d/init.d/sshd restart
```

Note that these commands might differ depending on the version of the OS. For details, see the documentation of the applicable OS.

#1

For details about the items to be set and how to set them in `sshd_config`, see the documentation for your SSH server.

#2

If you do not set these items, make sure that the host on which KVM has been installed can perform name resolution as follows.

- The host can resolve the IP address of the manager host to the manager host name.
- The IP address resolved from the host name of the manager host matches the IP address of the manager host.

If you are using a DNS server for name resolution and the host on which KVM has been installed cannot connect to the DNS server, the collection of virtualization configuration information from KVM might be delayed. If a delay occurs, startup or collection might time out and fail. To prevent this problem, we recommend that you set `no` for `UseDNS` and `LookupClientHostnames`.

(b) Initially creating keys

Log on to the JP1/IM - Manager host in a UNIX environment a user with `root` privileges and execute the `ssh-keygen` command to create keys. You only need to do this the first time that you create keys.

You can choose the type of keys (RSA or DSA).

1. Log on to the JP1/IM - Manager host as a user with root privileges.

2. Execute the `ssh-keygen` command.

Enter the command as follows:

- When creating RSA keys: `ssh-keygen -t rsa`
- When creating DSA keys: `ssh-keygen -t dsa`

3. Determine the names of the file in which the private key will be stored and the directory that will hold the file.

The path and the file name must not contain multibyte characters. The default setting is `~/.ssh/id_rsa`.

4. Press the **Return** key twice.

When you are prompted to enter the passphrase for the private key, enter nothing and press the **Return** key. When you are prompted again, enter nothing and press the **Return** key again.

The following is an example of executing the `ssh-keygen -t rsa` command.

```
[root@HOST]$ ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/home/ssh-user/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/ssh-user/.ssh/id_rsa.
Your public key has been saved in /home/ssh-user/.ssh/id_rsa.pub.
The key fingerprint is:
ax:xx:xx:xx:xx:bx:xx:xc:xx:xx:xx:xd:xd:xa:ed:xx root@HOST
```

Cautionary notes

- Manage private keys with the utmost care.
- The creation of keys (public key and a private key pair) does not depend on any environment or tool. You can create keys in any environment using any tool. However, after you create keys, you must place the private keys and public keys in the appropriate locations.

(c) Placing the public key on the host on which KVM has been installed

Place the public key created in [3.3.1\(9\)\(b\) Initially creating keys](#) on the host on which KVM has been installed. To do so, follow the procedure below.

Before you start the procedure, make sure that only the owner of the keys has write permission for the directory above the `.ssh` directory. If anyone other than the owner has write permission for the higher-level directory, SSH connections will fail.

1. Log on to the host on which KVM has been installed as a user who can collect virtualization configuration information from KVM.
2. Navigate to the `.ssh` directory.

If the home directory of the user who collects virtualization configuration information from KVM does not contain the `.ssh` directory, create one. Set `700` as the attribute of the directory.

3. Execute the `scp` command to copy the public key file to the host on which KVM has been installed.
Copy the public key file created as described in [3.3.1\(9\)\(b\) Initially creating keys](#) to the host on which KVM has been installed. Copy the file to the `.ssh` directory in the home directory of the user who will collect virtualization configuration information from KVM.
4. Execute the `cat` command to add the contents of the public key file to the authentication key file.
5. Delete the copied public key file.
6. Execute the `chmod` command to change the attribute of the authentication key file to `600`.
7. Configure `AuthorizedKeysFile` in `/etc/ssh/sshd_config`.
By default, `~/.ssh/authorized_keys` or `~/.ssh/authorized_keys` is set. If you change the path for the authentication key file created in step 6, check and, if necessary, revise the value of `AuthorizedKeysFile`. If you change any settings in `sshd_config`, restart the `sshd` service as a superuser.

An example of executing the `scp`, `cat`, and `chmod` commands is shown below. In this example, the host name of the JP1/IM - Manager host where keys are created as described in [3.3.1\(9\)\(b\) Initially creating keys](#) is `IMHost`.

- Example of executing the commands:

```
[ClientUser@TargetHost ]$ cd .ssh
[ClientUser@TargetHost .ssh]$ scp root@IMHost:/home/ssh-user/.ssh/
id_rsa.pub ./
root@IMHost's password: Enter a password here.
id_rsa.pub 100% 233 0.2KB/s 00:00
[ClientUser@TargetHost .ssh]$ cat id_rsa.pub >> authorized_keys
[ClientUser@TargetHost .ssh]$ rm id_rsa.pub
[ClientUser@TargetHost .ssh]$ chmod 600 authorized_keys
```

(d) Checking connections

To check whether the JP1/IM - Manager host can connect to the host on which KVM has been installed:

1. Log on to the JP1/IM - Manager host as a user with root privileges.
2. Use the created private key to execute the `ssh` command on the host on which KVM has been installed.

If the connection succeeds without any entry, the SSH setting has been completed.

If an error occurs or you are prompted to enter a password and a passphrase, check whether the settings are specified correctly as described. Also check the settings of the OS to make sure that the OS will allow SSH connections.

The following example executes the `ssh` command to check connections:

In this example, the host name of the JP1/IM - Manager host is `IMHost`, the host name of the monitored host is `TargetHost`, and the user name that will collect virtualization configuration information from KVM is `ssh-user`.

- Example of executing the commands:

```
[root@IMHost]$ /usr/bin/ssh -i /home/ssh-user/.ssh/id_rsa -p 22 ssh-
user@TargetHost
```

```

The authenticity of host 'TargetHost (xxx.xxx.xxx.xxx)' can't be
established.
RSA key fingerprint is xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'TargetHost,xxx.xxx.xxx.xxx' (RSA) to the list of
known hosts.
Last login: Mon Mar 23 17:17:52 2011 from xxx.xxx.xxx.xxx
[ssh-user@TargetHost ~]$ exit
logout
Connection to TargetHost closed.
[root@IMHost]$

```

Note that when virtualization configuration information from KVM is collected, the following commands must be executable on the hosts on which KVM has been installed. Make sure that the users that collect virtualization configuration information from KVM can execute these commands. If these commands cannot be executed, make sure that KVM has been installed correctly and that the command path has been set correctly.

- `virsh version`
- `virsh list --all`

3.3.2 Collecting virtualization system configuration information

You can use windows or commands to collect (import) virtualization system configuration information. This subsection describes both methods.

(1) Using windows to collect virtualization system configuration information

1. In the IM Configuration Management window, check whether the virtualization system management host is registered.
If the virtualization system management host is not registered, register it. For details about the procedure, see [3.3.1\(2\) \(a\) Using the Register Host window to register virtual hosts](#).
2. Use either of the following methods to collect virtualization system configuration information:
 - To centrally collect the information, in the IM Configuration Management window, from the menu bar, choose **Operation, Virtualization Configuration**, and then **Batch Collect Virtualization Configurations**.
 - To collect the information from a specific host, in the IM Configuration Management window, select the target host. From the menu bar, choose **Operation, Virtualization Configuration**, and then **Collect Virtualization Configuration**.

When all of the information has been collected, the host names are added under **Host List** in the IM Configuration Management window.

Note that virtual hosts are displayed in the sequence they are registered on the manager. Perform the following procedure to find the virtual host whose information you want to view.

1. Open the **Host List** page. Click the **Lower Host Information** button.

- In the **Lower Host Information** section, click the item name (host name, IP address, host type) that can be used to identify the host whose information you want to view and sort the hosts.

If the virtualization configuration information for the host has changed, perform step 2 again.

(2) Using commands to collect (import) virtualization configuration information

The following describes how to import the virtualization configuration information collected from the virtualization software and virtualization management software to the manager running IM Configuration Management in order to register new hosts.

- Execute the `jcsdbexport` command to export monitoring tree information from Central Scope.
The exported information is output to the configuration file for monitoring tree.
- Execute the `jcfcolvmesx` command to collect virtualization configuration information from VMware ESX.
Specify the following options in the `jcfcolvmesx` command.

Option	Value
-m	Specify <code>https</code> when using SSL for communication with VMware ESX. When you use SSL for communication with VMware ESX, you need to obtain beforehand a certificate from the applicable VMware ESX host and install it in IM Configuration Management. For details about how to obtain and install certificates, see 3.3.1(5) Installing certificates .
-u	Specify the name of the VMware ESX user.
-p	Specify the password for VMware ESX.
-c	Specify the VMware ESX host from which virtualization configuration information is to be collected.
-o	Specify the name of the virtualization configuration information file for storing the virtualization configuration information.

When you execute this command, the `KNAN24030-I` and `KNAN24031-I` messages appear, and virtualization configuration information is collected.

- Execute the `jcfexport` command to export the information managed by IM Configuration Management.
Execute the `jcfexport` command on the manager running IM Configuration Management.
The command exports the information managed by IM Configuration Management, which is stored in the IM Configuration Management database (host input information file (`host_input_data.csv`)).
For details about the information managed by IM Configuration Management that can be exported, see [6.8.1 Types of information that can be imported or exported in the JP1/Integrated Management - Manager Overview and System Design Guide](#).
- Execute the `jcfmkhostsdata` command on the manager running IM Configuration Management to create a host input information file to hold the virtualization configuration information.
Specify the following options in the `jcfmkhostsdata` command.

Option	Value
-imcf	Specify the name of the host input information file (<code>host_input_data.csv</code>) exported in step 3.
-vm	Specify the name of the virtualization configuration information file created in step 2.
-o	Specify the output destination for the host input information file (<code>host_input_data.csv</code>) that is to be updated with the virtualization configuration information.

5. Overwrite the host input information file exported in step 3 with the host input information file created in step 4.
6. Execute the `jcfimport` command to import the host input information file created in step 5 to IM Configuration Management.

When you execute the `jcfimport` command, the three types of information that IM Configuration Management holds (host, system hierarchy (IM configurations), and profile) will be deleted. To manage profiles, you need to collect these three types of information after the import. Perform the following procedure to collect the three types of information.

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

The profiles are collected all at one time.

3.3.3 Using Central Scope to monitor a virtualization configuration

This subsection describes how to configure a monitoring tree that allows Central Scope to monitor a virtualization configuration.

(1) Prerequisites for the Central Scope monitoring tree

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.

(2) Applying virtualization configuration information to the Central Scope monitoring tree

Use either of the following methods to apply virtualization configuration information to the Central Scope monitoring tree.

(a) Using the IM Configuration Management window

1. In the IM Configuration Management window, from the menu bar, choose **Operation, Virtualization Configuration**, and then **Apply to Central Scope Monitoring Tree**.

The virtualization configuration information is applied to the Central Scope monitoring tree.

(b) Importing virtualization configuration information

After you collect virtualization configuration information, perform the procedure below to import it. For details about how to collect virtualization configuration information, see [3.3.2 Collecting virtualization system configuration information](#).

For details about the commands described here, see the command descriptions in the manual *JPI/Integrated Management - Manager Command and Definition File Reference*.

- `jcfexport` command: See *jcfexport* in *Chapter 1. Commands*.
- `jcfmkcsdata` command: See *jcfmkcsdata* in *Chapter 1. Commands*.
- `jcsdbimport` command: See *jcsdbimport* in *Chapter 1. Commands*.
- `jcsdbexport` command: See *jcsdbexport* in *Chapter 1. Commands*.

1. Execute the `jcfexport` command to export the information managed by IM Configuration Management.

The exported information is output to the host input information file (`host_input_data.csv`).

For details about the information managed by IM Configuration Management that can be exported, see *6.8.1 Types of information that can be imported or exported* in the *JP1/Integrated Management - Manager Overview and System Design Guide*.

2. Execute the `jcfmkcsdata` command to create a configuration file for monitoring tree to be updated with the information managed by IM Configuration Management.

Specify the following options in the `jcfmkcsdata` command.

Option	Value
<code>-f</code>	Specify the name of the host input information file (<code>host_input_data.csv</code>) exported in step 1 and the name of the configuration file for monitoring tree that was created beforehand by using the <code>jcsdbexport</code> command.
<code>-o</code>	Specify the output destination for the configuration file for monitoring tree that is updated with the information managed by IM Configuration Management.

3. Execute the `jcsdbimport` command to import the configuration file for monitoring tree created in step 2 to Central Scope.

When you execute the `jcsdbimport` command, all the statuses in the monitoring tree are deleted.

3.4 Setting business groups

The following prerequisites must be satisfied to set business groups:

- The IM databases (the integrated monitoring database and the IM Configuration Management database) are enabled. For details about how to enable the IM databases, see *1.4 Creating IM databases (for Windows)* for Windows and *2.4 Creating IM databases (for UNIX)* for UNIX.
- Information about the JP1 users that will manage the business groups is in hand. For details about the JP1 users for business groups, see *11.5.4 Considerations for business groups* in the *JP1/Integrated Management - Manager Overview and System Design Guide*.

This section covers the following topics.

- Creating business groups
- Adding hosts to business groups
- Deleting hosts from business groups
- Using Central Scope to monitor business groups

3.4.1 Creating business groups

This subsection describes how to create business groups.

(1) Setting up business groups

The following describes how to create business groups and assign hosts to them. Business group setup consists of all or some of the following steps:

- Creating a business group
- Editing the properties of a business group
- Deleting a business group
- Adding hosts to a business group or deleting hosts from a business group
- Listing the hosts in a business group

(a) Creating a business group

To create a business group:

1. In the IM Configuration Management window, click the **Business Group** tab.
The **Business Group** page is displayed.
2. On the **Business Group** page, select the **Acquire update right** check box.
3. On the **Business Group** page, in the tree area, select and right-click the root node. From the pop-up menu, choose **New**.
The Create Business Group window appears.
4. In the Create Business Group window, enter values in the **Business group name** box, the **Assigned JP1 asset group name** box, and the **Comment** box.

5. Click the **OK** button.

A business group is created.

For details about the Create Business Group window, see *4.14 Create Business Group window* in the manual *JPI/Integrated Management - Manager GUI Reference*.

(b) Editing the properties of a business group

To edit the properties of a business group:

1. In the IM Configuration Management window, click the **Business Group** tab.

The **Business Group** page is displayed.

2. On the **Business Group** page, select the **Acquire update right** check box.

3. On the **Business Group** page, in the tree area, select and right-click a node. From the pop-up menu, choose **Edit Basic Information**.

The Edit Business Group Basic Information window appears.

4. In the Edit Business Group Basic Information window, edit the values in the **Business group name** box, the **Assigned JPI asset group name** box, and the **Comment** box.

5. Click the **OK** button.

The edited information for the business group is registered.

For details about the Edit Business Group Basic Information window, see *4.15 Edit Business Group Basic Information window* in the manual *JPI/Integrated Management - Manager GUI Reference*.

(c) Deleting a business group

To delete a business group:

1. In the IM Configuration Management window, click the **Business Group** tab.

The **Business Group** page is displayed.

2. On the **Business Group** page, select the **Acquire update right** check box.

3. On the **Business Group** page, in the tree area, select and right-click a node. From the pop-up menu, choose **Delete**.

The selected business group and all the monitoring groups below it are deleted.

For details about the IM Configuration Management window, see *4.1 IM Configuration Management window* in the manual *JPI/Integrated Management - Manager GUI Reference*.

(d) Adding hosts to a business group or deleting hosts from a business group

To add a host to a business group or delete a host from a business group:

1. In the IM Configuration Management window, click the **Business Group** tab.

The **Business Group** page is displayed.

2. On the **Business Group** page, select the **Acquire update right** check box.

3. On the **Business Group** page, in the tree area, select and right-click the business group node you want to add a host to or delete a host from. From the pop-up menu, choose **Add or Delete Affiliated Hosts**.

The Add or Delete Affiliated Hosts window appears.

4. If you want to add a host, in the Add or Delete Affiliated Hosts window, in the **Host List** section, select the host you want to add and click the **Add** button. If you want to delete a host, in the **Added Hosts** section, select the host you want to delete and click the **Delete** button.

The selected host is added or deleted.

For details about the Add or Delete Affiliated Hosts window, see *4.18 Add or Delete Affiliated Hosts window* in the manual *JP1/Integrated Management - Manager GUI Reference*.

(e) Listing the hosts in a business group

To list the hosts in a business group:

1. In the IM Configuration Management window, click the **Business Group** tab.
The **Business Group** page is displayed.
2. On the **Business Group** page, in the tree area, select the business group node whose hosts you want to list.
3. On the **Business Group** page, in the node information display area, click the **Affiliated Host List** button.
A list of hosts in the selected business group appears. If you want to display the basic information, click the **Basic Information** button.

For details about the IM Configuration Management window, see *4.1 IM Configuration Management window* in the manual *JP1/Integrated Management - Manager GUI Reference*.

(2) Setting up monitoring groups

The hosts in a business group can be further grouped as subgroups within the same business group. These subgroups are called monitoring groups. The administrator who monitors the entire system should consult the administrators who monitor business systems to create monitoring groups. Monitoring group setup consists of all or some of the following steps:

- Creating a monitoring group
- Editing the properties of a monitoring group
- Deleting a monitoring group
- Copying a monitoring group
- Cutting a monitoring group
- Pasting a monitoring group
- Adding hosts to a monitoring group or deleting hosts from a monitoring group
- Listing the hosts in a monitoring group

(a) Creating a monitoring group

To create a monitoring group:

1. In the IM Configuration Management window, click the **Business Group** tab.
The **Business Group** page is displayed.
2. On the **Business Group** page, select the **Acquire update right** check box.
3. On the **Business Group** page, in the tree area, select and right-click a business group node. From the pop-up menu, choose **New**.

The Create Monitoring Group window appears.

4. In the Create Monitoring Group window, enter values in the **Monitoring group name** box and the **Comment** box.
5. Click the **OK** button.

A monitoring group is created under the selected business group. If you have selected a monitoring group in the tree area, a monitoring group is created under that group.

For details about the Create Monitoring Group window, see *4.16 Create Monitoring Group window* in the manual *JP1/Integrated Management - Manager GUI Reference*.

(b) Editing the properties of a monitoring group

To edit the properties of a monitoring group:

1. In the IM Configuration Management window, click the **Business Group** tab.
The **Business Group** page is displayed.
2. On the **Business Group** page, select the **Acquire update right** check box.
3. On the **Business Group** page, in the tree area, select and right-click a node. From the pop-up menu, choose **Edit Basic Information**.
The Edit Monitoring Group window appears.
4. In the Edit Monitoring Group window, edit the values in the **Monitoring group name** box and the **Comment** box.
5. Click the **OK** button.
The edited information for the monitoring group is registered.

For details about the Edit Monitoring Group window, see *4.17 Edit Monitoring Group window* in the manual *JP1/Integrated Management - Manager GUI Reference*.

(c) Deleting a monitoring group

To delete a monitoring group:

1. In the IM Configuration Management window, click the **Business Group** tab.
The **Business Group** page is displayed.
2. On the **Business Group** page, select the **Acquire update right** check box.
3. On the **Business Group** page, in the tree area, select and right-click a node. From the pop-up menu, choose **Delete**.
The selected monitoring group and all the monitoring groups under it are deleted.

(d) Copying a monitoring group

To copy a monitoring group:

1. In the IM Configuration Management window, click the **Business Group** tab.
The **Business Group** page is displayed.
2. On the **Business Group** page, in the tree area, select and right-click a node. From the pop-up menu, choose **Copy**.
The selected monitoring group and all the monitoring groups under it are copied.

(e) Cutting a monitoring group

To cut a monitoring group:

1. In the IM Configuration Management window, click the **Business Group** tab.
The **Business Group** page is displayed.
2. On the **Business Group** page, in the tree area, select and right-click a node. From the pop-up menu, choose **Cut**.
The selected monitoring group and all the monitoring groups under it are cut.

(f) Pasting a monitoring group

You can paste one or more monitoring groups you have copied in [3.4.1\(2\)\(d\) Copying a monitoring group](#) or cut in [3.4.1\(2\)\(e\) Cutting a monitoring group](#). You can paste the monitoring groups only on nodes in the same business group.

To paste a monitoring group:

1. On the **Business Group** page, in the tree area, select and right-click a node. From the pop-up menu, choose **Paste**.
The copied or cut monitoring group is pasted under the selected node. If the paste destination contains a monitoring group or a host with the same name, the Change Monitoring Group Name window appears. Change the name of the monitoring group.

(g) Adding hosts to a monitoring group or deleting hosts from a monitoring group

Perform the following procedure to add hosts to a monitoring group or delete hosts from a monitoring group. As a prerequisite, the hosts to be added to the monitoring group must have already been registered in the business group.

1. In the IM Configuration Management window, click the **Business Group** tab.
The **Business Group** page is displayed.
2. On the **Business Group** page, select the **Acquire update right** check box.
3. On the **Business Group** page, in the tree area, select and right-click the monitoring group node you want to add a host to or delete a host from. From the pop-up menu, choose **Add or Delete Affiliated Hosts**.
The Add or Delete Affiliated Hosts window appears.
4. If you want to add a host, in the Add or Delete Affiliated Hosts window, in the **Host List** section, select the host you want to add and click the **Add** button. If you want to delete a host, in the **Added Hosts** section, select the host you want to delete and click the **Delete** button.
The selected host is added or deleted.

For details about the Add or Delete Affiliated Hosts window, see [4.18 Add or Delete Affiliated Hosts window](#) in the manual *JP1/Integrated Management - Manager GUI Reference*.

(h) Listing the hosts in a monitoring group

To list the hosts in a monitoring group:

1. In the IM Configuration Management window, click the **Business Group** tab.
The **Business Group** page is displayed.
2. On the **Business Group** page, in the tree area, select the monitoring group node whose hosts you want to list.
3. On the **Business Group** page, in the node information display area, click the **Affiliated Host List** button.

A list of hosts in the selected monitoring group appears. If you want to display the basic information, click the **Basic Information** button.

(3) Applying an edited business group to the IM Configuration Management database and Central Console

Perform the following procedure to apply an edited business group or monitoring group to the IM Configuration Management database and Central Console.

When you apply a modified business group or monitoring group, the old name of the business group or monitoring group, which is set in the Central Scope definitions listed below, is replaced with a new name. When you delete a business group or a monitoring group, the name of the business group or the monitoring group is replaced with a slash (/) and is no longer valid in Central Console.

- Severe event definitions
- Event search conditions
- Event acquisition filters (common exclusion-conditions in extended mode)
- Event receiver filters
- View filters
- Correlation event generation definitions
- Automated action definitions
- Action result update conditions
- Command button definitions
- Severity changing definitions
- Display message change definitions
- Event-source-host mapping definitions

To apply an edited business group:

1. In the IM Configuration Management window, click the **Business Group** tab.
The **Business Group** page is displayed.
2. On the **Business Group** page, select the **Acquire update right** check box.
3. From the menu bar, choose **Operation, Business Group**, and then **Apply Business Group**.
The host information is updated to the settings displayed on the **Business Group** page and the latest configuration definition information takes effect.
4. On the **Business Group** page, clear the **Acquire update right** check box.

(4) Setting reference and operation restrictions on a business group

The system administrator can set reference and operation restrictions on business groups and apply these restrictions to administrators who monitor business systems. For details about how to set reference and operation restrictions, see [4.20 Setting reference and operation restrictions on business groups](#).

After restrictions are set, the administrators who monitor business systems can reference and operate only the business systems they manage.

3.4.2 Adding hosts to business groups

This subsection describes how to add hosts to business groups.

(1) Adding monitored hosts to a business group

If requested by an administrator who monitors a business system, the administrator who monitors the entire system adds hosts that are to be monitored to the business group that contains the business system. For details about how to add monitored hosts to a business group, see [3.4.1\(1\)\(d\) Adding hosts to a business group or deleting hosts from a business group](#).

(2) Adding monitored hosts to a monitoring group

When an administrator who monitors a business system requests that monitored hosts be added to a monitoring group, the administrator who monitors the entire system adds the hosts to the monitoring group. For details about how to add monitored hosts to a monitoring group, see [3.4.1\(2\)\(g\) Adding hosts to a monitoring group or deleting hosts from a monitoring group](#).

3.4.3 Deleting hosts from business groups

(1) Deleting monitored hosts from a business group

When an administrator who monitors a business system requests that monitored hosts be removed from a business group, the administrator who monitors the entire system deletes the monitored hosts from the applicable business group. For details about how to delete monitored hosts from a business group, see [3.4.1\(1\)\(d\) Adding hosts to a business group or deleting hosts from a business group](#).

3.4.4 Using Central Scope to monitor business groups

This subsection describes how to use Central Scope to monitor business groups. Business groups that you want to apply to Central Scope can be applied only to a server-oriented tree.

(1) Prerequisites

The following prerequisites must be satisfied to apply business group information and monitoring group information to the Central Scope monitoring tree.

- Central Scope is enabled and the data version of the monitoring object database of Central Scope is 081000 or later.
- Business groups have already been recorded in the IM Configuration Management database.
- The user who logs on to IM Configuration Management has both the JP1_CF_Admin permission and the JP1_Console_Admin permission in the JP1_Console resource group.

(2) Applying business group information and monitoring group information to the Central Scope monitoring tree

Use either of the following methods to apply business group information and monitoring group information to the Central Scope monitoring tree.

Note that when you apply the hierarchy of business groups and monitoring groups to the Central Scope monitoring tree, the sequence in which hosts are displayed might change.

(a) Applying information from the IM Configuration Management window

1. In the IM Configuration Management window, from the menu bar, choose **Operation, Business Group**, and then **Apply to Central Scope Monitoring Tree**.

Business group information and monitoring group information are applied to the Central Scope monitoring tree.

(b) Importing business group information and monitoring group information

1. Export business group information and monitoring group information.

On the manager running IM Configuration Management, execute the `jcfexport` command to export the business group information and monitoring group information registered in the IM Configuration Management database.

- When exporting only business group information and monitoring group information
Execute the `jcfexport` command with the `-g` option.
- When exporting all the information managed by IM Configuration Management
Execute the `jcfexport` command with the `-a` option.

For details about the information managed by IM Configuration Management that is exportable, see *6.8.1 Types of information that can be imported or exported* in the *JP1/Integrated Management - Manager Overview and System Design Guide*.

2. Export the monitoring tree information of Central Scope.

On the same manager, execute the `jcsdbexport` command to export the monitoring tree information of Central Scope.

3. Merge the exported business group information and monitoring group information and the monitoring tree information of Central Scope.

On the same manager, execute the `jcfmkcsdata` command to merge the exported business group information and monitoring group information and the monitoring tree information of Central Scope.

- When only business group information and monitoring group information are exported in step 1
Execute the `jcfmkcsdata` command with the `-g` option.
- When all the information managed by IM Configuration Management is exported in step 1
Execute the `jcfmkcsdata` command with the `-a` option.

4. Import the information merged in step 3 to Central Scope.

On the same manager, execute the `jcsdbimport` command to import the exported business group information and monitoring group information. The monitoring tree of business groups and monitoring groups is added to the Central Scope monitoring tree.

3.5 Setting the profiles

This section describes how to set the profiles that will be used on the hosts to be monitored when you configure a JP1/IM system. You can also set profiles from the hosts added as monitored hosts, and manage the profiles.

The procedure for setting profiles is different for hosts in an agent configuration and hosts in a remote monitoring configuration. The following subsections provide details.

3.5.1 Setting the profiles on hosts in an agent configuration

The following profiles for information can be set in the configuration file:

- Profiles (Information in the configuration file)
This is the configuration file stored at the agent. The JP1/Base services do not use the settings in a configuration file. If you edit a configuration file but do not apply the modified information to the services, the valid configuration information will differ from the settings in the configuration file.

The following table describes the types of profiles you can manipulate, the types of operations you can perform on profiles, and the configuration files that correspond to the profiles.

Table 3–3: Types of profiles and configuration files that correspond to the profiles

Operation	Type of profile you can manipulate	Corresponding configuration file
Add, delete	Log file trap information	<ul style="list-style-type: none">• Log file trap action-definition file• Log-file trap startup definition file
Edit, save, temporarily apply, apply by reloading configuration files, apply by restarting log file traps	<ul style="list-style-type: none">• Event transfer information• Log file trap information• Event log trap information• Local action information	<ul style="list-style-type: none">• Log file trap action-definition file• Log-file trap startup definition file

Note that you can start and stop only log file traps.

For details about the prerequisites for setting the profiles on hosts in an agent configuration, see [3.5.1\(8\) Prerequisites for managing profiles on agents](#).

(1) 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. On the **IM Configuration** page, in the tree area, select the agent from which you want to obtain a list of profiles.
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, select a JP1 product name (JP1/Base), and then use either of the following methods to obtain exclusive editing rights:
 - From the menu bar, choose **Edit**, and then **Exclusive Editing Settings**.
 - Right-click to display a pop-up menu and choose **Exclusive Editing Settings**.

This step is unnecessary if exclusive editing rights have already been obtained.

5. 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.

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 was performed and on profiles whose information is still the same as at the agents, such operations might have adverse effects on future operations. Therefore, eliminate the cause of the error, and then perform the profile tree rebuild processing again.
- Collection of profile lists fails if multiple log file traps are started using the same operation definition file or using operation definition files with the same name in different directories. Note that when the OS of the JP1/IM - Manager host is Windows, the names of configuration files used on agents are not case sensitive.
- When you rebuild a profile tree, all the profiles stored on the manager are deleted and profile lists are collected from the agents again. If the profiles have not been applied to agents, apply them first and then rebuild the profile tree.

(2) 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.

(a) Collecting profiles in batch mode

The following describes how to batch-collect JP1/Base profiles from all the agents defined in a system hierarchy (IM configuration).

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**.
When a confirmation message asking whether you wish to collect profiles in batch mode is displayed, choose **Yes**. Profiles are collected in batch mode and stored on the manager running IM Configuration Management. The execution result is displayed in the Execution Results window.

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 agent 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.

(b) Collecting profiles individually from each agent

The following describes how to collect profiles individually from each agent.

Note that profiles cannot be collected while another user has exclusive editing rights for the configuration files.

1. In the IM Configuration Management window, click the **IM Configuration** tab.
The **IM Configuration** page is displayed.
2. On the **IM Configuration** page, in the tree area, select the agent from which you want to collect profiles.
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**.

This step is unnecessary if exclusive editing rights have already been obtained.

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. On the **Configuration File** page, in the tree area, select a profile you want to obtain. Then use either 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) Displaying profiles

You can display the profiles stored on the manager running IM Configuration Management by using either of two methods according to the information to be displayed. This subsection describes both methods.

(a) Displaying the valid configuration information

To display the valid configuration information for each agent:

1. In the IM Configuration Management window, click the **IM Configuration** tab.
The **IM Configuration** page is displayed.
2. On the **IM Configuration** page, in the tree area, select the agent whose valid configuration information you want to display.
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 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 *4.9.1 Valid Configuration Information page* in the manual *JPI/Integrated Management - Manager GUI Reference*.

(b) Displaying configuration files

The following describes how to display the configuration files of each agent. These 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. On the **IM Configuration** page, in the tree area, select the agent whose configuration files you want to display.
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 *4.9.2 Configuration File page* in the manual *JPI/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 [3.5.1\(5\) Editing configuration files](#).

(4) Adding or deleting profiles

You can use IM Configuration Management to add profiles to the existing profiles stored on the manager running IM Configuration Management or delete profiles from the manager.

(a) Adding profiles

To add a profile:

1. In the IM Configuration Management window, click the IM Configuration tab.
The **IM Configuration** page is displayed.
2. On the **IM Configuration** page, in the tree area, select the agent whose profile you want to add to the manager.
3. Use either of the following methods to display the Display/Edit Profiles window:
 - From the menu bar, choose **View**, and then **Display Profiles**.
 - Right-click to display a pop-up menu, and choose **Display Profiles**.
4. In the tree area, select a JP1 product name (JP1/Base), and then use either of the following methods to obtain exclusive editing rights:
 - From the menu bar, choose **Edit**, and then **Exclusive Editing Settings**.
 - Right-click to display a pop-up menu, and choose **Exclusive Editing Settings**.

This step is unnecessary if exclusive editing rights have already been obtained.

5. Click the **Configuration File** button.
The **Configuration File** page is displayed.
6. On the **Configuration File** page, in the tree area, select **Log File Trapping**.
7. Use either of the following methods to display the Add Profile window:
 - From the menu bar, choose **Edit**, and then **Add Profile**.
 - Right-click to display a pop-up menu, and choose **Add Profile**.
8. Enter values in the following boxes.
 - **Log file trap name**
You cannot specify an existing log file trap name or a name that is the same as the log file trap action-definition file. For details, see [4.10 Add Profile window](#) in the manual *JP1/Integrated Management - Manager GUI Reference*.
When you configure a log file trap for a cluster system, specify the same log file trap name in the Add Profile window on the physical host running as the active server and in the Add Profile window on the physical host running as the standby server. This item is mandatory.
 - **Cluster ID**
When you configure a log file trap for a cluster system, on the physical host running as the active server, select the **Enable** check box and enter a cluster ID in the **ID** box.
On the physical host running as the standby server, in the Add Profile window, enter the same cluster ID you entered on the active server. This item is optional.

9. Click the **OK** button.

The name of the added log file trap name of the log file trap appears in the tree area.

For details about how to edit the configuration file for log file traps, see [3.5.1\(5\) Editing configuration files](#).

When you add the profile of a log file trap, the log file trap name is displayed in gray in the tree area because the log file trap is not running yet. For details about how to start log file traps, see [3.5.1\(7\)\(a\) Starting log file traps](#).

(b) Deleting profiles

The following describes how to delete profiles.

You cannot delete profiles in the following case:

- The log file trap corresponding to the selected profile is running.
If the log file trap is running, stop it. For details about how to stop log file traps, see [3.5.1\(7\)\(b\) Stopping log file traps](#).

To delete a profile:

1. In the IM Configuration Management window, click the IM Configuration tab.
The **IM Configuration** page is displayed.
2. On the **IM Configuration** page, in the tree area, select the agent whose profile you want to delete from the manager.
3. Use either of the following methods to display the Display/Edit Profiles window:
 - From the menu bar, choose **View**, and then **Display Profiles**.
 - Right-click to display a pop-up menu, and choose **Display Profiles**.
4. In the tree area, select a JP1 product name (JP1/Base), and then use either of the following methods to obtain exclusive editing rights:
 - From the menu bar, choose **Edit**, and then **Exclusive Editing Settings**.
 - Right-click to display a pop-up menu, and choose **Exclusive Editing Settings**.

This step is unnecessary if exclusive editing rights have already been obtained.

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

The **Configuration File** page is displayed.

6. On the **Configuration File** page, in the tree area, select the applicable log file trap name.

In the tree area, under **Log File Trapping**, a list of the log file trap names appears. Select the log file trap name you want to delete.

7. Use either of the following methods to delete the log file trap name:

- From the menu bar, choose **Edit**, and then **Delete Profile**.
- Right-click to display a pop-up menu, and choose **Delete Profile**.

When a message appears asking whether you want to delete the log file trap name, click the **Yes** button.

The log file trap name is deleted.

(5) Editing configuration files

The following describes how to edit and save the configuration files collected as described in [3.5.1\(2\) Collecting profiles](#). You can use the Display/Edit Profiles window to edit and save a configuration file.

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. On the **IM Configuration** page, in the tree area, select the agent whose configuration file you want to edit.
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:
When you cut or paste the character strings in a configuration file, make sure that you obtain exclusive editing rights first.
 - 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**.This step is unnecessary if exclusive editing rights have already been obtained or you are copying only the character strings in a configuration file.
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 *4.9.2 Configuration File page* in the manual *JP1/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 agent. 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 *3.5.1(6) 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 agent, the configuration file will be overwritten by the collected information. If you want to apply a configuration file to the agent, make sure that you do so before you collect profiles.

(6) Applying edited information in configuration files

After you edit a configuration file on the manager, you can apply the new information to all the agents in batch mode or to each agent individually.

After applying a configuration file, you can check whether the operation was successful on the **Configuration File** page in the Display/Edit Profiles window. If it was successful, **Application status** is **Applied**. If the configuration file could not be applied, **Application status** is **Application failed**. If the configuration files stored on the manager are not used, **Application status** is blank (not applied). If configuration files are stored on the manager but not used on the target agent, **Application status** is **Saved on the server**.

When **Application status** is **Application failed** or **Saved on the server**, the icon displayed in the tree area on the **Configuration File** page indicates that the configuration file is being edited.

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.

After applying a configuration file, you can check the status of the agent on the **IM Configuration** page in the IM Configuration Management window. If **Application status** of any of the configuration files is **Application failed** or **Saved on the server** on the **Configuration File** page, the agent icon in the tree area of the **IM Configuration** page indicates an error. To view the details, click the **Basic Information** button in the node information display area on the **IM Configuration** page.

(a) Using the batch mode to apply edited information in configuration files

The following describes how to batch-apply the modified information in configuration files to all the agents registered in a system hierarchy (IM configuration) at one time.

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. If no configuration files are found on the manager, the KNAN22497-1 message appears and no configuration file is applied.

(b) Applying edited information in configuration files individually to each agent

Three methods are available for applying the modified information in configuration files to each agent.

■ By reloading

You can reload configuration files onto an agent to apply the modified information in the configuration files.

You cannot use reloading to apply the modified information in configuration files in the following case:

- The selected log file trap is not running when you attempt to apply the log file trap profile.

To apply the modified information in a configuration file by reloading the configuration file:

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

The **IM Configuration** page is displayed.

2. On the **IM Configuration** page, in the tree area, select the agent to which you want to apply the modified information in a configuration file by reloading the file.

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**.
 This step is unnecessary if exclusive editing rights have already been obtained.
 5. In the tree area, select the profile you want to apply, and then click the **Configuration File** button. The **Configuration File** page is displayed. This step is unnecessary if you are currently editing the profile (configuration file) you want to apply.
 6. On the **Configuration File** page, in the node information display area, in the **Saving/application** section, click the two options below. Then click the **Execute** button.
 - **Apply**
 - **Reload**
 The profile is applied.
 When a message appears asking whether you want to apply the information in the configuration file, click the **Yes** button.

■ By restarting a log file trap

The following describes how to apply the modified information in configuration files by restarting a log file trap.

You cannot apply the modified information in configuration files by restarting a log file trap in the following cases:

- The selected log file trap is not running.
- The selected log file trap is not specified in the log-file trap startup definition file.
- A cluster ID is specified.

To apply the modified information in a configuration file by restarting a log file trap:

1. In the IM Configuration Management window, click the IM Configuration tab. The IM Configuration page is displayed.
2. On the **IM Configuration** page, in the tree area, select the agent to which you want to apply the modified information in a configuration file by restarting a log file trap.
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**.
 This step is unnecessary if exclusive editing rights have already been obtained.
5. In the tree area, select the log file trap name you want to apply, and click the **Configuration File** button.

The **Configuration File** page is displayed.

This step is unnecessary if you are currently editing the profile (configuration file) you want to apply.

6. On the **Configuration File** page, in the node information display area, in the **Saving/application** section, click the following two options.

- **Apply**
- **Restart**

When a message appears asking whether you want to apply the information in the configuration file, click the **Yes** button. The profile is applied.

■ By sending configuration files to agents

The following describes how to apply the modified information in configuration files by sending the configuration files from the manager to agents.

The following are the methods of applying modified information through file transmission:

- Applying the modified information by sending the configuration files collected from agents
- Applying the modified information by sending the configuration files added from IM Configuration Management

IM Configuration Management can collect configuration files from the agents' folders shown in the following. When the collected configuration files are sent, the configuration files are applied to the same folders as those from which they were collected.

Table 3–4: Send destinations for configuration files (when sending the configuration files collected from agents)

Configuration file	Type of OS on agent	Send destination
Log file trap action-definition file	Windows	<i>Base-path</i> \conf
		<i>Base-path</i> \conf\ <i>any-folder</i>
		<i>Base-path</i> \conf\cf_log_file_trap
	UNIX	/etc/opt/jplbase/conf
		/etc/opt/jplbase/conf/ <i>any-directory</i>
		/etc/opt/jplbase/conf/cf_log_file_trap
Log-file trap startup definition file	Windows	<i>Base-path</i> \conf\event\
	UNIX	/etc/opt/jplbase/conf/event/

When the configuration files added from IM Configuration Management are used to apply information, the configuration files are sent to the following folders.

Table 3–5: Send destinations for configuration files (when sending the configuration files added from IM Configuration Management)

Configuration file	Type of OS on agent	Send destination
Log file trap action-definition file	Windows	<i>Base-path</i> \conf\cf_log_file_trap\
	UNIX	/etc/opt/jplbase/conf/cf_log_file_trap/

Configuration file	Type of OS on agent	Send destination
Log-file trap startup definition file	Windows	<i>Base-path</i> \conf\event\
	UNIX	/etc/opt/jp1base/conf/event/

You cannot apply the modified information in configuration files to agents by sending them in the following cases:

- The version of JP1/Base on agents is earlier than 09-10.
- The selected log file trap is running on agents.
- The agent's JP1/Base version is earlier than 11-10 and a cluster ID is not specified.

To apply the modified information in a configuration file by sending a file:

1. In the IM Configuration Management window, click the IM Configuration tab.
The IM Configuration page is displayed.
2. On the **IM Configuration** page, in the tree area, select the agent to which you want to apply the modified information in a configuration file.
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**.

This step is unnecessary if exclusive editing rights have already been obtained.
5. In the tree area, select the applicable log file trap name and click the **Configuration File** button.
The **Configuration File** page is displayed.
This step is unnecessary if you are currently editing the profile (configuration file) you want to apply.
6. On the **Configuration File** page, in the node information display area, in the **Saving/application** section, click the two options below. Then click the **Execute** button.
 - **Apply**
 - **Send a file**

The profile is applied.

When a message appears asking whether you want to apply the information in the configuration file, click the **Yes** button. The configuration file is sent to a preset folder.

(7) Starting or stopping log file traps

You can start or stop log file traps on agents.

(a) Starting log file traps

The following describes how to start log file traps.

You cannot start a log file trap in the following cases:

- The selected log file trap is already running.
- The version of JP1/Base is earlier than 09-10.
- A cluster ID is specified.

To start a log file trap:

1. In the IM Configuration Management window, click the **IM Configuration** tab.
The **IM Configuration** page is displayed.
2. On the **IM Configuration** page, in the tree area, select the agent on which you want to start a log file trap.
3. Use either of the following methods to display the Display/Edit Profiles window:
 - From the menu bar, choose **View**, and then **Display Profiles**.
 - Right-click to display a pop-up menu, and choose **Display Profiles**.
4. In the tree area, select a JP1 product name (JP1/Base), and then use either of the following methods to obtain exclusive editing rights:
 - From the menu bar, choose **Edit**, and then **Exclusive Editing Settings**.
 - Right-click to display a pop-up menu, and choose **Exclusive Editing Settings**.This step is unnecessary if exclusive editing rights have already been obtained.
5. In the tree area, select the applicable log file trap name.
6. Use either of the following methods to start the log file trap:
 - From the menu bar, choose **Operation**, and then **Start Process**.
 - Right-click to display a pop-up menu, and choose **Start Process**.

When a message appears asking whether you want to start the log file trap, click the **Yes** button. The log file trap starts.

(b) Stopping log file traps

The following describes how to stop log file traps.

You cannot stop log file traps in the following cases:

- The version of JP1/Base on agents is earlier than 09-10.
- The selected log file trap is not running.
- A cluster ID is specified.

To stop a log file trap:

1. In the IM Configuration Management window, click the **IM Configuration** tab.
The **IM Configuration** page is displayed.
2. On the **IM Configuration** page, in the tree area, select the agent on which you want to stop a log file trap.
3. Use either of the following methods to display the Display/Edit Profiles window:
 - From the menu bar, choose **View**, and then **Display Profiles**.

- Right-click to display a pop-up menu, and choose **Display Profiles**.
4. In the tree area, select a JP1 product name (JP1/Base), and then use either of the following methods to obtain exclusive editing rights:
- From the menu bar, choose **Edit**, and then **Exclusive Editing Settings**.
 - Right-click to display a pop-up menu, and choose **Exclusive Editing Settings**.

This step is unnecessary if exclusive editing rights have already been obtained.

5. In the tree area, select the applicable log file trap name.
6. Use either of the following methods to stop the log file trap:
- From the menu bar, choose **Operation**, and then **Stop Process**.
 - Right-click to display a pop-up menu, and choose **Stop Process**.

When a message appears asking whether you want to stop the log file trap, click the **Yes** button. The log file trap stops.

(c) Starting or stopping log file traps for cluster systems

If you want to start or stop a log file trap for cluster systems, register the following commands in the cluster software:

- `jevlogstart` command (only for cluster systems)
- `jevlogstop` command (only for cluster systems)

For details, see the description of these commands in the *JP1/Base User's Guide*.

(8) Prerequisites for managing profiles on agents

- When using both profile management by IM Configuration Management and profile management by JP1/Base
The version of JP1/Base on agents must be 11-10 or later.

- When manipulating log file traps

If you want to perform the following operations, the version of JP1/Base on agents must be 09-10 or later:

- *3.5.1(4) Adding or deleting profiles*
- *3.5.1(6)(b) Applying edited information in configuration files individually to each agent*
 - By restarting a log file trap
 - By sending configuration files to agents
- *3.5.1(7) Starting or stopping log file traps*

If the version of JP1/Base on agents is a version before 09-10, perform an overwrite installation of JP1/Base to version 09-10 or later. For details about overwrite installations, see the chapter on installation and setup in the *JP1/Base User's Guide*. To perform an overwrite installation to upgrade JP1/Base version earlier than 09-10 to 09-10 or later, perform the following operations:

- When log file traps are configured to start by using the start sequence definition file or the `jbs_start` command, move the definition of log file traps to the log-file trap startup definition file.
For details, see the cautionary notes on installation and uninstallation in the *JP1/Base User's Guide*.
- Use IM Configuration Management to collect information from agents.
For details, see *3.1.3 Collecting information from hosts*.
- When manipulating profile lists and profiles

If you want to perform the following operations, the version of JP1/Base on agents must be 9 or later.

- Collecting profile lists
- Collecting profiles
- Displaying profiles

If the version of JP1/Base is 9 and an attempt to apply the edited information in the configuration files to agents fails, the modified configuration files are rolled back to the previous configuration files.

- When log file traps are defined

If you upgrade JP1/Base on agents from a version earlier than 09-10 to 09-10 or later and log file traps are configured to start by using the start sequence definition file or the `jobs_start` command, you need to move the definition of log file traps to the log-file trap startup definition file. For details about how to move definitions, see the cautionary notes on installation and uninstallation in the *JP1/Base User's Guide*.

- When starting or stopping log file traps for cluster systems

- The information in the configuration files stored on the standby server must match the information in the configuration files stored on the active server.
- If you change the configuration files on the active server or the standby server, you need to send the modified configuration files to JP1/Base on agents to apply the changes. For details about how to apply changes by sending configuration files, see *By sending configuration files to agents* in 3.5.1(6)(b) *Applying edited information in configuration files individually to each agent*.
- To start or stop log file traps, execute cluster software commands. For details, see 3.5.1(7)(c) *Starting or stopping log file traps for cluster systems*.

3.5.2 Setting the profiles on hosts in a remote monitoring configuration

There are two types of profiles: valid configuration information profiles and configuration file profiles.

- Profiles (Valid configuration information)

Valid configuration information consists of the settings that are currently used by the remote monitoring services. When a service starts successfully, IM Configuration Management collects this information from the hosts in a remote monitoring configuration (hosts that are monitored remotely). You can display collected information as valid configuration information.

- Profiles (configuration files)

The configuration files are stored on the manager running IM Configuration Management. The valid configuration information that IM Configuration Management collects from remotely monitored hosts does not necessarily match the settings in the configuration files. If you edit a configuration file but do not apply the modified information to the remotely managed hosts by reloading the configuration files or restarting remote monitoring log file traps, the valid configuration information and the contents of the configuration files will not match.

The following table describes the types of profiles you can manipulate, the types of operations you can perform on the profiles, and the configuration files that correspond to the profiles.

Table 3–6: Types of profiles and configuration files that correspond to the profiles

Operation	Type of profile you can manipulate	Corresponding configuration file
Add, delete	Remote-monitoring log file trap information	Remote-monitoring log file trap action-definition file
<ul style="list-style-type: none"> • Edit, save 	<ul style="list-style-type: none"> • Remote-monitoring log file trap information 	<ul style="list-style-type: none"> • Remote-monitoring log file trap action-definition file

Operation	Type of profile you can manipulate	Corresponding configuration file
<ul style="list-style-type: none"> Apply in batch mode Apply by reloading configuration files Apply by restarting remote monitoring log file traps 	<ul style="list-style-type: none"> Remote-monitoring event log trap information 	<ul style="list-style-type: none"> Remote-monitoring event log trap action-definition file

The types of traps you can start and stop on remotely monitored hosts are remote-monitoring log file traps and remote-monitoring event log traps.

Application by reloading configuration files is not immediately performed when the JP1/IM - Manager host is connected to a remotely monitored host and is collecting log data from the remote host. In such cases, the reload operation will be performed the next time that log data is collected. While the JP1/IM - Manager host is collecting log data, the operation for applying configuration files by reloading them waits until log data collection finishes. If collection takes time, the reload operation might also take time. If you want to apply profiles immediately, use the application by restarting remote monitoring log file traps method. For details about the prerequisites for setting profiles on remotely monitored hosts, see [3.5.2\(6\) Prerequisites for setting profiles on remotely monitored hosts](#).

(1) Adding or deleting profiles

You can use IM Configuration Management to add profiles to existing profiles stored on the manager running IM Configuration Management or delete profiles from the manager.

(a) Adding profiles

To add a profile:

- In the IM Configuration Management window, click the **IM Configuration** tab.
The **IM Configuration** page is displayed.
- On the **IM Configuration** page, in the tree area, select the remotely monitored host whose profile you want to add to the manager.
- Use either of the following methods to display the Display/Edit Profiles window:
 - From the menu bar, choose **View**, and then **Display Profiles**.
 - Right-click to display a pop-up menu, and choose **Display Profiles**.
- In the tree area, select the profile folder for remote monitoring (**Remote Monitoring**), and then use either of the following methods to obtain exclusive editing rights:
 - From the menu bar, choose **Edit**, and then **Exclusive Editing Settings**.
 - Right-click to display a pop-up menu, and choose **Exclusive Editing Settings**.

This step is unnecessary if exclusive editing rights have already been obtained.
- In the tree area, select **Log File Trapping**.
- Use either of the following methods to display the Add Profile window:
 - From the menu bar, choose **Edit**, and then **Add Profile**.
 - Right-click to display a pop-up menu, and choose **Add Profile**.
- Enter values in the following boxes.
 - Log file trap name**

You cannot specify an existing log file trap name or a name that is the same as the remote-monitoring log file trap action-definition file. Specification of this item is mandatory. For details, see *4.10 Add Profile window* in the manual *JP1/Integrated Management - Manager GUI Reference*. This item is mandatory.

8. Click the **OK** button.

The log file trap name of the added remote-monitoring log file trap appears in the tree area.

For details about how to edit the configuration file for remote-monitoring log file traps, see *3.5.1(5) Editing configuration files*.

When you add the profile of a remote-monitoring log file trap, the log file trap name is displayed in gray in the tree area because the remote-monitoring log file trap is not running yet. For details about how to start remote-monitoring log file traps, see *3.5.2(3) Editing configuration files*.

(b) Deleting profiles

The following describes how to delete profiles.

You cannot delete profiles in the following case:

- The remote-monitoring log file trap corresponding to the selected profile is running.
If the remote-monitoring log file trap is running, stop it. For details about how to stop remote-monitoring log file traps, see *3.5.2(5)(b) Stopping remote-monitoring log file traps*.

To delete a profile:

1. In the IM Configuration Management window, click the **IM Configuration** tab.
The **IM Configuration** page is displayed.
2. On the **IM Configuration** page, in the tree area, select the remotely monitored host whose profile you want to delete from the manager.
3. Use either of the following methods to display the Display/Edit Profiles window:
 - From the menu bar, choose **View**, and then **Display Profiles**.
 - Right-click to display a pop-up menu, and choose **Display Profiles**.
4. In the tree area, select the profile folder for remote monitoring (**Remote Monitoring**), and then use either of the following methods to obtain exclusive editing rights:
 - From the menu bar, choose **Edit**, and then **Exclusive Editing Settings**.
 - Right-click to display a pop-up menu, and choose **Exclusive Editing Settings**.This step is unnecessary if exclusive editing rights have already been obtained.
5. In the tree area, select the log file trap name of the applicable remote monitoring log file trap.
In the tree area, under **Log File Trapping**, a list of the log file trap names of the remote-monitoring log file traps appears. Select the log file trap name you want to delete.
6. Use either of the following methods to delete log file trap name of the profile:
 - From the menu bar, choose **Edit**, and then **Delete Profile**.
 - Right-click to display a pop-up menu, and choose **Delete Profile**.

When a message appears asking whether you want to delete the log file trap name, click the **Yes** button.

The log file trap name is deleted.

(2) Displaying profiles

You can display the profiles stored on the manager running IM Configuration Management using either of two methods according to the information to be displayed. This subsection describes both methods.

(a) Displaying the valid configuration information

To display the valid configuration information of each remotely monitored host:

1. In the IM Configuration Management window, click the **IM Configuration** tab.
The **IM Configuration** page is displayed.
2. On the **IM Configuration** page, in the tree area, select the remotely monitored host whose valid configuration information you want to display.
3. Use either of the following methods to display the Display/Edit Profiles window:
 - From the menu bar, choose **View**, and then **Display Profiles**.
 - Right-click to display a pop-up menu, and choose **Display Profiles**.
4. In the Display/Edit Profiles window, in the tree area, select the item you want to display on the **Valid Configuration Information** page.
5. Click the **Valid Configuration Information** button.

The settings in the valid configuration information that will be displayed depend 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 *4.9.1 Valid Configuration Information page* in the manual *JP1/Integrated Management - Manager GUI Reference*.

(b) Displaying configuration files

The following describes how to display the configuration files of each remotely monitored host. These 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. On the **IM Configuration** page, in the tree area, select the remotely monitored host whose configuration files you want to display.
3. Use either of the following methods to display the Display/Edit Profiles window:
 - From the menu bar, choose **View**, and then **Display Profiles**.
 - Right-click to display a pop-up menu, and choose **Display Profiles**.
4. In the Display/Edit Profiles window, in the tree area, select an item you want to display on the **Configuration File** page.
5. Click the **Configuration File** button.

The settings in the configuration file that are displayed depend on the item selected in the tree area of the Display/Edit Profiles window. For details, see *4.9.2 Configuration File page* in the manual *JP1/Integrated Management - Manager GUI Reference*.

Whether the information displayed on the **Configuration File** page can be edited depends on the item.

(3) Editing configuration files

The following describes how to edit and save the configuration files collected by the manager running IM Configuration Management. You can use the Display/Edit Profiles window to edit and save a configuration file.

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. On the **IM Configuration** page, in the tree area, select the remotely monitored host whose configuration file you want to edit.
3. Use either of the following methods to display the Display/Edit Profiles window:
 - From the menu bar, choose **View**, and then **Display Profiles**.
 - Right-click to display a pop-up menu, and choose **Display Profiles**.
4. In the tree area, select the profile folder for remote monitoring (**Remote Monitoring**), and then use either of the following methods to obtain exclusive editing rights:
If you intend to cut or paste the character strings in a configuration file, make sure that you obtain exclusive editing rights first.
 - From the menu bar, choose **Edit**, and then **Exclusive Editing Settings**.
 - Right-click to display a pop-up menu, and choose **Exclusive Editing Settings**.This step is unnecessary if exclusive editing rights have already been obtained or you are copying only the character strings in a configuration file.
5. In the Display/Edit Profiles window, in the tree area, select the configuration file you want to edit.
6. In the Display/Edit Profiles window, in the node information display area, click the **Configuration File** button.
The contents of the selected configuration file that is stored on the manager running IM Configuration Management appear. For details about the items that can be edited, see *4.9.2 Configuration File page* in the manual *JP1/Integrated Management - Manager GUI Reference* and *Remote-monitoring log file-trap action definition file* and *Remote-monitoring event log trap action-definition file* in *Chapter 2. Definition Files* in the manual *JP1/Integrated Management - Manager Command and Definition File 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 on the manager running IM Configuration Management.

(4) Applying edited information in configuration files

After you edit a configuration file on the manager, you can apply the new information to all the remote hosts in batch mode or to each remote host individually.

After applying a configuration file, you can check whether the operation was successful on the **Configuration File** page in the Display/Edit Profiles window. If it was successful, **Application status** is **Applied**. If the configuration file could not be applied, **Application status** is **Application failed**. If the configuration files stored on the manager are not used, **Application status** is blank (not applied). If configuration files are stored on the manager but not used on the target host, **Application status** is **Saved on the server**.

When **Application status** is **Application failed** or **Saved on the server**, the icon displayed in the tree area on the **Configuration File** page indicates the configuration file is being edited.

After applying a configuration file, you can check the status of the remotely monitored host on the **IM Configuration** page in the IM Configuration Management window. If **Application status** of any of the configuration files is **Application failed** or **Saved on the server** on the **Configuration File** page, the host icon in the tree area of the **IM Configuration** page indicates an error. To view the details, click the **Basic Information** button in the node information display area on the **IM Configuration** page.

(a) Using batch mode to apply edited information in configuration files

The following describes how to batch-apply the modified information in configuration files to all the remotely monitored hosts registered in a system hierarchy.

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 application of edited information in configuration files.
- JP1/IM - Manager is not running.
- There are no monitored hosts in the remote monitoring configuration.
- Host information about remotely monitored hosts has not been collected yet.
- The OS of the JP1/IM - Manager host and the OS of the remotely monitored hosts are Windows, WMI is used to monitor event logs, and DCOM is not configured.
- No event log trap is running.

The following describes how to use batch mode to apply edited information in configuration files.

■ Configuration files for remote-monitoring log file traps

1. Execute the `jcfallogdef` command to overwrite the configuration files for the currently running remote-monitoring log file traps.

The configuration files for the currently running remote-monitoring log file traps are overwritten.

2. Execute the `jcfallogreload` command to batch-reload the configuration files.

The configuration files for remote-monitoring log file traps are reloaded in batch mode.

■ Configuration files for remote-monitoring event log traps

1. Execute the `jcfaleltdf` command to overwrite the configuration files for the currently running remote-monitoring event log traps.

This command can be executed when the OS of the JP1/IM - Manager host is Windows.

The configuration files for the currently running remote-monitoring event log traps are overwritten.

2. Execute the `jcfaleltrreload` command to batch-reload the configuration files.

This command can be executed when the OS of the JP1/IM - Manager host is Windows.

The configuration files for remote-monitoring event log traps are reloaded in batch mode.

(b) Applying edited information in configuration files individually to each remotely monitored host

Two methods are available for applying the modified information in configuration files to each remotely monitored host.

■ By reloading

You can reload configuration files onto a remotely monitored host to apply the modified information in the configuration files.

You cannot apply the modified information in configuration files by reloading in the following case:

- The selected remote-monitoring log file trap is not running when you attempt to apply the profile of a remote-monitoring log file trap.

To apply the modified information in a configuration file by reloading the configuration file:

1. In the IM Configuration Management window, click the **IM Configuration** tab.
The **IM Configuration** page is displayed.
2. On the **IM Configuration** page, in the tree area, select the remotely monitored host to which you want to apply the modified information in a configuration file by reloading the file.
3. Use either of the following methods to display the Display/Edit Profiles window:
 - From the menu bar, choose **View**, and then **Display Profiles**.
 - Right-click to display a pop-up menu, and choose **Display Profiles**.
4. In the tree area, select the profile folder for remote monitoring (**Remote Monitoring**), and then use either of the following methods to obtain exclusive editing rights:
 - From the menu bar, choose **Edit**, and then **Exclusive Editing Settings**.
 - Right-click to display a pop-up menu, and choose **Exclusive Editing Settings**.This step is unnecessary if exclusive editing rights have already been obtained.
5. In the tree area, select the profile you want to apply, and then click the **Configuration File** button.
The **Configuration File** page is displayed.
This step is unnecessary if you are currently editing the profile (configuration file) you want to apply.
6. On the **Configuration File** page, in the node information display area, in the **Saving/application** section, click the two options below. Then click the **Execute** button.

- **Apply**
- **Reload**

When a message appears asking whether you want to apply the information in the configuration file, click the **Yes** button. The profile is applied.

■ By restarting a remote-monitoring log file trap

The following describes how to apply the modified information in configuration files by restarting a remote monitoring log file trap.

You cannot apply the modified information in configuration files by restarting a remote monitoring log file trap in the following cases:

- The selected remote-monitoring log file trap is not running.
- The selected remote-monitoring log file trap is not specified in the remote-monitoring log file trap startup-definition file.

To apply the modified information in a configuration file by restarting a remote-monitoring log file trap:

1. In the IM Configuration Management window, click the **IM Configuration** tab.
The **IM Configuration** page is displayed.
2. On the **IM Configuration** page, in the tree area, select the remotely monitored host to which you want to apply the modified information in a configuration file by restarting a remote monitoring log file trap.
3. Use either of the following methods to display the Display/Edit Profiles window:
 - From the menu bar, choose **View**, and then **Display Profiles**.
 - Right-click to display a pop-up menu, and choose **Display Profiles**.
4. In the tree area, select the profile folder for remote monitoring (**Remote Monitoring**), and then use either of the following methods to obtain exclusive editing rights:
 - From the menu bar, choose **Edit**, and then **Exclusive Editing Settings**.
 - Right-click to display a pop-up menu, and choose **Exclusive Editing Settings**.

This step is unnecessary if exclusive editing rights have already been obtained.
5. In the tree area, select the name of the remote-monitoring log file trap name you want to apply, and click the **Configuration File** button.
The **Configuration File** page is displayed.
This step is unnecessary if you are currently editing the profile (configuration file) you want to apply.
6. On the **Configuration File** page, in the node information display area, in the **Saving/application** section, click the two options below. Then click the **Execute** button.
 - **Apply**
 - **Restart**

When a message appears asking whether you want to apply the information in the configuration file, click the **Yes** button. The profile is applied.

(5) Starting or stopping remote-monitoring log file traps

You can start or stop remote-monitoring log file traps on remotely monitored hosts.

(a) Starting remote-monitoring log file traps

The following describes how to start remote-monitoring log file traps.

Note that a log-file trap startup definition file is not provided by default and cannot be created or distributed independently. A log-file trap startup definition file is created or updated simultaneously with other setting files in the following cases:

- Edited information in a setting file is applied by restarting a log file trap.
- Edited information in a setting file is applied by sending the setting file.
- A log file trap is started.

- A log file trap is stopped.

You cannot start remote-monitoring log file traps in the following case:

- The selected remote-monitoring log file trap is already running.

To start a remote-monitoring log file trap:

1. In the IM Configuration Management window, click the **IM Configuration** tab.
The **IM Configuration** page is displayed.
2. On the **IM Configuration** page, in the tree area, select the remotely monitored host on which you want to start a remote-monitoring log file trap.
3. Use either of the following methods to display the Display/Edit Profiles window:
 - From the menu bar, choose **View**, and then **Display Profiles**.
 - Right-click to display a pop-up menu, and choose **Display Profiles**.
4. In the tree area, select the profile folder for remote monitoring (**Remote Monitoring**), and then use either of the following methods to obtain exclusive editing rights:
 - From the menu bar, choose **Edit**, and then **Exclusive Editing Settings**.
 - Right-click to display a pop-up menu, and choose **Exclusive Editing Settings**.This step is unnecessary if exclusive editing rights have already been obtained.
5. In the tree area, select the log file trap name of the remote-monitoring log file trap you want to start.
6. Use either of the following methods to start the remote-monitoring log file trap:
 - From the menu bar, choose **Operation**, and then **Start Process**.
 - Right-click to display a pop-up menu, and choose **Start Process**.

When a message appears asking whether you want to start the remote-monitoring log file trap, click the **Yes** button. The remote-monitoring log file trap starts.

(b) Stopping remote-monitoring log file traps

The following describes how to stop remote-monitoring log file traps.

You cannot stop remote-monitoring log file traps in the following case:

- The selected remote-monitoring log file trap is not running.

To stop a remote-monitoring log file trap:

1. In the IM Configuration Management window, click the **IM Configuration** tab.
The **IM Configuration** page is displayed.
2. On the **IM Configuration** page, in the tree area, select the remotely monitored host on which you want to stop a remote-monitoring log file trap.
3. Use either of the following methods to display the Display/Edit Profiles window:
 - From the menu bar, choose **View**, and then **Display Profiles**.
 - Right-click to display a pop-up menu, and choose **Display Profiles**.

4. In the tree area, select the profile folder for remote monitoring (**Remote Monitoring**), and then use either of the following methods to obtain exclusive editing rights:

- From the menu bar, choose **Edit**, and then **Exclusive Editing Settings**.
- Right-click to display a pop-up menu, and choose **Exclusive Editing Settings**.

This step is unnecessary if exclusive editing rights have already been obtained.

5. In the tree area, select the log file trap name of the remote-monitoring log file trap you want to stop.

6. Use either of the following methods to stop the remote monitoring log file trap:

- From the menu bar, choose **Operation**, and then **Stop Process**.
- Right-click to display a pop-up menu, and choose **Stop Process**.

When a message appears asking whether you want to stop the remote-monitoring log file trap, click the **Yes** button. The remote-monitoring log file trap stops.

(6) Prerequisites for setting profiles on remotely monitored hosts

If you want to use IM Configuration Management to set the profiles on remotely monitored hosts, the version of JP1/Base on the manager running IM Configuration Management must be 09-50 or later.

3.6 Importing and exporting the management information in IM Configuration Management

This section describes how to set the system hierarchy (IM configuration) by exporting and importing the information managed by IM Configuration Management when a JP1/IM system is configured.

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 *6.8 Exporting and importing IM Configuration Management information* in the *JP1/Integrated Management - Manager Overview and System Design Guide*.

For details about the export procedure, see *8.7.1 Exporting management information of IM Configuration Management* in the *JP1/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 system is running, execute the `jcfimport` command to import the management information for IM Configuration Management that was exported.

For details about the import function, see *6.8 Exporting and importing IM Configuration Management information* in the *JP1/Integrated Management - Manager Overview and System Design Guide*.

For details about the import procedure, see *8.7.2 Importing management information of IM Configuration Management* in the *JP1/Integrated Management - Manager Administration Guide*.

4. Apply the system hierarchy to the system that is being run and managed by JP1/IM.

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 *3.2.4(3) Applying a system hierarchy to a system managed by IM Configuration Management*.

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

You can specify settings for operations to be performed when JP1/IM - Manager acquires JP1 events that are registered in Event Service, such as setting event acquisition filter conditions, setting the buffer size, and the range of events to be acquired from the integrated monitoring database at login when JP1 events are buffered in the manager's memory.

Normally, you can use the default settings, but you can 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
- Setting the range of events to be acquired at login

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 *JP1/Integrated Management - Manager GUI Reference*.

Important

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 might not function correctly.

4.1.1 Displaying events by specifying the event acquisition range at login

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

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

To specify the event acquisition range:

1. From the menu in the Event Console window, select **Options**, and then **System Environment Settings**.
The System Environment Settings window appears.
2. On the **Display** tab, select the **Enable the Monitor Events page** or **Enable the Severe Events page** check box.
Range of events to be collected is activated.
3. Specify **day(s)** and **Base time**, or **hours**.
For **Base time**, you can specify the time that separates days in the range from 00:00 to 23:59. By default, the base time is 09:00.



Note

The display range of events depends on whether base time or current time is larger on the host on which Central Console is running at login. The following shows the display range of JP1 events for both cases:

- When the current time on the host on which Central Console is running at login is larger than the base time of the current day:
The base time of the day calculated by $(current-day - (set-number-of-days - 1))$ is set for the event acquisition start location.
- When the current time on the host on which Central Console is running at login is smaller than the base time of the current day:
The base time of the day calculated by $(current-day - set-number-of-days)$ is set for the event acquisition start location.

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

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

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

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

4. Click the **OK** button.

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

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

For details about the event acquisition range at login, see *3.17 Range of events to be collected at login* in the *JP1/Integrated Management - Manager Overview and System Design Guide*.

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 or the **Severe 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 or the **Severe 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 set are as follows: **Event source host name**^{#1}, **Source host**, **Event level**, **Object type**, **Object name**, **Root object type**, **Root object name**, **Occurrence**, **User name**, **Message**, **Product name**, **Event ID**, **Response status**, **Action**^{#2}, and program-specific extended attributes.

If you are using the integrated monitoring database, you can also set the following items: **Memo**^{#3}, **New severity level**^{#4}, **Original severity level**^{#4}, **New display message**^{#5}, **Changed display message**^{#5}, **Repeated events**^{#6}, and **Suppressed event ID**^{#6}.

#1: This item can be set if the mapping of the event source host is enabled.

#2: If linkage with JP1/IM - Rule Operation is enabled, you can specify an action type as a condition.

#3: This item can be set if the memo function is enabled.

#4: This item can be set if the severity changing function is enabled.

#5: This item can be set if the display message change function is enabled.

#6: This item can be set if the repeated event monitoring suppression function is enabled.

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.

If the repeated event monitoring suppression function is enabled, the **Read Suppressed Event ID From Selected Event** button appears. To apply the suppressed event ID of the repeated event selected in the Event Console window to **Suppressed event ID** in the conditions list, click this button. For the repeated events that are consolidated into a single consolidation event, the same suppressed event ID is assigned. Therefore, you can filter the repeated events that are consolidated into a single consolidation event (the repeated events that has the same suppressed event ID as the selected repeated event).

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, or the **Severe 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.

To apply the suppressed event ID of the repeated event selected in the Event Console window to **Suppressed event ID** in the conditions list, click the **Read Suppressed Event ID From Selected Event** button. For the repeated events that are consolidated into a single consolidation event, the same suppressed event ID is assigned. Therefore, you can filter the repeated events that are related to the selected repeated event.

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` permission. If reference and operation restrictions are set on business groups, you might not be able to set event receiver filters depending on the combinations of JP1 resource groups and JP1 permission levels. For details, see *3.1.4(2) Assigning a JP1 resource group and permission level to a JP1 user* in the *JP1/Integrated Management - Manager Overview and System Design Guide*.

(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, action status, and program-specific extended attributes. If you enable event source host mapping, you can also specify event source host name.
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` permission.

If reference and operation restrictions are set on business groups, you might not be able to set severe events filters depending on the combinations of JP1 resource groups and JP1 permission levels. For details, see *3.1.4(2) Assigning a JP1 resource group and permission level to a JP1 user* in the *JP1/Integrated Management - Manager Overview and System Design Guide*.

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, event level, object type, object name, root object type, root object name, occurrence, user name, message, product name, event ID, action status, and program-specific extended attributes. If you enable event source host mapping, you can also specify event source host name.

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.

Important

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 describes how to set only one event acquisition filter and how to set an event acquisition filter by switching the filter conditions. Event acquisition filters are set regardless of whether the integrated monitoring database is being used.

The event acquisition filters described here are used to limit the JP1 events that will be distributed to all the services of JP1/IM - Manager.

For details about how to set an event acquisition filter (for compatibility), see [4.2.4\(4\) Setting an event acquisition filter \(for compatibility\)](#).

(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. In order to start the System Environment Settings window, you need JP1_Console_Admin permission.

If reference and operation restrictions are set on business groups, you might not be able to set the event acquisition filter depending on the combinations of JP1 resource groups and JP1 permission levels. For details, see [3.1.4\(2\) Assigning a JP1 resource group and permission level to a JP1 user](#) in the *JP1/Integrated Management - Manager Overview and System Design Guide*.

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.

In order to start the System Environment Settings window, you need `JP1_Console_Admin` permission. If reference and operation restrictions are set on business groups, you might not be able to set event acquisition filters depending on the combinations of JP1 resource groups and JP1 permission levels. For details, see *3.1.4(2) Assigning a JP1 resource group and permission level to a JP1 user* in the *JP1/Integrated Management - Manager Overview and System Design Guide*.

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 common exclusion-conditions

This subsection explains how to set common exclusion-conditions to temporarily exclude JP1 events that are issued by a host undergoing maintenance from the acquisition target or automated-action execution. Two operating modes are available for common exclusion-conditions: basic mode and extended mode. Use the `jcochcefmode` command to switch between basic and extended as the operating mode. You must use extended mode if you want to use common exclusion-conditions to exclude JP1 events from automated-action execution.

To set common exclusion-conditions, for basic mode, use the Common Exclusion-Conditions Settings window. For extended mode, use the Common Exclusion-Condition Settings (Extended) window. For extended mode, you can also use the common-exclusion-conditions extended definition file and the `jcochfilter` command with the `-ef` option to set common exclusion-conditions. For details about how to enable or disable common exclusion-conditions, see [5.5.3 Switching the event acquisition filter to be applied](#) in the *JP1/Integrated Management - Manager Administration Guide*.

In extended mode, you can register a common exclusion-condition by selecting and right-clicking a JP1 event that you do not want to monitor in the Event Console window and choosing **Exclude by Common Exclusion-Conditions** from the pop-up menu.

The registered common exclusion-condition is displayed in the System Environment Settings window as an additional common exclusion-condition. If you are in basic mode and you want to register a common exclusion-condition from the Event Console window, see [4.2.4\(3\)\(a\) Switching between common exclusion-conditions basic mode and extended mode](#) and switch to extended mode. Then add a common exclusion-condition. For details about how to add common exclusion-conditions, see [5.5.4 Setting an additional common exclusion-condition to exclude a JP1 event from the monitoring target or action execution](#) in the *JP1/Integrated Management - Manager Administration Guide*.

The method of editing an additional common exclusion-condition is the same as that of editing a common exclusion-condition. See [4.2.4\(3\)\(b\) Setting common exclusion-conditions \(by using the Common Exclusion-Conditions Settings window or the Common Exclusion-Condition Settings \(Extended\) window\)](#) to edit an additional common exclusion-condition.

(a) Switching between common exclusion-conditions basic mode and extended mode

To switch the common exclusion-conditions operating mode:

1. Stop JP1/IM - Manager.
2. When you change the common exclusion-conditions operating mode from basic mode to extended mode, change the regular expressions of JP1/Base to extended regular expressions.
For details about extended regular expressions, see the explanation of how to extend regular expressions in the *JP1/Base User's Guide*.
If you changed the common exclusion-conditions operating mode from extended mode to basic mode, go to step 3.
3. Execute either of the following commands:
 - To switch from basic mode to extended mode:
`jcochcefmode -m extended`
 - To switch from extended mode to basic mode:
`jcochcefmode -m normal`The common exclusion-conditions operating mode is changed.
4. Start JP1/IM - Manager.

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

(b) Setting common exclusion-conditions (by using the Common Exclusion-Conditions Settings window or the Common Exclusion-Condition Settings (Extended) window)

The following describes how to use the Common Exclusion-Conditions Settings window (for basic mode) or the Common Exclusion-Condition Settings (Extended) window (for extended mode) to set common exclusion-conditions.

In order to start the System Environment Settings window, you need `JP1_Console_Admin` permission. If reference and operation restrictions are set on business groups, you might not be able to set common exclusion-conditions depending on the combinations of JP1 resource groups and JP1 permission levels. For details, see *3.1.4(2) Assigning a JP1 resource group and permission level to a JP1 user* in the *JP1/Integrated Management - Manager Overview and System Design Guide*.

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. For basic mode, you can specify a maximum of 30 common exclusion-conditions groups. For extended mode, you

can specify a maximum of 2,500 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.

When you edit an additional common exclusion-condition, you cannot specify a common exclusion-conditions group ID.

- 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.

- Target for exclusion (only in the Common Exclusion-Condition Settings (Extended) window)

Specify the exclusion target of the common exclusion-conditions group (extended).

Select **Do not acquire events** to prevent a JP1 event from being acquired when the event satisfies the common exclusion-condition. Select **Acquire events but do not execute automatic actions** to exclude a JP1 event from automated-action execution when the event satisfies the common exclusion-condition.

- 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.

You can select the following attributes.

For basic mode

Source host, Event level (or JP1/SES event), Object type, Object name, Root object type, Root object name, Occurrence, User name, Message, Product name, and Event ID

For extended mode

Event ID, Registered reason, Source process ID, Registered time, Arrived time, Source user ID, Source group ID, Source user name, Source group name, Source host, Source IP address, Message, Event level, User name, Product name, Object type, Object name, Root object type, Root object name, Object ID, Occurrence, Start time, End time, Return code, Event source host name, and Extended attribute

Note that **Event level** is displayed as **Original severity level** when the severity changing function is enabled.

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 boxes under **Apply**.

7. Click the **Apply** button.

The specified settings take effect.

For details about the System Environment Settings window, the Common Exclusion-Conditions Settings window, and the Common Exclusion-Condition Settings (Extended) window, see the following sections in the manual *JP1/Integrated Management - Manager GUI Reference*:

- System Environment Settings window
See *2.11 System Environment Settings window*.
- Common Exclusion-Conditions Settings window
See *2.15 Common Exclusion-Conditions Settings window*.
- Common Exclusion-Condition Settings (Extended) window
See *2.16 Common Exclusion-Condition Settings (Extended) window*.

(c) Setting common exclusion-conditions (by using the common-exclusion-conditions extended definition file and the `jcochfilter` command)

For extended mode, you can use the common-exclusion-conditions extended definition file and the `jcochfilter` command with the `-ef` option to set common exclusion-conditions. For details of the setting method, see below.

1. In the common-exclusion-conditions extended definition file, define condition groups.
2. Execute the `jcochfilter` command to batch-apply the defined condition groups.

Enter the command as follows:

