

JP1 Version 13

**JP1/Integrated Management 3 - Manager
Configuration Guide**

3021-3-L03-40(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 3 - Manager and JP1/Integrated Management 3 - View, see the release notes for the relevant product.

JP1/Integrated Management 3 - Manager (for Windows):

P-2A2C-8EDL JP1/Integrated Management 3 - Manager 13-50

The above product includes the following:

P-CC2A2C-9MDL JP1/Integrated Management 3 - Manager 13-50 (for Windows Server 2025, Windows Server 2022, Windows Server 2019, Windows Server 2016)

P-CC2A2C-6HDL JP1/Integrated Management 3 - View 13-00 (for Windows Server 2025, Windows 11, Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows 10)

P-CC2A2C-9GDL JP1/Integrated Management 3 - Agent 13-50 (for Windows Server 2025, Windows Server 2022, Windows Server 2019, Windows Server 2016)

P-CC842C-9GDL JP1/Integrated Management 3 - Agent 13-50 (for Linux 9, Linux 8, Linux 7, Oracle Linux 9, Oracle Linux 8, Oracle Linux 7, SUSE Linux 15, SUSE Linux 12, Amazon Linux 2023)

P-CC2A2C-6LDL JP1/Base 13-10 (for Windows Server 2025, Windows Server 2022, Windows Server 2019, Windows Server 2016)

P-CC842C-6LDL JP1/Base 13-10 (for Linux 9, Linux 8, Linux 7, Oracle Linux 9, Oracle Linux 8, Oracle Linux 7, SUSE Linux 15, SUSE Linux 12, Amazon Linux 2023)

P-CC1M2C-6LDL JP1/Base 13-10 (for AIX)

JP1/Integrated Management 3 - Manager (for Linux):

P-842C-8EDL JP1/Integrated Management 3 - Manager 13-50

The above product includes the following:

P-CC842C-9MDL JP1/Integrated Management 3 - Manager 13-50 (for Linux 9, Linux 8, Linux 7, Oracle Linux 9, Oracle Linux 8, Oracle Linux 7)

P-CC9W2C-9MDL JP1/Integrated Management 3 - Manager 13-50 (for SUSE Linux 15, SUSE Linux 12)

P-CC2A2C-6HDL JP1/Integrated Management 3 - View 13-00 (for Windows Server 2025, Windows 11, Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows 10)

P-CC2A2C-9GDL JP1/Integrated Management 3 - Agent 13-50 (for Windows Server 2025, Windows Server 2022, Windows Server 2019, Windows Server 2016)

P-CC842C-9GDL JP1/Integrated Management 3 - Agent 13-50 (for Linux 9, Linux 8, Linux 7, Oracle Linux 9, Oracle Linux 8, Oracle Linux 7, SUSE Linux 15, SUSE Linux 12, Amazon Linux 2023)

P-CC2A2C-6LDL JP1/Base 13-10 (for Windows Server 2025, Windows Server 2022, Windows Server 2019, Windows Server 2016)

P-CC842C-6LDL JP1/Base 13-10 (for Linux 9, Linux 8, Linux 7, Oracle Linux 9, Oracle Linux 8, Oracle Linux 7, SUSE Linux 15, SUSE Linux 12, Amazon Linux 2023)

P-CC1M2C-6LDL JP1/Base 13-10 (for AIX)

■ Trademarks

The 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/>).

1. This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit.

(<http://www.openssl.org/>)

2. This product includes cryptographic software written by Eric Young (eyay@cryptsoft.com)

3. This product includes software written by Tim Hudson (tjh@cryptsoft.com)

4. This product includes the OpenSSL Toolkit software used under OpenSSL License and Original SSLeay License. OpenSSL License and Original SSLeay License are as follow:

LICENSE ISSUES

=====

The OpenSSL toolkit stays under a double license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit.

See below for the actual license texts. Actually both licenses are BSD-style

Open Source licenses. In case of any license issues related to OpenSSL

please contact openssl-core@openssl.org.

OpenSSL License

/* =====

* Copyright (c) 1998-2018 The OpenSSL Project. All rights reserved.

*

* Redistribution and use in source and binary forms, with or without

* modification, are permitted provided that the following conditions

* are met:

*

* 1. Redistributions of source code must retain the above copyright

* notice, this list of conditions and the following disclaimer.