```
jcochfilter -ef name-of-common-exclusion-conditions-extended-definition-file
```

For details about the common-exclusion-conditions extended definition file, see *Common-exclusion-conditions extended definition file* in *Chapter 2. Definition Files* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

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

(4) Setting an event acquisition filter (for compatibility)

The following describes how to set the filter conditions when Event Console Service obtains events from Event Base Service. Note that the procedure described here can only be performed when event acquisition filters (for compatibility) are used.

If you set an event acquisition filter (for compatibility), it is used even when the integrated monitoring database is being used.

The procedure is described below. In order to start the System Environment Settings window, you need `JP1_Console_Admin` permission. If reference and operation restrictions are set on business groups, you might not be able to set event acquisition filters (for compatibility) depending on the combinations of JP1 resource groups and

JP1 permission levels. For details, see *3.1.4(2) Assigning a JP1 resource group and permission level to a JP1 user in the JP1/Integrated Management - Manager Overview and System Design Guide*.

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

The System Environment Settings window appears.

2. In the System Environment Settings window, in the **Event acquisition conditions** section, at the right of the drop-down list, click the **Configure** button.

The Event Acquisition Settings window (for compatibility) appears.

3. Set the filter conditions for obtaining events from Event Base Service.

If you want to display JP1/SES events in the Event Console window, in the Event Acquisition Settings window (for compatibility), in the **JP1/SES events** section, select the **Acquire** check box.

If you want to specify the event levels of JP1 events, in the Event Acquisition Settings window (for compatibility), select the **Event level** check box. Then select desired levels from **Emergency, Alert, Critical, Error, Warning, Notice, Information, and Debug**. If the **Event level** check box is not selected, all the events defined with event levels will be obtained.

If you want to specify an event ID, in the Event Acquisition Settings window (for compatibility), select the **Event ID** check box and then specify the ID of a JP1 event. If you want to specify multiple event IDs, separate them by using a comma.

The conditions that are specified here are passed to Event Base Service as an AND relationship of JP1/SES event and event ID or an AND relationship of event level and event ID.

4. Click the **OK** button.

The System Environment Settings window returns.

5. Click the **Apply** button.

The specified settings take effect.

4.3 Setting monitoring of repeated events to be prevented

This subsection describes the procedure for preventing monitoring of repeated events. You can prevent monitoring of repeated events when you are using an integrated monitoring database. For details about how to set up an integrated monitoring database, see the following section:

- For Windows
1.4.2 Setting up the integrated monitoring database (for Windows)
- For UNIX
2.4.2 Setting up the integrated monitoring database (for UNIX)

Note that when you enable prevention of monitoring of repeated events, consolidated display of repeated events is disabled.

1. Enable prevention of monitoring of repeated events.

Execute `jcoimdef -storm ON`.

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

2. Restart JP1/IM - Manager.

3. Restart JP1/IM - View.

Monitoring of repeated events is now prevented.

4.4 Setting the display colors of JP1 events

You can specify the display colors of the events that will be displayed in the list of events for each event level. To do so, specify the display colors in the system color definition file, and then enable the colors for each user in the Preferences window. Note that you can specify event display colors only for the system, not for individual users.

To specify display colors for JP1 events:

1. Edit the system color definition file (`systemColor.conf`).

For details about the definitions in the system color definition file, see *System color definition file (systemColor.conf)* in *Chapter 2. Definition Files* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

2. In the Event Console window, choose **Options**, and then **User Preferences**.

The Preferences window appears.

For details about the Preferences window, see *2.24 Preferences window* in the manual *JP1/Integrated Management - Manager GUI Reference*.

3. In the **Coloring** section, select the **Enable** check box. If you want to set the display color for the **Severe Events** page, enable the **Include the Severe Events page** radio button.

4. Click the **OK** button.

The specified settings take effect.

4.5 Setting automated actions

This section describes the settings for using the automated action function.

4.5.1 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.update`). 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 *Chapter 2. Definition Files* in the manual *JPI/Integrated Management - Manager Command and Definition File Reference*.

2. Terminate JPI/IM - Manager.
3. Execute the `jbssetcnf` command to apply the definitions.

In Windows:

```
jbssetcnf Console-path\conf\action.conf
```

In UNIX:

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

When you execute the `jbssetcnf` command, the execution environment settings for the automated action function are applied to the JPI common definition information. For details about the `jbssetcnf` command, see the *JPI/Base User's Guide*.

4. Start JPI/IM - Manager.

4.5.2 Setting the execution conditions and details of automated actions

You can use the GUI of JPI/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 11-10 or earlier, you must update the definition file.

For details about the updating procedure, see [1.18.3\(2\) 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 11-10 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. To disable existing automated action conditions, clear the **Apply** check boxes for them.

4. Click the **Apply** button.

The specified settings take effect.

For details about the Action Parameter Definitions window, see [2.32 Action Parameter Definitions window](#) in the manual *JP1/Integrated Management - Manager GUI Reference*.

For details about the Action Parameter Detailed Definitions window, see [2.33.1 Action Parameter Detailed Definitions window](#) in the manual *JP1/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	For a physical host: <code>Console-path\conf\action\</code>

OS	Storage location
	For a logical host: <i>shared-folder\jplcons\conf\action\</i>
UNIX	For a physical host: <i>/etc/opt/jplcons/conf/action/</i>
	For a logical host: <i>shared-directory/jplcons/conf/action/</i>

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 `jchange` 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 Chapter 2. *Definition Files* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

4.5.3 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:

- *2.32 Action Parameter Definitions window* in the manual *JP1/Integrated Management - Manager GUI Reference*
- *2.33.1 Action Parameter Detailed Definitions window* in the manual *JP1/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 Chapter 2. *Definition Files* in the manual *JP1/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 *Chapter 2. Definition Files* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

4.5.4 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 *2.33.1 Action Parameter Detailed Definitions window* in the manual *JP1/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 *Chapter 2. Definition Files* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

4.5.5 Setting email transmissions

To specify the settings for using the email notification function of JP1/IM - Manager:

1. Configure the communication environment.

- Name resolution of the mail server host

Configure one of the files below so that the host name of the SMTP server name and POP3 server name can be resolved.

The files are referenced in the following order:

- The `jp1hosts` file in JP1/Base on the manager host
- The `jp1hosts2` file in JP1/Base on the manager host
- The `hosts` file or DNS

You can use only an IPv4 address to specify the IP address of the mail server.

- Firewall settings

Set the firewall passage direction to allow the `jimmail` command and the mail server to perform SMTP/POP3 communication.

For details about the firewall settings, see *8.3.1 Basic information about firewalls*.

2. Define a notification email.

Define the command line of the `jimmail` command to create a notification email.

An example of defining a notification email in automated action is shown below:

```
jimmail.exe -to user@hitachi.com -s "[severity:$EVSEV] Error occurrence
notice" -b "An error occurred in the business server.\n---\n Serial
number=$EVSEQNO\n Occurrence date/time=$EVDATE $EVTIME\n Event ID=
$EVIDBASE\n Severity=$EVSEV\n Product name=$EV"PRODUCT_NAME"\n Message=
$EVMSG\n---\nFrom:IM-M Host ($ACTHOST) "
```

For details about the `jimmail` command, see *jimmail (Windows only)* in *Chapter 1. Commands* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

3. Open the email environment definition file by using a text editor.

- For a physical host:
`console-path\conf\mail\jimmail.conf`
- For a logical host:
`shared-folder\JP1Cons\conf\mail\jimmail.conf`

4. Set the items shown in the following table in the email environment definition file:

Parameter name	Setting item	Necessity to set	Description
Charset	Character set of email	N	The following is an example of character sets that can be specified: <ul style="list-style-type: none"> • iso-2022-jp • shift_jis • euc-jp • utf-8 • iso-8859-1 • us-ascii • GB18030 The default value is iso-8859-1.
From	Transmission-source email address	Y	Specify one address in the range from 1 to 256 bytes. Usable characters are: <ul style="list-style-type: none"> • 0-9, a-z (single-byte alphanumeric character) • @ (at sign) • . (period) • - (hyphen) • _ (underscore)
DefaultTo	Default transmission-destination email address	N	Specify the default email address to which an email is transmitted. If the <code>-to</code> option is specified in the <code>jimmail</code> command, the <code>-to</code> option has priority.
SmtServer	SMTP server host name	Y	Specify the host name or IP address of the SMTP server to be connected at email transmission. Only IPv4 is

Parameter name	Setting item	Necessity to set	Description
			supported. Multiple SMTP servers cannot be specified.
SmtPort	SMTP port number	N	Specify the port number of a communication port of the SMTP server. This item is only enabled when NONE or POP is specified in AuthMethod. The default value is 25.
AuthMethod	Authentication method at email transmission	Y	Specify the authentication method at email transmission. <ul style="list-style-type: none"> NONE: No authentication POP: POP-before-SMTP authentication SMTP: SMTP-AUTH authentication (LOGIN/PLAIN) The default value is NONE.
SmtAuthPort	Submission port number for SMTP-AUTH authentication	N	Specify the submission port number of a communication port for SMTP-AUTH authentication. This item is enabled only when SMTP is specified in AuthMethod. Specify a value in the range from 1 to 65535. The default value is 587.
Pop3Server	POP3 server host name	N	This item is needed for POP-before-SMTP authentication. Specify the host name or IP address of the POP3 server to be used for POP-before-SMTP authentication. Only IPv4 is supported. Multiple values cannot be specified.
Pop3Port	POP3 port number	N	Specify the port number of a communication port of the POP3 server to be used for POP-before-SMTP authentication. Specify a value in the range from 1 to 65535. The default value is 110.
AuthUser	Authentication account name	N	Specify an authentication account name to be used for POP-before-SMTP authentication or SMTP-AUTH authentication. Specify single-byte characters in the range from 1 to 255 bytes.
AuthPassword	Authentication password	N	The value that is set by the jimmailpasswd command

Parameter name	Setting item	Necessity to set	Description
			in step 5 is encrypted and set in this item.
ConnectTimeout	Network connection timeout time	N	Specify a timeout time for the wait for the SMTP and POP3 servers to complete a connection. Specify the timeout time with a value in the range from 1,000 to 3,600,000 (milliseconds). The default value is 10,000 (milliseconds) (10 seconds).
SoTimeout	Communication timeout time	N	Specify a timeout time until a response from the SMTP and POP3 servers is received with a value in the range from 1,000 to 3,600,000 (milliseconds). The default value is 10,000 (milliseconds) (10 seconds).
MailSubjectCutting	Mail subject cutting setting	N	Specify whether to cut the subject of an email and forcibly transmit the email if its subject exceeds the maximum length at email transmission. <ul style="list-style-type: none"> • OFF: The subject is not cut and an abnormal termination occurs. • ON: The subject is cut at 512 bytes and the email is transmitted. The default value is OFF.
MailNewLine	Line feed code of email	N	Specify a line feed code to be used in the email body. <ul style="list-style-type: none"> • CRLF: CR (0x0d) + LF (0x0A) • LF: LF (0x0A) • CR: CR (0x0d) The default value is CRLF.

Legend:

Y: Required

N: Optional

For details about the email environment definition file, see *Email environment definition file (jimmail.conf)* in *Chapter 2. Definition Files* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

5. Set the authentication password by using the `jimmailpasswd` command.

If the authentication method at email transmission that is set in the email environment definition file is POP-before-SMTP authentication or SMTP-AUTH authentication, set the POP3 authentication password or SMTP authentication password in the email environment definition file.

For details about the `jimmailpasswd` command, see *jimmailpasswd (Windows only)* in *Chapter 1. Commands* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

6. Perform an email transmission test.

Perform an email transmission test by executing the `jimmail` command to confirm whether the email transmission environment is correctly set. Transmit a test email on the command prompt and confirm that the `jimmail` command is terminated normally and the transmission-destination user can receive the email.

An example of transmitting an email to `user@hitachi.com` is shown below:

```
$ jimmail -to user@hitachi.com -s IMTestMail -b IMTestMail
```

4.6 Settings for generating correlation events

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

4.6.1 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 *Chapter 1. Commands* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

4.6.2 Setting the size and number of correlation event generation history files

This subsection describes 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 *Chapter 2. Definition Files* in the manual *JP1/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	For a physical host: <i>Console-path\default\</i>
	For a logical host: <i>shared-folder\jplcons\default\</i>
UNIX	For a physical host: <i>/etc/opt/jplcons/default/</i>
	For a logical host: <i>shared-directory/jplcons/default/</i>

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 *JP1/Base User's 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 *Chapter 1. Commands* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

4.6.3 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 *Chapter 2. Definition Files* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

2. 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 *Chapter 1. Commands* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

4.6.4 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 Chapter 2. *Definition Files* in the manual *JP1/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	For a physical host: <code>Console-path\conf\evgen\define\</code>
	For a logical host: <code>shared-folder\jplcons\conf\evgen\define\</code>
UNIX	For a physical host: <code>/etc/opt/jplcons/conf/evgen/define/</code>
	For a logical host: <code>shared-directory/jplcons/conf/evgen/define/</code>

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.

2. Execute the `jcoegscheck` command to check for errors in the correlation event generation definition.

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

3. 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 Chapter 1. *Commands* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

4.7 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` permission. 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 *2.24 Preferences window* in the manual *JP1/Integrated Management - Manager GUI Reference*.

For details about how to edit memo entries, see *5.2.1 Editing JP1 memo entries* in the *JP1/Integrated Management - Manager Administration Guide*.

4.8 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 might 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 3.10 *Event guide function* in the *JP1/Integrated Management - Manager Overview and System Design Guide*.
- About the concept of event guides
See 11.1.10 *Considerations for setting event guide information* in the *JP1/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 *Chapter 2. Definition Files* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

4.8.1 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_ja.txt` or `sample_jco_guide_en.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	Environment	Folder/directory for the sample file
Windows	Japanese	<code>Console-path\conf\guide\sample_jco_guide_ja.txt</code>
		<code>shared-folder\conf\guide\sample_jco_guide_ja.txt</code>
	English	<code>Console-path\conf\guide\sample_jco_guide_en.txt</code>
		<code>shared-folder\conf\guide\sample_jco_guide_en.txt</code>
UNIX	Japanese	<code>/etc/opt/jplcons/conf/guide/sample_jco_guide_ja.txt</code>
		<code>shared-directory/jplcons/conf/guide/sample_jco_guide_ja.txt</code>
	English	<code>/etc/opt/jplcons/conf/guide/sample_jco_guide_en.txt</code>

OS	Environment	Folder/directory for the sample file
		<i>shared-directory</i> /jp1cons/conf/guide/sample_jco_guide_en.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_spmc_reload* command to reload JP1/IM.
- Restart JP1/IM - Manager (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/

#: In Windows, this value might be different depending on the environment because the value of *system-drive*: \Program Files is determined by the setting of an OS environment variable at the time of installation.

- 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.

4.9 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. Start JP1/IM - Manager.

The settings take effect once JP1/IM - Manager has started.

About the JP1 event issuance settings:

- About the status event definition file (`processupdate.conf`)

See *Status event definition file (processupdate.conf)* in *Chapter 2. Definition Files* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

4.10 Adding program-specific attributes

The following explains how to add program-specific attributes to JP1 events.

1. Specify additional event attribute definitions in the additional extended attribute settings file of JP1/Base.

In the additional extended attribute settings file, specify conditions for adding attributes and the extended attributes to be added when the conditions are satisfied.

The specification format for attribute addition conditions is specified using JP1/Base event filters.

The first seven bytes of an extended attribute name must be JP1ADD_.

For details about the additional extended attribute settings file, see the *JP1/Base User's Guide*.

Example of settings specified in the additional extended attribute settings file:

```
# Event : Extended attribute adding setting
add
filter
# input Event-filter
B.ID IN 111
end-filter
# input Extended-attribute
E.JP1ADD_SYSTEMNAME SystemA
end-add
```

2. Start JP1/Base or execute the `jevextreload` command:

```
jevextreload [-h event-server-name] {-recv | -send}
```

The additional extended attribute settings file is enabled.

3. Use the extended attribute `E.JP1ADD_SYSTEMNAME` as a condition for automated actions and various filters.

For details about the additional extended attribute settings file and the `jevextreload` command, see the *JP1/Base User's Guide*.

4.11 Setting the display and specification of program-specific extended attributes

This section explains how to specify the settings for displaying any item names for program-specific extended attributes in the events list in the Event Console window and in the Event Details window and specifying any item names for program-specific extended attributes in event conditions.

Note that the Web-based JP1/IM - View cannot display in the events list the item names defined in the definition file for extended event attributes (extended file).

1. Change the name of the definition file for extended event attributes (extended file).

When JP1/IM - Manager is installed, a template file for definition files for extended event attributes (extended file) is stored. A definition file for extended event attributes (extended file) is provided for each operating language of JP1/IM - Manager. Rename the file for the corresponding language by deleting `template_` at the beginning of the file name.

The following table shows the storage locations of the definition files for extended event attributes (extended file).

Table 4–8: Storage locations of definition files for extended event attributes (extended file)

OS	Storage location	
Windows	Physical host	<code>Console-path\conf\console\attribute\extend</code>
	Logical host	<code>shared-folder\JP1Cons\conf\console\attribute\extend</code>
UNIX	Physical host	<code>/etc/opt/jp1cons/conf/console/attribute/extend</code>
	Logical host	<code>shared-folder/jp1cons/conf/console/attribute/extend</code>

The following table shows the file name for each operating language and the file name after the change.

Table 4–9: File names of definition files for extended event attributes (extended file)

Language	Stored file name	File name after the change
Japanese	<code>template_extend_attr_ja.conf</code>	<code>extend_attr_ja.conf</code>
English	<code>template_extend_attr_en.conf</code>	<code>extend_attr_en.conf</code>
Chinese	<code>template_extend_attr_zh.conf</code>	<code>extend_attr_zh.conf</code>

2. Edit the definition file for extended event attributes (extended file).

In the definition file for extended event attributes (extended file) of JP1/IM - Manager, define item names for program-specific extended attributes. The following parameters must be edited:

```
attr name="E.attribute-name", title="item-name";
```

The following is an example definition:

```
@encode UTF-8
@file type="extended-attributes-definition", version="0300";
@define-block type="event-attr-def";
attr name="E.SYSTEM", title="System Name";
attr name="E.ROLE ", title="Server Usage";
@define-block-end;
```

For details about the definition file for extended event attributes (extended file), see *Definition file for extended event attributes (extended file)* in Chapter 2. *Definition Files* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

JP1/IM provides the `jcoattrfcheck` command to check the contents of a definition file for extended event attributes (extended file). For details about this command, see `jcoattrfcheck` in *Chapter 1. Commands* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

3. Execute the `jco_spm�_reload` command to apply the definition file for extended event attributes (extended file) to JP1/IM - Manager.

If JP1/IM - Manager is running, execute the `jco_spm�_reload` command to apply the definition file for extended event attributes (extended file) to JP1/IM - Manager. If JP1/IM - Manager is not running, the definition file for extended event attributes (extended file) is applied to JP1/IM - Manager when JP1/IM - Manager starts.

For details about the `jco_spm�_reload` command, see `jco_spm�_reload` in *Chapter 1. Commands* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

4. Log in to JP1/IM - Manager (Central Console) from JP1/IM - View.

When you log in to JP1/IM - Manager (Central Console) from JP1/IM - View, the contents of the definition file for extended event attributes (extended file) defined in JP1/IM - Manager are applied to the JP1/IM - View window. If JP1/IM - View is already connected at the time the definition file for extended event attributes (extended file) is applied to JP1/IM - Manager, you must restart JP1/IM - View.

To display the item names set for program-specific extended attributes in the events list, you must add the item names to the display items in the Preferences window. For details, see *5.9.1 Displaying program-specific extended attributes of JP1 events (displaying program-specific extended attributes)* in the *JP1/Integrated Management - Manager Administration Guide*.



Note

If you have defined program-specific extended attributes in the definition file for extended event attributes (extended file), you can assign one column to each program-specific extended attribute in the same manner as with basic attributes, shared extended attributes, and IM attributes when JP1 events are output to event reports in CSV format. To set whether the function for assigning one column to each program-specific extended attribute is to be enabled, use the `PROGRAM_SPECIFIC_EX_ATTR_COLUMN` parameter in the environment definition file for event report output (`evtreport.conf`). This function is enabled when you perform a new installation. If you have upgraded from version 10-50 or earlier, this function is disabled. If necessary, configure the environment definition file for event report output.

For details about the environment definition file for event report output, see *Environment definition file for event report output (evtreport.conf)* in *Chapter 2. Definition Files* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

4.12 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 *JP1/Base Function Reference*.

You can also use the `jvsend` and `jvsendd` 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 `jvsend` and `jvsendd` commands in JP1/Base, see the *JP1/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.`
- 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 4–10: Attributes of the startup event

Attribute type	Item	Attribute name	Description
Basic attribute	Event ID	--	<code>0x00000001</code>
	Message	--	<code>The SAMPLE application now starts.</code>

Attribute type	Item	Attribute name	Description
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 (user-specific information)	SAMPLE common attribute 1	COMMON_ATTR1	NATIVE
	SAMPLE common attribute 2	COMMON_ATTR2	TRUE
	SAMPLE start attribute 1	START_ATTR1	SAMPLE1
	SAMPLE start attribute 2	START_ATTR2	SAMPLE2

Legend:

--: None

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 4–11: 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

Attribute type	Item	Attribute name	Description
	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.
	Result code	RESULT_CODE	Result 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

Legend:

--: None

4.12.1 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 Chapter 2. *Definition Files* in the manual *JP1/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 *Chapter 1. Commands* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

Example of definition:

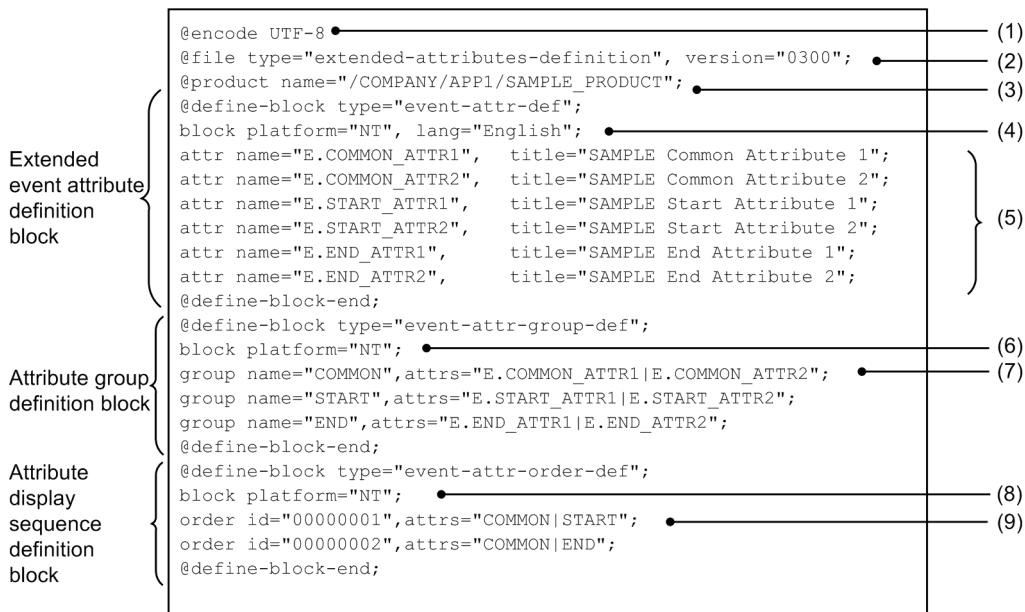
This example defines in the definition file for the extended event attributes the user-specific events that are issued by the `SAMPLE` application. This definition file defines the attributes of all JP1 events that are issued by a single application. This sample defines the JP1 events with event IDs `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) The following encodings can be specified: C, EUCJIS, SJIS, or UTF-8.
- (2) Only "0300" can be specified for the version.
- (3) This is the value specified for the `PRODUCT_NAME` extended event attribute.
- (4) The value of `platform=` is the value specified for the `PLATFORM` extended event attribute.
- (5) `title=` defines a name that is displayed in the detailed information.
- (6) The value of `platform=` is the value specified for the `PLATFORM` extended event attribute.
- (7) Defines an attribute group.
- (8) The value of `platform=` is the value specified for the `PLATFORM` extended event attribute.
- (9) The group name specified in (7) 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 *Chapter 2. Definition Files* in the manual *JP1/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]
```

4.12.2 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 4–12: When the definition files take effect

Definition file	When it takes effect
Definition file for the extended event attributes	When the <code>jco_spmd_reload</code> command is executed or when JP1/IM - Manager is restarted
Definition file for objects types	When JP1/IM - View is restarted

4.13 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. The procedure for setting the severity changing function is shown in the following sections.

4.13.1 Setting the severity changing function from the Severity Change Definition Settings window

(1) Creating a severity changing definition

To create a severity changing definition:

1. Confirm that the event severity changing function is enabled.

Execute the `jcoimdef` command and check the `-chsev` option. If the option is disabled, use the `jcoimdef` command to enable the event severity changing function. This function is disabled by default. If you enable the severity changing function, restart JP1/IM - Manager. For details about the `jcoimdef` command, see *jcoimdef* in *Chapter 1. Commands* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

2. Select **Options** and then **Severity Change Definitions** in the Event Console window.

The View Severity Change Definitions window appears.

3. When you create a severity changing definition, click the **Add** button, and when you reuse an existing severity changing definition, click the **Copy** button, and then click the **Edit** button.

If you click the **Add** button, the Severity Change Definition Settings window appears.

If you click the **Copy** button, a copied severity change definition name is added to the filter. In this case, select the copied severity change definition name, and then click the **Edit** button to display the Severity Change Definition Settings window.

4. Specify the severity level in the Severity Change Definition Settings window.

Specify an event condition to change the severity level. Then, select the severity level after the change from **New severity level**, and click the **OK** button.

5. Click the **Apply** button in the View Severity Change Definitions window to enable the definition.

Select the severity changing definition that was set in the Severity Change Definition Settings window from the View Severity Change Definitions window, and then select the **Apply** check box to enable the definition. If you want to set multiple severity changing definitions, repeat steps 3 to 5.

6. Click the **Yes** button in the confirmation dialog box.

(2) Changing a severity changing definition

To change an existing severity changing definition:

1. Confirm that the event severity changing function is enabled.

Execute the `jcoimdef` command and check the `-chsev` option. If the option is disabled, use the `jcoimdef` command to enable the event severity changing function. This function is disabled by default. If you enable the severity changing function, restart JP1/IM - Manager. For details about the `jcoimdef` command, see *jcoimdef* in

Chapter 1. Commands in the manual JP1/Integrated Management - Manager Command and Definition File Reference.

2. Select **Options**, and then **Severity Change Definitions** in the Event Console window.
The View Severity Change Definitions window appears.
3. Select a severity changing definition which you want to change in the View Severity Change Definitions window, and then click the **Edit** button.
The Severity Change Definition Settings window appears.
4. Change the severity level in the Severity Change Definition Settings window.
Specify an event condition to change the severity level. Then, select the severity level after the change from **New severity level**, and click the **OK** button.
5. Select the **Apply** check box in the View Severity Change Definitions window to enable the definition.
Select the severity changing definition that was set in the Severity Change Definition Settings window from the View Severity Change Definitions window, and then select the **Apply** check box to enable the definition.
If you want to set multiple events, repeat steps 3 to 5.
6. Click the **Yes** button in the confirmation dialog box.

(3) Deleting a severity changing definition

To delete an existing severity changing definition:

1. Confirm that the event severity changing function is enabled.
Execute the `jcoimdef` command and check the `-chsev` option. If the option is disabled, use the `jcoimdef` command to enable the event severity changing function. This function is disabled by default. If you enable the severity changing function, restart JP1/IM - Manager. For details about the `jcoimdef` command, see *jcoimdef* in *Chapter 1. Commands in the manual JP1/Integrated Management - Manager Command and Definition File Reference*.
2. Select **Options** and then **Severity Change Definitions** in the Event Console window.
The View Severity Change Definitions window appears.
3. Select a severity changing definition that you want to delete in the View Severity Change Definitions window, and then click the **Delete** button.
The selected severity changing definition is deleted.
4. Click the **Yes** button in the confirmation dialog box.

4.13.2 Setting the severity changing function by using the severity changing definition file

1. Confirm that the event severity changing function is enabled.
Execute the `jcoimdef` command and check the `-chsev` option. If the option is disabled, use the `jcoimdef` command to enable the event severity changing function. This function is disabled by default. If you enable the severity changing function, restart JP1/IM - Manager. For details about the `jcoimdef` command, see *jcoimdef* in *Chapter 1. Commands in the manual JP1/Integrated Management - Manager Command and Definition File Reference*.

2. Edit the severity changing definition file.

For details about the information to be edited, see *5.9.4 Changing the severity level of JPI events* in the *JPI/Integrated Management - Manager Administration Guide*.

3. Execute the `jco_spm�_reload` command or restart JPI/IM - Manager.

If, in step 1, you enabled the severity changing function while it was disabled, you need to restart JPI/IM - Manager.

If you edited the severity changing definition file while the severity changing function was enabled, execute the `jco_spm�_reload` command to apply the definitions. For details about the `jco_spm�_reload` command, see *jco_spm�_reload* in *Chapter 1. Commands* in the manual *JPI/Integrated Management - Manager Command and Definition File Reference*.

4.14 Setting the display message change function

This section explains how to configure the display message change function. The display message change function is used with the integrated monitoring database.

There are two ways to configure the display message change function. One uses a GUI and the other uses the display message change definition file to specify settings and then applying the settings by executing the `jco_spmc_reload` command.

Important

Do not use both the GUI and the definition file to specify the settings. If a user updates the definition file, for example, with a text editor at the same time that a definition is being updated via the GUI, the contents of the definition file might no longer match the data in memory.

The following subsections explain each of the procedures.

4.14.1 Configuring from the Display Message Change Definition Settings window

(1) Creating display message change definitions

The following explains how to create a display message change definition:

1. Verify that the display message change function is enabled for events.

In the Event Console window, under Options, check whether **Display Message Change Definitions** is displayed. If it is not displayed, enable the integrated monitoring database to enable the display message change function. If you have to enable the display message change function, restart JPI/IM - Manager.

If you have not updated the IM databases by executing the `jimdbupdate` command since performing an upgrade installation from version 10-50 or earlier, you must update the IM databases. For details about the `jimdbupdate` command, see *jimdbupdate* in *Chapter 1. Commands* in the manual *JPI/Integrated Management - Manager Command and Definition File Reference*.

2. In the Event Console window, select **Options**, and then **Display Message Change Definitions**.

The Display Message Change Definitions window is displayed.

3. Click the **Add** button to create a display message change definition or the **Copy** button to use an existing display message change definition, and then click the **Edit** button.

Clicking the **Add** button displays the Display Message Change Definition Settings window.

Clicking the **Copy** button adds **Source display message change definition** to the filter. In this case, select **Source display message change definition**, and then click the **Edit** button to display the Display Message Change Definition Settings window.

4. In the Display Message Change Definition Settings window, specify the desired display message change settings.

Specify the event condition to be used to change a display message. Then specify in **Message after the change** the message format after the change. The event inheritance information conversion function enables you to obtain a readable uniform display format for message texts and numeric values. For details about the event inheritance information conversion function, see *Display message change definition file (jcochmsg.conf)* in *Chapter 2*.

Definition Files in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*. After you have specified the settings, click the **OK** button.

5. In the Display Message Change Definitions window, select the **Apply** button.

From the Display Message Change Definitions window, select the display message change definition specified in the Display Message Change Definitions window, and then select the **Apply** check box. If you want to specify another display message change definition, repeat steps 3 to 5.

6. In the confirmation dialog box, click the **Yes** button.

(2) Changing display message change definitions

The following explains how to change an existing display message change definition:

1. Verify that the display message change function is enabled for events.

In the Event Console window, verify that the items from **Options** to **Display Message Change Definitions** are displayed. If these items are not displayed, enable the integrated monitoring database to enable the display message change function. If you have had to enable the display message change function, restart JP1/IM - Manager.

2. In the Event Console window, select **Options**, and then **Display Message Change Definitions**.

The Display Message Change Definitions window is displayed.

3. In the Display Message Change Definitions window, select the display message change definition that you want to change, and then click the **Edit** button.

The Display Message Change Definition Settings window is displayed.

4. In the Display Message Change Definition Settings window, change the display message settings.

Specify the event condition to be used to change the display message. Then specify in **Message after the change** the message format after the change. The event inheritance information conversion function enables you to obtain a readable uniform display format for message texts and numeric values. For details about the event inheritance information conversion function, see *Display message change definition file (jcochmsg.conf)* in *Chapter 2*.

Definition Files in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*. After you have specified the settings, click the **OK** button.

5. In the Display Message Change Definitions window, select the **Apply** button.

From the Display Message Change Definitions window, select the display message change definition specified in the Display Message Change Definitions window, and then select the **Apply** check box. If you want to specify another event, repeat steps 3 to 5.

6. In the confirmation dialog box, click the **Yes** button.

(3) Deleting display message change definitions

The following explains how to delete an existing display message change definition:

1. Verify that the display message change function is enabled for events.

In the Event Console window, verify that **Options - Display Message Change Definitions** are displayed. If these items are not displayed, enable the integrated monitoring database to enable the display message change function. If you have had to enable the display message change function, restart JP1/IM - Manager.

2. In the Event Console window, select **Options**, and then **Display Message Change Definitions**.

The Display Message Change Definitions window is displayed.

3. In the Display Message Change Definitions window, select the display message change definition that you want to delete, and then click the **Delete** button.

The selected display message change definition is deleted.

4. In the confirmation dialog box, click the **Yes** button.

4.14.2 Configuring from the display message change definition file

1. Verify that the display message change function is enabled for events.

In the Event Console window, verify that the items from **Options** to **Display Message Change Definitions** are displayed. If these items are not displayed, enable the integrated monitoring database to enable the display message change function. If you have had to enable the display message change function, restart JP1/IM - Manager.

If you have not updated the IM databases by executing the `jimdbupdate` command since performing an upgrade installation from version 10-50 or earlier, you must update the IM databases. For details about the `jimdbupdate` command, see *jimdbupdate* in *Chapter 1. Commands* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

2. Edit the display message change definition file.

For details about the contents to be edited, see *5.9.5(2) Setting a display message change definition in the display message change definition file* in the *JP1/Integrated Management - Manager Administration Guide*.

3. Execute the `jco_spmd_reload` command or restart JP1/IM - Manager.

If you have edited the display message change definition file while the display message change function is enabled, execute the `jco_spmd_reload` command to apply the edited information. For details about the `jco_spmd_reload` command, see *jco_spmd_reload* in *Chapter 1. Commands* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

4. Log in to JP1/IM - Manager (Central Console) from JP1/IM - View.

When you log in to JP1/IM - Manager (Central Console) from JP1/IM - View, the contents of the display message change definition file defined in JP1/IM - Manager are applied to the JP1/IM - View window. If you have applied the display message change definition while the Display Message Change Definition Settings window or the Display Message Change Definitions window was displayed with JP1/IM - View connected, click the **Cancel** button in the Display Message Change Definition Settings window and the **Close** button in the Display Message Change Definitions window to close the window, and then open the window again.

4.14.3 Procedure for issuing events after display messages have been changed

The following explains the procedure for issuing events after display messages have been changed:

1. Edit the environment definition file for events after the display message is changed.

Specify `00000001` for `"SEND_CHANGE_MESSAGE_EVENT"=dword:`.

For details about the environment definition file for events after the display message is changed, see *Environment definition file for events after the display message is changed (chmsgevent.conf)* in *Chapter 2. Definition Files* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

2. Execute the `jbssetcnf` command.

Execute the `jbssetcnf` command of JP1/Base to apply the contents of the environment definition file for events after the display message is changed to the JP1 common definition information. For details about the `jbssetcnf` command, see the *JP1/Base User's Guide*.

3. Restart JP1/IM - Manager.

Events will be issued after display messages have been changed. For this reason, set event ID 00006400 in the exclusion conditions using an event acquisition filter so that the same events will not be acquired again. For details about event acquisition filters, see [4.2.4 Settings for event acquisition filters](#).

4.15 Setting event source host mapping

This section describes how to set event source host mapping. Event source host mapping is available when the integrated monitoring database is being used.

To set event source host mapping:

1. Enable event source host mapping.

```
jcoimdef -hostmap ON
```

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

2. Edit the event-source-host mapping definition file.#

Edit the event-source-host mapping definition file. The definition file can contain a maximum of 1,000 definitions. When you enable event source host mapping, the JP1 events listed in the table below are automatically mapped. JP1 events that are not listed in the following table must be set individually. In addition, although you define the events as indicated in the table in the definition file for event source host mapping, the settings in the table take precedence.

Table 4–13: JP1 events to be mapped

No	Product name	JP1 event to be mapped	Attribute name indicating event source host	Remarks
1	JP1/Base	JP1 events with event ID 3A71 and extended attribute E.PPNAME set to /HITACHI/JP1/NTEVENT_LOGTRAP	E.SOURCESERVER	The JP1 events are mapped when changing of the attributes of JP1 events is specified in the common definition settings file for that purpose.
2		JP1 events with the following event ID: • 3A71	E.A1	The JP1 events are mapped when changing of the attributes of JP1 events is not specified in the common definition setting file for that purpose.
3		JP1 events with the following event ID: • 3A80	E.SNMP_SOURCE	--
4	JP1/AJS2 and JP1/AJS3	JP1 events with the following event IDs: • 4105 • 4106 • 4107 • 4109 • 410A • 4125 • 4126 • 4127	E.C0	--
5	JP1/PFM	JP1 events with the following product names: • /PFM/ALARM_EVENT • /HITACHI/JP1/PFM/ALARM_EVENT	E.JPC_AGENT	--

No	Product name	JP1 event to be mapped	Attribute name indicating event source host	Remarks
		<ul style="list-style-type: none"> /HITACHI/JP1/PFM/STATE_EVENT 		
6		JP1 events with the following product name: <ul style="list-style-type: none"> /HITACHI/JP1/PFM 	E.JPC_MGR	--
7	JP1/Cm2/SSO HP NNM JP1/PFM/SSO - Agent for Process	JP1 events with the following event ID: <ul style="list-style-type: none"> 3A80 	The value of one of the following attributes containing a host name is mapped: <ul style="list-style-type: none"> E.SNMP_VARBIND1 E.SNMP_VARBIND2 E.SNMP_VARBIND3 E.SNMP_VARBIND6 E.SNMP_VARBIND12 	--
8	JP1/PAM	JP1 events with the following product name: <ul style="list-style-type: none"> /HITACHI/JP1/PAM 	E.PAM_HOSTNAME	--
9	JP1/SCIM	JP1 events with the following event IDs: <ul style="list-style-type: none"> 432B 432C 	E.SCIM_AGENT_ADDR	--
10	Cosminexus	JP1 events with the following event IDs: <ul style="list-style-type: none"> 12000 12080 	E.HOST_NAME	--
11	JP1/ServerConductor	JP1 events with the following product name: <ul style="list-style-type: none"> /HITACHI/SYSTEM_MANAGER 	E.HSM_SERVER	--
12	JP1/IM - EG for NNMi	JP1 events with the following event ID: <ul style="list-style-type: none"> 6100 	E.NNMI_SRC_NODE_NAME	--
13	JP1/Console Agent for VOS3	<ul style="list-style-type: none"> JP1 events with the following event IDs: <ul style="list-style-type: none"> 11503 11504 11505 11506 11516 11520 11521 11522 11523 1159F JP1 events with event IDs 11502 and 1150A, and object type CPN 	E.CIF_PNAM	--
14	JP1/Software Distribution	JP1 events with the following event IDs:	E.A2	--

No	Product name	JP1 event to be mapped	Attribute name indicating event source host	Remarks
		<ul style="list-style-type: none"> • 10110 • 10112 • 10111 • 10410 • 10411 • 10412 		
15		JP1 events with the following event IDs: <ul style="list-style-type: none"> • 10420 • 10421 • 10422 	E.O3	--
16	JP1/IM - MO	JP1 events with the following event ID: <ul style="list-style-type: none"> • 6400 	E.EVTSRC_INFO	--
17	JP1/IM - Manager	JP1 events with the following event ID: <ul style="list-style-type: none"> • 3A71 	E.A1	--
18		JP1 events with the following event ID: <ul style="list-style-type: none"> • 6400 	E.EVTSRC_INFO	Event with message after change that is issued when the function for issuing events after display message has been changed is enabled.

Legend:

--: None

For details about the items to be edited, see *Event-source-host mapping definition file (user_hostmap.conf)* in *Chapter 2. Definition Files* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

#:

For remote-monitoring log file trap, the event source host name (E.JP1_SOURCEHOST) is set regardless of the settings. Therefore, you do not need to edit the event-source-host mapping definition file.

3. Restart JP1/IM - Manager.

If, in step 1, you enabled event source host mapping while it was disabled, you need to restart JP1/IM - Manager. If you edited the definition file for event source host mapping while event source host mapping was enabled, execute the `jco_spmd_reload` command to apply the definitions.

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

4.16 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.

4.16.1 Settings for JP1/IM - View

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, changed display message, new display message, display message change definition, Event source host name, memo, and program-specific extended attributes. If the severity changing function is disabled, the original severity level and the new severity level are not displayed. If the display message change function is disabled, a changed display message, new display message, and display message change definition cannot be displayed. If the memo entry settings are disabled, no memo is displayed. If event source host mapping is disabled, no event source host name is displayed. For the program-specific extended attributes, the item names defined in the definition file for extended event attributes (extended file) are displayed.

- Whether the state of a page that is displayed in the Event Console window is to be saved

You can specify whether to save the state of view filters and the **View filter** check box in the page (**Monitor Events** page and **Severe Events** page) selected in the Event Console window at logout of JP1/IM - View, and restore the same state at login.

- 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.

- Font size of the text in the events list in the Event Console window

You can change the font size of the text displayed in the events list in the range from 12 points to 72 points. Increasing the font size improves the readability of text when, for example, a large monitor is viewed from a distance. You can change the font size of the text in the events list displayed on the **Monitor Events** page, the **Severe Events** page, and the **Search Events** page in the Event Console window.

- 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**, **Severe Events**, and **Search Events** pages.

This setting is applicable to events with the event levels *Emergency*, *Alert*, *Critical*, *Error*, *Debug*, *Notice*, *Information*, and *Warning*.

You can change the text color and the background color of contained events in the system color definition file (`systemColor.conf`). For details, see *System color definition file (systemColor.conf)* in *Chapter 2. Definition Files* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

- Whether consolidated display is to be used for repeated events

You can specify whether to use the repeated event consolidated display function to consolidate a large number of identical events that occur in a short period of time for display in the Event Console window.

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.

Note that when you enable the function of preventing monitoring of repeated events, the repeated event consolidated display function cannot be used.

- Number of rows to be displayed as execution results in the Command window
- Display of events that occurred during a specified period

4.16.2 Procedure for specifying JP1/IM - View settings

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 *2.24 Preferences window* in the manual *JP1/Integrated Management - Manager GUI Reference*.



Important

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 *JP1/Integrated Management - Manager Command and Definition File Reference*. If such changes are made, JP1/IM - View might not function correctly.

4.17 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).

Important

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.

4.17.1 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.

For details about this definition file, see *Definition file for opening monitor windows* in *Chapter 2. Definition Files* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

- Definition file for executing applications

This definition file defines the association between paths and application execution definition identifiers defined in the definition file for opening monitor windows. Create this definition file on the machine where JP1/IM - View is installed.

For details about this definition file, see *Definition file for executing applications* in *Chapter 2. Definition Files* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

3. Execute the `jco_spmc_reload` command to apply the contents of the definition file for opening monitor windows to JP1/IM - Manager.

If JP1/IM - Manager is running, execute the `jco_spmc_reload` command. The contents of the definition file for opening monitor windows are immediately applied to JP1/IM - Manager. If JP1/IM - Manager is not running, the contents of that file are automatically applied to JP1/IM - Manager the next time JP1/IM - Manager starts. For details about the `jco_spmc_reload` command, see `jco_spmc_reload` in *Chapter 1. Commands* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

4. From JP1/IM - View, log in to JP1/IM - Manager (Central Console).

When JP1/IM - View starts, the contents of the definition file for executing applications are applied to JP1/IM - View. If JP1/IM - View is connected with JP1/IM - Manager when the contents of the definition file for opening monitor windows are applied by using the command, you must restart JP1/IM - View.

The following subsections provide details of each step.

4.17.2 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 *3.14 Displaying user-defined event attributes* in the *JP1/Integrated Management - Manager Overview and System Design Guide*.

4.17.3 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 *Chapter 2. Definition Files* in the manual *JP1/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 *Chapter 2. Definition Files* in the manual *JP1/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 *Chapter 1. Commands* in the manual *JP1/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 *Chapter 2. Definition Files* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

JP1/IM provides the `jcoappexecfcheck` (Windows only) command for checking the definition file for executing applications. For details about this command, see *jcoappexecfcheck (Windows only)* in *Chapter 1. Commands* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

4.18 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.

4.18.1 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 (application window) 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 *JP1/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 *4.18.4 Creating the definition files*. It describes the prerequisites for the settings and provides examples.

Important

Some linked products might require a different procedure from that shown above. For details about the setup method, also see the documentation for the particular product.

4.18.2 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.

4.18.3 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 × 16 pixels. If you do not specify an icon, the default icon is used.

4.18.4 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 *Chapter 2. Definition Files* in the manual *JPI/Integrated Management - Manager Command and Definition File Reference*. For details about the definition file for executing applications, see *Definition file for executing applications* in *Chapter 2. Definition Files* in the manual *JPI/Integrated Management - Manager Command and Definition File Reference*.

JPI/IM provides the `jcfuncfcheck` (Windows only) command for checking the definition file for the Tool Launcher window. For details about this command, see *jcfuncfcheck (Windows only)* in *Chapter 1. Commands* in the manual *JPI/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 JPI/IM - View is restarted.

View-path\conf\function\en\

(c) Example of definition

This subsection presents the following example:

Application

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

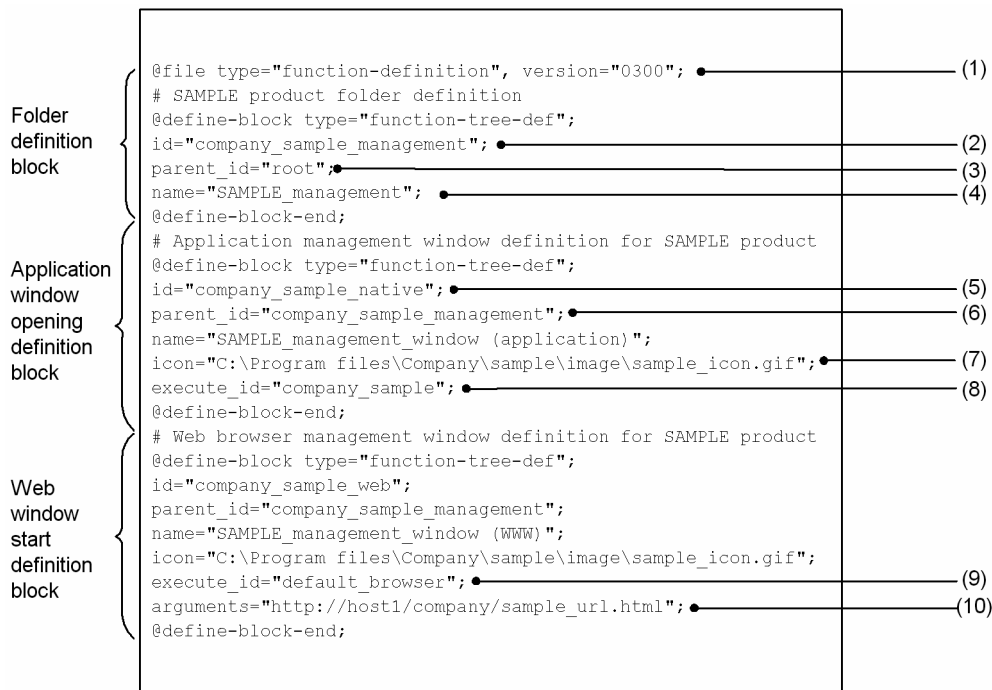
http://host1/company/sample_url.html

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 *Chapter 2. Definition Files* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

JP1/IM provides the `jcoappexecfcheck` (Windows only) command for checking the definition file for executing applications. For details about this command, see *jcoappexecfcheck (Windows only)* in *Chapter 1. Commands* in the manual *JP1/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.

4.18.5 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 *Chapter 2. Definition Files* in the manual *JP1/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.

4.19 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 web-based version of JP1/IM - View has two modes: Compatibility mode, which requires the browser plug-ins included in the JRE; and plug-in free mode, which does not require plug-ins. When you perform a new installation of JP1/IM - Manager, the settings are configured to use plug-in free mode. If you have upgraded JP1/IM - Manager from version 11-01 or earlier, the settings are configured to use compatibility mode. For details about how to switch between compatibility mode and plug-in free mode, see *Web-based operation definition file (console_xx.html)* in *Chapter 2. Definition Files* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

Note that the web-based version of JP1/IM - View is not supported for cluster systems. If you monitor events in a cluster system, use JP1/IM - View.

The following is an outline of the procedure:

1. Install an HTTP server.
2. Set up the HTTP server.
3. Add a MIME type.
4. Change the port number.
5. Set up a Web browser.
6. Specify display settings for the Java Console window.
7. Set timeout values.
8. Specify the settings for the web-based version of JP1/IM - View.

4.19.1 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.

4.19.2 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 4–14: Alias to be added to the HTTP server

Alias name	Reference path
/JP1IM	<i>Console-path</i> \www\

(1) Adding a MIME type

Add the MIME type shown below to JP1IM, which is the alias of the HTTP server. Note that if you use the Web-based version of JP1/IM - View in compatibility mode, you do not need to add this MIME type.

File extension: .jnlp

MIME type: application/x-java-jnlp-file

(2) 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 4–15: Parameter in the HTML file

HTML file	Parameter
<code>Console-path\www\console.html</code>	<code><param name="PORT" value="value"></code>

4.19.3 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.

4.19.4 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.

4.19.5 Setting timeout values for Web-based operation

In the web-based startup definition file (`console_xx.jnlp`), set the timeout values for the web-based version of JP1/IM - View.

For details about the web-based startup definition file (`console_xx.jnlp`), see *Web-based startup definition file (console_xx.jnlp)* in *Chapter 2. Definition Files* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

4.19.6 Setting the URL of the web-based version of JP1/IM - View

In the web-based startup definition file (`console_xx.jnlp`), set the URL to be used when the web-based version of JP1/IM - View starts. Note that if you use the web-based version of JP1/IM - View in compatibility mode, you do not need to set this URL.

For details about the web-based startup definition file (`console_xx.jnlp`), see *Web-based startup definition file (console_xx.jnlp)* in *Chapter 2. Definition Files* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

4.20 Setting reference and operation restrictions on business groups

This section describes how to set reference and operation restrictions on business groups. Before you start, determine the JP1 resource groups and the JP1 permission levels to be assigned to JP1 users.

When you enable reference and operation restrictions on business groups, the integrated monitoring database, the IM Configuration Management database, and event source host mapping must all be enabled.

To set reference and operation restrictions on business groups:

1. Enable reference and operation restrictions on business groups.

```
jcoimdef -bizmonmode ON
```

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

2. Restart JP1/IM - Manager.

3. Restart JP1/IM - View.

The status in effect before the restrictions are set remains in effect until you restart JP1/IM - View. Therefore, when you enable or disable reference and operation restrictions on business groups, make sure that you restart JP1/IM - View.

4. Apply the settings for business groups to Central Console.

Apply the settings for business groups from IM Configuration Management - View. For details about how to do this, see [3.4.1\(3\) Applying an edited business group to the IM Configuration Management database and Central Console](#).

For details about JP1 resource groups and JP1 permission levels, business groups, the integrated monitoring database, the IM Configuration Management database, and event source host mapping, see the following:

About JP1 resource groups and JP1 permission levels

- Combinations of JP1 resource groups and JP1 permission levels for business groups
See [3.1.4 Restrictions on viewing and operating business groups](#) in the *JP1/Integrated Management - Manager Overview and System Design Guide*.
- Assigning JP1 resource groups and JP1 permission levels
See the chapter on configuring user management in the *JP1/Base User's Guide*.

About business groups

- Overview of business groups
See [6.4 Managing business groups](#) in the *JP1/Integrated Management - Manager Overview and System Design Guide*.
- Setting business groups
See [3.4 Setting business groups](#).

About the integrated monitoring database

- Setting up the integrated monitoring database
See the following:
For Windows: [1.4.2 Setting up the integrated monitoring database \(for Windows\)](#)
For UNIX: [2.4.2 Setting up the integrated monitoring database \(for UNIX\)](#)

About the IM Configuration Management database

- Setting up the IM Configuration Management database

See the following:

For Windows: [1.4.3 Setting up the IM Configuration Management database \(for Windows\)](#)

For UNIX: [2.4.3 Setting up the IM Configuration Management database \(for UNIX\)](#)

About event source host mapping

- Overview of event source host mapping

See [3.9 Mapping of the event source hosts](#) in the *JP1/Integrated Management - Manager Overview and System Design Guide*.

- Setting event source host mapping

See [4.15 Setting event source host mapping](#).

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

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.

5.1.1 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 *Chapter 1. Overview of JP1/Integrated Management* in the *JP1/Integrated Management - Manager Overview and System Design Guide*.
See *Chapter 2. Overview of Functions* in the *JP1/Integrated Management - Manager Overview and System Design Guide*.
- About the functions of Central Scope
See *Chapter 4. Objective-Oriented System Monitoring Using the Central Scope* in the *JP1/Integrated Management - Manager Overview and System Design Guide*.

Configuring a JP1/IM operating environment

- Installing and setting up JP1/IM
See *Chapter 1. Installation and Setup (for Windows)*.
See *Chapter 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:

- Execute the `jco_spmc_reload` command
- Restart JP1/IM - Manager

For details about setting host information, see the following:

About setting host information:

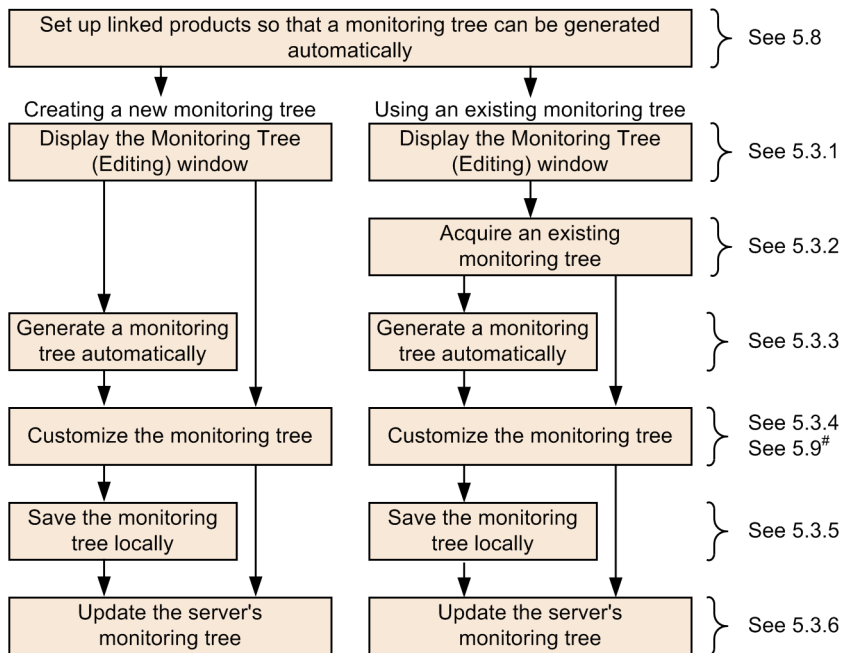
- About host information
See *4.11.2 Host information* in the *JP1/Integrated Management - Manager Overview and System Design Guide*.
- About the format of host information file
See *Host information file (jcs_hosts)* in *Chapter 2. Definition Files* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.
- About the `jcshostsimport` command
See *jcshostsimport* in *Chapter 1. Commands* in the manual *JP1/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.

To edit the monitoring tree:

1. Open the Monitoring Tree (Editing) window.

Use one of the following methods:

- From the **Start** menu, choose **All 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).

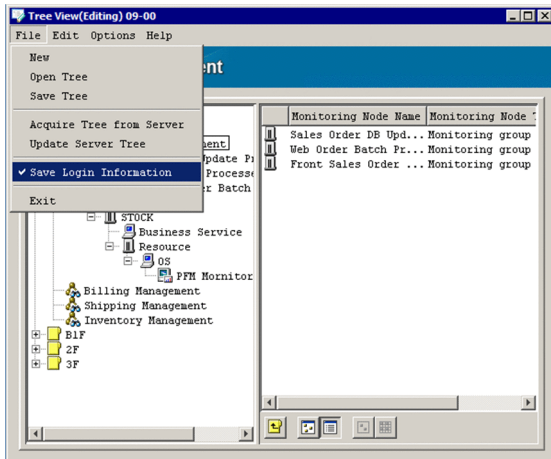
Saving the login information

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 5–2: 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 (Central Scope) being used at the server or the version of the acquired file.

Important

If the monitoring tree is obtained from CSV files on the local host and the file version displayed on the title bar of the Monitoring Tree(Editing) window is old, 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 (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 permission. 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:

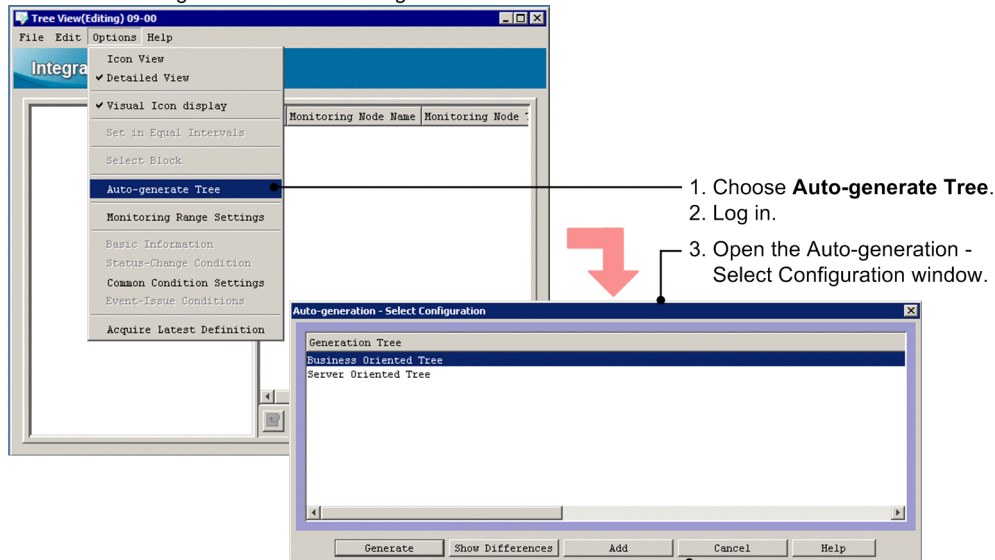
About monitoring tree automatic generation:

- About the monitoring tree automatic generation function
See 4.2 *Monitoring tree* in the *JP1/Integrated Management - Manager Overview and System Design Guide*.
See 4.3 *Automatically generating a monitoring tree* in the *JP1/Integrated Management - Manager Overview and System Design Guide*.
- About the monitoring tree model that is generated automatically
See *Chapter 5. Monitoring Tree Models (for Central Scope)* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

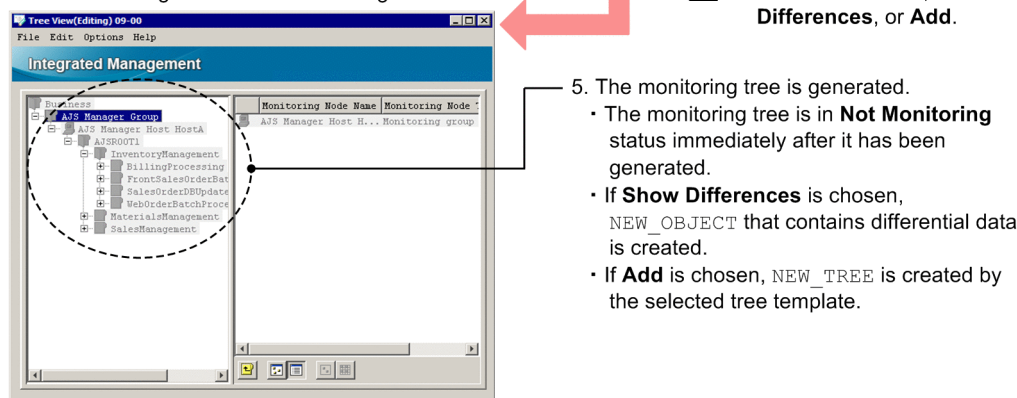
The following figure shows the procedure for generating a monitoring tree automatically.

Figure 5–3: Procedure for generating a monitoring tree automatically

Before automatic generation of monitoring tree



After automatic generation of monitoring tree



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 (Central Scope) is displayed.

Log in as the `jpladmin` user.

For the host to connect, specify the name of a host on which JP1/IM - Manager to which you log in exists. Specify the host name that is defined in the viewer or the IP address.

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 a new monitoring tree from the differential data between the monitoring tree in the editing window and the collected definition information (including monitoring objects and monitoring groups). The new monitoring tree is created in the `NEW_OBJECT` monitoring group.
- **Add**: Creates a new monitoring tree from the monitoring tree in the editing window. 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 *JP1/Integrated Management - Manager Overview and System Design Guide*.

See 4.3 *Automatically generating a monitoring tree* in the *JPI/Integrated Management - Manager Overview and System Design Guide*.

See 4.4 *Editing a monitoring tree* in the *JPI/Integrated Management - Manager Overview and System Design Guide*.

See 4.11 *Central Scope* in the *JPI/Integrated Management - Manager Overview and System Design Guide*.

- About the settings for a monitoring tree

See 4.2 *Monitoring tree* in the *JPI/Integrated Management - Manager Overview and System Design Guide*.

- About the system-monitoring objects for which basic settings have been defined

See *Chapter 4. Lists of System-Monitoring Objects (for Central Scope)* in the manual *JPI/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 JPI/IM - View when you generate a new monitoring tree.