*

* 2. Redistributions in binary form must reproduce the above copyright

* notice, this list of conditions and the following disclaimer in

* the documentation and/or other materials provided with the

* distribution.

*

```

* 3. All advertising materials mentioning features or use of this
* software must display the following acknowledgment:
* "This product includes software developed by the OpenSSL Project
* for use in the OpenSSL Toolkit. (http://www.openssl.org/)"
*
* 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to
* endorse or promote products derived from this software without
* prior written permission. For written permission, please contact
* openssl-core@openssl.org.
*
* 5. Products derived from this software may not be called "OpenSSL"
* nor may "OpenSSL" appear in their names without prior written
* permission of the OpenSSL Project.
*
* 6. Redistributions of any form whatsoever must retain the following
* acknowledgment:
* "This product includes software developed by the OpenSSL Project
* for use in the OpenSSL Toolkit (http://www.openssl.org/)"
*
* THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS" AND ANY
* EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
* PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR
* ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
* SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
* NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;
* LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
* STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
* ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED
* OF THE POSSIBILITY OF SUCH DAMAGE.
* =====
*
* This product includes cryptographic software written by Eric Young
* (eay@cryptsoft.com). This product includes software written by Tim
* Hudson (tjh@cryptsoft.com).
*
*/
Original SSLeay License
-----
/* Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)
* All rights reserved.

```


- *
 - * This package is an SSL implementation written
 - * by Eric Young (eay@cryptsoft.com).
 - * The implementation was written so as to conform with Netscapes SSL.
 - *
 - * This library is free for commercial and non-commercial use as long as
 - * the following conditions are aheared to. The following conditions
 - * apply to all code found in this distribution, be it the RC4, RSA,
 - * lhash, DES, etc., code; not just the SSL code. The SSL documentation
 - * included with this distribution is covered by the same copyright terms
 - * except that the holder is Tim Hudson (tjh@cryptsoft.com).
 - *
 - * Copyright remains Eric Young's, and as such any Copyright notices in
 - * the code are not to be removed.
 - * If this package is used in a product, Eric Young should be given attribution
 - * as the author of the parts of the library used.
 - * This can be in the form of a textual message at program startup or
 - * in documentation (online or textual) provided with the package.
 - *
 - * Redistribution and use in source and binary forms, with or without
 - * modification, are permitted provided that the following conditions
 - * are met:
 - * 1. Redistributions of source code must retain the copyright
 - * notice, this list of conditions and the following disclaimer.
 - * 2. Redistributions in binary form must reproduce the above copyright
 - * notice, this list of conditions and the following disclaimer in the
 - * documentation and/or other materials provided with the distribution.
 - * 3. All advertising materials mentioning features or use of this software
 - * must display the following acknowledgement:
 - * "This product includes cryptographic software written by
 - * Eric Young (eay@cryptsoft.com)"
 - * The word 'cryptographic' can be left out if the rouines from the library
 - * being used are not cryptographic related :-).
 - * 4. If you include any Windows specific code (or a derivative thereof) from
 - * the apps directory (application code) you must include an acknowledgement:
 - * "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"
 - *
 - * THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS" AND
 - * ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
 - * IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
 - * ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE
 - * FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL

* DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
* OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
* LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
* OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
* SUCH DAMAGE.

*

* The licence and distribution terms for any publically available version or
* derivative of this code cannot be changed. i.e. this code cannot simply be
* copied and put under another distribution licence
* [including the GNU Public Licence.]

*/

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/>).

Java is a registered trademark of Oracle and/or its affiliates.



■ 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) 2012 Hyper-V ^(R)

Abbreviation	Full name or meaning
SCVMM	Microsoft ^(R) System Center Virtual Machine Manager 2012
Windows 10	Windows ^(R) 10 Enterprise 64-bit
	Windows ^(R) 10 Home 64-bit
	Windows ^(R) 10 Pro 64-bit
Windows 11	Windows ^(R) 11 Enterprise
	Windows ^(R) 11 Home
	Windows ^(R) 11 Pro
Windows Server 2016	Microsoft ^(R) Windows Server ^(R) 2016 Datacenter
	Microsoft ^(R) Windows Server ^(R) 2016 Standard
Windows Server 2019	Microsoft ^(R) Windows Server ^(R) 2019 Datacenter
	Microsoft ^(R) Windows Server ^(R) 2019 Standard
Windows Server 2022	Microsoft ^(R) Windows Server ^(R) 2022 Datacenter
	Microsoft ^(R) Windows Server ^(R) 2022 Standard
Windows Server 2025	Microsoft ^(R) Windows Server ^(R) 2025 Datacenter
	Microsoft ^(R) Windows Server ^(R) 2025 Standard

Windows is often used generically to refer to Windows Server 2025, Windows 11, Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows 10.