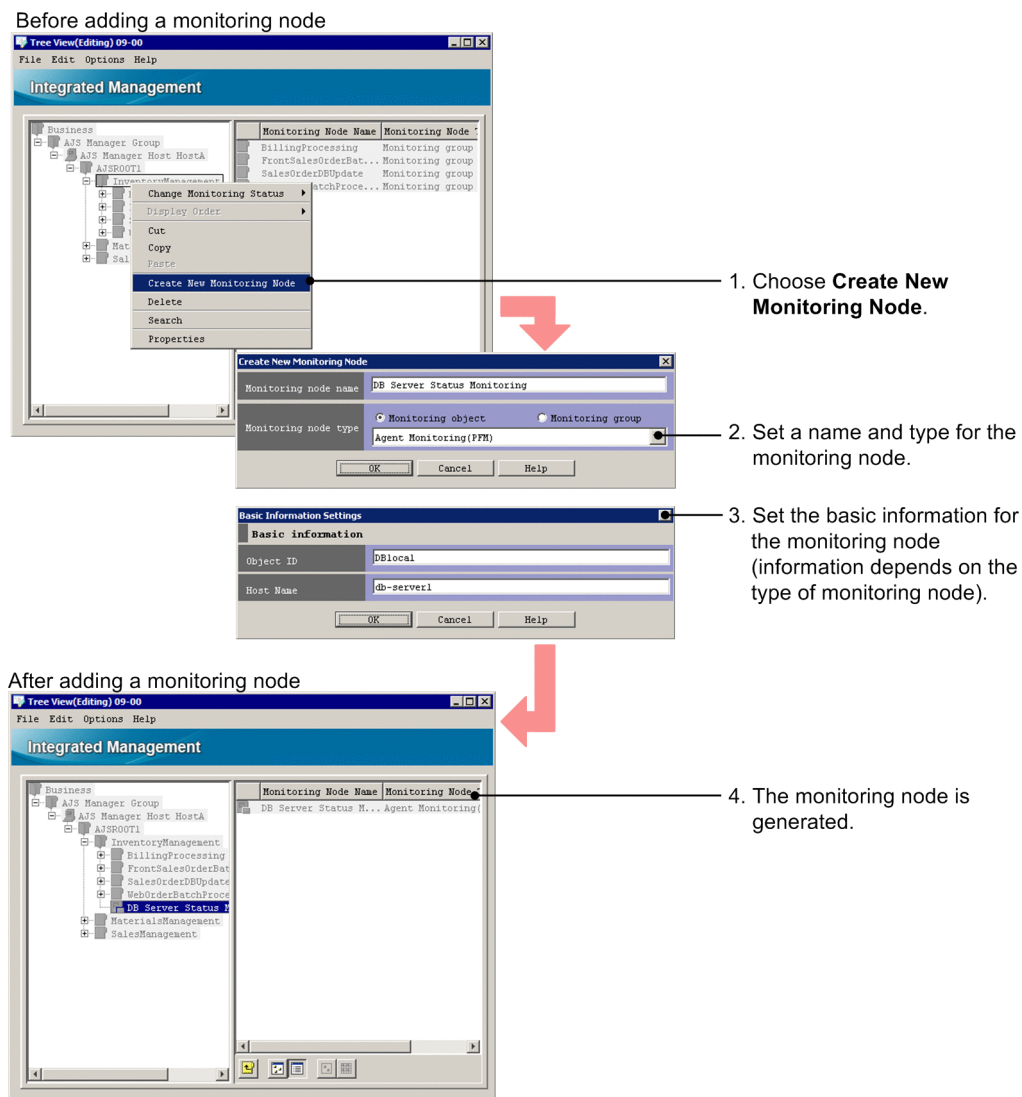
To acquire common conditions:

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 5–4: Procedure for 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 *Chapter 4. Lists of System-Monitoring Objects (for Central Scope)* in the manual *JP1/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**.
 - 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**.
 - 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 *Chapter 4. Lists of System-Monitoring Objects (for Central Scope)* in the manual *JP1/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.

Figure 5–5: Example of using the General page to set a monitoring node's monitoring status to Monitoring

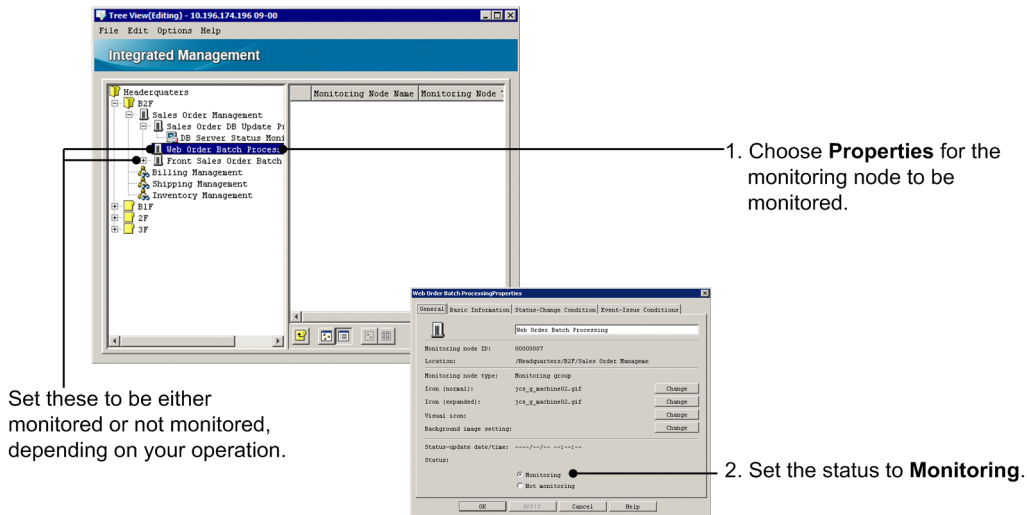


Figure 5–6: Example of settings on the Basic Information page

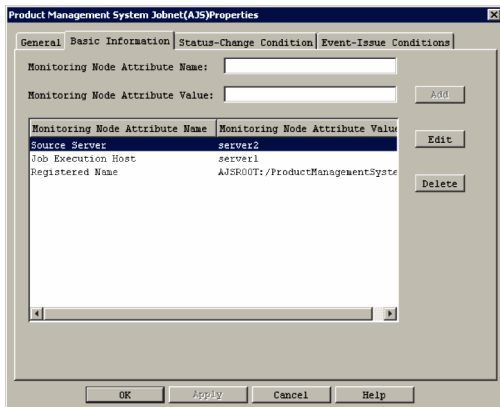


Figure 5–7: Example of using the Status-Change Condition page to set the status change condition for a monitoring node

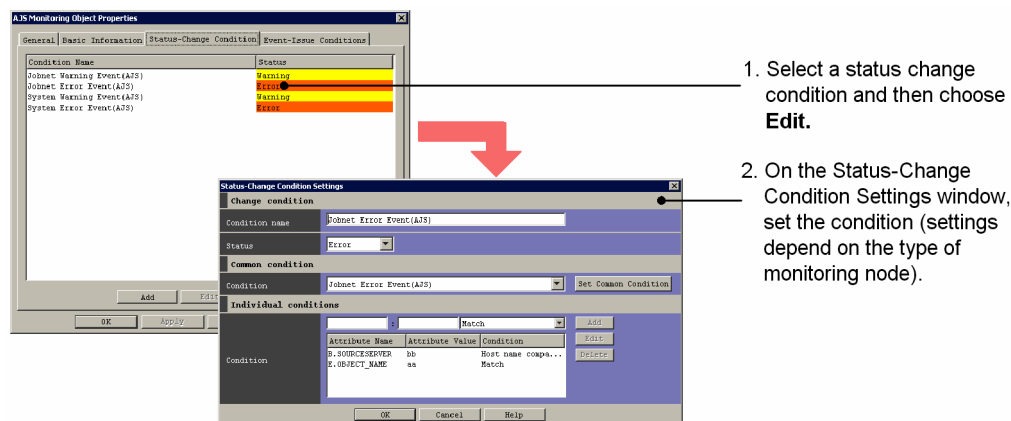
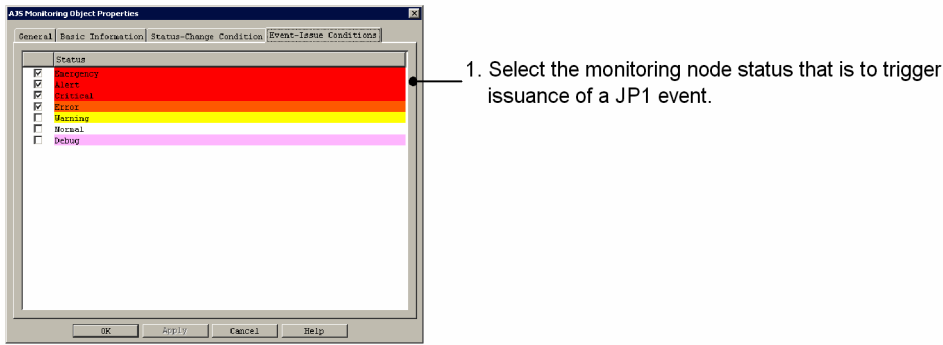


Figure 5–8: Example of setting JP1 event issuance on the Event-Issue Conditions page



(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 × 24 pixels, maximum 2,048 × 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 correspondence between monitoring node statuses and colors (status colors) at the time of installation.

Table 5–2: Correspondence between monitoring node statuses and status colors

Monitoring node status	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 status 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.

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.

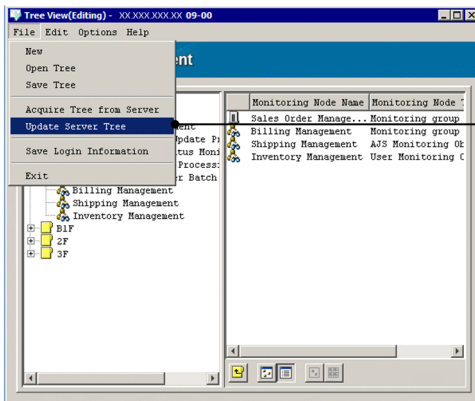
When the Save Tree window appears, specify a desired folder name and file name, and then save the monitoring tree.

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 5–9: 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 (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 permission.

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.

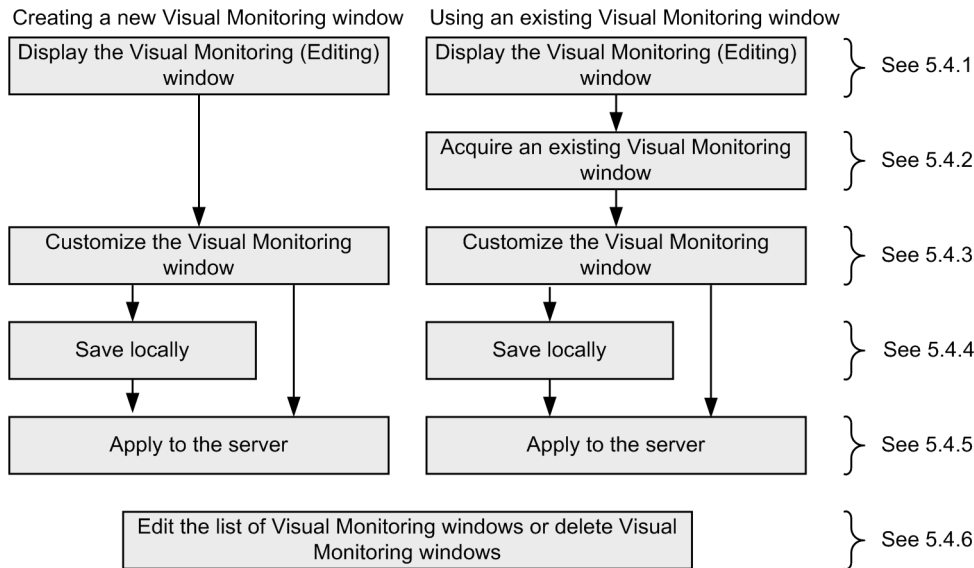
To check the applied monitoring tree, log in to JP1/IM - Manager (Central Scope), and then check the Monitoring Tree window.

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.

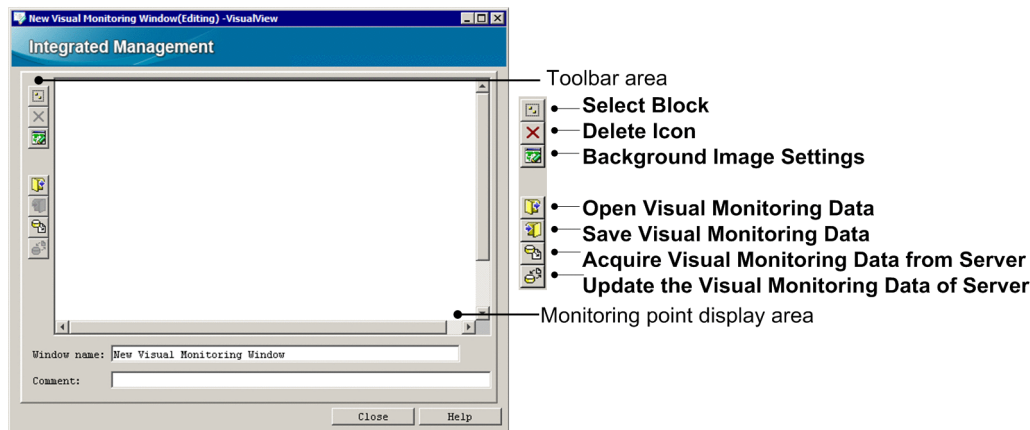
Figure 5–10: Procedure for using the GUI to create a Visual Monitoring window



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 5–11: Visual Monitoring (Editing) window



To open an edit window for the Visual Monitoring window:

1. In the Monitoring Tree (Editing) window, from the menu bar, select **Edit**, and then **Create New Visual Monitoring Window**.

The Visual Monitoring (Editing) window is launched.


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. If you have the settings (a CSV file) for a Visual Monitoring window that have been saved locally, you can also use those 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 (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 permission.

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.

(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:

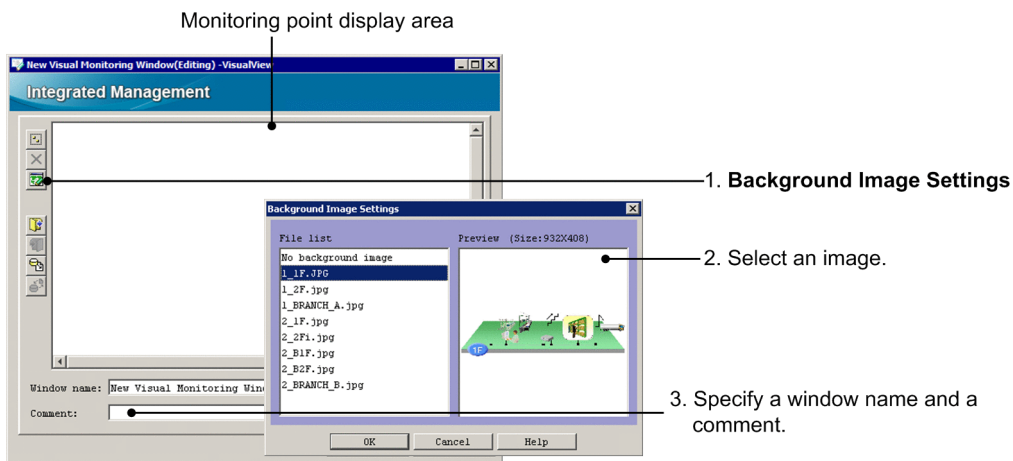
- Set a background image
- Add monitoring nodes
- Delete monitoring nodes
- Set attributes of monitoring nodes
- Change the monitoring status of monitoring nodes
- Search for monitoring nodes

(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 5–12: 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.

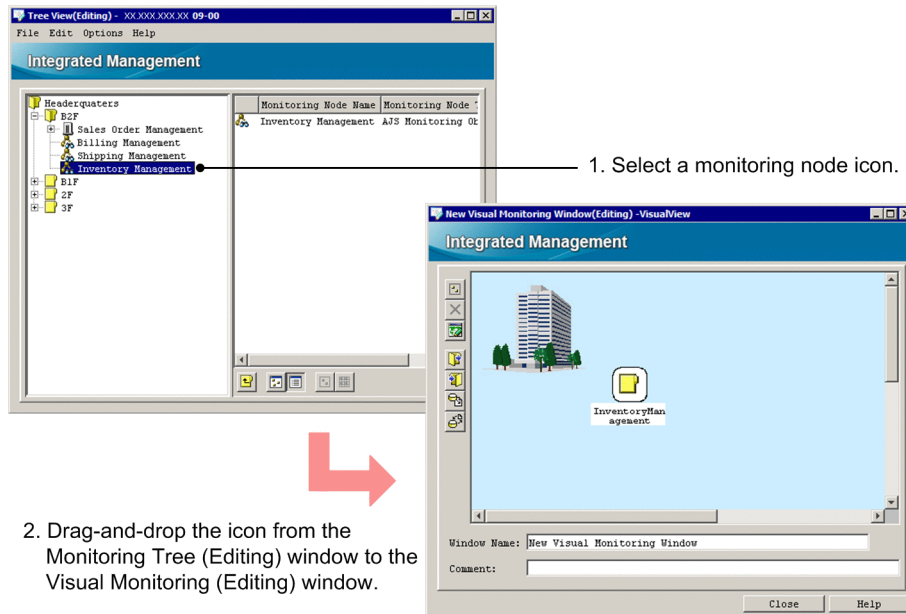
Hints on Visual Monitoring window operation

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 5–13: Adding monitoring nodes to a Visual Monitoring window



1. Select a monitoring node icon.

2. Drag-and-drop the icon from the Monitoring Tree (Editing) window to the Visual Monitoring (Editing) 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 *Chapter 4. Lists of System-Monitoring Objects (for Central Scope)* in the manual *JP1/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 .

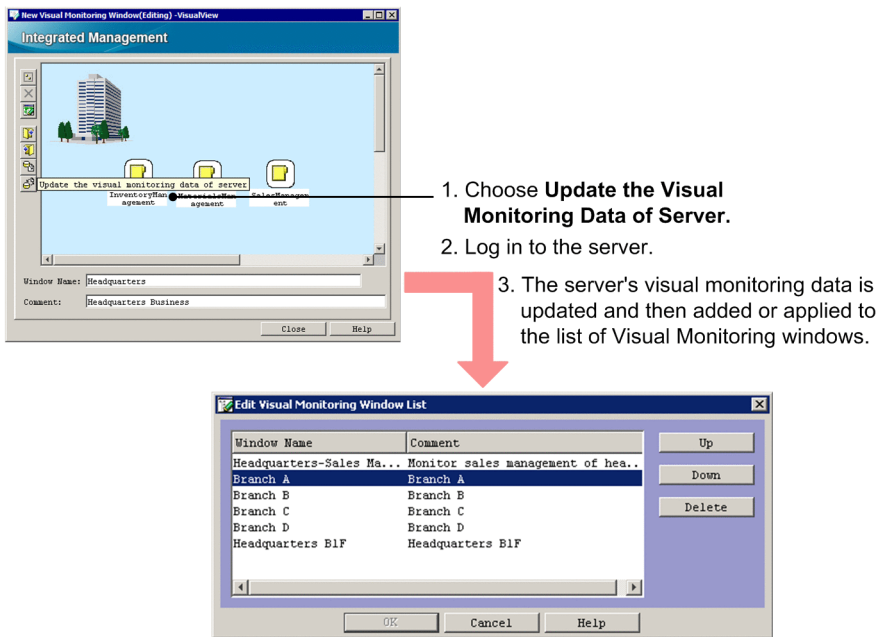
2. Save the Visual Monitoring window under a desired file name in any folder.

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 5–14: 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 (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 permission.

For the host to connect, enter the host name of JP1/IM - Manager.

3. The customized Visual Monitoring window is applied to the server.

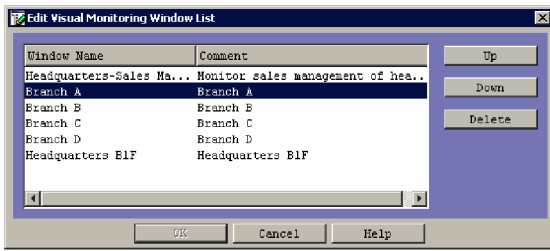
A dialog box is displayed while the processing is in progress. This dialog box closes when the processing is completed. When the Visual Monitoring window has been applied to the manager, the Visual Monitoring window is added or applied to the list of visual windows.

To check the applied Visual Monitoring window, log in to JP1/IM - Manager (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 5–15: 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**, **Down**, 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 (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 permission.
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 Editing the saved CSV file to create the Monitoring Tree window

You can change the environment settings of many monitoring nodes in the batch mode by editing the locally saved CSV files.

For details about the setup procedure, see the following:

Using the CSV files to create monitoring windows (Monitoring Tree window):

- Saving monitoring window settings as a CSV file
See [5.3.5 Saving a customized monitoring tree at the local host](#).
- Creating monitoring windows from the CSV files
See [5.3.4 Customizing a monitoring tree](#).
- Details of the configuration file for monitoring tree
See *Configuration file for monitoring tree* in *Chapter 2. Definition Files* in the manual *JP1/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 4.8 *Guide function* in the *JP1/Integrated Management - Manager Overview and System Design Guide*.
- Format of a guide information file
See *Guide information file (jcs_guide.txt)* in *Chapter 2. Definition Files* in the manual *JP1/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	Language type	Language encoding JP1/IM - Manager uses for operation	Guide information file to be edited
Windows ^{#1}	Japanese ^{#2}		<i>Scope-path</i> \conf\jcs_guide_sjis.txt
			<i>shared-folder</i> \jplscope\conf\jcs_guide_sjis.txt
	English ^{#3}		<i>Scope-path</i> \conf\jcs_guide.txt
			<i>shared-folder</i> \jplscope\conf\jcs_guide.txt
	Chinese ^{#4}		<i>Scope-path</i> \conf\jcs_guide_GB18030.txt ^{#5}
			<i>shared-folder</i> \jplscope\conf\jcs_guide_GB18030.txt ^{#5}
UNIX ^{#1}	Japanese	Shift JIS	/etc/opt/jplscope/conf/jcs_guide_sjis.txt
			<i>shared-directory</i> /jplscope/conf/jcs_guide_sjis.txt
	EUC	/etc/opt/jplscope/conf/jcs_guide_euc.txt	

OS	Language type	Language encoding JP1/IM - Manager uses for operation	Guide information file to be edited
			<i>shared-directory</i> /jplscope/conf/jcs_guide_euc.txt
		UTF-8	/etc/opt/jplscope/conf/jcs_guide_UTF-8.txt
			<i>shared-directory</i> /jplscope/conf/jcs_guide_UTF-8.txt
		English	
			<i>shared-directory</i> /jplscope/conf/jcs_guide.txt
	Chinese		/etc/opt/jplscope/conf/jcs_guide_GB18030.txt ^{#5}
			<i>shared-directory</i> /jplscope/conf/jcs_guide_GB18030.txt ^{#5}

#1

The language encoding JP1/IM - Manager uses for operation determines which guide information file is to be edited. Edit the guide information file corresponding to the applicable language encoding. Guide information files for unsupported language encodings are not provided with JP1/IM products.

If you want to use a guide-message file in such cases, use a text editor to create one.

#2

In the case of Japanese OS, JP1/IM - Manager uses this language encoding for operation.

#3

In the case of English OS, JP1/IM - Manager uses this language encoding for operation.

#4

In the case of Chinese OS, JP1/IM - Manager uses this language encoding for operation.

#5

The user must create this file manually; it is not created during installation.

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	<i>system-drive</i> : \Program Files\Hitachi\HNTRLib2\spool\#
UNIX	/var/opt/hitachi/HNTRLib2/spool/

#: In Windows, this value might be different depending on the environment because the value of *system-drive*: \Program Files is determined by the setting of an OS environment variable at the time of installation.

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

- When JP1/IM - Manager was reloaded:

KAVB7394-I

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).

In JP1/IM - Manager that has been installed as a new installation, this setting (issuance of a warning JP1 event) is initially enabled. In JP1/IM - Manager that has been installed as an upgrade installation, the same setting that was specified in the previous version is initially retained. 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 *JP1/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 *Chapter 2. Definition Files* in the manual *JP1/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 JP1/IM - Manager that has been installed as a new installation, this setting is initially enabled. In JP1/IM - Manager that has been installed as an upgrade installation, the same setting that was specified in the previous version is initially retained. 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 *JP1/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 *Chapter 2. Definition Files* in the manual *JP1/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

You can enable or disable the function that automatically deletes the status change events of monitoring objects when JP1 event handling is completed.

In JP1/IM - Manager that has been installed as a new installation, this function is initially enabled. In JP1/IM - Manager that has been installed as an upgrade installation, the same setting that was specified in the previous version is initially retained. You should change the setting as appropriate to your operation.

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 *Chapter 2. Definition Files* in the manual *JP1/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 *JP1/Base User's Guide*.
5. Start JP1/IM - Manager.

5.7.4 Settings for initializing monitoring objects when JP1 events are received

You can enable or disable the function that initializes monitoring objects when JP1 events are received.

In JP1/IM - Manager that has been installed as a new installation, this function is initially disabled. In JP1/IM - Manager that has been installed as an upgrade installation, the same setting that was specified in the previous version is initially retained. You should change the setting as appropriate to your operation.

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 Chapter 2. *Definition Files* in the manual *JP1/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 *JP1/Base User's Guide*.
4. Start JP1/IM - Manager.

5.7.5 Setting the memory-resident status change condition function

You can enable or disable the function for making status change conditions resident in memory.

In JP1/IM - Manager that has been installed as a new installation, this function is initially enabled. In JP1/IM - Manager that has been installed as an upgrade installation, the same setting that was specified in the previous version is initially retained. You should change the setting as appropriate to your operation.

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 Chapter 2. *Definition Files* in the manual *JP1/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 *JP1/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 (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 *Chapter 2. Definition Files* in the manual *JP1/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 *Chapter 2. Definition Files* in the manual *JP1/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 *Chapter 2. Definition Files* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

5.7.7 Settings for suppressing the display of a monitoring node name and the icon margin

The following subsections explain the procedures for suppressing the display of the monitoring node name and the icon margin of a monitoring node for each window to which the settings are to be applied.

(1) Suppressing the display of a monitoring node name and the icon margin (for map display in the Monitoring Tree window and Visual Monitoring window)

The procedure for suppressing the display of a monitoring node name and the icon margin in map display in the Monitoring Tree window and the Visual Monitoring window is described below. These settings take effect when you log in to JP1/IM - Manager (Central Scope).

1. Open the system profile of Central Scope (jcs_sysprofile_xxx.def) by using a text editor.
The system profile of Central Scope (jcs_sysprofile_xxx.def) is stored in the following folder:
 - In Windows (physical host)

Scope-path\conf

- In Windows (logical host)
shared-folder\jplscope\conf
- In UNIX (physical host)
/etc/opt/jplscope/conf
- In UNIX (logical host)
shared-directory/jplscope/conf

2. Edit the contents of the `FrameVisible` parameter.

About the file settings

For details about the file settings, see *System profile of Central Scope (jcs_sysprofile_xxx.def)* in Chapter 2. *Definition Files* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

(2) Suppressing the display of a monitoring node name and the icon margin (for map display in the Monitoring Tree (Editing) window and Visual Monitoring (Editing) window)

The procedure for suppressing the display of a monitoring node name and the icon margin for map display in the Monitoring Tree (Editing) window and Visual Monitoring (Editing) window is described below. These settings take effect when you open the Monitoring Tree (Editing) window or Visual Monitoring (Editing) window.

1. Open the system profile of the Central Scope viewer (`system.conf`) by using a text editor.

The system profile of the Central Scope viewer (`system.conf`) is stored in the following folder:

- For OSs in Japanese
View-path\conf\sovsystem\ja
- For OSs in English
View-path\conf\sovsystem\en
- For OSs in Chinese
View-path\conf\sovsystem\zh

2. Edit the contents of the `FrameVisible` parameter.

About the file settings

For details about the file settings, see *System profile of the Central Scope viewer (system.conf)* in Chapter 2. *Definition Files* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

5.7.8 Settings of the status color of a monitoring node name and monitoring node

The following subsections explain the procedure for setting the status color of a monitoring node name and monitoring node for each window to which the settings are to be applied.

(1) Setting the status color of a monitoring node name and monitoring node (for the Monitoring Tree window and Visual Monitoring window)

The procedure for setting the status color of a monitoring node name and monitoring node in the Monitoring Tree window and Visual Monitoring window is described below. These settings take effect when you log in to JP1/IM - Manager (Central Scope).

1. Open the system profile of Central Scope (`jcs_sysprofile_xxx.def`) by using a text editor.

The system profile of Central Scope (`jcs_sysprofile_xxx.def`) is stored in the following folder:

- In Windows (physical host)
`Scope-path\conf`
- In Windows (logical host)
`shared-folder\jp1scope\conf`
- In UNIX (physical host)
`/etc/opt/jp1scope/conf`
- In UNIX (logical host)
- `shared-directory/jp1scope/conf`

2. Change the contents of the range of fields from [ColorItem] to [End] in which a color status you want to change is defined.

If you want to set the status color of a monitoring node name, change the RGB values in the range of fields from [TEXT] to [End].

If you want to set the status color of a monitoring node, change the RGBA values in the range of fields from [Label] to [End].

About the file settings

For details about the file settings, see *System profile of Central Scope (jcs_sysprofile_xxx.def)* in Chapter 2. *Definition Files* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

(2) Setting the status color of a monitoring node name and monitoring node (in the Monitoring Tree (Editing) window and Visual Monitoring (Editing) window)

The procedure for setting the status color of a monitoring node name and monitoring node in the Monitoring Tree (Editing) window and Visual Monitoring (Editing) window is described below. These settings take effect when you open the Monitoring Tree (Editing) window or Visual Monitoring (Editing) window. Note that only the settings of the status color for the initial state are applied to the window.

1. Open the system profile of the Central Scope viewer (`system.conf`) by using a text editor.

The system profile of the Central Scope viewer (`system.conf`) is stored in the following folder:

- For OSs in Japanese
`View-path\conf\sovsystem\ja`
- For OSs in English
`View-path\conf\sovsystem\en`
- For OSs in Chinese
`View-path\conf\sovsystem\zh`

2. Change the contents of the range of fields from [ColorItem] to [End] in which the initial state settings are defined.
If you want to set the status color of a monitoring node name, change the RGB values in the range of fields from [TEXT] to [End].
If you want to set the status color of a monitoring node, change the RGBA values in the range of fields from [Label] to [End].

About the file settings

For details about the file settings, see *System profile of the Central Scope viewer (system.conf)* in Chapter 2. *Definition Files* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

5.7.9 Settings for suppressing the movement of the icon of a monitoring node

The procedure for suppressing the movement of the icon of a monitoring node in map display in the Monitoring Tree window and Visual Monitoring window is described below. These settings take effect when you log in to JP1/IM - Manager (Central Scope).

1. Open the system profile of Central Scope (`jcs_sysprofile_xxx.def`) by using a text editor.
The system profile of Central Scope (`jcs_sysprofile_xxx.def`) is stored in the following folder:
 - In Windows (physical host)
`Scope-path\conf`
 - In Windows (logical host)
`shared-folder\jp1scope\conf`
 - In UNIX (physical host)
`/etc/opt/jp1scope/conf`
 - In UNIX (logical host)
`shared-directory/jp1scope/conf`
2. Edit the contents of the `Movable` parameter.

About the file settings

For details about the file settings, see *System profile of Central Scope (jcs_sysprofile_xxx.def)* in Chapter 2. *Definition Files* in the manual *JP1/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 a system hierarchy (IM configuration)**
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)**
When the product to be linked is JP1/Cm2/SSO version 8 or earlier, or HP NNM version 8 or earlier, SNMP traps are issued instead of 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 monitoring jobnets using JP1/IM in the *JP1/Automatic Job Management System 3 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 monitoring jobnets using JP1/IM in the *JP1/Automatic Job Management System 3 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/Cm2/SSO

This subsection describes the setup process for linking with JP1/Cm2/SSO version 8 or earlier.

(1) Setup for using system-monitoring objects for monitoring

To link with JP1/Cm2/SSO version 8 or earlier, you must convert SNMP traps issued by JP1/Cm2/SSO via HP NNM version 8 or earlier to JP1 events to enable Central Scope to monitor them.

For additional details about setting up the linkage, see the following manual:

- Description of converting SNMP traps to JP1 events
See the description of the settings for event conversion in the *JP1/Base User's Guide*.

(a) For the JP1/Cm2/SSO host

To perform setup on the manager where JP1/Cm2/SSO version 8 or earlier (and 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. The settings for SNMP trap conversion in JP1/Base are the same as those used to link HP NNM version 8 or earlier.

For details about how to set SNMP trap conversion, see the chapter that describes the event conversion settings in the *JP1/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 for NNM.
- Set the JP1 event destination.
- Set the filter definition file (`snmpfilter.conf`).

2. Edit the filter definition file for SNMP trap conversion in JP1/Base.

Add the contents of the sample file (`snmpfilter_im_sample.conf`) that contains the settings for converting the SNMP traps handled by Central Scope to the filter definition file for SNMP trap conversion (`snmpfilter.conf`) in JP1/Base.

The file names are as follows:

- Filter definition file for SNMP trap conversion

In Windows:

```
Base-path\conf\evtgw\snmpfilter.conf
```

In UNIX:

```
/etc/opt/jp1base/conf/evtgw/snmpfilter.conf
```

- Sample file in Central Scope

In Windows:

```
Scope-path\conf\snmpfilter_im_sample.conf
```

In UNIX:

```
/etc/opt/jp1scope/conf/snmpfilter_im_sample.conf
```

Important

- The plus sign (+) at the beginning of the sample file is a setting that SNMP trap variable binding to JP1 events is loaded. Do not remove it.
- The size of a filter definition file is limited. In the filter definition file, add only the definitions of SNMP traps that are to be monitored in the operating environment.

For details about the limitation on the size of a filter definition file, see the *JP1/Base User's Guide*.

3. Set the daemon operation definition files for JP1/Cm2/SSO.

Edit the settings in the daemon operation definition files (`ssoapmon.def` and `ssocolmng.def`) for JP1/Cm2/SSO version 8 or earlier so that SNMP traps will contain the information required by Central Scope.

Set the following two files:

- Location of the file

```
JP1/Cm2/SSO-installation-folder\conf\ssoapmon.def
```

- Settings

Configure the issuance of events that indicate changes in the process status (`threshold-event`) and the loading of source names in variable bindings (`source-name`).

```
threshold-event: on
source-name: on
```

- Location of the file

```
JP1/Cm2/SSO-installation-folder\conf\ssocolmng.def
```

- Settings

Configure the issuance of events that indicate changes in the monitoring status of resource threshold values.

```
threshold-event: on
```

(2) Setup for automatic generation of a monitoring tree

JP1/Cm2/SSO version 8 or earlier supports automatic generation of a monitoring tree. To enable the linkage for automatic generation, set up the linkage program.

For additional details about setting up the linkage, see the following manual:

- Description of converting SNMP traps to JP1 events
See the description of the settings for event conversion in the *JP1/Base User's Guide*.

(a) For the JP1/Cm2/SSO host

1. Setting up the linkage program for JP1/Cm2/SSO

Execute the following command to enable the collection of definition information from JP1/Cm2/SSO version 8 or earlier when generation of the monitoring tree is automatic:

```
ssoimsetup -install (to enable linkage for automatic generation)
```

If the setup described above is not completed, a monitoring object for JP1/Cm2/SSO version 8 or earlier is not created when an attempt is made to generate a monitoring tree automatically.

To release the linkage, execute the following command:

```
ssoimsetup -uninstall (to release the linkage for automatic generation)
```

Note that the following conditions must be satisfied to automatically create the monitoring objects for JP1/Cm2/SSO version 8 or earlier when generation of a monitoring tree is automatic:

- Before you automatically generate a monitoring tree for JP1/Cm2/SSO version 8 or earlier, close the window of JP1/Cm2/SSO. If these windows remain open, definitions cannot be obtained from SSO.
- When a monitoring tree is automatically generated for JP1/Cm2/SSO version 8 or earlier, the definitions to be obtained from SSO are the resource information whose collection status is `Being collected`.

5.8.3 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 *JP1/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 *JP1/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)
```

5.8.4 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 additional details about setting up the linkage, see the following manual:

- Description of conversion from SNMP traps to JP1 events
See the description of event conversion settings in the *JP1/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. The JP1/Base SNMP trap conversion settings are the same as those used to link JP1/Cm2/SSO version 8 or earlier.

For details about how to set the SNMP trap conversion function, see the chapter that describes event conversion settings in the *JP1/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/jp1base/conf/evtgw/snmpfilter.conf
```

- Sample file of Central Scope

In Windows:

```
Scope-path\conf\snmpfilter_im_sample.conf
```

In UNIX:

```
/etc/opt/jp1scope/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 *JP1/Base User's Guide*.

5.8.5 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 *JP1/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.

5.8.6 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 *JP1/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 (`pamjplev.conf`) for JP1/PAM as follows:

- File to be set
`pamjplev.conf`
- Settings
Specify `Y` for the settings as to whether to issue JP1 events (`jplevt_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.
`jplevt_flag=Y`
`metricNW=Y`
:

5.8.7 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 server-oriented tree by automatic generation, you must include in the JP1/IM system configuration all operations management servers and business servers.

5.8.8 Setup for linkage with HiRDB

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*.

5.8.9 Setup for linkage with JP1/ServerConductor

To use a JP1/ServerConductor system-monitoring object, you must set JP1/ServerConductor to report to JP1/IM alerts detected by JP1/ServerConductor as JP1 events.

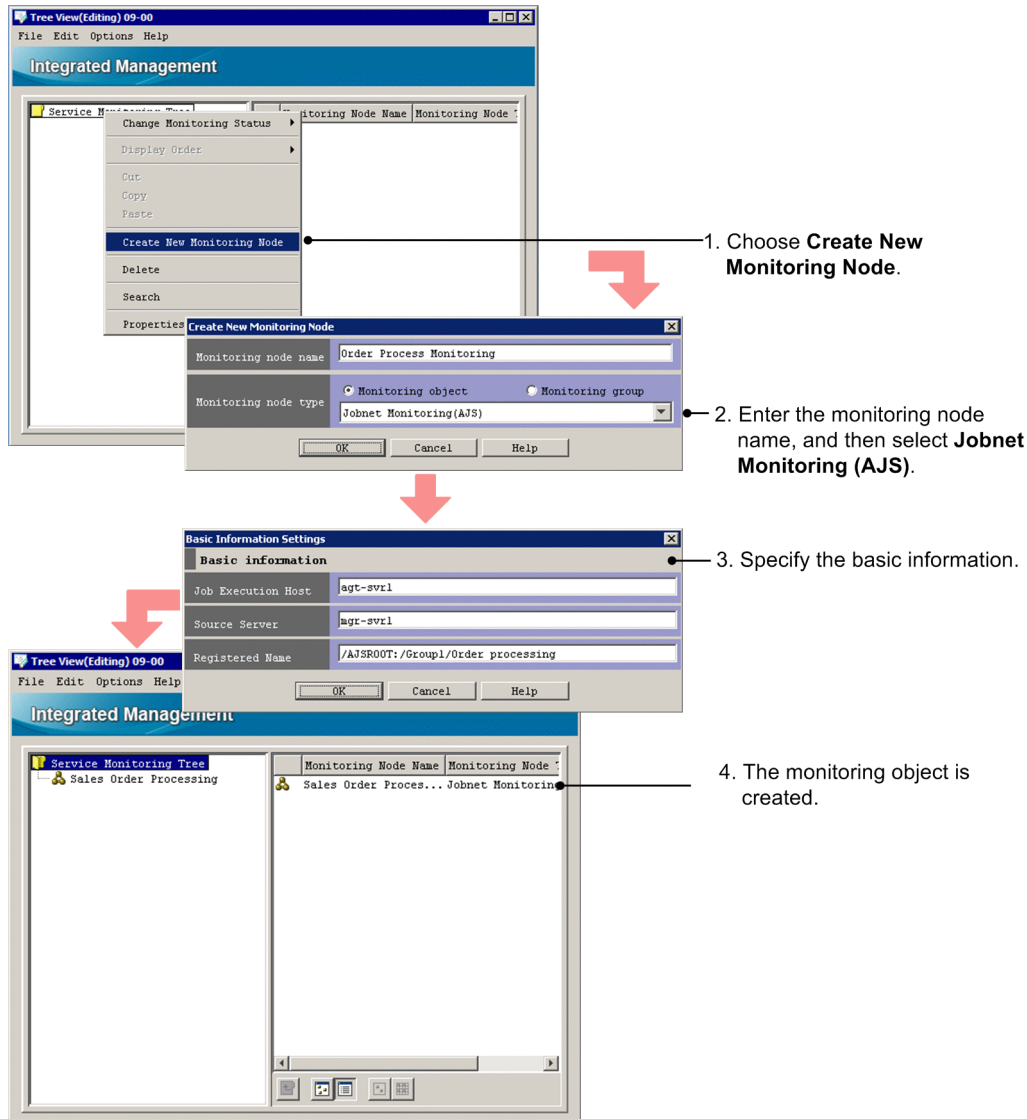
5.9 Examples of monitoring object creation

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 5–16: 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 monitoring object (CPU monitoring by JP1/Cm2/SSO)

If you want to monitor items that are not supported by the automatic generation of monitoring trees (for example, you want to use JP1/Cm2/SSO version 8 or earlier to monitor CPUs), you need to create a monitoring object manually.

(1) What you need to know before creating the object

If you want to use JP1/IM to monitor products that output SNMP traps, such as JP1/Cm2/SSO version 8 or earlier, you need to convert SNMP traps to JP1 events first. This is necessary because Central Scope uses the attribute names and attribute values of JP1 events as keys for monitoring objects.

You can use JP1/Base SNMP trap conversion to convert SNMP traps to JP1 events. With SNMP trap conversion, you can map the SNMP fields to the attributes of JP1 events.

The following table describes the correspondence between the attributes of a JP1 event that is converted from an SNMP trap and the fields of the SNMP trap.

Table 5–6: JP1 event attributes and SNMP trap fields

JP1 event created as a result of conversion		SNMP trap to be converted	
Basic attribute		Message	PDU Type
Extended attribute	Common information	SEVERITY	specific trap
		--	--
	Program-specific information	SNMP_OID	Enterprise
		SNMP_DATE	Time stamp
		SNMP_SOURCE	Agent address
		SNMP_SEVERITY	Specific trap
		SNMP_URL	--
		SNMP_VARBIND_RESULT	--
		SNMP_VARBIND_NUM	--
		SNMP_VARBIND1	Value of Data 1 in the variable binding
		SNMP_VARBIND2	Value of Data 2 in the variable binding
		(Omitted)	(Omitted)
SNMP_VARBIND28	Value of Data 28 in the variable binding		

Legend:

--: Indicates that no applicable information exists for the corresponding program-specific information in the message.

For details about SNMP trap conversion, see the *JP1/Base User's Guide*.

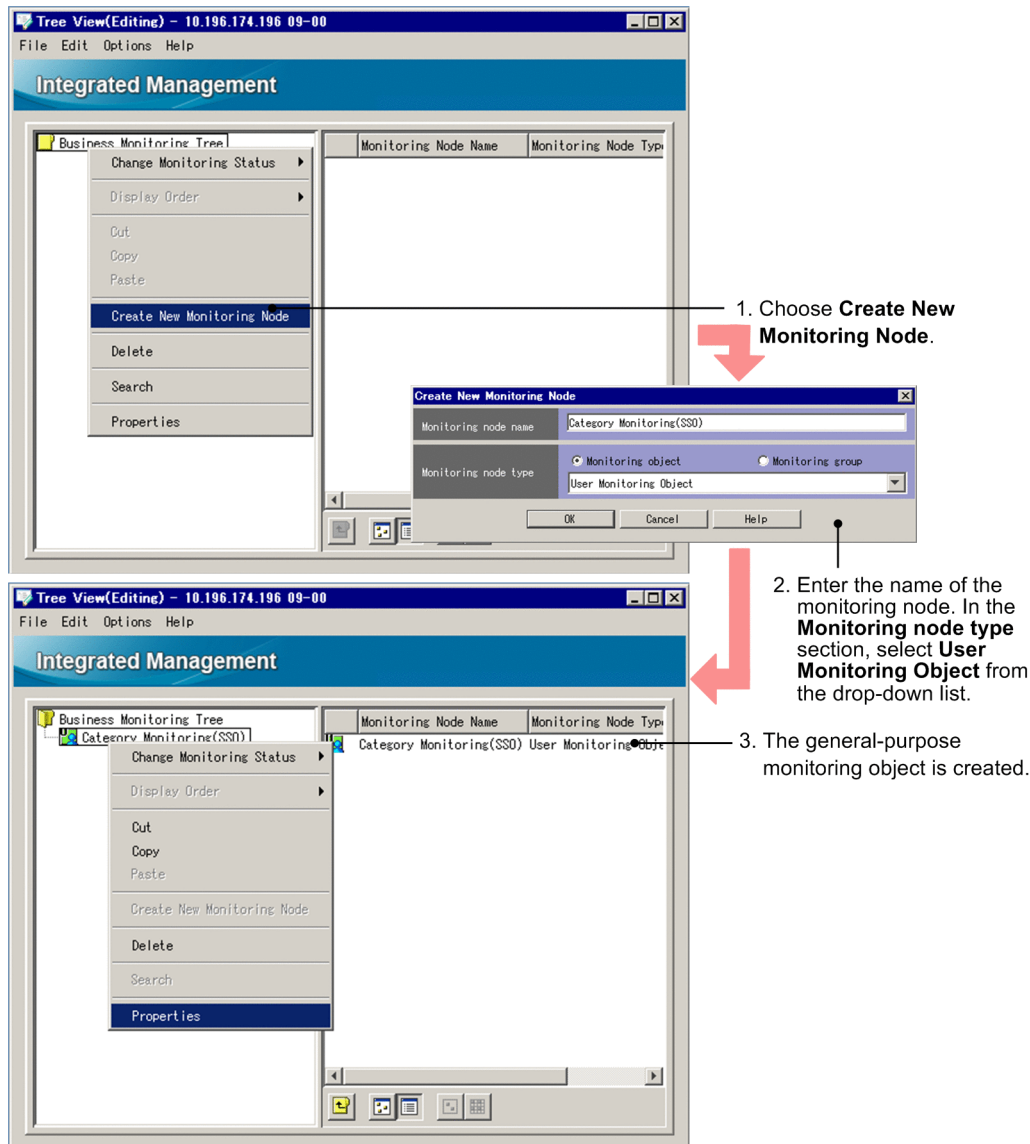
(2) Confirmation before creating a monitoring object

Confirm the following before you create a monitoring object for monitoring CPUs.

- The setup of JP1/Cm2/SSO version 8 or earlier has been completed on the agents, and JP1 events are sent to the manager.
In Central Console, in the Event Console window, make sure that the events for monitoring CPUs by JP1/Cm2/SSO version 8 or earlier are displayed.
- On agents on which JP1/Cm2/SSO version 8 or earlier monitors CPUs, the setup for linkage with Central Scope has been completed.
When you automatically generate a monitoring tree in Central Scope, make sure that an SSO Monitoring monitoring object is generated and that the status of the object changes when JP1 events are received.

(3) Creating a monitoring object (CPU monitoring)

Figure 5–17: Creating a general monitoring object



To create a monitoring object:

1. In the Monitoring Tree (Editing) window, from the menu bar, choose **Edit**, and then **Create New Monitoring Node**. The Create New Monitoring Node window appears.
2. Enter the node name, select the node type, and then click the **OK** button.

Table 5–7: Settings in the Monitoring node name and Monitoring node type

Item	Setting
Monitoring node name	Enter any name. We recommend a name that is easily recognizable. In this example, enter <i>Category Monitoring (SSO)</i> .
Monitoring node type	Click Monitoring object . From the drop-down list, select User Monitoring Object .

The monitoring object *Category Monitoring (SSO)* is added to the monitoring tree.

(4) Setting up the monitoring object (CPU monitoring)

Figure 5–18: Setting up the general monitoring object (adding a status change condition - 1)

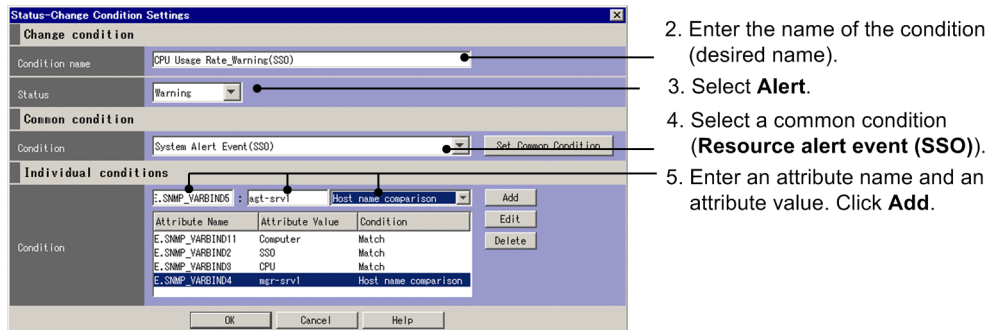
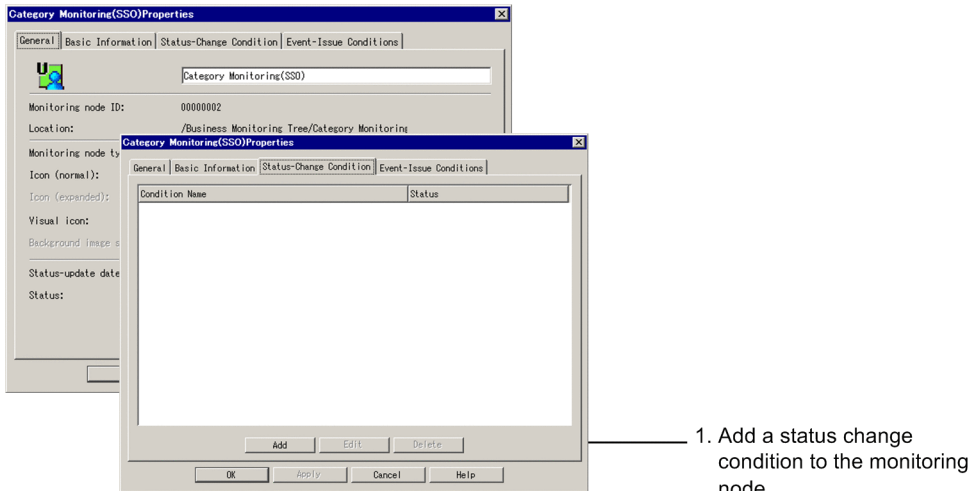
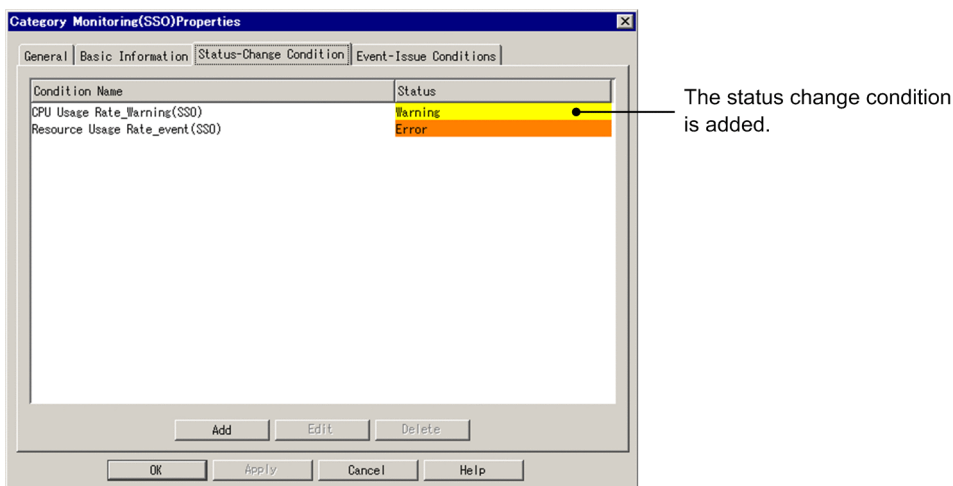


Figure 5–19: Setting up the general monitoring object (adding a status change condition - 2)



To set up the monitoring object:

1. Select the created monitoring object (**Category Monitoring (SSO)**). From the menu bar, choose **Edit**, and then **Properties**.

The Properties window appears.

- In the Properties window, choose the **Status-Change Condition** tab. On the **Status-Change Condition** page, click the **Add** button.

The Status-Change Condition Settings window appears.

- In the Status-Change Condition Settings window, specify a common condition, individual conditions, and other items.

The status of the selected monitoring node changes when JP1/IM - Manager receives JP1 events. Specify the types of JP1 events that cause the monitoring node status to change.

Enter a status change condition and then click the **OK** button. (When you click the **OK** button, the **Status-Change Condition** page returns.) If you want to enter another status change condition, click the **Add** button again and enter a condition in the Status-Change Condition Settings window.

In the Status-Change Condition Settings window, enter or select values as described in the following tables.

Table 5–8: Settings in the Status-Change Condition Settings

Condition name (any)	Status	Common condition
CPU usage rate alert event (SSO)	Alert	Resource alert event (SSO)
CPU usage rate error event (SSO)	Error	Resource error event (SSO)

For each status change condition, specify individual conditions as follows. Click **Add** each time you add an individual condition.

Table 5–9: Settings in the Status-Change Condition Settings (individual conditions section)

Monitoring node attribute name	Attribute name	Attribute value (example)	Condition
Category name	E.SNMP_VARBIND2	SSO	Match
Group name	E.SNMP_VARBIND3	Computer	Match
Resource name	E.SNMP_VARBIND4	CPU usage rate ^{#1}	Match
Event-issuing host	E.SNMP_VARBIND11	mgr-svr1 ^{#2}	Host name comparison
Host name	E.SNMP_VARBIND12	agt-srv1 ^{#3}	Host name comparison

#1: Specify the name of a resource that JP1/Cm2/SSO version 8 or earlier is to monitor.

- For monitoring CPUs: CPU usage rate
- For monitoring memory: Memory usage rate

#2: Specify the event source host name. You can obtain the host name by executing `gethostname`. Specify the host name in the format displayed by the `hostname` command.

#3: Specify the name of the host that is to be monitored. You can obtain host name by executing `gethostbyaddr`. When there is a DNS server, specify the name suffixed with the suffix provided by the DNS server. If there is no DNS server, specify the host name in the format written in the `hosts` file.

- When you have finished the settings, on the **Status-Change Condition** page, click the **OK** button.

In the Monitoring Tree (Editing) window, from the menu bar, choose **File**, and then **Update Server Tree**. Check whether the monitoring node has been added to the monitoring object database of Central Scope.

You can also use a `Category Monitoring (SSO)` system-monitoring object to create the `CPU Usage Rate Management (SSO)` monitoring object for JP1/Cm2/SSO version 8 or earlier. After you create a `Category Monitoring (SSO)` system-monitoring object, add the required individual conditions to the status change condition.

! Important

For JP1/IM to monitor JP1/Cm2/SSO version 8 or earlier, all JP1/Cm2/SSO and JP1/Base on the agents must be version 7 or 8.

If JP1/Cm2/SSO and JP1/Base on the agents are version 6, JP1/IM can monitor them. However, JP1/IM cannot automatically collect information from JP1/Cm2/SSO or JP1/Base, which results in extensive manual work in addition to the above procedure. For this reason, we do not recommend monitoring of JP1/Cm2/SSO version 6.

Note that the product name of JP1/Cm2/SSO is JP1/PFM/SSO for version 7 and JP1/SSO for version 6.

5.9.3 Example of creating a general 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.

Note

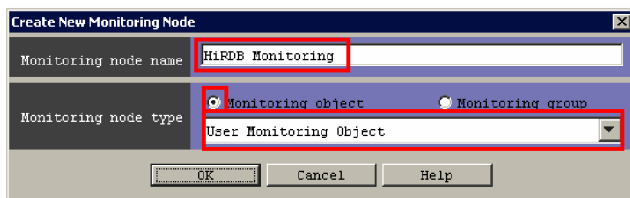
HiRDB version 07-02 or later can issue JP1 events, not JP1/SES events (the output settings are required at HiRDB). In this case, use the system-monitoring object provided by Central Scope to create a monitoring object for HiRDB.

(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 5–20: Create New Monitoring Node window



The settings in the Create New Monitoring Node window are as follows.

Table 5–10: 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 <code>HiRDB Monitoring</code> .
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.

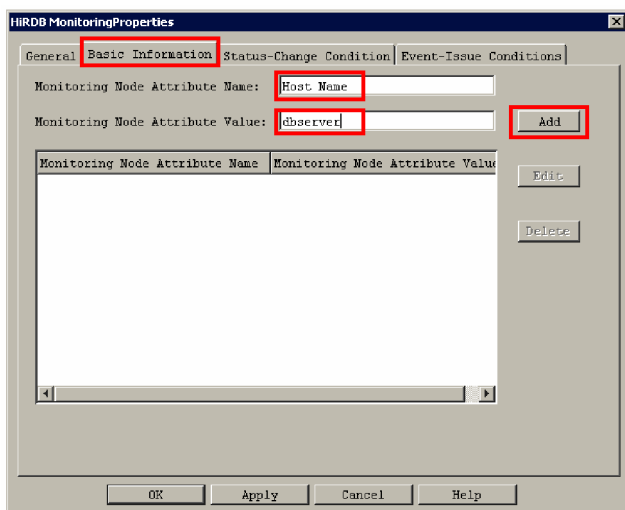
(2) Setting up the monitoring object (HiRDB monitoring)

(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 5–21: Basic Information page



The settings on the **Basic Information** page are as follows.

Table 5–11: 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 <code>HiRDB</code> .

Note: 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.

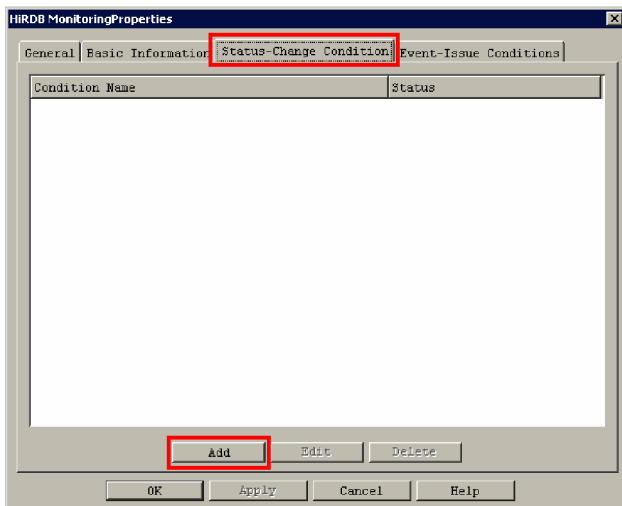
The basic information is set for the monitoring object.

(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.

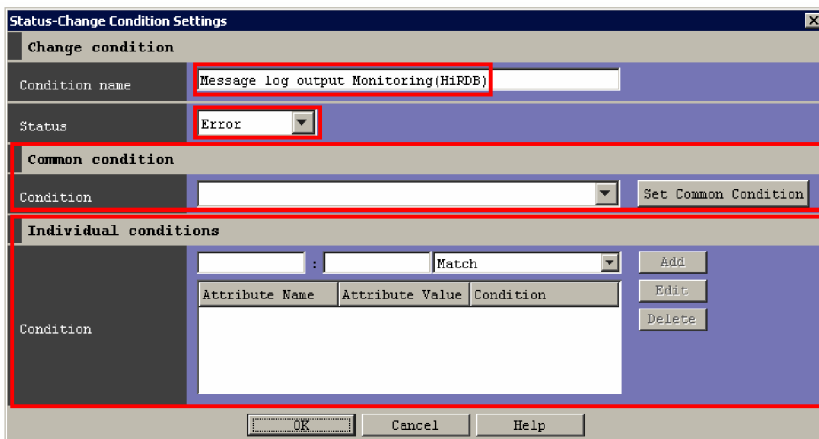
Figure 5–22: Status-Change Condition page



4. Click the **Add** button.

The Status-Change Condition Settings window appears.

Figure 5–23: Status-Change Condition Settings window



The settings in the Status-Change Condition Settings window are as follows.

Table 5–12: Settings in the Status-Change Condition Settings window

Item	Setting
Condition name	Specify a name for the condition.

Item	Setting
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.

5. After you have entered a condition name, status, common condition, and individual condition, click the **OK** button.

Specifying the common condition:

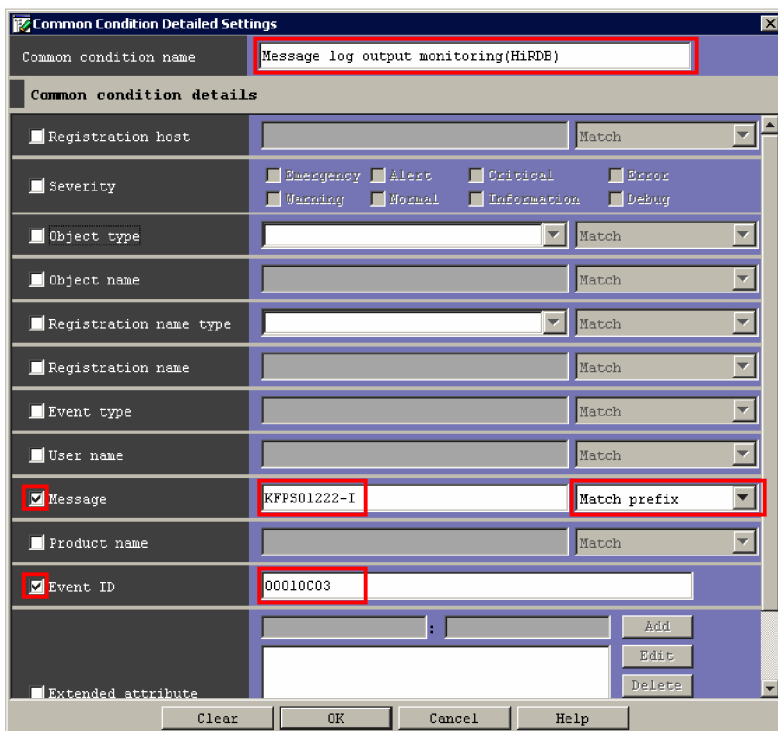
For the common condition, specify the information needed to identify the event or the product that caused the event.

To specify the common condition:

1. 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 5–24: Common Condition Detailed Settings window



The settings in the Common Condition Detailed Settings window are as follows.

Table 5–13: 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.

Item	Setting
	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 (00010C03).

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 5–14: Settings for individual conditions

Attribute name	Attribute value	Description
<code>B.SOURCESERVER</code>	<code>dbserver</code>	For the attribute name, enter <code>B.SOURCESERVER</code> 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.
<code>B.MESSAGE</code>	<i>HiRDB-server-name</i>	If product-specific message information is output as event information, use that message information for narrowing. This is because the message might contain information that identifies the location where the event occurred (such as a message log event issued by HiRDB). If you want to identify the location of the event on the basis of information in the message, enter <code>B.MESSAGE</code> as the attribute name and a keyword that can be narrowed down as the attribute value. For example, log swap messages of HiRDB contain a HiRDB server name. If you specify <code>B.MESSAGE</code> 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. If you specify <code>B.MESSAGE</code> , make sure that no message that is not monitored satisfies the conditions.

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.

5.9.4 Example of creating a general monitoring object (Cosminexus resource monitoring by JP1/Cm2/SSO)

You can use JP1/Cm2/SSO version 8 or earlier to monitor the operating performance of J2EE applications and some logical servers defined by using Cosminexus.

Central Scope allows you to link (automatically generate monitoring trees for) Cosminexus and JP1/Cm2/SSO version 8 or earlier by using the setup commands. When the following requirements are satisfied, you can automatically generate a general monitoring object that monitors the JP1 events issued when the status of the resources of the J2EE applications and logical servers monitored by JP1/Cm2/SSO changes (when Cosminexus and JP1/Cm2/SSO are linked to JP1/IM).

Requirements for automatically generating monitoring trees

- The version of Cosminexus is 06-00 or later, and the version of JP1/Cm2/SSO is 7 or 8 (the product name of JP1/Cm2/SSO version 7 is JP1/PFM/SSO).
- The products to be linked (Cosminexus and JP1/Cm2/SSO) have already been set up.
- The setup commands for linking Cosminexus and JP1/Cm2/SSO to JP1/IM have already been executed.
- JP1/Cm2/SSO version 8 or earlier is monitoring the J2EE applications or logical servers that were defined by using Cosminexus.
- In the Auto-generation - Select Configuration window, **Business Oriented Tree** is selected (no monitoring tree is automatically generated when **Server Oriented Tree** is selected).

The following table describes the types of monitoring objects you can automatically generate when Cosminexus and JP1/Cm2/SSO are linked to JP1/IM.

Table 5–15: Types of monitoring objects that can be automatically generated when Cosminexus and SSO are linked to JP1/IM

Type of monitoring object	Description	Item monitored
J2EE Server Resource Monitoring (SSO)	Monitors the status of resources used by Cosminexus J2EE servers [#] . The status of this object changes when an event related to a J2EE server resource is issued.	J2EE server
CTM Resource Monitoring (SSO)	Monitors the status of resources used by Cosminexus CTM [#] . The status of this object changes when an event related to a CTM resource is issued.	CTM
SFO Resource Monitoring (SSO)	Monitors the status of resources used by Cosminexus SFO servers [#] . The status of this object changes when an event related to an SFO server resource is issued.	SFO server
J2EE Application Resource Monitoring (SSO)	Monitors the status of resources used by Cosminexus J2EE applications [#] . The status of this object changes when an event related to a J2EE application resource is issued.	J2EE application server

[#]: The events that are monitored by the monitoring object are SNMP traps with event level `warning` or higher.

If you want to monitor the status of resources in the Cosminexus environment when the requirements for automatic generation of monitoring trees are not satisfied, you need to create a monitoring object manually.

The following describes how to manually create a monitoring object. Note that the description assumes that you want to monitor the status of resources of J2EE servers, CTM, SFO servers, and J2EE applications of Cosminexus that are defined in the following table.

Table 5–16: Information about the Cosminexus servers and applications to be monitored

Item to be monitored	Type of monitoring object	Item to be specified	Value to be entered
J2EE server	J2EE Server Resource Monitoring (SSO)	Domain name	DefaultDomain
		Logical server name	J2EE_SV1
		Name of the manager running JP1/Cm2/SSO version 8 or earlier (event-issuing host)	HostA
		Name of the host running the logical server (host name)	HostB
CTM	CTM Resource Monitoring (SSO)	Domain name	DefaultDomain
		Logical server name	CTM_SV1
		Name of the manager running JP1/Cm2/SSO version 8 or earlier (event-issuing host)	HostA
		Name of the host running the logical server (host name)	HostB
SFO server	SFO Resource Monitoring (SSO)	Domain name	DefaultDomain
		Logical server name	SFO_SV1
		Name of the manager running JP1/Cm2/SSO version 8 or earlier (event-issuing host)	HostA
		Name of the host running the logical server (host name)	HostB
J2EE application	J2EE Application Resource Monitoring (SSO)	Domain name	DefaultDomain
		Logical server name	J2EE_SV1
		Name of the manager running JP1/Cm2/SSO version 8 or earlier (event-issuing host)	HostA
		Name of the host running the logical server (host name)	HostB

When you create a monitoring object for monitoring the status of resources of the servers and applications described in the above table, you need to enter values for some items during definition. The table below describes the items you need to select as monitoring conditions and the values you need to enter. These items are underlined in the table.

Table 5–17: Items to be selected as monitoring conditions and values to be entered

Type of monitoring object	Window to be used	Monitoring node attribute name	Attribute name	Monitoring node attribute value	Condition
J2EE Server Resource Monitoring (SSO)	Basic Information Settings window	Category name	E.SNMP_VARBIND2	<u>COSMINEXUS</u>	Match
		Event-issuing host	E.SNMP_VARBIND11	<u>HostA</u> #	Host name comparison

Type of monitoring object	Window to be used	Monitoring node attribute name	Attribute name	Monitoring node attribute value	Condition
	Status-Change Condition Settings window	Host name	E.SNMP_VARBIND12	<u>HostB</u> #	Host name comparison
		Resource group name	<u>E.SNMP_VARBIND3</u>	<u>Server</u>	<u>Match</u>
		Instance name	<u>E.SNMP_VARBIND6</u>	<u>^DefaultDomain: J2EE_SV1 (:.* \$)</u>	<u>Regular expression</u>
CTM Resource Monitoring (SSO)	Basic Information Settings window	Category name	E.SNMP_VARBIND2	<u>COSMINEXUS</u>	Match
		Event-issuing host	E.SNMP_VARBIND11	<u>HostA</u> #	Host name comparison
		Host name	E.SNMP_VARBIND12	<u>HostB</u> #	Host name comparison
	Status-Change Condition Settings window	Resource group name	<u>E.SNMP_VARBIND3</u>	<u>Scheduler (CTM)</u>	<u>Match</u>
		Instance name	<u>E.SNMP_VARBIND6</u>	<u>^DefaultDomain: CTM_SV1 (:.* \$)</u>	<u>Regular expression</u>
SFO Resource Monitoring (SSO)	Basic Information Settings window	Category name	E.SNMP_VARBIND2	<u>COSMINEXUS</u>	Match
		Event-issuing host	E.SNMP_VARBIND11	<u>HostA</u> #	Host name comparison
		Host name	E.SNMP_VARBIND12	<u>HostB</u> #	Host name comparison
	Status-Change Condition Settings window	Instance name	<u>E.SNMP_VARBIND6</u>	<u>^DefaultDomain: SFO_SV1 (:.* \$)</u>	<u>Regular expression</u>
	J2EE Application Resource Monitoring (SSO)	Basic Information Settings window	Category name	E.SNMP_VARBIND2	<u>COSMINEXUS</u>
Event-issuing host			E.SNMP_VARBIND11	<u>HostA</u> #	Host name comparison
Host name			E.SNMP_VARBIND12	<u>HostB</u> #	Host name comparison
Status-Change Condition Settings window		Instance name	<u>E.SNMP_VARBIND6</u>	<u>^DefaultDomain: J2EE_SV1:API (:.* \$)</u>	<u>Regular expression</u>

#: Map beforehand as the host names the host names used by Cosminexus and the host names used by JP1/Cm2/SSO version 8 or earlier.

The following describes how to set a J2EE Server Resource Monitoring (SSO) monitoring object. The procedure for setting the monitoring objects of other types (CTM Resource Monitoring (SSO), SFO Resource Monitoring (SSO), and J2EE Application Resource Monitoring (SSO)) is omitted because the only difference is the value you enter in step 7. (For the value to be entered in step 7 for each type, see [Table 5-16 Information about the Cosminexus servers and applications to be monitored.](#))

Figure 5–25: Creating a J2EE Server Resource Monitoring (SSO) a monitoring object (steps 1 to 4)

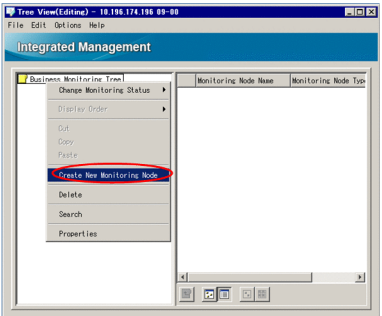
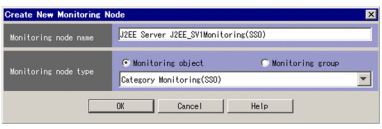
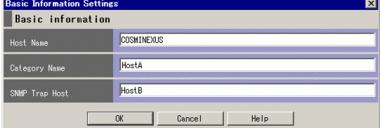
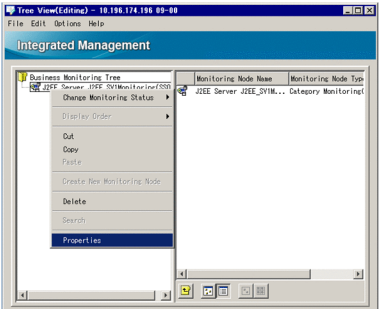
JP1/IM - View window	Step
	<p>Step 1: Operation in the Monitoring Tree (Editing) window</p> <p>Select the monitoring group to which the monitoring object is to belong. Right-click the monitoring group to display a pop-up menu. Choose Create New Monitoring Node.</p>
	<p>Step 2: Operation in the Create New Monitoring Node window</p> <ul style="list-style-type: none"> - Enter the name of the monitoring node. In the Monitoring node name box, enter <i>type logical-server-name</i> Monitoring (SSO) so that you can easily identify which logical server you are monitoring. Example: J2EE Server J2EE_SV1 Monitoring (SSO) - In the Monitoring node type section, select Category Monitoring (SSO) from the drop-down list.
	<p>Step 3: Operation in the Basic Information Settings window</p> <ul style="list-style-type: none"> - In the Category name box, enter COSMINEXUS. - In the Event-issuing host box, enter the name of the manager host running JP1/Cm2/SSO. Example: HostA - In the Host name box, enter the name of the host running the logical server. Example: HostB
	<p>Step 4</p> <p>Click the OK button to return to the Monitoring Tree (Editing) window.</p>

Figure 5–26: Creating a J2EE Server Resource Monitoring (SSO) a monitoring object (steps 5 to 8)

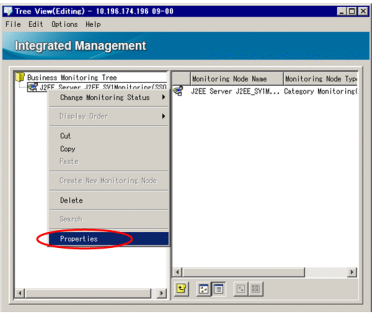
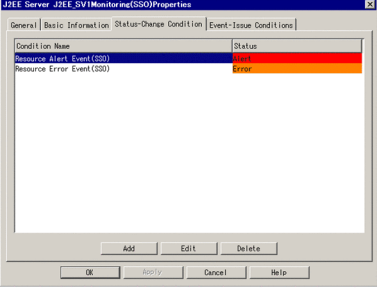
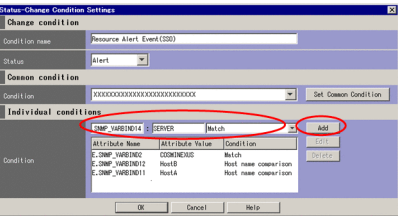
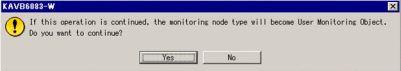
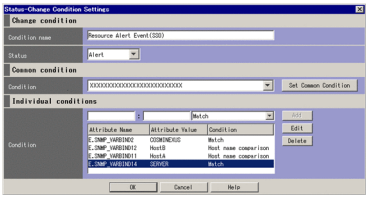
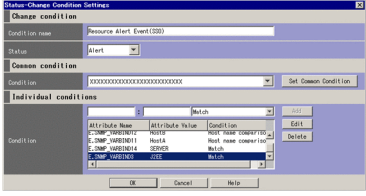
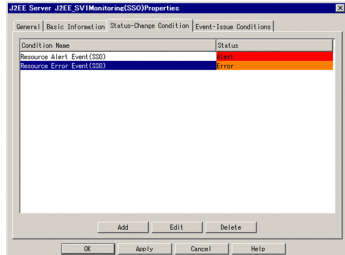
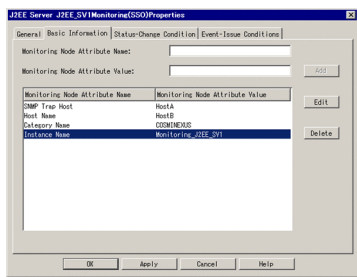
JP1/IM - View window	Step
	<p>Step 5: Operation in the Monitoring Tree (Editing) window</p> <p>Select and right-click the monitoring object created in steps 1 to 4 to display a pop-up menu. Choose Properties.</p>
	<p>Step 6: Operation in the Properties window</p> <p>Click the Status-Change Condition tab. On the Status-Change Condition page, select Resource alert event (SSO). Then click the Edit button.</p>
	<p>Step 7: Operation in the Status-Change Condition Settings window</p> <p>See Table 5-16 and add the necessary individual conditions[#]. [#] The conditions to be added differ according to the type of monitoring object. Example: For J2EE Server Resource Monitoring (SSO) E.SNMP_VARBIND3 Server E.SNMP_VARBIND6 ^DefaultDomain: J2EE_SV1 (:.* \$)</p>
	<p>Step 8</p> <p>When you click the Add button, the KAVB6083-W message appears. Click Yes.</p>

Figure 5–27: Creating a J2EE Server Resource Monitoring (SSO) a monitoring object (steps 9 to 12)

JP1/IM - View window	Step
	<p>Step 9: Operation in the Status-Change Condition Settings window</p> <p>Add other conditions as necessary (the dialog box in step 8 will not appear later).</p>
	<p>Step 10</p> <p>Click the OK button to close the Status-Change Condition Settings window.</p>
	<p>Step 11: Operation in the Properties window</p> <p>Repeat steps 7, 9, and 10 for Resource Error Event (SSO) and to also add individual conditions.</p>
	<p>Step 12: Operation in the Properties window (optional)</p> <p>Click the Basic Information tab. On the Basic Information page, enter the attribute name of the monitoring node and the attribute value[#].</p> <p>[#] The entered attribute name and value do not affect the status change conditions. However, the name and the value can be used as the conditions for searching for monitoring nodes. In the example, the instance name is <i>domain-name:logical-server-name</i>, which is easily searchable (the format is the same format as the format used for the values that are set when monitoring trees are automatically generated). For J2EE applications, the instance name is <i>domain-name:logical-server-name:J2EE-application-name</i>. Click the Apply button or the OK button to finish the settings procedure.</p>



When you have completed the settings, apply the changes to the monitoring tree (in the Monitoring Tree (Editing) window, from the menu bar, choose **File**, and then **Update Server Tree**).

6

Operation and Environment Configuration in a Cluster System (for Windows)

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 for Windows. For details about the procedure for starting up JP1/IM - Manager after setup, see *Chapter 3. Starting and Stopping JP1/IM - Manager* in the *JP1/Integrated Management - Manager Administration Guide*.

Before you use this function, make sure that your cluster software supports JP1/IM - Manager.

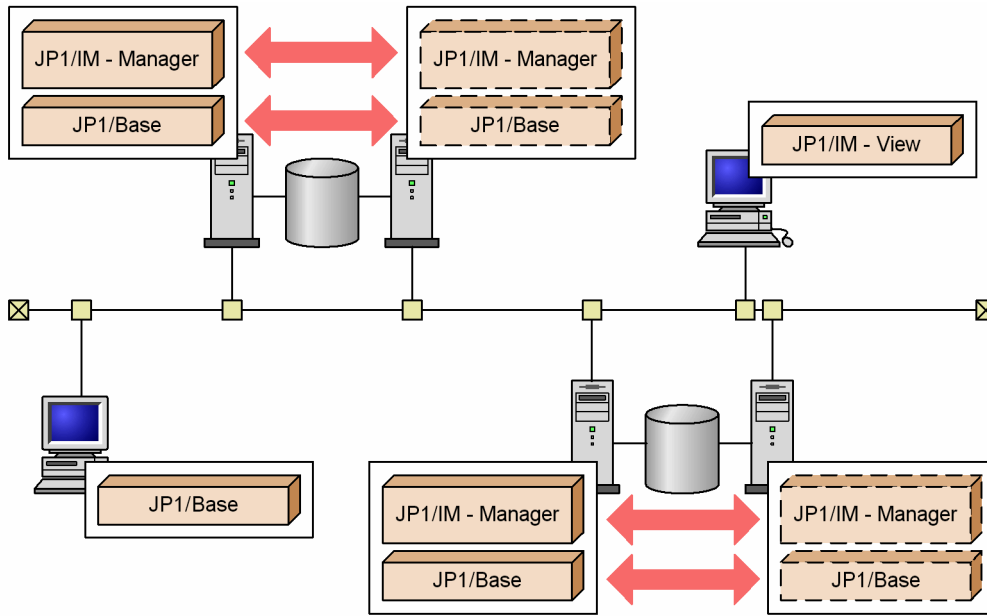
6.1 Overview of cluster operation (for Windows)

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 *JP1/Base User's Guide*.

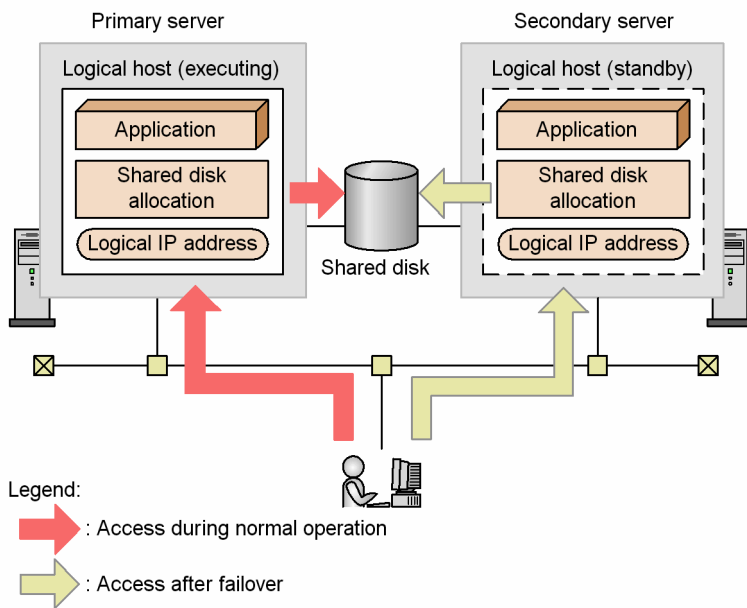
This section focuses on using a cluster system to achieve high availability (HA). This section does not describe use of a cluster system for such purposes as evening out load distribution.

6.1.1 Overview of a cluster system (for Windows)

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*.

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 (for Windows)

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.

Important

Depending on the system configuration and environment configuration, the cluster software supported by JP1/IM - Manager might 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.• 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 are not satisfied, problems such as the following might 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 (host names that are displayed when the <code>hostname</code> command is executed). (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.
Service	<ul style="list-style-type: none"> For a remote monitoring configuration, the JP1/Base log file trap service must be running.

#

With some cluster software, the IP address corresponding to a physical host name (host name that is displayed when the `hostname` command is executed) might 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.

(4) Physical host names

When IM databases are used, a physical host name must be a character string of not more than 32 characters consisting of only one-byte alphanumeric characters, `_`, `-`, `/`, `.` (period), and `@`.

(5) Logical host names

Note the following when you specify a logical host name:

- The logical host name must be specified in the `hosts` file or on the name server to enable TCP/IP communication.
- JP1/Base, the prerequisite product, must be able to handle the logical host name. For details, see the *JP1/Base User's Guide*.

- When IM databases are used, a logical host name must be a character string of not more than 32 characters consisting of only one-byte alphanumeric characters and one-byte hyphens (-).

6.1.3 JP1/IM configuration in a cluster system (for Windows)

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.

Table 6–4: File organization on the shared disk (Windows)

Function	Type of shared file	Folder name
Central Console	Definition file	<i>shared-folder</i> \jp1cons\conf\
	Log file	<i>shared-folder</i> \jp1cons\log\
	Temporary file	<i>shared-folder</i> \jp1cons\tmp\
	History file [#]	<i>shared-folder</i> \jp1cons\operation\
Central Scope	Definition file	<i>shared-folder</i> \jp1scope\conf\
	Log file	<i>shared-folder</i> \jp1scope\log\
	Temporary file	<i>shared-folder</i> \jp1scope\tmp\
	Database	<i>shared-folder</i> \jp1scope\database\
IM Configuration Management	Definition file	<i>shared-folder</i> \JP1IMM\conf\imcf\
	Log file	<i>shared-folder</i> \JP1IMM\log\imcf\
	Temporary file	<i>shared-folder</i> \JP1IMM\tmp\
	IM configuration data and profile data	<i>shared-folder</i> \JP1IMM\data\imcf\

Function	Type of shared file	Folder name
IM database	Database	<i>user-specified-folder-on-shared-disk</i> \imdb

#: Event Generation Service processing, exclusion processing caused by common exclusion-conditions, and update processing of common exclusion-conditions definition are 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.

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 6–5: Services of JP1/IM - Manager (Windows)

Displayed name	Service name
JP1/IM-Manager_ <i>logical-host-name</i>	JP1_Console_ <i>logical-host-name</i>
JP1/IM-Manager DB Server_ <i>logical-host-name</i> ^{#1}	HiRDBEmbeddedEdition_JM<n> ^{#2}
JP1/IM-Manager DB Cluster Service_ <i>logical-host-name</i> ^{#1}	HiRDBClusterService_JM<n> ^{#2}

#1

Registered when IM databases are used.

#2

<n> is a number from 1 to 9, and is the value of LOGICALHOSTNUMBER in the cluster setup information file. For details, see *Cluster setup information file (jimdbclustersetupinfo.conf)* in Chapter 2, *Definition Files* in the manual *JP1/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. Specify these names as service names in WSFC (Windows Server^(R) Failover Cluster).

(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.

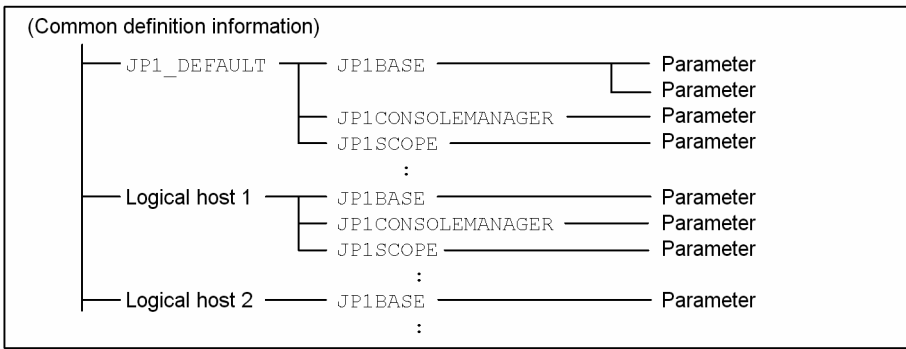
For details about the communication methods, see the descriptions of the JP1/Base communication methods in the *JP1/Base User's Guide*. JP1/IM - Manager uses the same communication methods as JP1/Base.

(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.

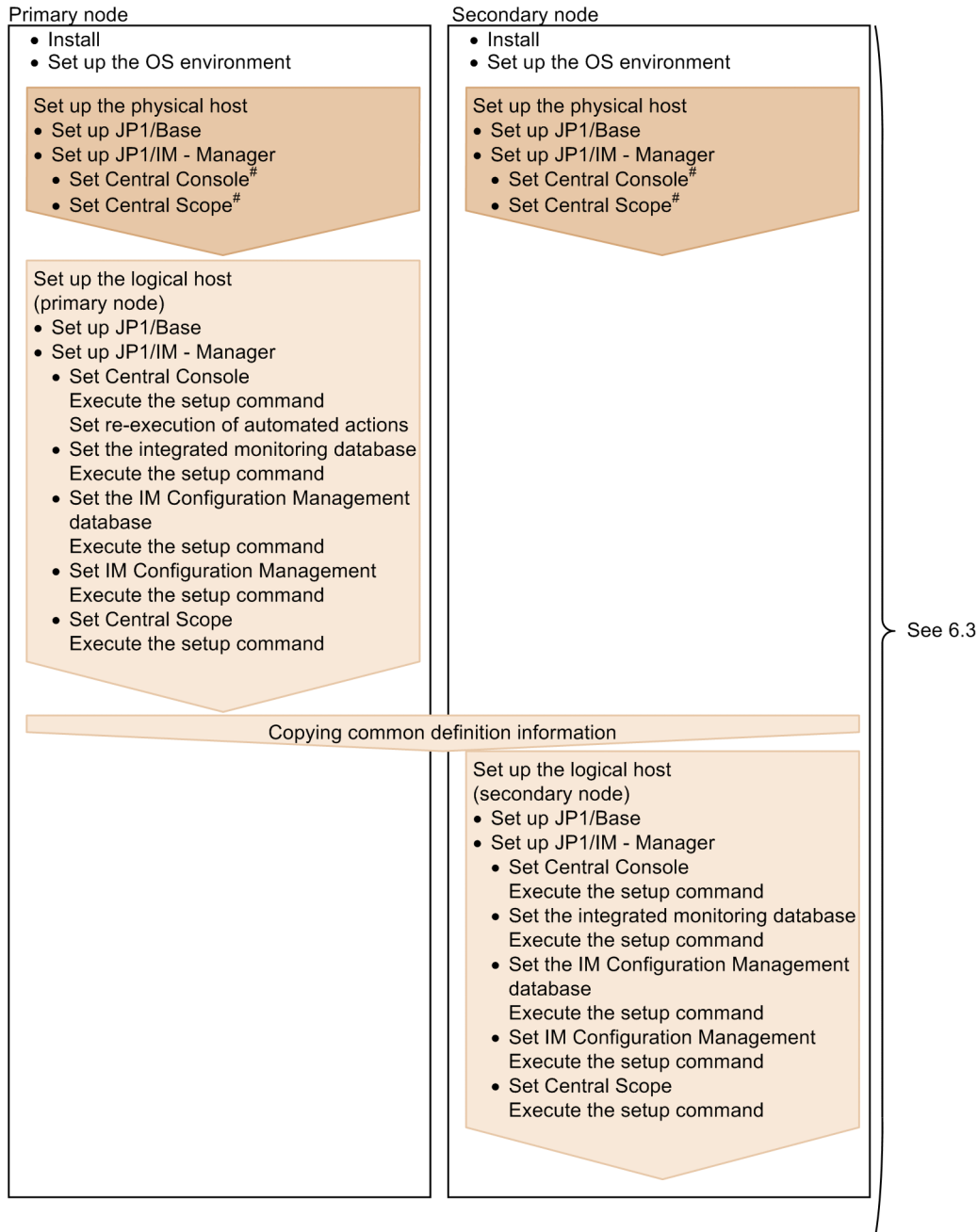
JP1/IM - Manager, JP1/Base, JP1/AJS, and JP1/Power Monitor (06-02 or later) use the common definition information to store the settings.


6.2 Environment setup procedure for cluster operation (for Windows)


This section describes the environment setup for JP1/IM - Manager that supports cluster operation.

The following figure shows the setup procedure.

Figure 6–4: Setup procedure (when setting up a new environment)

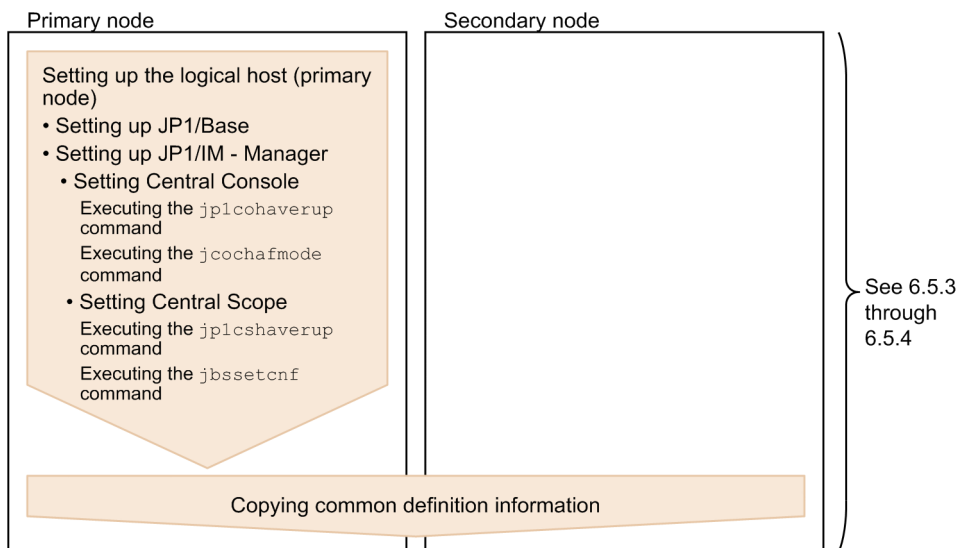


Legend:  : Setting at the physical host


 : Setting at the logical host

#: Setting required when JP1/IM - Manager is started at the physical host.

Figure 6–5: Setup procedure (when upgrading the existing logical host environment)



Legend:

 : Setting at the logical host

6.3 Installing and setting up logical hosts (new installation and setup) (for Windows)

This subsection describes the new installation and setup of a 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 6–6: 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 \(for Windows\)](#).

Once you have finished checking the above items, you are ready to start the installation and setup.

Note that logical host names are case sensitive. Specify the logical host names set in JP1/Base in the correct form, including case. If you set up and install a logical host after specifying an incorrect logical host name, delete the IM databases and the logical host, and then install and set up the logical host again. For details about how to delete IM databases and logical hosts, see [6.6.1 Deleting logical hosts \(for Windows\)](#).

6.3.1 Newly installing JP1/Base and JP1/IM - Manager (for Windows)

Install JP1/IM - Manager and JP1/Base on the local disk of both the primary server and the secondary server.

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.

6.3.2 Setting up the physical host environment during new installation (for Windows)

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 *JP1/Base User's Guide*.

The setup procedure for JP1/IM - Manager is the same as for non-cluster operation. For details about the procedure, see *Chapter 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.

6.3.3 Setting up the logical host environment (primary node) during new installation (for Windows)

(1) Preparations for setup

To prepare for setup:

1. Make sure that the services of JP1/IM and JP1/Base are stopped.
Make sure that the services of JP1/IM and JP1/Base are stopped on the physical host and all logical hosts. If JP1/IM - MO is used, also stop the JP1/IM - Message Optimizer service of JP1/IM - MO on the connection source.
2. Make sure that the shared disk is available.

(2) Setting up JP1/Base

To set up JP1/Base:

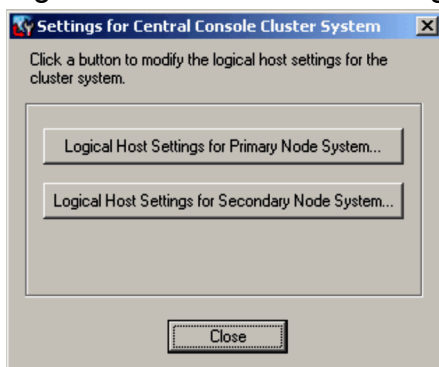
1. Set up the logical host for JP1/Base (primary node).
For details about the procedure, see the *JP1/Base User's Guide*.
2. Set up a command execution environment for JP1/Base.
Execute the `jcocmddef` command to set up a command execution environment for JP1/Base. For details about the `jcocmddef` command, see the *JP1/Base User's Guide*.

(3) 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.

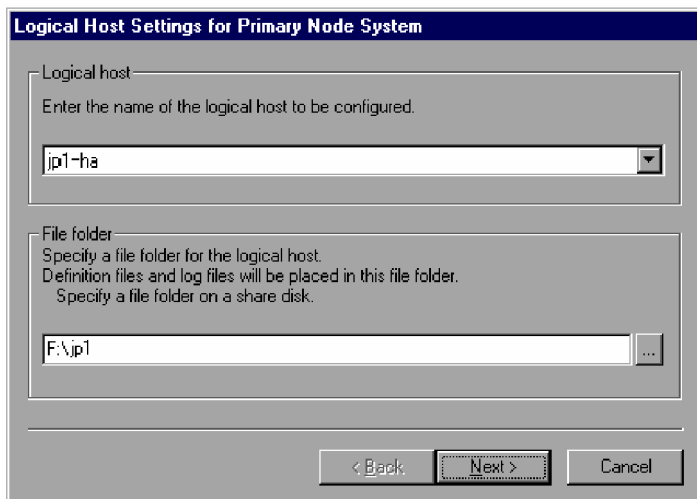
Figure 6–6: Window for setting the logical host (primary node)



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.

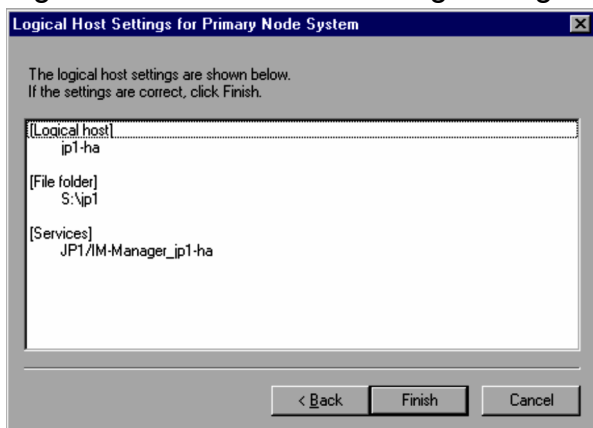
- Logical host name
The logical host names created in JP1/Base are displayed. Select the logical host name.
- File folder
Specify a folder on the shared disk. A set of JP1/IM - Manager files for the logical host is created under *specified-folder-name*\jp1cons\.

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 ensure correct re-execution of automated actions in the event of a failover, 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
```

You can set the re-execution of the actions for any of the following statuses at failover:

- Waiting to be sent
- Waiting to be sent (being canceled)
- Waiting to be sent (failed to be canceled)
- Sending
- Sending (being canceled)
- Sending (failed to be canceled)
- Queuing
- Queuing (being canceled)
- Queuing (failed to be canceled)
- Running
- Running (being canceled)
- Running (failed to be canceled)

If you specify `EXE`, the actions will be re-executed. If you specify `OUTPUT`, a list of actions will be output to a file. If you specify `OFF`, the actions will not be performed. Specify this setting according to your evaluation during the system design. This setting is optional.