■ 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

Sep. 2025: 3021-3-L03-40(E)

■ Copyright

Copyright (C) 2023, 2025 Hitachi, Ltd.

Copyright (C) 2023, 2025 Hitachi Solutions, Ltd.

Summary of amendments

The following table lists changes in this manual (3021-3-L03-40(E)) and product changes related to this manual.

Changes	Location
Added notes for upgrading JP1/IM - Manager from version 13-00 to 13-11 to version 13-50 or later.	1.3.3(16) , 2.3.4(11)
Added a description of how to use the <code>jimgndbsetup</code> command to check the version of the Intelligent Integrated Management Database and a description of the version of the Intelligent Integrated Management Database for whichi you must be run the <code>jimgndbupdate</code> command.	1.19.7(8) , 2.18.11(10)
Added <code>\$stepTime{minSeconds="minimum-seconds"}</code> to dynamically calculate to include all data according to the dashboard trend data display range as a range vector selector that can be specified in promql of metric definition file. Accordingly, settings to be applied when upgrading JP1/IM - Manager from version 13-00 to 13-11 to version 13-50 or later have been added.	1.19.3(1)(d)
A job monitoring function has been added that can detect performance issues by monitoring the transitions in the execution times of JP1/AJS3 root jobnets. Accordingly, the explanation of the monitored target name when Windows exporter monitors the Script exporter service (<code>jpc_script_exporter_service</code>) that collects the performance data of the job information of JP1/AJS3 was added.	1.21.2(18)(b)

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

Preface

This manual explains how to set up JP1/Integrated Management 3 - Manager and JP1/Integrated Management 3 - View systems.

In this manual, JP1/Integrated Management is abbreviated to *JP1*, and JP1/Integrated Management 3 - Manager and JP1/Integrated Management 3 - View are collectively referred to as *JP1/Integrated Management* or *JP1/IM*. In addition, in this manual, read JP1/Integrated Management - Manager and JP1/Integrated Management - View as JP1/Integrated Management 3 - Manager and JP1/Integrated Management 3 - View, respectively.

■ 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 the Intelligent Integrated Management Base

Chapter 4 explains how to set an environment for using the Intelligent Integrated Management Base.

5. Setting up Central Console

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

6. Setting up Central Scope

Chapter 6 explains how to set up an environment for using Central Scope.

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

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

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

Chapter 8 describes the operation and environment configuration of JP1/IM - Manager in a cluster system for UNIX.

9. Operation and Environment Configuration Depending on the Network Configuration

Chapter 9 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).

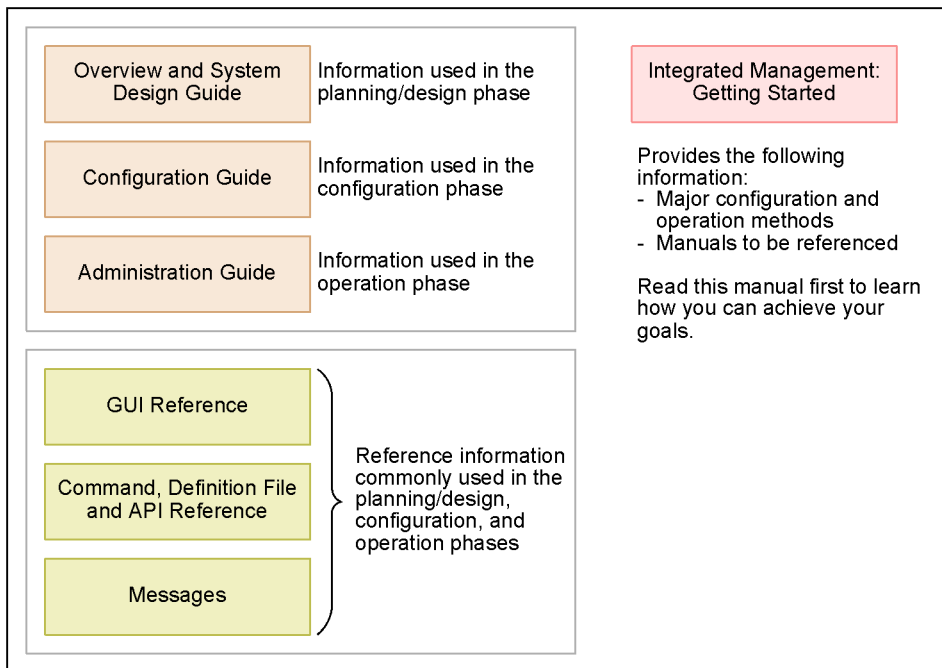
10. Settings for Linking to Other JP1 Products