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

(4) Setting JP1/IM - Manager (integrated monitoring database) (optional)

Perform this setting procedure when you will be using JP1/IM - Manager (integrated monitoring database). If you intend to use an integrated monitoring database to manage JP1 events, you must create the integrated monitoring database.

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 the integrated monitoring database and the database storage directory.

For details about the settings in the cluster setup information file, see *Cluster setup information file (jimdbclustersetupinfo.conf)* in *Chapter 2. Definition Files* in the manual *JP1/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, and setup type.

- `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.
As the logical host name, specify the logical host name set in JP1/Base in the correct form, including case. For details about how to set up JP1/Base, see *6.3.3(2) Setting up JP1/Base*.
- Setup type (-c option)
Specify the setup type (`online`) of the active host.
When you specify `online`, mount the shared disk and permit the logical host to access it.

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

(5) Setting JP1/IM - Manager (IM Configuration Management database) (optional)

Perform this setting procedure when you will be using JP1/IM - Manager (IM Configuration Management database). If you intend to use an IM Configuration Management database to manage system hierarchies (IM configurations), you must create the IM Configuration Management database.

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 the IM Configuration Management database and the database storage directory.

For details about the settings in the cluster setup information file, see *Cluster setup information file (jimdbclustersetupinfo.conf)* in *Chapter 2. Definition Files* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

2. 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, and setup type.

- *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.

As the logical host name, specify the logical host name set in JP1/Base in the correct form, including case. For details about how to set up JP1/Base, see *6.3.3(2) Setting up JP1/Base*.

- Setup type (-c option)

Specify the setup type (`online`) of the active host.

When you specify `online`, mount the shared disk and permit the logical host to access it.

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

3. 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 *Chapter 1. Commands* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

(6) Setting JP1/IM - Manager (IM Configuration Management) (optional)

Perform this setting procedure when you will be 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\jplcfhsetup.exe command.

2. Click the **Logical Host Settings for Primary Node System** button.

In the Logical Host Settings for Primary Node System window, specify a logical host name and a file folder.

- Logical host name

The name of the logical host created in JP1/Base appears. Select this name.

- File folder

Specify a folder on the shared disk. The files for JP1/IM - Manager on the logical host are created under the *specified-folder-name*\jplimm\ 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.

(7) Setting JP1/IM - Manager (Central Scope) (optional)

Perform this setting procedure when you will be using JP1/IM - Manager (Central Console). 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\jplcshsetup.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*\jplscope\ 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.

6.3.4 Copying the common definition information during new installation (for Windows)

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
```

Note that the logical host name is case sensitive. Specify the logical host name set in JP1/Base in the correct form, including case.

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
```

6.3.5 Setting up the logical host environment (secondary node) during new installation (for Windows)

(1) Preparations for setup

To prepare for setup:

1. Make sure that the services of JP1/IM and JP1/Base are stopped.

Make sure that all services of JP1/IM and JP1/Base are stopped on the physical host and all logical hosts. If JP1/IM - MO is used, also stop the JP1/IM - Message Optimizer service of JP1/IM - MO on the connection source.

2. If you set up the IM database on the primary server, copy the cluster setup information file that was used in the primary server onto the secondary server. (This operation is not necessary if the IM database is not set up on the primary server.)

Store the copied file in *Manager-path*\conf\imdb\setup.

Note that there is no need for the shared disk to be available for use at the secondary server.

(2) 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 *JP1/Base User's Guide*.
2. Set up a command execution environment for JP1/Base.

Execute the `jcocmddef` command to set up a command execution environment for JP1/Base. For details about the `jcocmddef` command, see the *JP1/Base User's Guide*.

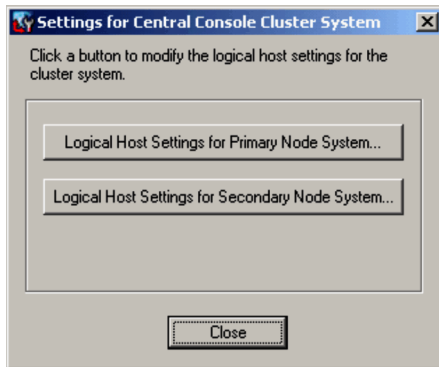
(3) Setting JP1/IM - Manager (Central Console)

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.

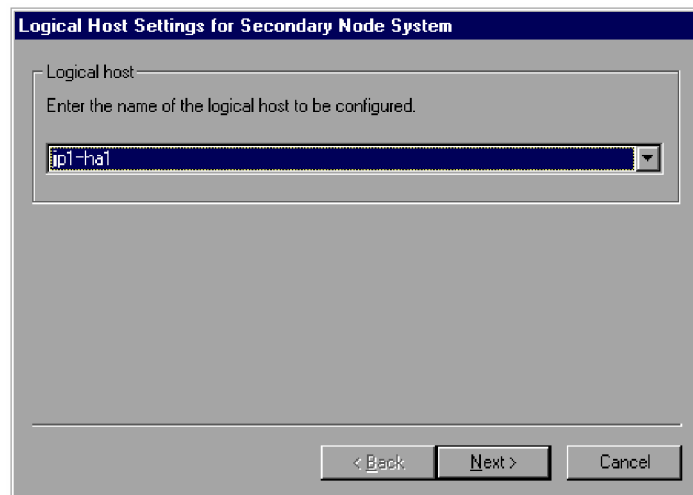
Figure 6–9: Window for setting the logical host (secondary node)



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.

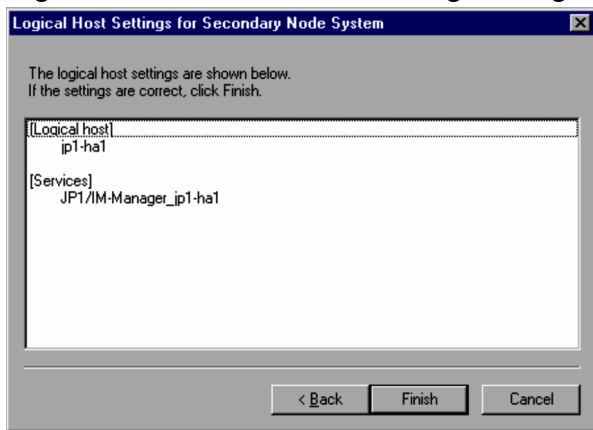
- Logical host name
Select the logical host that was set up at the primary server.

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.

(4) Setting JP1/IM - Manager (integrated monitoring database) (optional)

Perform this setting procedure when you will be using JP1/IM - Manager (integrated monitoring database). If you intend to use an integrated monitoring database to manage JP1 events, you must create the integrated monitoring database.

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 the integrated monitoring database and the database storage directory. Check the contents of the cluster setup information file that was copied from the active host in [6.3.5\(1\) Preparations for setup](#). 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 *Chapter 2. Definition Files* in the manual *JP1/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, and setup type.

- *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.

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

(5) Setting JP1/IM - Manager (IM Configuration Management database) (optional)

Perform this setting procedure when you will be using JP1/IM - Manager (IM Configuration Management database). If you intend to use an IM Configuration Management database to manage system hierarchies (IM configurations), you must create the IM Configuration Management database.

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 the IM Configuration Management database and the database storage directory. Check the contents of the cluster setup information file that was copied from the active host in *6.3.5(1) Preparations for setup*. 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 *Chapter 2. Definition Files* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

2. Execute the `jcfdbssetup` command to create an IM Configuration Management database.

```
jcfdbssetup - 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, and setup type.

- *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.

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

(6) Setting JP1/IM - Manager (IM Configuration Management) (optional)

Perform this setting procedure when you will be 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\jplcfhsetup.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.

(7) Setting JP1/IM - Manager (Central Scope) (optional)

Perform this setting procedure when you will be 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\jplcshasetup.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.

6.4 Registering into the cluster software during new installation and setup (for Windows)

To apply cluster operation to JP1/IM - Manager during new installation and setup, 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 table below shows the settings for JP1/IM - Manager that are to be registered in the cluster software.

Start the services in the order from No. 1 to No. 4 in the table below. (Start the JP1/Base services and then JP1/IM - Manager services.)

Table 6–7: 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 Server_ <i>logical-host-name</i> ^{#1}	HiRDBEmbeddedEdition_JM<n> ^{#2}	Cluster resources of Nos. 1 and 2
4	JP1/IM-Manager DB Cluster Service_ <i>logical-host-name</i> ^{#1}	HiRDBClusterService_JM<n> ^{#2}	Cluster resources of Nos. 1, 2, and 3
5	JP1/IM-Manager_ <i>logical-host-name</i>	JP1_Console_ <i>logical-host-name</i>	Cluster resources of Nos. 1, 2, 3, and 4 ^{#3}

#1

Register the service in the cluster software only when the IM databases are used.

#2

<n> is a number from 1 to 9, and is the value specified in LOGICALHOSTNUMBER in the cluster setup information file. For details, see *Cluster setup information file (jimdbclustersetupinfo.conf)* in Chapter 2. *Definition Files* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

#3

If you do not use the IM database, remove the cluster resources of Nos. 3 and 4 from the dependencies.

6.4.1 Registering into the cluster software (for Windows)

(1) 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.

(2) 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 *7.4 Registering into the cluster software during new installation and setup (for UNIX)*.

6.4.2 Setting the resource start and stop sequence (for Windows)

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.

6.5 Upgrade installation and setup of logical hosts (for Windows)

This subsection describes the upgrade 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 6–8: 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 \(for Windows\)](#).

Once you have finished checking the above items, you are ready to start the installation and setup.

Note that logical host names are case sensitive. Specify the logical host names set in JP1/Base in the correct form, including case. If you set up and install a logical host after specifying an incorrect logical host name, delete the IM databases and the logical host, and then install and set up the logical host again. For details about how to delete IM databases and logical hosts, see [6.6.1 Deleting logical hosts \(for Windows\)](#).

6.5.1 Upgrade installation of logical hosts (for Windows)

Install JP1/IM - Manager and JP1/Base on the local disk of both the primary server and the secondary server.

To install:

1. Back up the settings and database.
For the backup method, see the manual for the old version.
2. Install JP1/Base.
3. Install JP1/IM - Manager.

Important

If you have upgraded JP1/IM - Manager in an environment in which IM databases have already been set up, use the `jimdbupdate` command to update the IM databases. If the IM databases have not been updated, a warning message will be displayed when JP1/IM - Manager starts.

6.5.2 Setting up the physical host environment during upgrade installation (for Windows)

If you use JP1/IM - Manager at the physical host, set up the physical host environment according to the procedure described in [1.18.3 Specifying settings for upgrading \(for Windows\)](#).

6.5.3 Setting up the logical host environment (primary node) during upgrade installation (for Windows)

If you use the functions of Central Scope, steps 5 through 7 are required. If you do not use the functions of Central Scope, skip steps 5 through 7.

1. Terminate JP1/IM - Manager.

Terminate the JP1/IM - Managers in both the physical and 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 *JP1/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 `jplcohaverup` command.

```
jplcohaverup -h logical-host-name
```

5. 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*.

6. Execute the `jplcshaverup.bat` command.

```
jplcshaverup.bat -h logical-host-name -w work-folder
```

7. 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:

- Monitoring of the maximum number of status change events
- Completed-action linkage function
- Automatically deleting status change events
- Initializing monitoring objects
- Making status change conditions resident in memory

To enable or disable one of the above functions, execute the `jbssetcnf` command by specifying the relevant file as an argument. For the file to be specified, see the following table.

Table 6–9: Files that are used to enable or disable the functions

File name	Description
Settings file for the maximum number of status change events (<code>evhist_warn_event_on.conf</code> , <code>evhist_warn_event_off.conf</code>)	Specify this file to enable or disable the function that issues a warning JP1 event when the number of status change events for a monitoring object exceeds the maximum value (100).
Settings file for completed-action linkage function (<code>action_complete_on.conf</code> , <code>action_complete_off.conf</code>)	Specify this file to enable or disable the completed-action linkage function.
Definition file for automatic delete mode of status change event	Specify this file to enable or disable the function that automatically deletes status change events when JP1 event handling is completed.
Definition file for monitoring object initialization mode	Specify this file to enable or disable the function that initializes monitoring objects when specific JP1 events are received.

File name	Description
Definition file for on memory mode of status change condition	Specify this file to enable or disable the function that makes status change conditions resident in memory.

8. Back up the common definition information.

```
jbsgetcnf -h logical-host-name > common-definition-information-backup-file-name
```

6.5.4 Copying the common definition information during upgrade installation (for Windows)

1. Terminate JP1/IM - Manager.

Terminate the JP1/IM - Managers in both the physical and logical host environments.

2. Copy the common definition information backup file (backed up on the primary server) to the secondary server.

Use a method such as FTP to copy the file.

3. Set the common definition information.

```
jbssetcnf common-definition-information-backup-file-name
```

6.6 Uninstalling logical hosts (for Windows)

This section describes how to uninstall logical hosts of JP1/IM - Manager. The subsections below first explain how to delete logical hosts and then explain how to uninstall JP1/IM - Manager and JP1/Base from the logical disk on the active server and the standby server.

6.6.1 Deleting logical hosts (for Windows)

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 *JP1/Integrated Management - Manager Administration Guide*.

To delete the IM databases:

1. Stop the services.

If JP1/Integrated Management is running in the physical host environment or in the logical host environment, stop all JP1/IM - Manager services (`JP1/IM-Manager` and `JP1/IM-Manager_logical-host-name`). In the logical host environment, use the cluster software to stop the services.

If JP1/IM - View is connected, disconnect it by logging out.

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

2. Change the status of the services for the IM databases on the logical host.

Make the following changes:

- IM database cluster service (`JP1/IM - Manager DB Cluster Service_logical-host-name`) on the logical host
Stop the service.
- IM database service (`JP1/IM - Manager DB Server_logical-host-name`) on the logical host
Start the service.

3. 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 and unsetup type.

- `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`.

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

- 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 and unsetup type.

- 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`.

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

- Delete the following files and folders.

Files under *shared-folder*\data\imcf\imconfig

Files and folders under *shared-folder*\data\imcf\profiles

(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:

- Execute the `jp1bshasetup.exe` command.
- In the Settings for Base Node Switching System window, click the **Delete Logical Host** button.
- Select the name of the logical host that you want to delete.
- Click the **Next** button.
- 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.

(3) Deleting only JP1/IM - Manager and IM databases on a logical host

To delete only JP1/IM - Manager and IM databases from a logical host on which JP1/Base, JP1/IM - Manager, JP1/AJS, and JP1/Power Monitor (06-02 or later) have been installed:

- Before stopping JP1/IM - Manager, log out from the JP1/IM - View instance connected to JP1/IM - Manager and disconnect JP1/IM - View.
- Use the cluster software to stop JP1/IM - Manager and JP1/Base in this order.
- If you are using IM databases, perform the procedure described in *6.6.1(1) Deleting the IM databases* and delete the IM databases.

4. On the primary node and the secondary node, execute the following commands to delete common definitions:

- [*logical-host-name*\JP1CONSOLEMANAGER\] key
`jbsunsetcnf -h logical-host-name -c JP1CONSOLEMANAGER`
- [*logical-host-name*\JP1SCOPE\] key
`jbsunsetcnf -h logical-host-name -c JP1SCOPE`
- [*logical-host-name*\JP1CONFIG\] key
`jbsunsetcnf -h logical-host-name -c JP1CONFIG`

5. Delete the JP1/IM - Manager shared files and shared folders.

6. Delete the JP1/IM - Manager settings on the logical host from the cluster software.

7. On the primary node and the secondary node, execute the following command to delete the JP1/IM - Manager services on the logical host.

```
spmsetsvcon -d -h logical-host-name
```

6.6.2 Uninstalling JP1/IM - Manager and JP1/Base (for Windows)

Uninstall JP1/IM - Manager and JP1/Base on the local disk on the active server and on the standby server.

1. Uninstall JP1/IM - Manager.
2. Uninstall JP1/Base.

6.7 Procedures for changing settings (for Windows)

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 might 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.

6.7.1 Changing settings in files (for Windows)

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
- Apply-IM-configuration-method definition file (`jp1cf_applyconfig.conf`)
- Remote log trap environment definition file (`jp1cf_remote_logtrap.conf`)
- Environment definition file for events after the display message is changed (`chmsgevent.conf`)
- Environment definition file for event report output (`evtreport.conf`)
- Operation log definition file (`imm_operationlog.conf`)
- Profile management environment definition file (`jp1cf_profile_manager.conf`)

Copy the common definition information using the setup procedure described in [6.3.4 Copying the common definition information during new installation \(for Windows\)](#).

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.

6.7.2 Using commands to change settings (for Windows)

If you have used the `jcocafmode`, `jcoccfemode`, or `jcocmdddef` command to change settings, you must also specify the same settings at the primary and secondary servers.

- When the `jcocafmode` 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 [6.3.4 Copying the common definition information during new installation \(for Windows\)](#).

- When the `jcochcefmode` command is executed

If you have changed the operation mode for the common exclusion conditions 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 [6.3.4 Copying the common definition information during new installation \(for Windows\)](#).

- 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.

6.7.3 Updating IM databases in a cluster environment (for Windows)

If you have upgraded JP1/IM - Manager or applied a corrected version of JP1/IM - Manager in a cluster environment while using IM databases, you must update the IM databases in the cluster environment. Use the procedure described below to update IM databases.

This procedure assumes that the host on which the JP1/IM - Manager of a logical host is running is the active host and the host on which the JP1/IM - Manager is not running is the standby host.

To update IM databases in a cluster environment:

1. Execute the `jimdbupdate` command on the standby host:

```
jimdbupdate -h logical-host-name
```

- If the following message is output, perform the procedure beginning with step 3:
KNAN11201-I The IM database service is the latest.
- If the following message is output, perform the procedure beginning with step 2:
KNAN11202-I The overwrite is necessary for the IM database.

2. Execute the `jimdbupdate` command to update the IM databases on the standby host:

```
jimdbupdate -h logical-host-name -i
```

3. On the active host, stop JP1/IM - Manager Service and JP1/IM - Manager DB Cluster Service.

JP1/IM - Manager Service on the logical host (service name that is displayed: `JP1/IM-Manager_`*logical-host-name*)

JP1/IM - Manager DB Cluster Service on the logical host (service name that is displayed: `JP1/IM-Manager DB Cluster Service_`*logical-host-name*)

4. Execute the `jimdbupdate` command on the active host:

```
jimdbupdate -h logical-host-name
```

- If the following message is output, perform step 7:
KNAN11201-I The IM database service is the latest.
- If the following message is output, perform the procedure beginning with step 5:
KNAN11202-I The overwrite is necessary for the IM database.

KNAN11207-I An update of the table schema of an IM database service is required.

5. Execute the `jimdbbackup` command to back up the IM databases on the active host:

```
jimdbbackup -h logical-host-name -o backup-file-name -m MAINT
```

6. Execute the `jimdbupdate` command to update the IM databases on the active host:

```
jimdbupdate -h logical-host-name -i
```

7. On the active host, start JP1/IM - Manager Service and JP1/IM - Manager DB Cluster Service from the cluster software.

JP1/IM - Manager Service on the logical host (service name that is displayed: JP1/IM-Manager_*logical-host-name*)

JP1/IM - Manager DB Cluster Service on the logical host (service name that is displayed: JP1/IM-Manager DB Cluster Service_*logical-host-name*)

Important

Do not restore any IM database backup data that was obtained before the `jimdbupdate` command was executed into an IM database obtained after the `jimdbupdate` command has been executed.

After you have executed the `jimdbupdate` command, execute the `jimdbbackup` command again to make a new backup.

6.8 Notes about cluster operation (for Windows)

- 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.
- Before you start JP1/IM - Manager in a cluster system, make sure that you configure the authentication server that will be used on the logical host. For details about how to configure an authentication server, see the *JP1/Base User's Guide*. In addition, before you start JP1/IM - Manager, make sure that the configured authentication server is running.
- 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.
- 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:
`shared-folder\jplbase\conf\route\jbs_route.conf`
- Do not rename hosts while JP1/IM - Manager is running by, for example, using a cluster software function. If you have renamed hosts, see *2.2.5 Tasks to be performed before a logical host name is changed in a cluster system* in the *JP1/Integrated Management - Manager Administration Guide* and perform the required tasks.

6.9 Logical host operation and environment configuration in a non-cluster system (for Windows)

This section provides an overview of the configuration and operation of logical hosts that do not employ failover.

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.

6.9.1 Evaluating the configuration for running logical hosts in a non-cluster system (for Windows)

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.

6.9.2 Environment setup for running logical hosts in a non-cluster system (for Windows)

This subsection explains how to run JP1/IM - Manager in a non-failover logical host environment.

(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 might 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 (*Chapter 6. Operation and Environment Configuration in a Cluster System (for Windows)*), 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

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 might not run correctly or might 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 *3.3 Automatic startup and automatic stop setting examples when a logical host operates in a non-cluster system* in the *JP1/Integrated Management - Manager Administration Guide*.

6.9.3 Notes about running logical hosts in a non-cluster system (for Windows)

(1) 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.

(2) 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.

7

Operation and Environment Configuration in a Cluster System (for UNIX)

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 for UNIX. For details about the procedure for starting up JP1/IM - Manager after setup, see *Chapter 3. Starting and Stopping JP1/IM - Manager* in the *JP1/Integrated Management - Manager Administration Guide*.

Before you use this function, make sure that your cluster software supports JP1/IM - Manager.

7.1 Overview of cluster operation (for UNIX)

The overview of cluster operation is the same as for Windows. For details, see *6.1 Overview of cluster operation (for Windows)*.

7.1.1 Overview of a cluster system (for UNIX)

The overview of a cluster system is the same as for Windows. For details, see *6.1.1 Overview of a cluster system (for Windows)*.

7.1.2 Prerequisites for cluster operation (for UNIX)

The prerequisites for cluster operation are the same as for Windows. For details, see *6.1.2 Prerequisites for cluster operation (for Windows)*.

7.1.3 JP1/IM configuration in a cluster system (for UNIX)

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 7–1: 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.

Table 7–2: File organization on the shared disk (UNIX)

Function	Type of shared file	Directory name
Central Console	Definition file	<i>shared-directory/jp1cons/conf/</i>

Function	Type of shared file	Directory name
	Log file	<i>shared-directory/jplcons/log/</i>
	Temporary file	<i>shared-directory/jplcons/tmp/</i>
	History file [#]	<i>shared-directory/jplcons/operation/</i>
Central Scope	Definition file	<i>shared-directory/jplscope/conf/</i>
	Log file	<i>shared-directory/jplscope/log/</i>
	Temporary file	<i>shared-directory/jplscope/tmp/</i>
	Database	<i>shared-directory/jplscope/database/</i>
IM Configuration Management	Definition file	<i>shared-directory/jplimm/conf/imcf/</i>
	Log file	<i>shared-directory/jplimm/log/imcf/</i>
	Temporary file	<i>shared-directory/jplimm/tmp/</i>
	IM configuration data and profile data	<i>shared-directory/jplimm/data/imcf/</i>
IM database	Database	<i>user-specified-directory-on-shared-disk/imdb</i>

[#]: Event Generation Service processing, exclusion processing caused by common exclusion-conditions, and update processing of common exclusion-conditions definition are 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.

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 *Appendix B. List of Processes* in the *JP1/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.

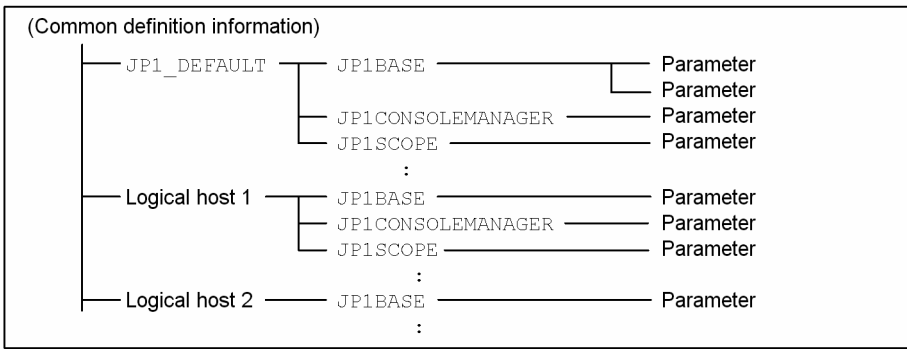
For details about the communication methods, see the descriptions of the JP1/Base communication methods in the *JP1/Base User's Guide*. JP1/IM - Manager uses the same communication methods as JP1/Base.

(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 7–1: 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.

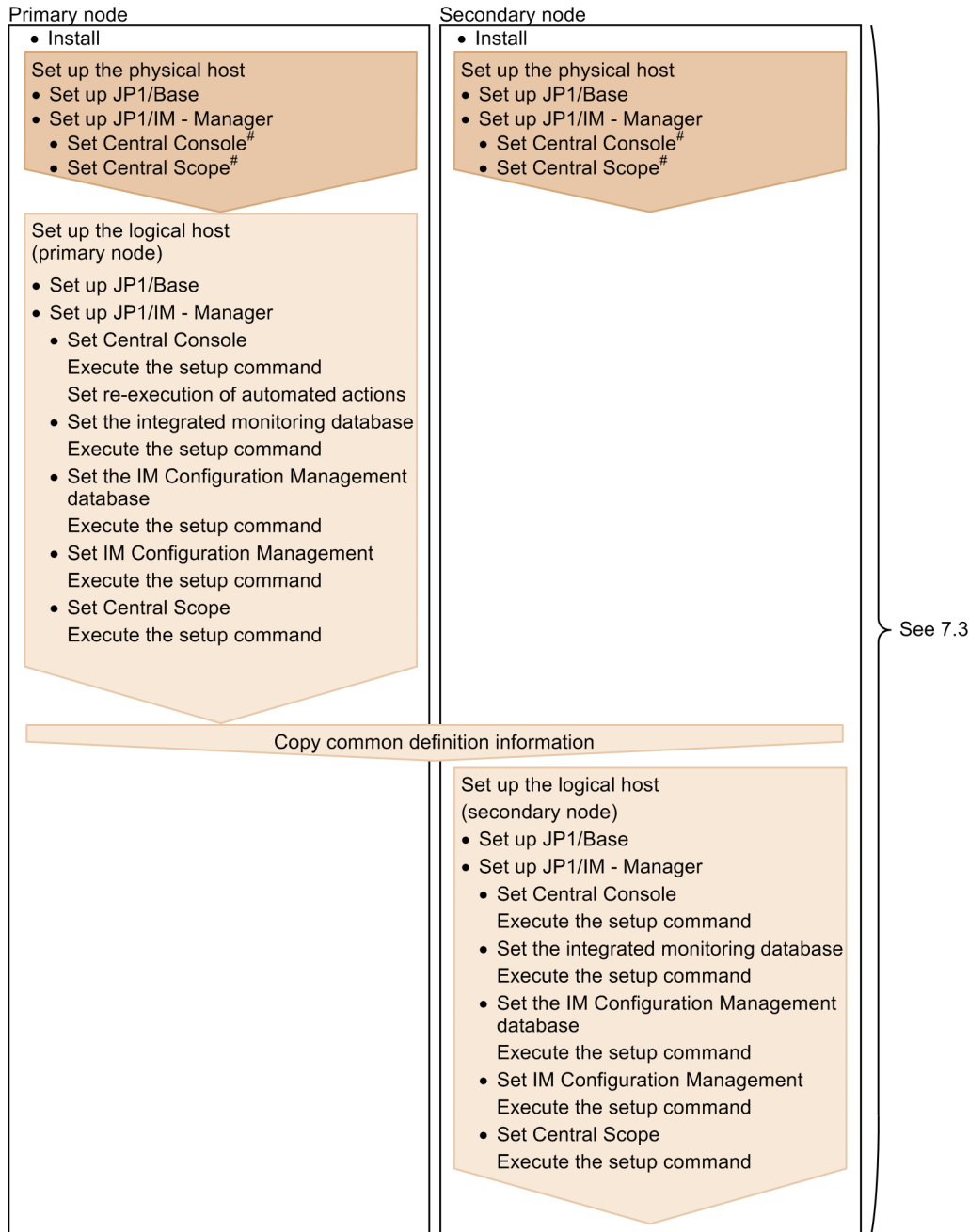
JP1/IM - Manager, JP1/Base, JP1/AJS, and JP1/Power Monitor (06-02 or later) use the common definition information to store the settings.


7.2 Environment setup procedure for cluster operation (for UNIX)


This section describes the environment setup for JP1/IM - Manager that supports cluster operation.

The following figure shows the setup procedure.

Figure 7–2: Setup procedure (when setting up a new environment)

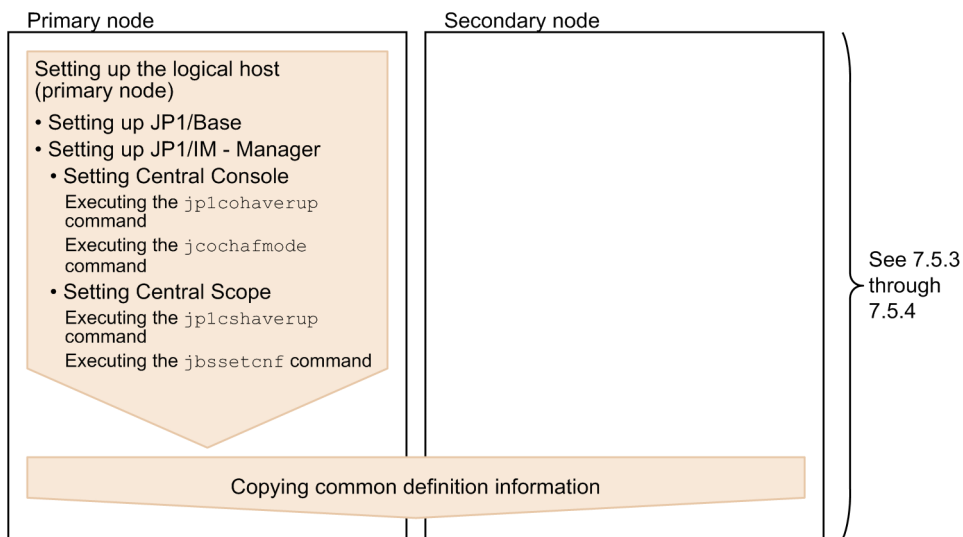


Legend:  : Setting at the physical host


 : Setting at the logical host

#: Setting required when JP1/IM - Manager is started at the physical host.

Figure 7–3: Setup procedure (when upgrading the existing logical host environment)



Legend:

 : Setting at the logical host

7.3 Installing and setting up logical hosts (new installation and setup) (for UNIX)

This subsection describes new installation and setup of a 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 7–3: 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 directory	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 \(for Windows\)](#).

Once you have finished checking the above items, you are ready to start the installation and setup.

Note that logical host names are case sensitive. Specify the logical host names set in JP1/Base in the correct form, including case. If you installed and set up the logical host after specifying an incorrect logical host name, delete the IM databases and the logical host, and then install and set up the logical host again. For details about how to delete the IM databases and logical hosts, see [7.6.1 Deleting logical hosts \(for UNIX\)](#).

7.3.1 Newly installing JP1/Base and JP1/IM - Manager (for UNIX)

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.

7.3.2 Setting up the physical host environment during new installation (for UNIX)

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 *JP1/Base User's Guide*.

The setup procedure for JP1/IM - Manager is the same as for non-cluster operation. For details about the procedure, 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.

7.3.3 Setting up the logical host environment (primary node) during new installation (for UNIX)

(1) Preparations for setup

1. Make sure that the services of JP1/IM and JP1/Base are stopped.
Make sure that the processes of JP1/IM and JP1/Base are stopped on the physical host and all logical hosts. If JP1/IM - MO is used, also stop the JP1/IM - Message Optimizer service of JP1/IM - MO on the connection source.
2. Make sure that the shared disk is available.
Execute the `mount` command to make sure that the shared disk is mounted.

(2) Setting up JP1/Base

1. Set up the logical host for JP1/Base (primary node).
For details about the procedure, see the *JP1/Base User's Guide*.
2. Set up a command execution environment for JP1/Base.
Execute the `jcocmddef` command to set up a command execution environment for JP1/Base. For details about the `jcocmddef` command, see the *JP1/Base User's Guide*.

(3) Setting 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 *Chapter 1. Commands* in the manual *JP1/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
```

You can set the re-execution of the actions for any of the following statuses at failover:

- Waiting to be sent
- Waiting to be sent (being canceled)
- Waiting to be sent (failed to be canceled)
- Sending
- Sending (being canceled)
- Sending (failed to be canceled)
- Queuing
- Queuing (being canceled)
- Queuing (failed to be canceled)
- Running
- Running (being canceled)
- Running (failed to be canceled)

If you specify `EXE`, the actions will be re-executed. If you specify `OUTPUT`, a list of actions will be output to a file. If you specify `OFF`, the actions will not be performed. Specify this setting according to your evaluation during the system design. This setting is optional.

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

(4) Setting JP1/IM - Manager (integrated monitoring database) (optional)

Perform this setting procedure when you will be using JP1/IM - Manager (integrated monitoring database). If you intend to use an integrated monitoring database to manage JP1 events, you must create the integrated monitoring 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 the integrated monitoring database and the database storage directory.

For details about the settings in the cluster setup information file, see *Cluster setup information file (jimdbclustersetupinfo.conf)* in *Chapter 2. Definition Files* in the manual *JP1/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, and setup type.

- *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.
As the logical host name, specify the logical host name set in JP1/Base in the correct form, including case. For details about how to set up JP1/Base, see [7.3.3\(2\) Setting up JP1/Base](#).
- Setup type (-c option)
Specify the setup type (`online`) of the active host.
When you specify `online`, mount the shared disk and permit the logical host to access it.

For details about the `jcodbsetup` command, see `jcodbsetup` in *Chapter 1. Commands* in the manual *JP1/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 *Chapter 1. Commands* in the manual *JP1/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) Setting JP1/IM - Manager (IM Configuration Management database) (optional)

Perform this setting procedure when you will be using JP1/IM - Manager (IM Configuration Management database). If you intend to use an IM Configuration Management database to manage system hierarchies (IM configurations), you must create the IM Configuration Management 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 the IM Configuration Management database and the database storage directory.

For details about the settings in the cluster setup information file, see *Cluster setup information file (jimdbclustersetupinfo.conf)* in *Chapter 2. Definition Files* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

2. 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, and setup type.

- *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.

As the logical host name, specify the logical host name set in JP1/Base in the correct form, including case. For details about how to set up JP1/Base, see *7.3.3(2) Setting up JP1/Base*.

- Setup type (-c option)

Specify the setup type (`online`) of the active host.

When you specify `online`, mount the shared disk and permit the logical host to access it.

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

3. 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 *Chapter 1. Commands* in the manual *JP1/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.

(6) Setting JP1/IM - Manager (IM Configuration Management) (optional)

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.

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 *Chapter 1. Commands* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

(7) Setting JP1/IM - Manager (Central Scope) (optional)

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 *Chapter 1. Commands* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

7.3.4 Copying the common definition information during new installation (for UNIX)

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.

```
/opt/jp1base/bin/jbsgetcnf -h logical-host-name > common-definition-information-backup-file-name
```

Note that the logical host name is case sensitive. Specify the logical host name set in JP1/Base in the correct form, including case.

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.

```
/opt/jp1base/bin/jbssetcnf common-definition-information-backup-file-name
```

7.3.5 Setting up the logical host environment (secondary node) during new installation (for UNIX)

(1) Preparations for setup

1. Make sure that the services of JP1/IM and JP1/Base are stopped.

Make sure that all processes of JP1/IM and JP1/Base are stopped on the physical host and all logical hosts. If JP1/IM - MO is used, also stop the JP1/IM - Message Optimizer service of JP1/IM - MO on the connection source.

2. If you set up the IM database on the primary server, copy the cluster setup information file that was used in the primary server onto the secondary server. (This operation is not necessary if the IM database is not set up on the primary server.)

Store the copied file in `/etc/opt/jp1imm/conf/imdb/setup/`.

Note that there is no need for the shared disk to be available for use at the secondary server.

(2) Setting up JP1/Base

1. Set up the logical host (secondary node) for JP1/Base.

For details about the procedure, see the *JP1/Base User's Guide*.

2. Set up a command execution environment for JP1/Base.

Execute the `jcocmddef` command to set up a command execution environment for JP1/Base. For details about the `jcocmddef` command, see the *JP1/Base User's Guide*.

(3) 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
```

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 *jp1cc_setup_cluster (UNIX only)* in *Chapter 1. Commands* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

(4) Setting JP1/IM - Manager (integrated monitoring database) (optional)

Perform this setting procedure when you will be using JP1/IM - Manager (integrated monitoring database). If you intend to use an integrated monitoring database to manage JP1 events, you must create the integrated monitoring 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 the integrated monitoring database and the database storage directory. Check the contents of the cluster setup information file that was copied from the active host in *7.3.5(1) Preparations for setup*. 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 *Chapter 2. Definition Files* in the manual *JP1/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, and setup type.

- *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.

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

(5) Setting JP1/IM - Manager (IM Configuration Management database) (optional)

Perform this setting procedure when you will be using JP1/IM - Manager (IM Configuration Management database). If you intend to use an IM Configuration Management database to manage system hierarchies (IM configurations), you must create the IM Configuration Management 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 the IM Configuration Management database and the database storage directory. Check the contents of the cluster setup information file that was copied from the active host in *7.3.5(1) Preparations for setup*. 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 *Chapter 2. Definition Files* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

2. Execute the `jcfdbssetup` command to create an IM Configuration Management database.

```
jcfdbssetup -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, and setup type.

- *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.

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

(6) Setting JP1/IM - Manager (IM Configuration Management) (optional)

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/jplimm/bin/imcf/jplcf_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.

For details about the command, see `jplcf_setup_cluster (UNIX only)` in *Chapter 1. Commands* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

(7) Setting JP1/IM - Manager (Central Scope) (optional)

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 `jplcs_setup_cluster (UNIX only)` in *Chapter 1. Commands* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

Setup of the secondary node is now complete.

7.4 Registering into the cluster software during new installation and setup (for UNIX)

To apply cluster operation to JP1/IM - Manager during new installation and setup, 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.

Start services in the order of resources, JP1/Base, and JP1/IM - Manager.

7.4.1 Creating a script to be registered into the cluster software (for UNIX)

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 7–4: 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_spm_status -h logical-host-name</code> <p>To determine whether JP1/IM - Manager is running normally, check the return value of the <code>jco_spm_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 The following explains how to interpret the return value: Return value = 0 (all running): JP1/IM - Manager is running normally. Return value = 1 (error): An unrecoverable error occurred. Treat this as a failure. <i>Note:</i> If you were to execute the <code>jco_spm_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. Return value = 4 (partially stopped): Some JP1/IM - Manager processes are stopped due to a problem. Treat this as a failure. Return value = 8 (all stopped): All JP1/IM - Manager processes are stopped due to a problem. Treat this as a failure. Return value = 12 (retriable error): While the <code>jco_spm_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.
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 logical-host-name</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 = 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 logical-host-name</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_spm_status` returns a value of 8.

 **Note****About JP1 restart**

When a JP1 failure is detected in a cluster operation system, restart of JP1 might 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 might be affected and normal operation might not be achieved. To restart JP1 successfully, use the cluster software to restart JP1.

7.4.2 Setting the resource start and stop sequence (for UNIX)

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.

7.5 Upgrade installation and setup of logical hosts (for UNIX)

This subsection describes the upgrade 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 7–5: 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 directory	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 \(for Windows\)](#).

Once you have finished checking the above items, you are ready to start the installation and setup.

Note that logical host names are case sensitive. Specify the logical host names set in JP1/Base in the correct form, including case. If you installed and set up the logical host after specifying an incorrect logical host name, delete the IM databases and the logical host, and then install and set up the logical host again. For details about how to delete the IM databases and logical hosts, see [7.6.1 Deleting logical hosts \(for UNIX\)](#).

7.5.1 Upgrade installation of logical hosts (for UNIX)

Install JP1/IM - Manager and JP1/Base on the local disk of both the primary server and the secondary server.

1. Back up the settings and database.
For the backup method, see the manual for the old version.
2. Install JP1/Base.
3. Install JP1/IM - Manager.

Important

If you have upgraded JP1/IM - Manager in an environment in which IM databases have already been set up, use the `jimdbupdate` command to update the IM databases. If the IM databases have not been updated, a warning message will be displayed when JP1/IM - Manager starts.

7.5.2 Setting up the physical host environment during upgrade installation (for UNIX)

If you use JP1/IM - Manager at the physical host, set up the physical host environment according to the procedure described in [2.17.5 Specifying settings for upgrading \(for UNIX\)](#).

7.5.3 Setting up the logical host environment (primary node) during upgrade installation (for UNIX)

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.

1. Terminate JP1/IM - Manager.

Terminate the JP1/IM - Managers in both the physical and 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 *JP1/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 `jplcohaverup` command.

```
/opt/jplcons/bin/jplcohaverup -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:

- Monitoring of the maximum number of status change events
- Completed-action linkage function
- Automatically deleting status change events
- Initializing monitoring objects
- Making status change conditions resident in memory

To enable or disable one of the above functions, execute the `jbssetcnf` command by specifying the relevant file as an argument. For the file to be specified, see the following table.

Table 7–6: Files that are used to enable or disable the functions

File name	Description
Settings file for the maximum number of status change events (<code>evhist_warn_event_on.conf</code> , <code>evhist_warn_event_off.conf</code>)	Specify this file to enable or disable the function that issues a warning JP1 event when the number of status change events for a monitoring object exceeds the maximum value (100).
Settings file for completed-action linkage function (<code>action_complete_on.conf</code> , <code>action_complete_off.conf</code>)	Specify this file to enable or disable the completed-action linkage function.

File name	Description
Definition file for automatic delete mode of status change event	Specify this file to enable or disable the function that automatically deletes status change events when JP1 event handling is completed.
Definition file for monitoring object initialization mode	Specify this file to enable or disable the function that initializes monitoring objects when specific JP1 events are received.
Definition file for on memory mode of status change condition	Specify this file to enable or disable the function that makes status change conditions resident in memory.

9. Back up the common definition file.

```
/opt/jplbase/bin/jbsgetcnf -h logical-host-name > common-definition-information-backup-file-name
```

7.5.4 Copying the common definition information during upgrade installation (for UNIX)

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 (backed up on the primary server) to the secondary server.

Use a method such as FTP to copy the file.

3. Set the common definition information.

```
/opt/jplbase/bin/jbssetcnf common-definition-information-backup-file-name
```


7.6 Uninstalling logical hosts (for UNIX)

This section describes how to uninstall logical hosts of JP1/IM - Manager. The subsections below first explain how to delete logical hosts and then explain how to uninstall JP1/IM - Manager and JP1/Base from the logical disk on the active server and the standby server.

7.6.1 Deleting logical hosts (for UNIX)

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 *JP1/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.

In the logical host environment, use the cluster software to terminate JP1/IM - Managers.

If JP1/IM - View is connected, disconnect it by logging out.

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

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 and unsetup type.

- *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`.

For details about the `jcodbunsetup` command, see `jcodbunsetup` in *Chapter 1. Commands* in the manual *JP1/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 and unsetup type.

- *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`.

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

4. Delete the following files and directories.

Files under `shared-directory/data/imcf/imconfig`

Files and directories under `shared-directory/data/imcf/profiles`

(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 *JP1/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.

(3) Deleting only JP1/IM - Manager and IM databases on a logical host

To delete only JP1/IM - Manager and IM databases from a logical host on which JP1/Base, JP1/IM - Manager, JP1/AJS, and JP1/Power Monitor (06-02 or later) have been installed:

1. Before stopping JP1/IM - Manager, log out from the JP1/IM - View instance connected to JP1/IM - Manager and disconnect JP1/IM - View.
2. Use the cluster software to stop JP1/IM - Manager and JP1/Base in this order.
3. If you are using IM databases, perform the procedure described in *7.6.1(1) Deleting the IM databases* and delete the IM databases.
4. On the primary node and the secondary node, execute the following commands to delete common definitions:
 - [`logical-host-name\JP1CONSOLEMANAGER\`] key
`/opt/jp1base/bin/jbsunsetcnf -h logical-host-name -c JP1CONSOLEMANAGER`
 - [`logical-host-name\JP1SCOPE\`] key
`/opt/jp1base/bin/jbsunsetcnf -h logical-host-name -c JP1SCOPE`
 - [`logical-host-name\JP1CONFIG\`] key
`/opt/jp1base/bin/jbsunsetcnf -h logical-host-name -c JP1CONFIG`
5. Delete the shared files and shared directories.
6. Check the JP1/IM - Manager settings in the cluster software to make sure that the cluster software will not execute the startup script (`jco_start.cluster`).

7.6.2 Uninstalling JP1/IM - Manager and JP1/Base (for UNIX)

Uninstall JP1/IM - Manager and JP1/Base on the local disk on the active server and on the standby server.

1. Uninstall JP1/IM - Manager.
2. Uninstall JP1/Base.

7.7 Procedures for changing settings (for UNIX)

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 might 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.

7.7.1 Changing settings in files (for UNIX)

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
- Apply-IM-configuration-method definition file (`jp1cf_applyconfig.conf`)
- Remote log trap environment definition file (`jp1cf_remote_logtrap.conf`)
- Environment definition file for events after the display message is changed (`chmsgevent.conf`)
- Environment definition file for event report output (`evtreport.conf`)
- Operation log definition file (`imm_operationlog.conf`)
- Profile management environment definition file (`jp1cf_profile_manager.conf`)

Copy the common definition information using the setup procedure described in [7.3.4 Copying the common definition information during new installation \(for UNIX\)](#).

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.

7.7.2 Using commands to change settings (for UNIX)

If you have used the `jcocafmode`, `jcoccfemode`, or `jcocmdddef` command to change settings, you must also specify the same settings at the primary and secondary servers.

- When the `jcocafmode` 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 [7.3.4 Copying the common definition information during new installation \(for UNIX\)](#).

- When the `jcochcefmode` command is executed

If you have changed the operation mode for the common exclusion conditions 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 [7.3.4 Copying the common definition information during new installation \(for UNIX\)](#).

- 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.

7.7.3 Updating IM databases in a cluster environment (for UNIX)

If you have upgraded JP1/IM - Manager or applied a corrected version of JP1/IM - Manager in a cluster environment while using IM databases, you must update the IM databases in the cluster environment. Use the procedure described below to update IM databases.

This procedure assumes that the host on which the JP1/IM - Manager of a logical host is running is the active host and the host on which the JP1/IM - Manager is not running is the standby host.

To update IM databases in a cluster environment:

1. Execute the `jimdbupdate` command on the standby host:

```
jimdbupdate -h logical-host-name
```

- If the following message is output, perform the procedure beginning with step 3:
`KNAN11201-I The IM database service is the latest.`
- If the following message is output, perform the procedure beginning with step 2:
`KNAN11202-I The overwrite is necessary for the IM database.`

2. Execute the `jimdbupdate` command to update the IM databases on the standby host:

```
jimdbupdate -h logical-host-name -i
```

3. On the active host, terminate JP1/IM - Manager on the logical host.

4. Execute the `jimdbupdate` command on the active host:

```
jimdbupdate -h logical-host-name
```

- If the following message is output, perform step 7:
`KNAN11201-I The IM database service is the latest.`
- If the following message is output, perform the procedure beginning with step 5:
`KNAN11202-I The overwrite is necessary for the IM database.`
`KNAN11207-I An update of the table schema of an IM database service is required.`

5. Execute the `jimdbbackup` command to back up the IM databases on the active host:

```
jimdbbackup -h logical-host-name -o backup-file-name -m MAINT
```

6. Execute the `jimdbupdate` command to update the IM databases on the active host:

```
jimdbupdate -h logical-host-name -i
```

7. On the active host, start JP1/IM - Manager on the logical host.

 **Important**

Do not restore into an IM database obtained after the `jimdbupdate` command has been executed any IM database backup data that was obtained before the `jimdbupdate` command was executed.

After you have executed the `jimdbupdate` command, execute the `jimdbbackup` command again to make a new backup.

7.8 Notes about cluster operation (for UNIX)

- 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.
- Before you start JP1/IM - Manager in a cluster system, make sure that you configure the authentication server that will be used on the logical host. For details about how to configure an authentication server, see the *JP1/Base User's Guide*. In addition, before you start JP1/IM - Manager, make sure that the configured authentication server is running.
- 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.
- 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:
shared-directory/jp1base/conf/route/jbs_route.conf
- Do not rename hosts while JP1/IM - Manager is running by, for example, using a cluster software function. If you have renamed hosts, see *2.2.5 Tasks to be performed before a logical host name is changed in a cluster system* in the *JP1/Integrated Management - Manager Administration Guide* and perform the required tasks.

7.9 Logical host operation and environment configuration in a non-cluster system (for UNIX)

This section provides an overview of the configuration and operation of logical hosts that do not employ failover.

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.

7.9.1 Evaluating the configuration for running logical hosts in a non-cluster system (for UNIX)

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.

7.9.2 Environment setup for running logical hosts in a non-cluster system (for UNIX)

This subsection explains how to run JP1/IM - Manager in a non-failover logical host environment.

(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 might 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 *Chapter 6. Operation and Environment Configuration in a Cluster System (for Windows)*, 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
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 might not run correctly or might 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 *3.3 Automatic startup and automatic stop setting examples when a logical host operates in a non-cluster system* in the *JP1/Integrated Management - Manager Administration Guide*.

7.9.3 Notes about running logical hosts in a non-cluster system (for UNIX)

(1) 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.

(2) 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.

8

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.

8.1 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 communication methods and settings used by JP1/Base, see the following information in the *JP1/Base User's Guide*:

- *Communication protocols of JP1/Base* in the *Details of JP1/Base Functions* chapter
- *JP1/Base Communication Settings Depending on the Network Configuration* chapter

8.2 Operating in multiple networks

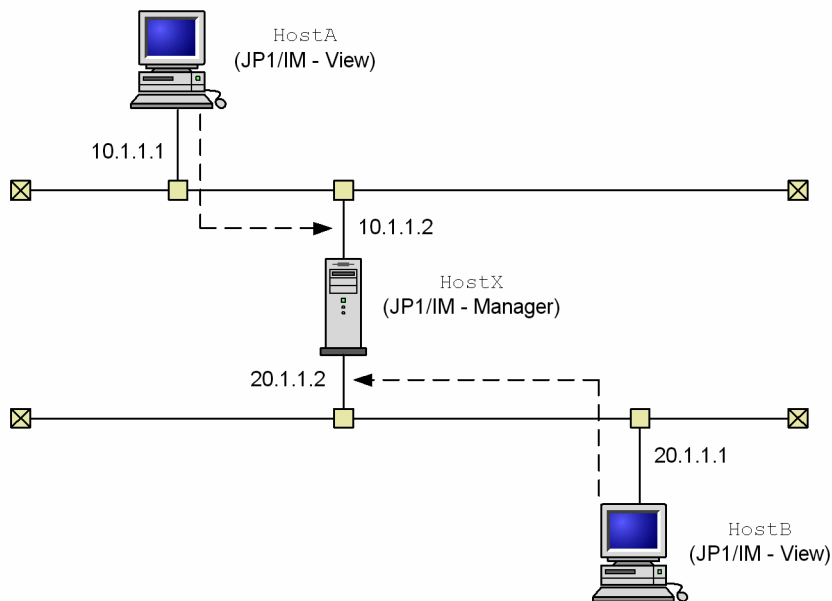
This section describes examples of system configurations that use multiple LANs (configurations in which multiple networks are connected), and the required communication settings based on the configuration examples.

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.

8.2.1 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 8–1: Connecting JP1/IM - View in a multi-LAN environment (non-cluster operation)



The following tables show the settings for each host.

Table 8–1: 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 8–2: Settings for HostA and HostB (JP1/IM - View)

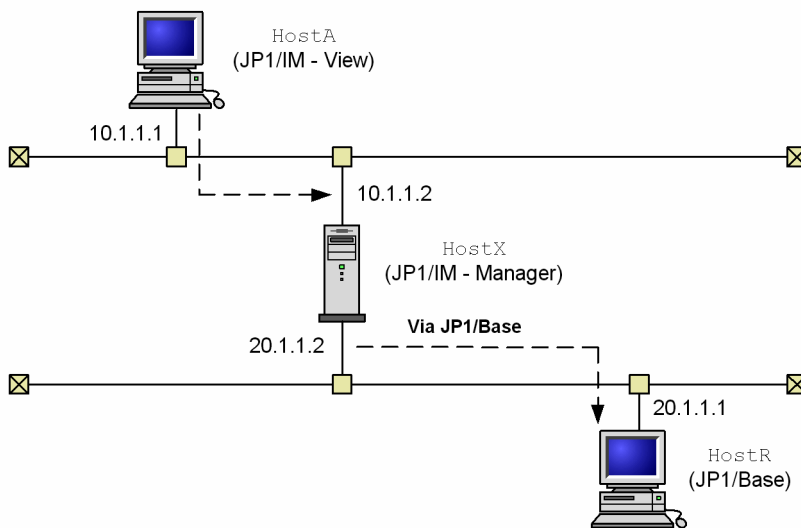
Host name	Host to connect	Other conditions [#]
HostA	HostX	Conversion from host name HostX to 10.1.1.2 must be possible.
HostB	HostX	Conversion from host name HostX to 20.1.1.2 must be possible.

[#]: Use the `hosts` file and DNS to resolve host names, because JP1/IM - View does not reference settings in the `jp1hosts` and `jp1hosts2` files.

8.2.2 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 8–2: Command execution in a multi-LAN environment (non-cluster operation)



The following tables show the settings for each host.

Table 8–3: 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).

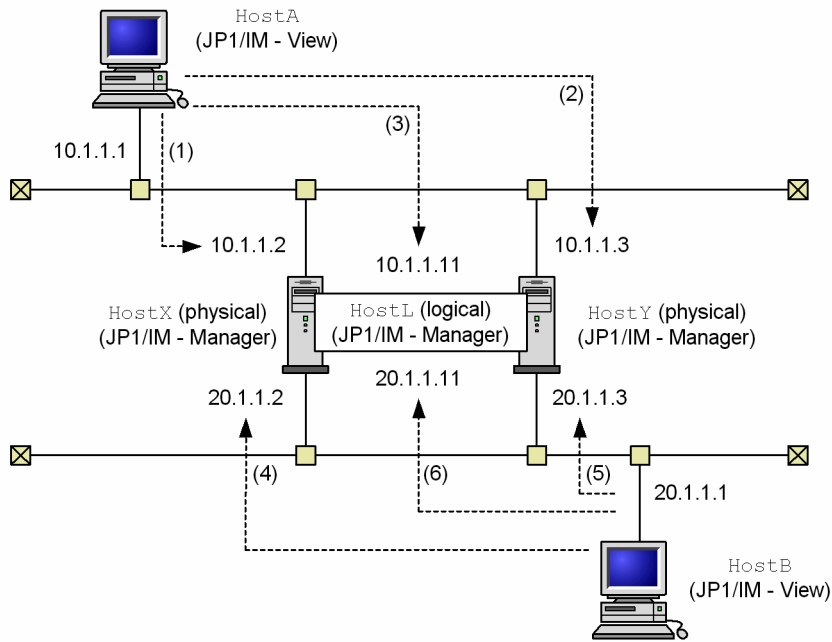
Table 8–4: Settings for HostA (JP1/IM - View)

Host name	Host to connect	Other conditions
HostA	HostX	Conversion from host name HostX to 10.1.1.2 must be possible.

8.2.3 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 8–3: Connecting JP1/IM - View in a multi-LAN environment (cluster operation)



The following tables show the settings for each host.

Table 8–5: 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 *JP1/Base User's Guide*.

Table 8–6: Settings for HostA (JP1/IM - View)

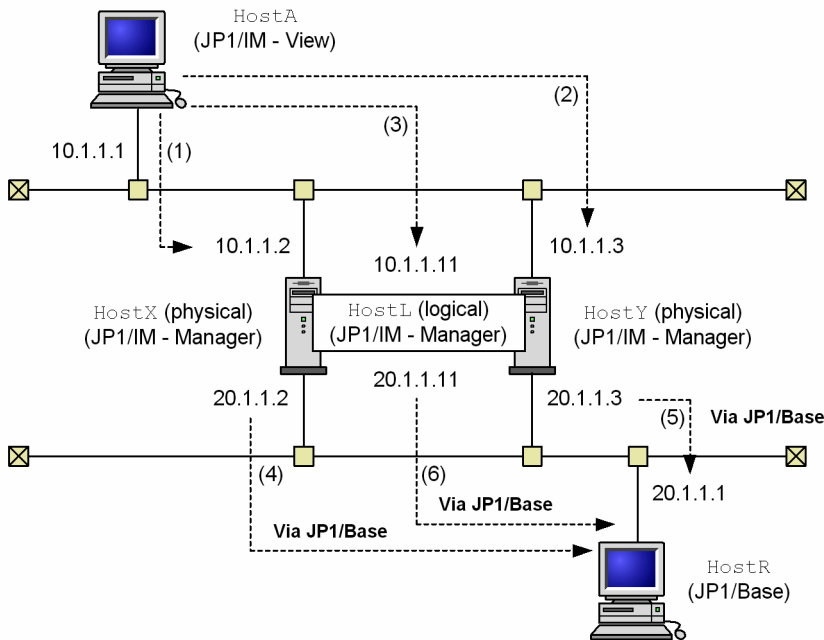
Host name	Host to connect	Other conditions	Correspondence to number in parentheses in figure
HostA	HostX	Conversion from host name HostX to 10.1.1.2 must be possible.	1

Host name	Host to connect	Other conditions	Correspondence to number in parentheses in figure
	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

8.2.4 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 8–4: Command execution in a multi-LAN environment (cluster operation)



The following tables show the settings for each host.

Table 8–7: 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 *JP1/Base User's Guide*.

Table 8–8: 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

8.3 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.

8.3.1 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.

Important

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 *Appendix C. Port Numbers* in the *JP1/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.

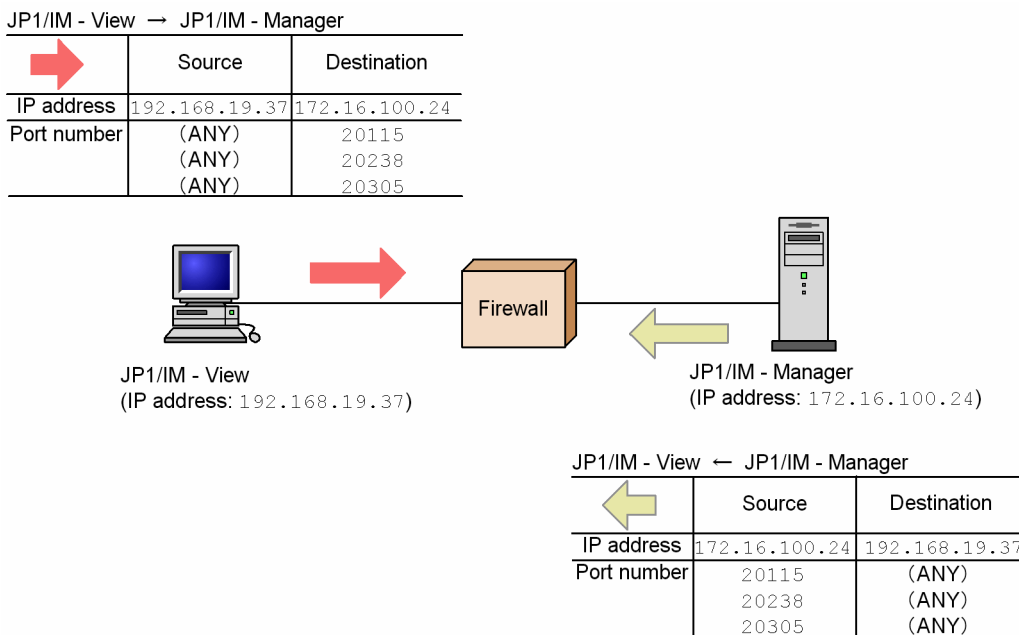
(b) Example of settings for JP1/IM

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 8–5: 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 *JP1/Integrated Management - Manager Overview and System Design Guide*, the port numbers used by JP1/IM are described as shown in the following table.

Table 8–9: Firewall passage directions

No.	Service name	Port number	Firewall passage direction
1	jplimevtcon	20115/tcp	JP1/IM - View → JP1/IM - Manager (Central Console)
2	jplimcmda	20238/tcp	JP1/IM - View → JP1/IM - Manager (Central Console) JP1/IM - Manager (Central Scope) → JP1/Base ^{#1}
3	jplimcss	20305/tcp	JP1/IM - View → JP1/IM - Manager (Central Console)
4	jplimegs	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	jplrmregistry	20380/tcp	JP1/IM - View → JP1/IM - Rule Operation
6	jplrmobject	20381/tcp	
7	http	80/tcp ^{#2}	Web-based JP1/IM - View (Web browser) → HTTP server

No.	Service name	Port number	Firewall passage direction
8	JP1/IM-Manager DB Server	20700/tcp	JP1/IM - Manager → JP1/IM - Manager DB Server
9	jplimfcs	20701/tcp	There is no need to set a firewall because communication is performed only locally on the machine on which JP1/IM - Manager is installed.
10	jplimcf	20702/tcp	JP1/IM - View → JP1/IM - Manager (IM Configuration Management)
11	jimmail	25/tcp ^{#3}	JP1/IM - Manager → Mail server (SMTP) (for no authentication)
12		587/tcp ^{#3}	JP1/IM - Manager → Mail server (SMTP) (for SMTP-AUTH authentication)
13		110/tcp ^{#3}	JP1/IM - Manager → Mail server (POP3) (for POP-before-SMTP authentication)

#1: This is the manager's JP1/Base.

#2: This might depend on the HTTP server settings.

#3: The port number at the connection destination might differ depending on the port used by the connection-destination server.

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 `jplimevtcon`), port number 20238 (service name `jplimcmnda`), and port number 20305 (service name `jplimcss`) 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 (Central Scope).

- 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 8–10: Passage conditions for packet filtering

No.	Source IP address	Destination IP 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

No.	Source IP address	Destination IP address	Protocol	Source port	Destination port	Control
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 might 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.

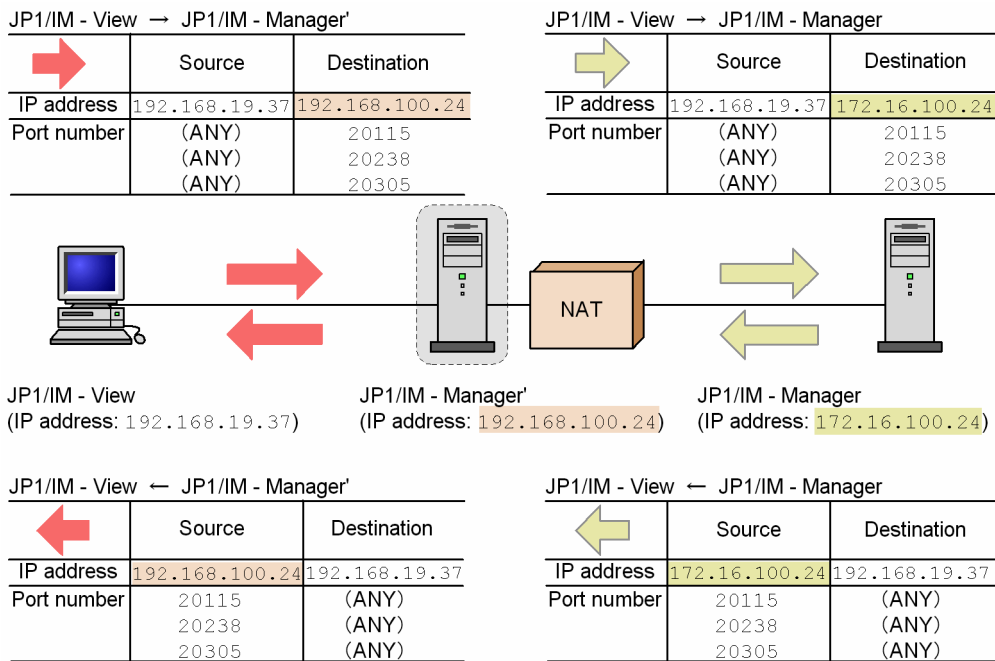
(b) Example of settings for JP1/IM

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 8–6: 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 (host name displayed by executing the `hostname` command).

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 8–11: Address translation rule

No.	Source IP address	Destination IP address	Source IP address (translated)	Destination IP 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 might 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.

8.3.2 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 *JP1/Base User's Guide*
- Port numbers of JP1/IM: *Appendix C. Port Numbers* in the *JP1/Integrated Management - Manager Overview and System Design Guide*

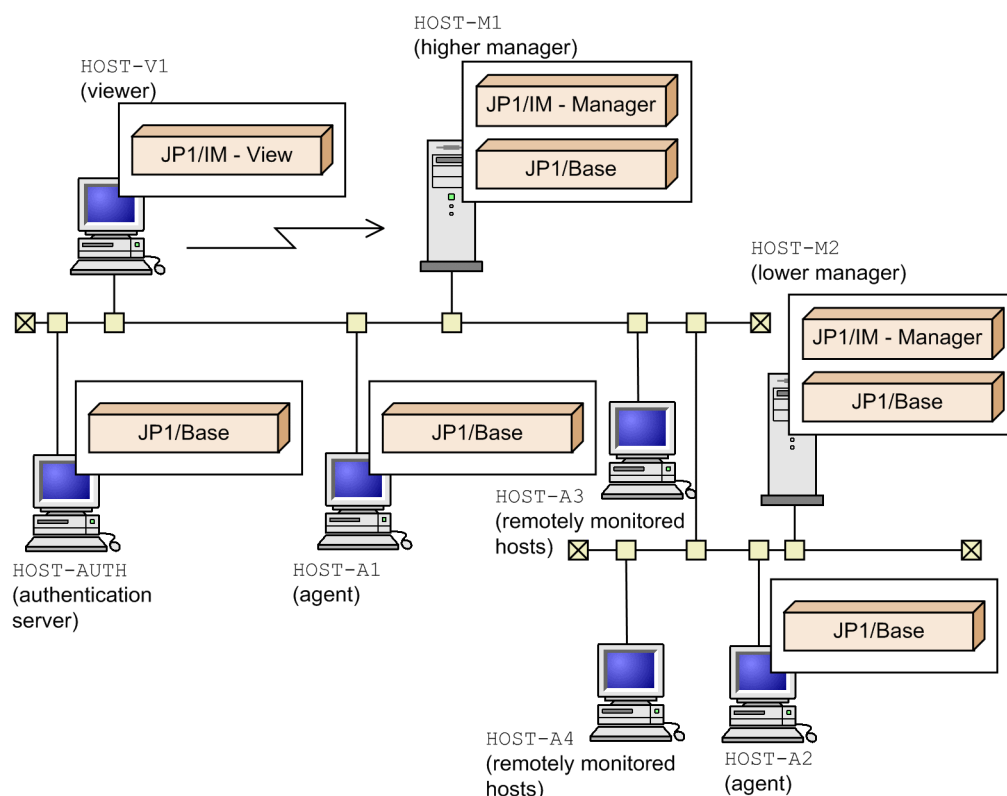
(b) Example of system configuration and communication

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.

Important

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 8–7: System configuration (example)



To set JP1/IM communication:

1. Connect to HOST-M1 by JP1/IM - View of HOST-V1.
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. Position HOST-A3 under HOST-M1 and HOST-A4 under HOST-M2 as remote monitored hosts.
5. 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 managers and remote monitored hosts

Manager(JP1/IM)	Passage direction	Remote monitored host
(ANY)	→	135/tcp (WMI) 445/tcp (WMI) Dynamic port (1024 or greater)/tcp (WMI) 137/udp (NetBIOS) 138/udp (NetBIOS)

Manager(JP1/IM)	Passage direction	Remote monitored host
		139/tcp (NetBIOS) 22/tcp (SSH) [#]

#: This may vary depending on the SSH server settings.

- Communication between viewer and manager

JP1/IM - View	Passage direction	Manager (JP1/IM and JP1/Base)
(ANY)	→	20115/tcp (jplimevtcon) 20238/tcp (jplimcmda) 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 (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 might 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)	→	20099/tcp (jplimevtapi) 20237/tcp (jplimrt) 20239/tcp (jplimcmdc) 20306/tcp (jplbsplugin) 20600/tcp (jplbscom) 20702/tcp (jplimcf) [#]
20098/tcp (jplimevt) 20239/tcp (jplimcmdc)	←	(ANY)
20600/tcp (jplbscom)	←	(ANY)

#: The port of jplimcf is used only when JP1/IM - Manager (IM Configuration Management) is used.

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/Base)	Passage direction	Agent (JP1/Base)
(ANY)	→	20099/tcp (jp1imevtapi) 20237/tcp (jp1imrt) 20239/tcp (jp1imcmdc) 20306/tcp (jp1bsplugin) 20600/tcp (jp1bscom)
20098/tcp (jp1imev) 20239/tcp (jp1imcmdc)	←	(ANY)
20600/tcp (jp1bscom)	←	(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 *JP1/Base User's Guide*.

(2) IP addresses

This subsection describes the IP addresses that are used by JP1/IM and JP1/Base.

Only IPv4 addresses can be used between JP1/IM - View and JP1/IM - Manager. Both IPv4 addresses and IPv6 addresses can be used between JP1/Base and JP1/IM - Manager.

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 required JP1/Base 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 *JP1/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 (host name displayed by executing the `hostname` command).
- 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 (host name displayed by executing the `hostname` command). 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 (host name displayed by executing the `hostname` command). 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 [8.3.2\(2\)\(a\) For a normal system](#) and [8.3.2\(2\)\(b\) For a cluster system](#) constitutes the standard communication settings when JP1 has just been set up. If you have customized multiple LAN connections by, for example, defining `jp1hosts` information or `jp1hosts2` information in JP1/Base, note that the operation is determined by the combination of the communication methods used by the receiver and the sender (ANY binding and IP binding).

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 [8.3.2\(2\)\(b\) For a cluster system](#), while the sender's operation is as discussed in [8.3.2\(2\)\(a\) For a normal system](#).

In addition, if host names and IP addresses are defined in the `jp1hosts` information or the `jp1hosts2` information when the `jp1hosts` information or the `jp1hosts2` information is configured, the definitions in the `hosts` file will not be referenced for those host names and IP addresses.

For example, suppose that the `jp1hosts` 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 `jp1hosts` information, the system configuration cannot be defined.

(d) Notes on using the email notification function of JP1/IM - Manager

The email notification function of JP1/IM - Manager communicates with a mail server by using IPv4 addresses.

Therefore, prepare a mail server which has IPv4 addresses. This function cannot perform communication using IPv6 addresses.

(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.

8.4 Configuring encrypted communication

This section explains the settings for newly using, making changes to, and disabling the communication encryption function, the JP1/IM - Manager settings for the communication encryption function, and how to check the settings of the communication encryption function.

Important

- When the communication encryption function is used, it might not be possible to establish communication with the previous configuration. For details, see *12.11.7 Communication encryption function setting (enable/disable) and connectivity among product versions* and *Appendix H. Connectivity with Previous Versions* in the *JP1/Integrated Management - Manager Overview and System Design Guide*.
- The administrator must back up private keys, server certificates, and root certificates so that they can be recovered. For details about the information to be backed up, see *1.1.1 Backup (in Windows)* or *1.1.3 Backup (in UNIX)* in the *JP1/Integrated Management - Manager Administration Guide*.

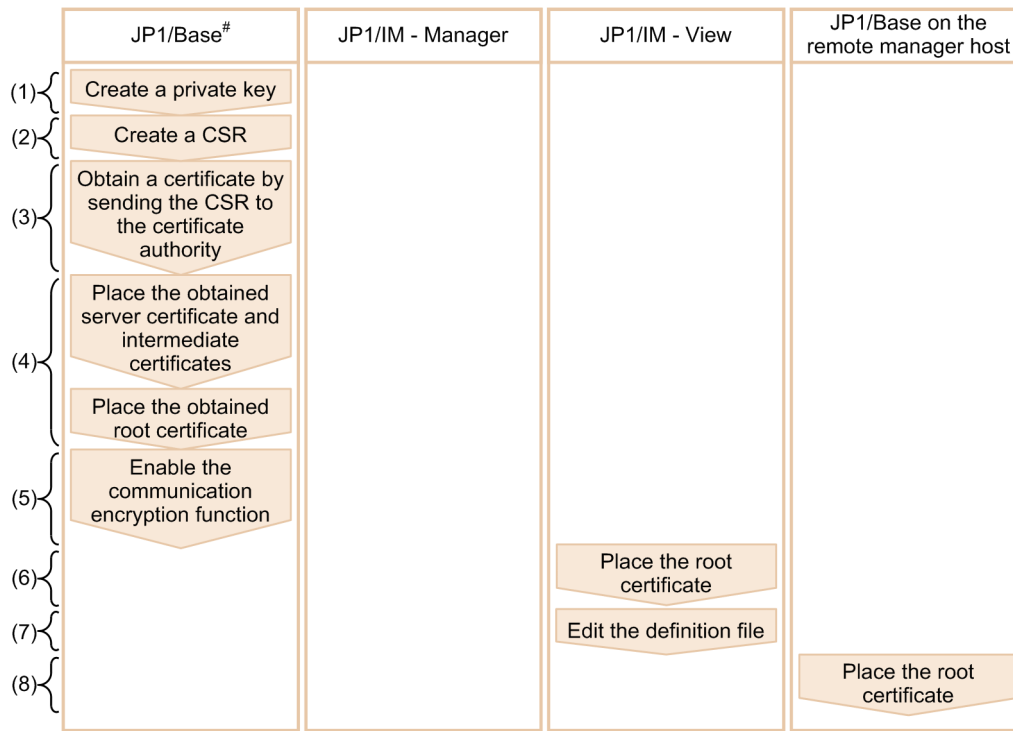
8.4.1 Newly using the communication encryption function

This subsection explains how a first-time user of the communication encryption function can specify settings on the manager host and the viewer host. There is no procedure to be set in JP1/IM - Manager. If there are multiple manager hosts, specify the settings on each host. For details about the system configuration, see *12.11.6 System configuration* in the *JP1/Integrated Management - Manager Overview and System Design Guide*.

JP1/IM - Manager, JP1/AJS3, and JP1/Base's communication encryption function all use the common definition information that is specified based on the private keys, CSRs, individual certificates, and the SSL communication definition file (`jp1bs_ssl.conf`) that are used on the manager host.

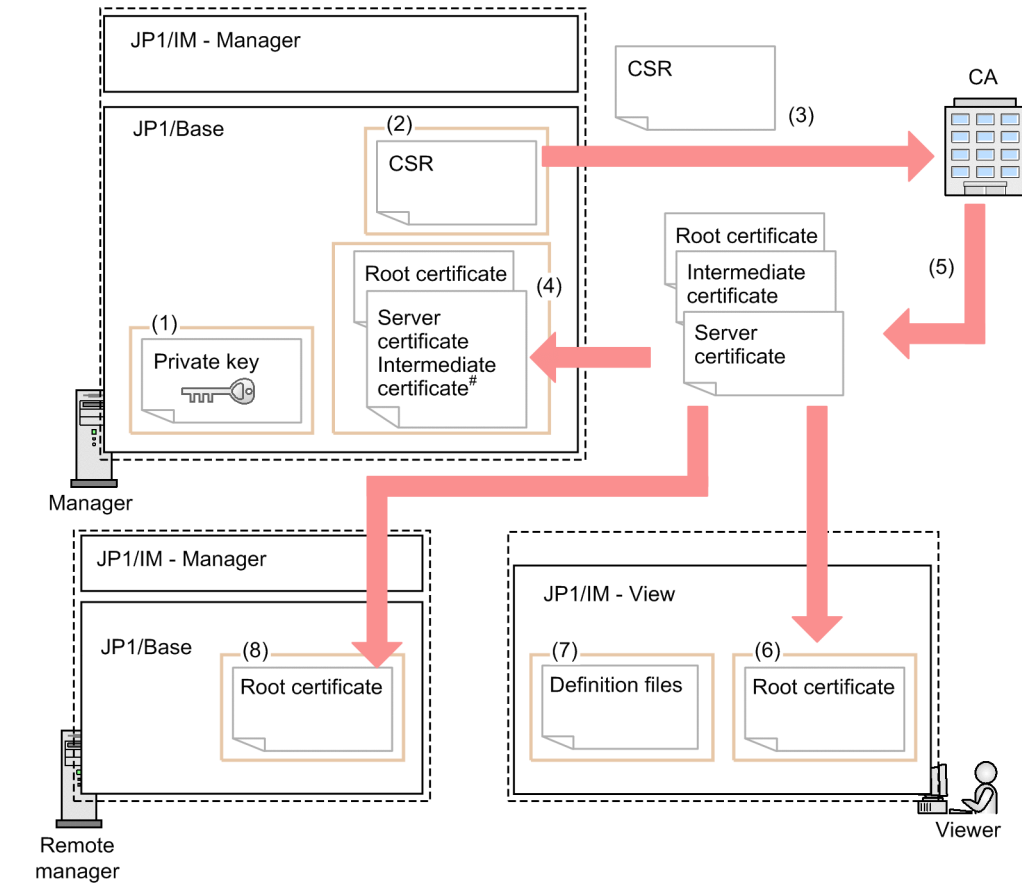
The following figures show the procedure for newly using the communication encryption function.

Figure 8–8: Procedure for newly using the communication encryption function



#: For details, see the *JP1/Base User's Guide*.

Figure 8–9: Overview of files that are edited by the user



Legend:

- : Same host
- : Product
- ➔ : Flow of processing

#: If an intermediate certificate is used, it is combined with the server certificate.

The following provides a detailed explanation (the numbers below correspond to the numbers in the figures).

1. Creating a private key in JP1/Base^{#1}

Do not set a passphrase for a private key. A private key with a passphrase cannot be used.

2. Creating a certificate signing request (CSR)^{#1}

Create a CSR by specifying the private key created in step 1. Specify the manager host name for CN (common name). This manager host name is used to verify the host name (CN and SAN) in server certificates.

For details about the verification of host names in server certificates (verification of CN and SAN), see *12.11.4(2) Verifying host names (CN and SAN) in server certificates* in the *JP1/Integrated Management - Manager Overview and System Design Guide*.

3. Send the CSR created in step 2 to the certificate authority to obtain certificates.^{#1}

Send the CSR created in step 2 to the certificate authority to obtain a server certificate and a root certificate.

If there is any intermediate CA certificate, obtain it.

If you will be using self-signed certificates, not the certificates signed by the certificate authority, do not send the CSR to the certificate authority.

4. Place the private key and the certificates in JP1/Base.^{#1, #2}

Place the private key created in step 1 and the server certificate and root certificate issued in step 3 in any folder on the server.

If there are any intermediate CA certificates, use a text editor (for example) to combine the intermediate CA certificates with the server certificate according to the certificate hierarchy.

The following shows combined server certificates:

```
-----BEGIN CERTIFICATE-----  
contents-of-server-certificate  
-----END CERTIFICATE-----  
-----BEGIN CERTIFICATE-----  
contents-of-intermediate-CA-certificate  
-----END CERTIFICATE-----
```

5. In JP1/Base, enable the communication encryption function.^{#1}

The following explains how to configure the communication encryption function:

1. Define the SSL communication definition file (`jp1bs_ssl.conf`).

Define in the SSL communication definition file the SSL communication settings, such as whether SSL communication is to be enabled, the file names of server certificates, and the storage locations of root certificates.

For details about the SSL communication definition file, see the chapter on SSL communication definition files in the *JP1/Base User's Guide*.

2. Execute the `jbssetcnf` command with the SSL communication definition file name specified in an argument.

When the `jbssetcnf` command is executed, the specified settings are applied to the common definition information. These settings are used to run the communication encryption function in JP1/IM - Manager, JP1/AJS3, and JP1/Base.

For details about the `jbssetcnf` command, see the *JP1/Base User's Guide*.

6. Place the root certificate issued in step 3 in JP1/IM - View.^{#2}

- Storage location for the root certificate

`View-path\conf\ssl\rootcer`

JP1/IM - View enables you to place multiple root certificate files.

When you place a root certificate in JP1/IM - View, you have to know the manager host to which the root certificate being placed corresponds. For details, see *12.11.3(1) Encryption between a manager host and a viewer host* in the *JP1/Integrated Management - Manager Overview and System Design Guide*.

7. Edit the file used to specify the hosts that will be able to establish non-encrypted communication.

A non-encryption communication host configuration file is used to specify the hosts that will be able to establish non-encrypted communication. With the initial settings, all hosts are set to establish non-encrypted communication. For details, see *Non-encryption communication host configuration file (nosslhost.conf)* in *Chapter 2. Definition Files* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

8. Place the root certificate on the remote manager host in the following cases.^{#2}

- The handling procedure is changed from the remote manager host by executing the `jcochstat` command with the `-j` option specified
If the remote manager host is not using the communication encryption function, enable the communication encryption function and add the root certificate issued in step 3 to the remote manager host's root certificate file.
- The IM Configuration Management function is being used by the higher manager.

Place the root certificate issued in step 3 in JP1/Base of the remote manager host that is the higher manager. In this case, you will have to specify the storage location of the root certificate (`CACERTIFICATEFILE` in the common definition information) in the remote manager host's JP1/Base, but you need not enable the communication encryption function.

If the remote manager host is using the communication encryption function, add the root certificate issued in step 3 to the remote manager host's root certificate file.

To add root certificates to the remote manager host, use a text editor (for example) to combine the root certificates. The following shows combined root certificates:

```
-----BEGIN CERTIFICATE-----  
contents-of-root-certificate  
-----END CERTIFICATE-----  
-----BEGIN CERTIFICATE-----  
contents-of-root-certificate  
-----END CERTIFICATE-----
```

#1: For details, see the *JP1/Base User's Guide*.

#2: To combine multiple certificates, open the certificates with a text editor, and then combine them.

Important

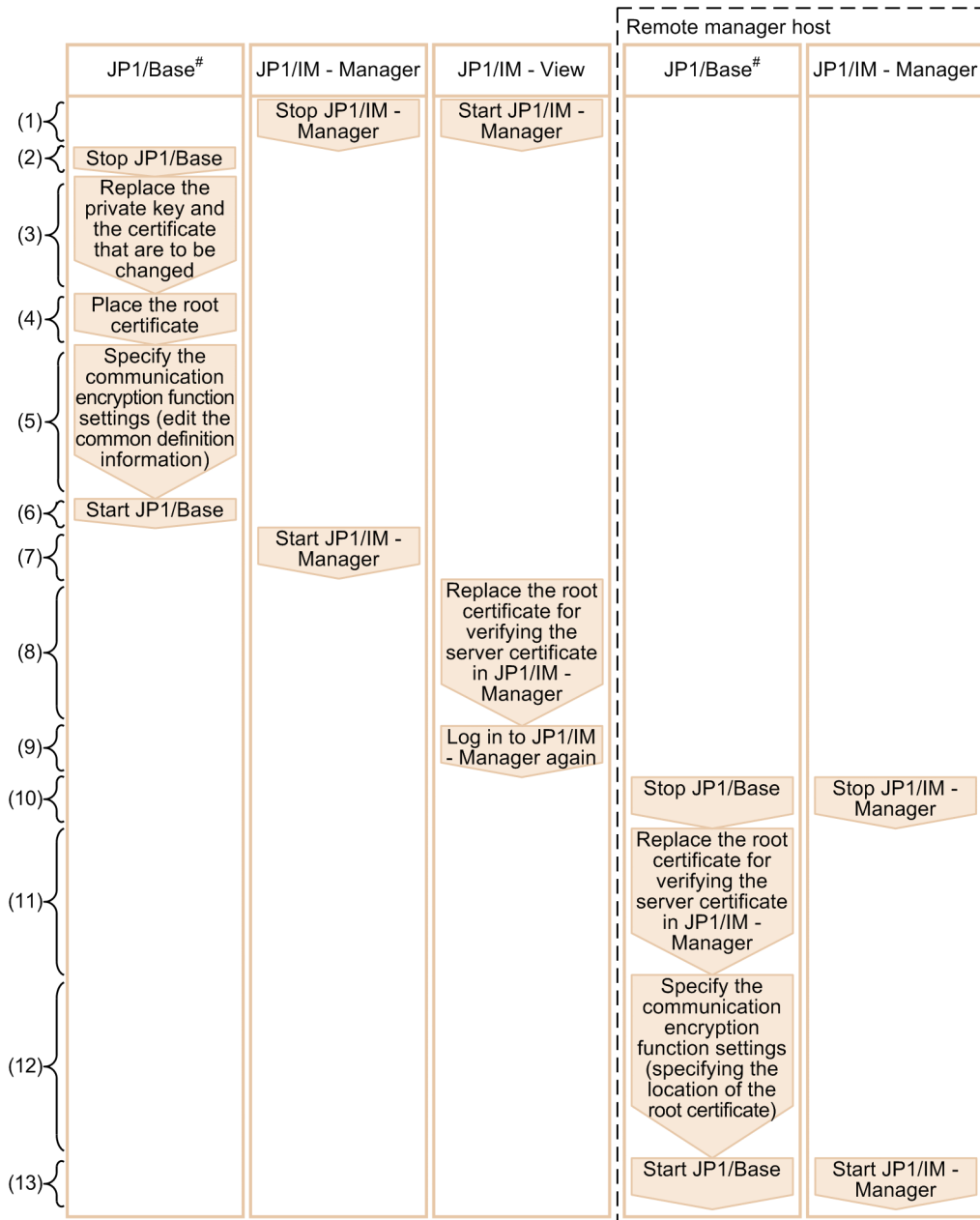
Communication encryption function settings cannot be changed while JP1/IM - Manager and JP1/Base are running. If you need to change communication encryption function settings for a reason such as to replace expired server or root certificates, you must first stop JP1/IM - Manager and JP1/Base.

After you have configured the communication encryption function, check that the function has been configured correctly. For details about the checking procedure, see [8.4.5 Checking whether the communication encryption function has been configured correctly](#).

8.4.2 Changing configured certificates

This subsection explains how to change configured certificates on the manager host and the viewer host. If there are multiple manager hosts, perform the procedure described below on each manager host.

Figure 8–10: Procedure for changing certificates



Legend:

□ □ □ : Same host

#: For details, see the *JP1/Base User's Guide*.

The following provides a detailed explanation (the numbers below correspond to the numbers in the figure).

1. Stop JP1/IM - View and JP1/IM - Manager.
2. Stop JP1/Base.
3. Replace the private key and the certificates that are to be changed.
4. If there is a change to the root certificate that corresponds to a server certificate replaced in step 3, replace the root certificate in JP1/Base.

5. If the file names or storage locations of the private key and certificates have been changed, specify the communication encryption function settings in JP1/Base (edit the common definition information).^{#1}
6. Start JP1/Base.
7. Start JP1/IM - Manager.
8. If the root certificate is to be changed in JP1/IM - View, replace the root certificate used to verify the server certificate of JP1/IM - Manager.^{#2, #3}
 - Root certificate storage location
`View-path\conf\ssl\rootcer`
9. Log in to JP1/IM - Manager again from JP1/IM - View.
10. Stop JP1/IM - Manager and JP1/Base on the remote host in the following cases:
 - The handling status is to be changed from the remote manager host by executing the `jcochstat` command with the `-h` option specified.
 - The IM Configuration Management function is being used on the higher manager.
11. Replace the root certificate on the remote manager host in the following cases:^{#3}
 - The handling status is to be changed from the remote manager host by executing the `jcochstat` command with the `-h` option specified.
 - The IM Configuration Management function is being used on the higher manager.

If the root certificate is to be changed, replace the root certificate used to verify the server certificate of JP1/IM - Manager. If the root certificate has been combined with other certificates, replace only the corresponding root certificate.
12. If you will be changing the file name or storage location of the root certificate in the following cases, configure the communication encryption function in JP1/Base on the remote manager host (edit the common definition information).^{#1}
 - The handling status is to be changed from the remote manager host by executing the `jcochstat` command with the `-h` option specified.
 - The IM Configuration Management function is being used on the higher manager.
13. Start JP1/IM - Manager and JP1/Base on the remote host in the following cases:
 - The handling status is to be changed from the remote manager host by executing the `jcochstat` command with the `-h` option specified.
 - The IM Configuration Management function is being used on the higher manager.

#1: For details, see the *JP1/Base User's Guide*.

#2: For details, see *12.11.3(1) Encryption between a manager host and a viewer host* in the *JP1/Integrated Management - Manager Overview and System Design Guide*.

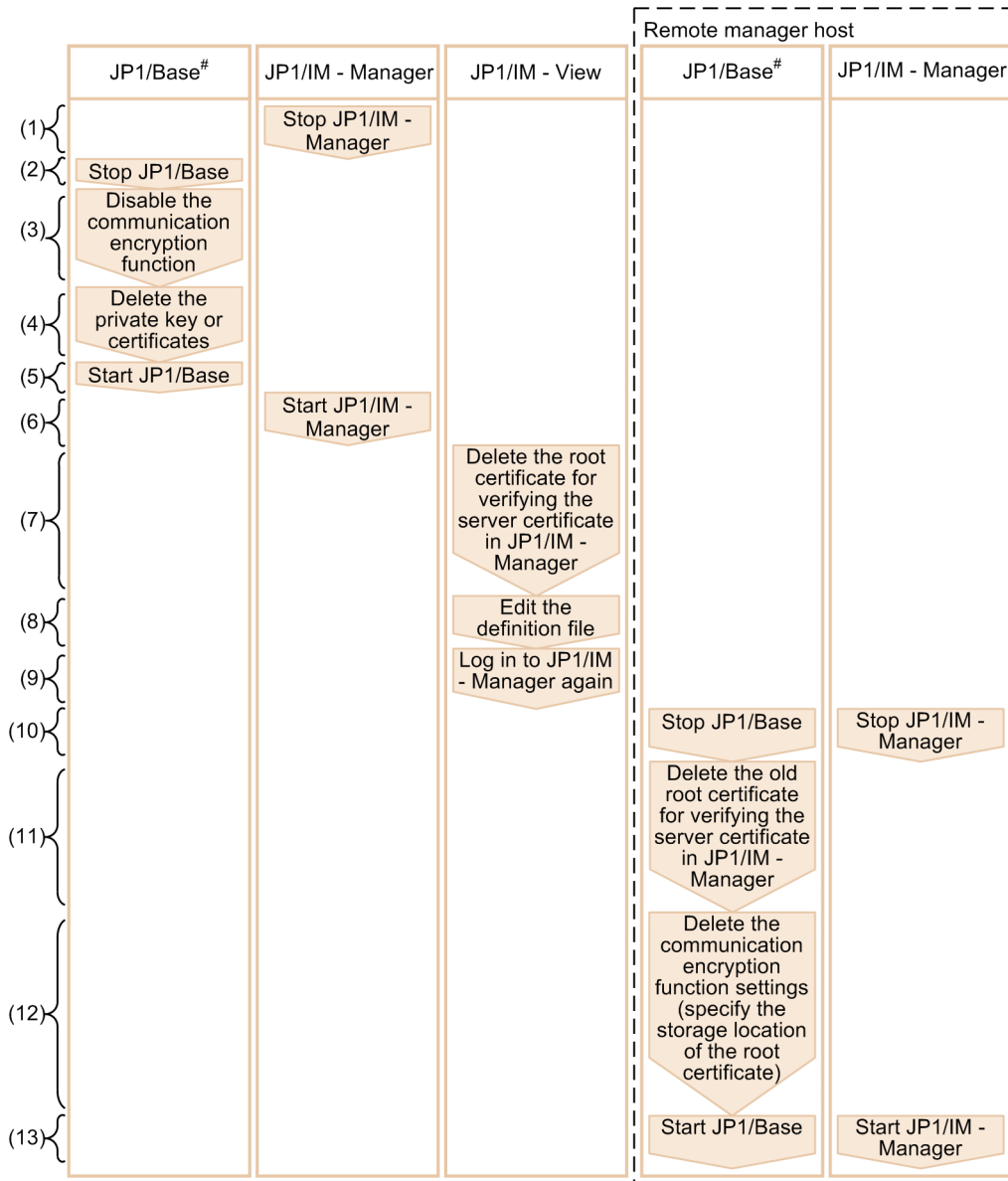
#3: To edit a certificate, use a text editor to open the certificate and edit its contents.

After you have configured the communication encryption function, check if the function has been configured correctly. For details about the checking procedure, see *8.4.5 Checking whether the communication encryption function has been configured correctly*.

8.4.3 Stopping using the communication encryption function

This subsection explains how to make changes on the manager host and the viewer host when the user stops using the communication encryption function. If you stop using the function temporarily, there is no need to perform steps 4, 7, and 11. If there are multiple manager hosts, perform this procedure on each of the manager hosts.

Figure 8–11: Procedure for stopping using the communication encryption function



Legend:

□ : Same host

#: For details, see the *JP1/Base User's Guide*.

The following provides a detailed explanation (the numbers below correspond to the numbers in the figure).

1. Stop JP1/IM - Manager.
2. Stop JP1/Base.
3. Disable the communication encryption function in JP1/Base.#1

4. Delete the private key and certificates in JP1/Base.
5. Start JP1/Base.
6. Start JP1/IM - Manager.
7. In JP1/IM - View, delete the root certificate for verifying the server certificate of JP1/IM - Manager on which the communication encryption function will no longer be used.^{#2}
 When you delete a root certificate in JP1/IM - View, you have to know the manager to which the host the root certificate being deleted corresponds. For details, see *12.11.3(1) Encryption between a manager host and a viewer host* in the *JP1/Integrated Management - Manager Overview and System Design Guide*.
 - Root certificate storage location
`View-path\conf\ssl\rootcer`
8. If you will be using non-encrypted communication with the manager host that will stop using the function, specify the host name of that manager host in the definition file in JP1/IM - View.
 For details, see *Non-encryption communication host configuration file (nosslhost.conf)* in *Chapter 2. Definition Files* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.
9. Log in to JP1/IM - Manager again from JP1/IM - View.
10. Stop JP1/IM - Manager and JP1/Base on the remote host in the following cases:
 - The handling status is to be changed from the remote manager host by executing the `jcochstat` command with the `-h` option specified.
 - The IM Configuration Management function is being used on the higher manager.
11. Delete the root certificate on the remote manager host in the following cases.^{#2}
 - The handling status is to be changed from the remote manager host by executing the `jcochstat` command with the `-h` option specified.
 - The IM Configuration Management function is being used on the higher manager.
 Delete the root certificate used for verifying the server certificate of JP1/IM - Manager that will stop using the communication encryption function. If the root certificate is combined with other certificates, delete only the corresponding root certificate.
12. If you have deleted all root certificates that have been placed in the following cases, delete the communication encryption function settings (edit the common definition information).^{#1}
 - The handling status is to be changed from the remote manager host by executing the `jcochstat` command with the `-h` option specified.
 - The IM Configuration Management function is being used on the higher manager.
13. Start JP1/IM - Manager and JP1/Base on the remote manager host in the following cases:
 - The handling status is to be changed from the remote manager host by executing the `jcochstat` command with the `-h` option specified.
 - The IM Configuration Management function is being used on the higher manager.

#1: For details, see the *JP1/Base User's Guide*.

#2: To edit a certificate, use a text editor to open the certificate and edit its contents.

After you have configured the communication encryption function, check that the function has been configured correctly. For details about the checking procedure, see [8.4.5 Checking whether the communication encryption function has been configured correctly](#).

8.4.4 Configuring JP1/IM - Manager

This subsection explains the settings for enabling and disabling the communication encryption function and placing certificates in JP1/IM - Manager.

(1) Enabling and disabling the communication encryption function

For the enable/disable setting for the communication encryption function, JP1/IM - Manager references the common definition information specified in JP1/Base.

When JP1/IM - Manager starts, it references the common definition information specified in JP1/Base. For details about the common definition information that is specified in JP1/Base, see the chapter on SSL communication definition files in the *JP1/Base User's Guide*.

Also when JP1/IM - Manager starts, it outputs a message confirming that the communication encryption function's enable/disable setting is the same on JP1/IM - Manager and JP1/Base (manager host). If the function is enabled, the `KAVB8810-I` message is output to the integrated trace log. If the function is disabled, the `KAVB8811-I` message is output to the integrated trace log. For details about the enable/disable setting for the communication encryption function, see [8.4.5 Checking whether the communication encryption function has been configured correctly](#).

(2) Specifying SSL versions and certificate locations

For the SSL version and certificate locations, JP1/IM - Manager references the common definition information specified in JP1/Base. For details about the common definition information that is specified in JP1/Base, see the chapter on SSL communication definition files in the *JP1/Base User's Guide*.

(3) Keystores for JP1/IM - Manager

If private keys or keystores for JP1/IM - Manager have been obtained, the JP1/IM - Manager administrator must manage them securely because encrypted communication data might be compromised. Set a folder that stores private keys or keystores for JP1/IM - Manager in such a manner that general users will not be able to reference the folder.

A keystore for JP1/IM - Manager is a file used by JP1/IM - Manager to establish encrypted communication. It stores the following data:

- Private keys
- Server certificates
- Intermediate CA certificates (if used)

Its storage location on the manager host is set as follows:

- For physical hosts
Windows: `Manager-path\conf\ssl\server.keystore`
UNIX: `/etc/opt/jp1imm/conf/ssl/server.keystore`
- For logical hosts
Windows: `shared-folder\JP1IMM\conf\ssl\server.keystore`

8.4.5 Checking whether the communication encryption function has been configured correctly

Use the procedure described below to check that the communication encryption function has been enabled or disabled. If there are multiple manager hosts, perform this procedure on each of the manager hosts.

1. Check the integrated trace log of the manager host.

- If you are verifying that the communication encryption function has been enabled, check that the `KAVB8810-I` message has been output to the integrated trace log.
- If you are verifying that the communication encryption function has been disabled, check that the `KAVB8811-I` message has been output to the integrated trace log.

2. Verify that you can connect from JP1/IM - View to JP1/IM - Manager.

Verify that you can log in to Central Console.

If you use Central Scope, verify that you can log in to Central Scope.

If you use IM Configuration Management, verify that you can log into IM Configuration Management.

For details about how to log in, see *Chapter 4. JP1/IM - Manager Login and Logout* in the *JP1/Integrated Management - Manager Administration Guide*.

3. Verify that commands can be executed and that command execution by automated actions is enabled.

From JP1/IM - View's Execute Command window, execute a command on the manager host and verify that the `KAVB2013-I` message reporting the completion of execution is displayed in **Log**.

Execute a command by automated action on the manager host and verify in the Action Log window or the List of Action Results window in JP1/IM - View that the executed action has terminated.

For details about how to execute commands, see *7.1 Executing a command* in the *JP1/Integrated Management - Manager Administration Guide*.

For details about how to execute commands by automated actions, see *4.5 Setting automated actions*.

4. Verify that **Synchronize IM Configuration** can be performed successfully.

If you are using IM Configuration Management to manage base managers, execute **Synchronize IM Configuration** from the IM Configuration Management window and verify that remote monitoring configuration information can be collected.

For details about how to execute **Synchronize IM Configuration**, see *3.2.5 Synchronizing the system hierarchy*.

9

Settings for Linking to Other JP1 Products

This chapter describes the environment setup for linking JP1/IM to other JP1 products.

9.1 Linking to JP1/Service Support

Before you can link to JP1/Service Support, you must set the system to allow the JP1/Service Support window to be called.

9.1.1 Enabling calling the JP1/Service Support window

To enable the Select the Destination Process Workboard window of JP1/Service Support to be called from JP1/IM - View, you must edit the definition file for registering incidents manually (`incident.conf`). This file is managed by the JP1/IM - Manager (Central Console) that you log in to from JP1/IM - View. When you set the incident registration mode to 3, you must edit the configuration file for incident inheritance information (`incident_info.conf`) to enable desired attributes or character strings of the JP1 event to be inherited as incidents.

Note that you must also specify the same settings when you call the Select the Destination Process Workboard window of JP1/Service Support from a Web-based JP1/IM - View.

To enable the JP1/Service Support window to be called:

1. Edit the definition file for manually registering incidents (`incident.conf`). (You can use a program such as text editor.)
2. When you set the incident registration mode to 3, edit the configuration file for incident inheritance information (`incident_info.conf`) by using a program such as text editor.
3. Specify the settings so that the port number specified for `SS_URL=` in the definition file for manually registering incidents (`incident.conf`) allows communication through the firewall.
Specify the settings to allow access through the firewall from the JP1/IM - View machine to the JP1/Service Support machine.
4. Execute the `jco_spm�_reload` command or restart JP1/IM - Manager.
5. Log in to JP1/IM - Manager (Central Console) from JP1/IM - View again.
The defined settings will take effect.

The URL used to call JP1/Service Support can have a maximum of 2,046 characters. When the incident registration mode is set to 2, the length of a message that can be passed is shorter than when the incident registration mode is set to 1 because the event ID is also passed. If the message is garbled or truncated, copy and paste into JP1/Service Support the message that is displayed in the Event Details window.

For details about the definition file for manually registering incidents (`incident.conf`), see *Definition file for manually registering incidents (incident.conf)* in Chapter 2. *Definition Files* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

For details about the configuration file for incident inheritance information (`incident_info.conf`), see *Configuration file for incident inheritance information (incident_info.conf)* in Chapter 2. *Definition Files* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

9.2 Linking to JP1/Navigation Platform

In order to link to JP1/Navigation Platform, you must first specify in the event guide information file the URL for the event guide message file.

For details about the event guide information file, see *Event guide information file (jco_guide.txt)* in *Chapter 2. Definition Files* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*. For details about URL settings, see the section on the URL for calling Navigation Platform from JP1 products in the JP1/Navigation Platform documentation.

To reference the job contents (operation procedure) by using single sign-on, use the same authentication server for JP1/IM - Manager and JP1/Navigation Platform. Also, the JP1/Base version of the authentication server must be 10-10 or later.

The following table shows the combination of products that allow the job contents (operation procedures) to be referenced by using single sign-on.

Table 9–1: Combination of products that allow the job contents (operation procedures) to be referenced by using single sign-on

Version	JP1/IM - View is earlier than 10-00			JP1/IM - View is 10-10 or later		
	JP1/IM - NP is 10-00 (uCNP09-50)	JP1/IM - NP is 10-10 (uCNP09-60)	JP1/IM - NP is 10-50 or later ^{#1} (HNP10-00 or later)	JP1/IM - NP is 10-00 (uCNP09-50)	JP1/IM - NP is 10-10 (uCNP09-60)	JP1/IM - NP is 10-50 or later ^{#1} (HNP10-00 or later)
JP1/IM - Manager is earlier than 10-00	N			N		
JP1/IM - Manager is 10-10 or later	N			N	Y ^{#2}	

Legend:

Y: The job contents (operation procedures) can be displayed by using single sign-on.

N: The job contents (operation procedures) cannot be displayed by using single sign-on (the Login window of JP1/IM - Navigation Platform is displayed).

#1

The product name of JP1/IM - NP version 11-00 or later has been changed to JP1/Navigation Platform.

#2

You must describe a single sign-on-capable URL in the event guide message file of the central console.

9.3 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

9.3.1 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 *Chapter 1. Commands* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

9.3.2 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 [4.5 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 [2.33.1 Action Parameter Detailed Definitions window](#) in the manual *JP1/Integrated Management - Manager GUI Reference*.
- About the automated action definition file (`actdef.conf`)
See [Automated action definition file \(actdef.conf\)](#) in [Chapter 2. Definition Files](#) in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*

Important

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.

9.3.3 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 (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.

For details about, see [2.24 Preferences window](#) in the manual *JP1/Integrated Management - Manager GUI Reference*.

9.4 Linking with JP1/AJS

This section explains the settings for linking with JP1/AJS.

9.4.1 Settings for launching a JP1/AJS window by monitor startup

For details about the settings for monitor startup, see [4.17 Setting monitor startup for linked products](#) and the JP1/AJS documentation.

9.4.2 Settings for launching a JP1/AJS window from the Tool Launcher window

By default, JP1/AJS - View is displayed in the Tool Launcher window. If you install JP1/AJS - View on the host on which JP1/IM - View is installed, you can launch JP1/AJS - View from the Tool Launcher window. For details, see [7.3.2 Functions that can be operated from the Tool Launcher window](#) in the *JP1/Integrated Management - Manager Administration Guide*. For details about the settings for the Tool Launcher window, see [4.18 Setting the Tool Launcher window](#).

9.4.3 Settings for displaying the monitor window from the event guide information

To display the monitor window of JP1/AJS - Web Console from a URL in the event guide information, specify the URL for linking JP1/AJS - Web Console in the event guide message file.

For details about the setting, see the JP1/AJS documentation.

9.4.4 Settings for displaying the monitor window from an email sent by an automated action

To display the monitor window from an email sent by an automated action, specify in the text of the email the URL of the JP1/AJS - Web Console's monitor window.

For details about the settings, see the JP1/AJS documentation.

9.5 Linking with JP1/PFM

This section explains the settings for linking with JP1/PFM.

9.5.1 Settings for launching a JP1/PFM window by monitor startup

For details about the settings for monitor startup, see [4.17 Setting monitor startup for linked products](#) and the JP1/PFM documentation.

9.5.2 Settings for launching a JP1/PFM window from the Tool Launcher window

For details about the settings for the Tool Launcher window, see [4.18 Setting the Tool Launcher window](#) and the JP1/PFM documentation.

9.5.3 Settings for displaying event-source-host performance reports

To use the event-source-host performance report display function, define the URL of the target JP1/PFM - Web Console in the performance report display definition file.

For details about the settings, see the JP1/PFM documentation.

Index

A

- abnormal process termination, restart settings in event of [72](#)
- acquiring existing Visual Monitoring window [295](#)
- action status change, setting JP1 event issuance during [242](#)
- adding
 - monitoring nodes to monitoring tree [284](#)
 - monitoring nodes to Visual Monitoring window [297](#)
- adding host to business group [184](#)
- adding or deleting profile (agent configuration) [190](#)
- adding or deleting profile (remote monitoring configuration) [200](#)
- adding profile (agent configuration) [190](#)
- adding profile (remote monitoring configuration) [200](#)
- addition of program-specific attribute, setting [243](#)
- address translation [412](#)
 - support of [419](#)
- alias name [271](#)
- applying
 - customized monitoring tree to manager [293](#)
 - customized Visual Monitoring window to manager [299](#)
- applying business group information and monitoring group information to monitoring tree of Central Scope [184](#)
- applying edited information in configuration file (remote monitoring configuration) [203](#)
- authentication server, specifying (UNIX) [103](#)
- authentication server, specifying (Windows) [37](#)
- automated action definition file, updating [75, 136](#)
- automated actions
 - setting [228](#)
 - setting details of [228](#)
 - setting execution conditions of [228](#)
 - settings for monitoring execution status of [230](#)
 - setting suppression of execution [231](#)
 - setting up execution environment for [228](#)
- automatic generation of monitoring tree [281](#)
- automatic startup (UNIX) [128](#)
- automatic stop (UNIX) [128](#)

B

- business group
 - setting reference and operation restrictions [274](#)

C

- Central Console, setting up [210](#)
- Central Scope
 - before starting environment setup for [277](#)
 - environment setup for [277](#)
 - executing upgrade command [74, 135](#)
 - registering host information [278](#)
 - settings for using functions (UNIX) [131](#)
 - settings for using functions (Windows) [71](#)
 - setting up [276](#)
 - setting up for linked products [313](#)
 - setting up operating environment for [306](#)
- changing communication type for vCenter [166](#)
- changing communication type for VMware ESX [165](#)
- changing configured certificates [424](#)
- changing settings in file (UNIX) [396](#)
- changing settings in file (Windows) [367](#)
- checking language environment setting of JP1/Base [95](#)
- cluster operation [340](#)
 - JP1/IM configuration in [343, 374](#)
 - JP1's support range [342](#)
- cluster software [339](#)
- cluster system
 - environment setup procedure for cluster operation (UNIX) [377](#)
 - environment setup procedure for cluster operation (Windows) [346](#)
 - JP1/IM configuration (UNIX) [374](#)
 - JP1/IM configuration (Windows) [343](#)
 - logical host [340](#)
 - new installation and setup of logical host (UNIX) [379](#)
 - new installation and setup of logical host (Windows) [348](#)
 - notes about cluster operation (UNIX) [399](#)
 - notes about cluster operation (Windows) [370](#)
 - operation and environment configuration in cluster system (UNIX) [373](#)
 - operation and environment configuration in cluster system (Windows) [338](#)
 - overview (UNIX) [374](#)
 - overview (Windows) [339](#)
 - overview of cluster operation (UNIX) [374](#)
 - overview of cluster operation (Windows) [339](#)
 - prerequisites for cluster operations (UNIX) [374](#)
 - prerequisites for cluster operations (Windows) [340](#)

- registering into cluster software (new installation and setup) (UNIX) 387
- registering into cluster software (new installation and setup) (Windows) 359
- upgrade installation and setup of logical hosts (UNIX) 390
- upgrade installation and setup of logical hosts (Windows) 361
- collecting and distributing Event Service definition information when IM Configuration Management is not used (UNIX) 116
- collecting and distributing Event Service definition information when IM Configuration Management is not used (Windows) 51
- collecting and distributing Event Service definition information when IM Configuration Management is used (UNIX) 115
- collecting and distributing Event Service definition information when IM Configuration Management is used (Windows) 50
- collecting virtualization system configuration information 174
- command execution
 - setting up execution environment (UNIX) 117
 - setting up execution environment (Windows) 52
- common definition information, setting 344, 375
- communication encryption function
 - checking whether configured correctly 430
- communication encryption function, newly using 420
- communication encryption function, stop using 427
- communication method 344, 375
- communications, controlling by JP1/Base 403
- completed-action linkage, setting 306
- configuration definition
 - notes about setting information (UNIX) 110
 - notes about setting information (Windows) 45
- configuration definition information
 - changing (UNIX) 110
 - changing (Windows) 45
 - deleting (UNIX) 110
 - deleting (Windows) 45
 - setting (UNIX) 109
 - setting (Windows) 44
- configuration files
 - applying edited information in 192
 - editing 191
- configuring
 - automatic startup (UNIX) 128
 - automatic stop (UNIX) 128
 - changing cluster operating environment settings (UNIX) 396
 - changing cluster operating environment settings (Windows) 367
 - cluster operating environment (UNIX) 377
 - cluster operating environment (Windows) 346
 - command execution environment (JP1/Base) (UNIX) 117
 - command execution environment (JP1/Base) (Windows) 52
 - Event Service (JP1/Base) (UNIX) 112
 - Event Service (JP1/Base) (Windows) 47
 - installing each JP1/IM program (UNIX) 91
 - installing each JP1/IM program (Windows) 26
 - JP1/IM - View operation (Windows) 78
 - settings for handling JP1/IM - Manager failures (UNIX) 131
 - settings for handling JP1/IM - Manager failures (Windows) 71
 - settings for handling JP1/IM - View failures (Windows) 78
 - settings for using the functions of Central Scope (UNIX) 131
 - settings for using the functions of Central Scope (Windows) 71
 - startup sequence for services (JP1/Base) (Windows) 36
 - uninstalling each JP1/IM program (UNIX) 141
 - uninstalling each JP1/IM program (Windows) 84
 - upgrade installation, for (UNIX) 135
 - upgrade installation, for (Windows) 74
- configuring JP1/IM - Manager 429
- configuring SSH (UNIX) 120
- configuring SSH (Windows) 63
- configuring WMI (Windows) 56
- consolidated display of repeated events 262
- conventions
 - diagrams 8
 - version numbers 11
- copying common definition information during new installation (UNIX) 383
- copying common definition information during new installation (Windows) 354
- copying common definition information during upgrade installation (UNIX) 392
- copying common definition information during upgrade installation (Windows) 363
- correlation event generation
 - creating and applying definition of 238
 - history files, setting size and number of 236

- setting 236
- setting startup of 236
- setting startup options 237
- Cosminexus, setup for linkage with 319
- creating IM database (UNIX) 97
- creating IM database (Windows) 31
- creating scripts to be registered into cluster software (UNIX) 387
- customizing
 - monitoring tree 283
 - toolbar for monitoring tree 308
 - Visual Monitoring window 295
- customizing JP1/IM - View operation (Windows) 78
- customizing operation
 - IM Configuration Management - View 80
- customizing operation of Central Console viewer and Central Scope viewer (Windows) 78

D

- data, preparations for collecting 71, 131
- definition files
 - creating 248, 264, 267
 - enabling 250
- deleting host from business group 184
- deleting monitoring nodes 289
- deleting profile (agent configuration) 191
- deleting profile (remote monitoring configuration) 201
- diagram conventions 8
- display and specification of program-specific extended attribute, setting 244
- displaying
 - event (by specifying event acquisition range at login) 211
- displaying source host (Windows) 76
- displaying the Start the process automatically when the log file trap service starts check box 76, 137
- display message change definition file, configuring from 256
- Display Message Change Definition Settings window, configuring from 254

E

- editing
 - event guide information 240
 - guide information 303
 - list of Visual Monitoring windows 300
- Enabling calling the JP1/Service Support window 432
- encrypted communication, configuring 420

- event acquisition filter
 - changing location of 135
 - setting, by switching filter conditions 220
 - setting common exclusion-conditions 221
 - setting only one 219
 - settings for 219
- event acquisition range
 - displaying event by specifying 211
- event guide information, editing 240
- event receiver filter
 - changing 217
 - creating new 216
 - deleting 217
 - settings for 215
- event report output format, specifying 76, 137
- event service
 - setting up (UNIX) 112
 - setting up (Windows) 47
- event service definition information
 - collecting and distributing (UNIX) 115
 - collecting and distributing (Windows) 50
- Event Service definition information, collecting and distributing (UNIX) 116
- Event Service definition information, collecting and distributing (Windows) 51
- executing the setup program
 - JP1/IM - Manager (UNIX) 128

F

- failover 339
- failure, preparations for collecting data in event of 71, 131
- filters, setting 213
- firewall
 - basic information about 409
 - communication settings for JP1 that is run in 414
 - environment, operating in 409
 - filtering through 409

G

- general monitoring object
 - example of creating (Cosminexus resource monitoring by JP1/Cm2/SSO) 332
 - example of creating (CPU monitoring by JP1/Cm2/SSO) 322
- general monitoring objects, example of creating 327
- generating correlation events

Settings 236

GUI

using to create monitoring tree 279

using to create Visual Monitoring window 294

guide information, editing 303

H

health check function, setting 73, 134

HiRDB

example of creating general monitoring objects 327

setup for linkage with 320

Hitachi PP Installer (UNIX) 92

Hitachi Program Product Installer

starting 92

hosts

registering 145

registering information of 278

how to use Hitachi Program Product Installer (UNIX) 92

HP NNM, setup for linkage with 317

HTTP server

installing 271

setting up 271

I

IM Configuration Management

importing and exporting management information in 209

settings for using functions of (UNIX) 100

settings for using functions of (Windows) 34

setting system hierarchy by using 144

setting using export and import functions of (UNIX) 108

setting using export and import functions of (Windows) 43

setting virtualization system configuration 160

IM Configuration Management database, setting (UNIX) 99

IM Configuration Management database, setting (Windows) 33

IM Configuration Management - View

customizing operation 80

setting using (UNIX) 106

setting using (Windows) 41

installation

notes (UNIX) 96

notes (Windows) 29

preparations required before (UNIX) 90

preparations required before (Windows) 25

prerequisite program (UNIX) 90

prerequisite program (Windows) 25

procedure (UNIX) 88, 91

procedure (Windows) 23, 26

types of 28, 91

UNIX 91

Windows 26

installation and setup procedure (UNIX) 88

installation and setup procedure (Windows) 23

installing

HTTP server 271

installing certificate 163

integrated monitoring database, setting (UNIX) 98

integrated monitoring database, setting (Windows) 32

IP addresses 417

support of 414

J

Java Console window, specifying display settings for 272

jcfview.conf 80

JP1/AJS

example of creating system-monitoring objects 321

setup for linkage with 313

JP1/Base

controlling communications by 403

copying primary authentication server settings (UNIX) 104

copying primary authentication server settings (Windows) 38

installing 25, 90

registering JP1 users (UNIX) 103

registering JP1 users (Windows) 38

setting operation permissions for JP1 users (UNIX) 103

setting operation permissions for JP1 users (Windows) 38

setting service startup sequence (Windows) 36

settings for handling failures (UNIX) 105

settings for handling failures (Windows) 40

settings for using the source host name of Event Service in the FQDN format (UNIX) 119

settings for using the source host name of Event Service in the FQDN format (Windows) 54

setting up command execution environment (UNIX) 117

- setting up command execution environment (Windows) 52
- setting up Event Service (UNIX) 112
- setting up Event Service (Windows) 47
- setting user authentication (UNIX) 102
- setting user authentication (Windows) 37
- setting user mapping (UNIX) 102
- setting user mapping (Windows) 37
- specifying authentication server (UNIX) 103
- specifying authentication server (Windows) 37
- JP1/Cm2/SSO
 - example of creating general monitoring object 322
 - example of creating general monitoring object (Cosminexus resource monitoring by JP1/Cm2/SSO) 332
 - setup for linkage 314
- JP1/IM
 - Central Scope environment setup 277
 - communication 414
 - controlling communications by JP1/Base 403
 - creating IM database (UNIX) 97
 - creating IM database (Windows) 31
 - designing setup details (UNIX) 90
 - designing setup details (Windows) 25
 - using to create monitoring tree 302
 - environment setup procedure for cluster operation (UNIX) 377
 - environment setup procedure for cluster operation (Windows) 346
 - installation and setup procedure (UNIX) 88
 - installation and setup procedure (Windows) 23
 - installing (UNIX) 87, 91
 - installing (Windows) 22, 26
 - linking to JP1/IM - Rule Operation 434
 - notes about cluster operation (UNIX) 399
 - notes about cluster operation (Windows) 370
 - operating in firewall environment 409
 - operating in multiple networks 404
 - operation and environment configuration depending on network configuration 402
 - operation and environment configuration in cluster system (UNIX) 373
 - operation and environment configuration in cluster system (Windows) 338
 - overview of cluster operation (UNIX) 374
 - overview of cluster operation (Windows) 339
 - preparations required before installing (UNIX) 90
 - preparations required before installing (Windows) 25
 - registering host information 278
 - setting automated actions 228
 - setting correlation event generation 236
 - setting monitor startup for linked products 263
 - settings for linking to other integrated management products 431
 - setting Tool Launcher window 266
 - setting up (UNIX) 87
 - setting up (Windows) 22
 - setting up Central Console 210
 - setting up Central Scope 276
 - setting up Central Scope operating environment 306
 - setting up IM Configuration Management View (Windows) 79
 - setting up JP1/IM - Manager (UNIX) 128
 - setting up JP1/IM - Manager (Windows) 71
 - setting up JP1/IM - View (Windows) 78
 - uninstalling (UNIX) 141
 - uninstalling (Windows) 84
- JP1/IM - Manager
 - automatic startup (UNIX) 128
 - automatic stop (UNIX) 128
 - executing the setup program (UNIX) 128
 - installing (UNIX) 91
 - installing (Windows) 26
 - services and processes of 344, 375
 - settings for handling failures (UNIX) 131
 - settings for handling failures (Windows) 71
 - setup (UNIX) 128
 - setup (Windows) 71
 - uninstalling (UNIX) 141
 - uninstalling (Windows) 84
- JP1/IM - Rule Operation
 - linking to 434
 - settings 434
 - settings for enabling linkage function of 434
 - settings for sending notifications to 435
 - setting up linkage (JP1/IM - View) (Windows) 80
 - setup (JP1/IM - View) (Windows) 80
- JP1/IM - View
 - customizing JP1/IM - View operation (Windows) 78
 - installing (Windows) 26
 - setting, for login user 261
 - settings for handling failures (Windows) 78
 - settings for using Web-based 271
 - setup (Windows) 78
 - uninstalling (Windows) 84

- JP1/IM - View settings 261
- JP1/IM - View settings, procedure for specifying 262
- JP1/PAM, setup for linkage with 319
- JP1/PFM, setup for linkage with 316
- JP1/ServerConductor
 - setup for linkage 320
- JP1/Software Distribution
 - remote installation using 28, 91
 - setup for linkage with 318
- jp1cohassetup.exe 349
- jp1cshasetup.exe 353
- JP1 events
 - displaying attributes of user specific 246
 - editing guide information of 240
 - setting filters for 213
 - setting forwarding of (UNIX) 114
 - setting forwarding of (Windows) 49
 - setting issuance of, during action status change 242
 - settings for operations to be performed during acquisition of 211
 - setting to issue, in event of abnormal process termination 72, 133
- JP1 users
 - setting operation permissions for (UNIX) 103
 - setting operation permissions for (Windows) 38

L

- language encoding 94
- launching a JP1/AJS window by monitor startup 436
- launching a JP1/PFM window by monitor startup 437
- linked products
 - setting monitor startup for 263
 - setting up for 313
- linking to JP1/IM - Navigation Platform 433
- linking to JP1/Service Support 432
- linking with JP1/AJS 436
- linking with JP1/PFM 437
- logical host 340
 - common definition information 344, 375
 - creating scripts to be registered into cluster software (UNIX) 387
 - deleting (UNIX) 393
 - deleting (Windows) 364
 - new installation and setup (UNIX) 379
 - new installation and setup (Windows) 348
 - registering into cluster software (Windows) 359
 - resource start and stop sequence (UNIX) 389

- resource start and stop sequence (Windows) 360
- upgrade installation and setup (UNIX) 390
- upgrade installation and setup (Windows) 361
- logical hosts
 - prerequisites for environment of 341
- logical IP address 340, 341
- login information, saving 279

M

- managing profile
 - displaying (remote monitoring configuration) 202
 - editing configuration file (remote monitoring configuration) 203
- map display settings 290
- mapping
 - event source host 258
- memory entries, setting 239
- MIME type, adding 271
- monitoring nodes
 - adding 284, 297
 - changing monitoring status of 298
 - deleting 289, 297
 - moving 289
 - searching for 292, 299
 - setting attributes of 286, 298
- monitoring object database, automatic backup and recovery settings for 73, 134
- monitoring objects, examples of creating 321
- monitoring tree
 - acquiring, from server 281
 - acquiring, stored locally 281
 - acquiring existing 280
 - applying customized 293
 - creating, by using GUI 279
 - customizing 283
 - customizing toolbar for 308
 - generating automatically 281
 - opening editing window 279
 - saving customized 292
 - searching for monitoring nodes in 292
 - setting monitoring range 290
 - settings for using visual icons 291
 - setting up for linked products 313
- Monitoring Tree (Editing) window, opening 279
- monitoring tree window
 - creating, by editing the saved CSV file 302
- monitor startup, setting 263

- monitor windows
 - determining window to be used for opening 264
 - opening 263
- moving monitoring nodes 289
- multi-LAN environment
 - command execution (cluster operation) 407
 - command execution (non-cluster operation) 405
 - JP1/IM - View connection (cluster operation) 406
 - JP1/IM - View connection (non-cluster operation) 404

N

- NAT 412
 - support of 419
- NetBIOS setting (NetBIOS over TCP/IP) (Windows) 62
- networks
 - operating in firewall environment 409
 - operating in multiple 404
 - operation and environment configuration depending on 402
- newly installing JP1/Base and JP1/IM - Manager (UNIX) 379
- newly installing JP1/Base and JP1/IM - Manager (Windows) 348
- non-cluster system
 - environment setup for running logical hosts (UNIX) 400
 - environment setup for running logical hosts (Windows) 371
 - evaluating configuration for running logical host (UNIX) 400
 - evaluating configuration for running logical host (Windows) 371
 - logical host operation and environment configuration (UNIX) 400
 - logical host operation and environment configuration (Windows) 371
 - notes about running logical hosts (UNIX) 401
 - notes about running logical hosts (Windows) 372
- notes
 - during cluster operation (UNIX) 399
 - during cluster operation (Windows) 370
 - setting configuration definition information (UNIX) 110
 - setting configuration definition information (Windows) 45
- notes about
 - installing (UNIX) 96
 - installing and uninstalling (Windows) 29
- notes about cluster operation (UNIX) 399

- notes about cluster operation (Windows) 370
- notes about setting configuration definition information (UNIX) 110
- notes about setting configuration definition information (Windows) 45
- notes on
 - uninstallation (UNIX) 143
 - uninstallation (Windows) 86
- number of connected-host log entries in Login window for IM Configuration Management 80
- number of connected-user log entries in Login window for IM Configuration Management 80
- number of events to acquire
 - at updating 261
 - per search 261

O

- opening edit window for Visual Monitoring window 294
- OS environment, configuring 25, 90

P

- packet filtering 409
- physical hosts 340
 - prerequisites for environment of 341
- port numbers 414
 - changing 272
 - support of 414
- preparation for creating IM database (UNIX) 97
- preparations for creating IM databases (for Windows) 31
- prerequisite program
 - installing (UNIX) 90
 - installing (Windows) 25
- preventing history of previously used JP1 login user names from appearing 78
- preventing names of JP1 users who are currently logged in from appearing 79, 80
- primary authentication server, copying settings for (UNIX) 104
- primary authentication server, copying settings for (Windows) 38
- procedure
 - installation and setup (UNIX) 88
 - installation and setup (Windows) 23
- profiles
 - collecting 187
 - collecting list of 186
 - displaying 189

R

- refresh interval 261
- registering JP1 users (UNIX) 103
- registering JP1 users (Windows) 38
- regular expressions, setting 228
- remote installation 91
- remote installation (Windows) 28
- repeated events, consolidated display of 262
- response timeout period when system hierarchy is applied 80

S

- saving
 - customized monitoring tree at local host 292
 - customized Visual Monitoring window at local host 299
- saving manuals to computer (UNIX) 139
- saving manuals to computer (Windows) 82
- server response timeout period 80
- service startup sequence, setting (Windows) 36
- setting
 - abnormal process termination, restart settings in event of 133
 - attributes of monitoring nodes 286
 - automated actions 228
 - Central Console 210
 - Central Scope 276
 - Central Scope operating environment 306
 - completed-action linkage function 306
 - correlation event generation 236
 - execution conditions and details of automated actions 228
 - execution environment for automated action function 228
 - health check function 73, 134
 - host information 278
 - JP1/IM - View for login user 261
 - JP1 event filtering 213
 - JP1 event issuance during action status change 242
 - maximum number of status change events 306
 - memo entries 239
 - memory-resident status change condition function 308
 - monitoring range 290
 - monitor startup for linked products 263
 - number of connected-host log entries in Login window 78

- path to start WWW browser 78
- system hierarchy (when IM Configuration Management is not used) (UNIX) 109
- system hierarchy (when IM Configuration Management is not used) (Windows) 44
- system hierarchy (when IM Configuration Management is used) (UNIX) 106
- system hierarchy (when IM Configuration Management is used) (Windows) 41
- Tool Launcher window 266
- whether List of Action Results window can start when Event Console window opens 78
- whether to allow copying to clipboard 78
- whether Tool Launcher window can start when Event Console window opens 78
- setting business group 178
- setting common exclusion-conditions 221
- setting common exclusion-conditions (by using common-exclusion-conditions extended definition file and jcochfilter command) 224
- setting common exclusion-conditions (by using Common Exclusion-Conditions Settings window or Common Exclusion-Condition Settings (Extended) window 222
- setting display color of JP1 event 227
- setting event acquisition filter (for compatibility) 224
- setting event source host mapping 258
- setting for monitoring logs while remote monitoring is stopped 77, 138
- setting JP1 event forwarding when IM Configuration Management is not used (UNIX) 114
- setting JP1 event forwarding when IM Configuration Management is not used (Windows) 49
- setting JP1 event forwarding when IM Configuration Management is used (UNIX) 113
- setting JP1 event forwarding when IM Configuration Management is used (Windows) 48
- setting language code in common definition 95
- setting language code in environment variable file 94
- setting monitoring of repeated events to be prevented 226
- setting number of connected-host log entries in Login window 78
- setting path to start WWW browser 78
- setting profile on host in remote monitoring configuration 199
- setting reference and operation restrictions 274
- setting reference and operation restrictions on business group 274
- setting required immediately after installation (UNIX) 94

- setting required immediately after installation (Windows) 28
- settings for
 - automatic backup and recovery for monitoring object database 73, 134
 - changing location of event acquisition filter 135
 - deleting status change events when JP1 event handling is completed 307
 - event acquisition filters 219
 - event receiver filters 215
 - handling JP1/Base failures (UNIX) 105
 - handling JP1/Base failures (Windows) 40
 - initializing monitoring objects when JP1 events are received 307
 - issuing JP1 events in event of abnormal process termination 72, 133
 - linking to other integrated management products 431
 - operations to be performed during JP1/IM event acquisition 211
 - restarting process in event of abnormal termination 72, 133
 - severe events filters 217
 - status color of monitoring node name and monitoring node 310
 - suppressing display of monitoring node name and icon margin 309
 - suppressing movement of icon of monitoring node 312
 - user authentication (UNIX) 102
 - user authentication (Windows) 37
 - user mapping (UNIX) 102
 - user mapping (Windows) 37
 - using visual icons 291
 - using Web-based JP1/IM - View 271
 - view filters 213
- settings for displaying event-source-host performance report 437
- settings for displaying the monitor window from an email sent by automated action 436
- settings for displaying the monitor window from event guide information 436
- settings for launching a JP1/AJS window from the Tool Launcher window 436
- settings for launching a JP1/PFM window from the Tool Launcher window 437
- settings for monitoring logs on remotely monitored host (UNIX) 120
- settings for monitoring logs on remotely monitored host (Windows) 56
- settings for upgrade installation (UNIX) 135
- settings for upgrade installation (Windows) 74
- settings for using the source host name of Event Service in the FQDN format (UNIX) 119
- settings for using the source host name of Event Service in the FQDN format (Windows) 54
- setting startup options 237
- Setting the display message change function 254
- setting up client application execution environment (UNIX) 118
- setting up client application execution environment (Windows) 53
- setting up command execution function for managed host (UNIX) 117
- setting up command execution function for managed host (Windows) 52
- setting up IM Configuration Management View 79
- setting up IM Configuration Management View (Windows) 79
- setting up logical host environment (primary node) during new installation (UNIX) 380
- setting up logical host environment (primary node) during new installation (Windows) 349
- setting up logical host environment (primary node) during upgrade installation (UNIX) 391
- setting up logical host environment (primary node) during upgrade installation (Windows) 362
- setting up logical host environment (secondary node) during new installation (UNIX) 384
- setting up logical host environment (secondary node) during new installation (Windows) 354
- setting up physical host environment during new installation (UNIX) 379
- setting up physical host environment during new installation (Windows) 348
- setting up SSH connection with host started by KVM (in UNIX) 170
- setting up SSH connection with host started by KVM (in Windows) 167
- setting whether List of Action Results window can start when Event Console window opens 78
- setting whether to allow copying to clipboard 78
- setting whether Tool Launcher window can start when Event Console window opens 78
- setup
 - JP1/IM - Manager (UNIX) 128
 - JP1/IM - Manager (Windows) 71
 - linked products 313
 - procedure (UNIX) 88
 - procedure (Windows) 23
- setup
 - JP1/IM - View 78

- severe events filters, setting 217
- severity changing function, setting 251
- shared disk 340, 341
 - file organization on 343, 374
- specifying the size of log information that can be collected per monitoring interval (for UNIX) 127
- specifying the size of log information that can be collected per monitoring interval (for Windows) 70
- starting JP1/Base and JP1/IM - Manager 96
- starting log file trap 196
- starting or stopping log file trap 196
- status change events, setting for maximum number 306
- stopping log file trap 197
- switching between basic mode and extended mode for common exclusion-condition 222
- system configurations using multiple LANs 404
- system environment
 - configuring (UNIX) 90
 - configuring (Windows) 25
- system hierarchy
 - setting 144
 - setting (when IM Configuration Management is not used) (UNIX) 109
 - setting (when IM Configuration Management is not used) (Windows) 44
 - setting (when IM Configuration Management is used) (UNIX) 106
 - setting (when IM Configuration Management is used) (Windows) 41
- system-monitoring objects, example of creating 321

T

- timeout values for Web-based operation, setting 272
- Tool Launcher window
 - adding new menus 266
 - determining window to be opened from 267
 - setting 266
 - settings for opening GUI of linked products from 266
 - settings for opening Web page of linked products from 270
- tuning.conf 79

U

- uninstallation
 - notes (UNIX) 143
 - notes (Windows) 86
 - UNIX 141
 - Windows 84

- uninstallation procedure (UNIX) 141
- uninstallation procedure (Windows) 84
- uninstalling
 - notes (Windows) 29
 - UNIX 141
 - Windows 84
- uninstalling JP1/IM - Manager and JP1/Base (UNIX) 395
- uninstalling JP1/IM - Manager and JP1/Base (Windows) 366
- uninstalling logical hosts (UNIX) 393
- uninstalling logical hosts (Windows) 364
- updated agent profile notification function 76, 137
- updating IM database (UNIX) 101
- updating IM database (Windows) 35
- updating IM database in a cluster environment (UNIX) 397
- updating IM database in a cluster environment (Windows) 368
- upgrade installation
 - changing location of event acquisition filter 135
- upgrade installation of logical hosts (UNIX) 390
- upgrade installation of logical hosts (Windows) 361
- URL for Web-based JP1/IM - View, setting 273
- user authentication, setting (UNIX) 102
- user authentication, setting (Windows) 37
- user mapping, setting (UNIX) 102, 104
- user mapping, setting (Windows) 37, 39
- user-specific event attributes, displaying 246
- using Central Scope to monitor business group 184
- using commands to change settings (UNIX) 396
- using commands to change settings (Windows) 367
- using IM Configuration Management to manage a virtualization configuration 160

V

- variable binding
 - loading to JP1 event 315
- version information, displaying 93
- version number conventions 11
- view filters
 - changing 215
 - creating new 213
 - deleting 215
 - settings for 213
- virtualization system configuration
 - setting 160
- virtualization system configuration (UNIX)

- settings for managing and monitoring (UNIX) 108
- virtualization system configuration (Windows)
 - settings for managing and monitoring (Windows) 43
- visual icons, settings for using 291
- Visual Monitoring window
 - acquiring, from server 295
 - acquiring existing 295
 - adding monitoring nodes to 297
 - applying customized 299
 - customizing 295
 - deleting 300
 - deleting monitoring nodes from 297
 - opening edit window for 294
 - saving customized 299
 - setting background image for 296
 - that has been saved locally, acquiring 295
 - using GUI to create 294

W

- Web-based JP1/IM - View, settings for using 271
- Web browser, setting up 272
- whether window display settings history functionality can be used
 - when IM Configuration Management window, Edit Agent Configuration window, Edit Remote Monitoring Configuration window, or Display/Edit Profiles window starts 80

 **Hitachi, Ltd.**

6-6, Marunouchi 1-chome, Chiyoda-ku, Tokyo, 100-8280 Japan