Chapter 10 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

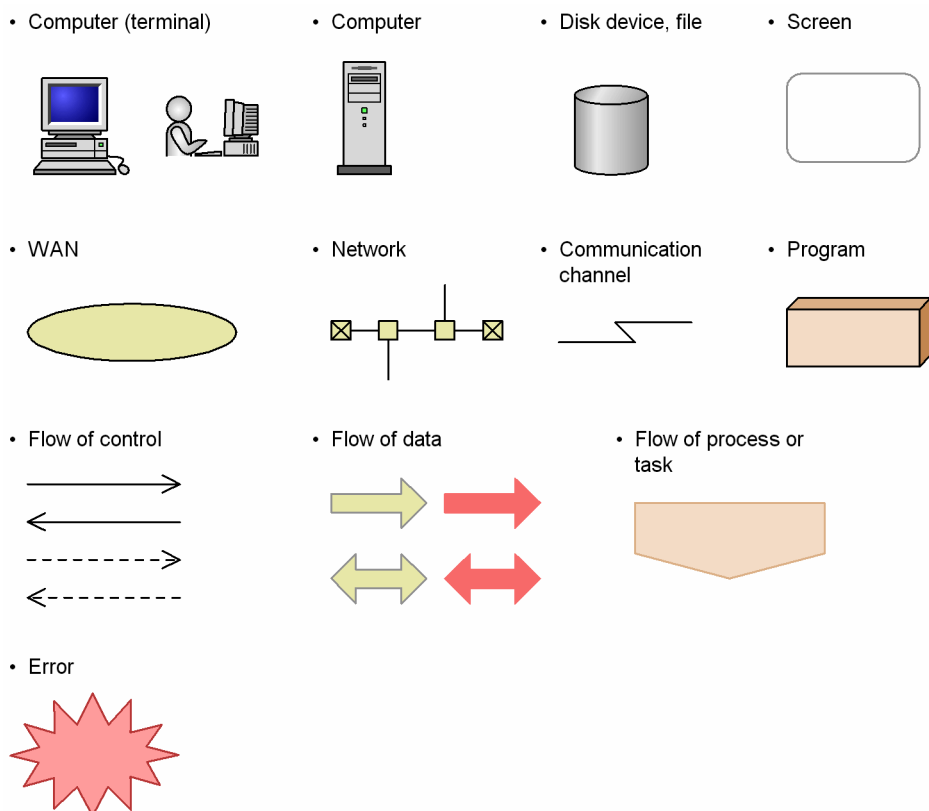
JP1/IM manuals provide necessary information according to the phases in the system life cycle, which include planning and design, configuration, and operation. Read the manual appropriate for the purpose.

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



■ Conventions: Diagrams

This manual uses the following conventions in diagrams:



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

Text formatting	Convention
Bold	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: - From the File menu, choose Open. - Click the Cancel button. - In the Enter name entry box, type your name.
<i>Italic</i>	Italic characters indicate a placeholder for some actual text to be provided by the user or system. For example: - 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>) Italic characters are also used for emphasis. For example: - Do <i>not</i> delete the configuration file.
Monospace	Monospace characters indicate text that the user enters without change, or text (such as messages) output by the system. For example: - 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/IM - Agent	<i>Agent-path</i>	<i>system-drive</i> : \Program Files\Hitachi\JP1IMA
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**.
- In Integrated Operation Viewer Window, choose **Help** and then **Online Manual**.

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.

■ Output destinations of Integrated trace log file

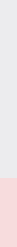
Starting with JP1/IM 12-10, all 32-bit Java processes for JP1/IM have been changed to 64-bit Java processes. Therefore, the integrated trace log output destination output by the Java process function of each function of JP1 / IM is changed.

The following is the destination of the integrated trace log for each JP1/IM function from version 12-10 or later. If you are using the log file trap function, you must change the settings as you change the destination.

Output destinations of Integrated trace log file (32 bit): *system-drive\Program Files (x86)\Hitachi\HNTRLib2\spool*

- IM database
- Central Scope Service
- Process management
- Command execution
- Automatic action
- Installation and Setup

Output destinations of Integrated trace log file (64 bit): *system-drive\Program Files\Hitachi\HNTRLib2\spool*

- 
- Event base service
 - Central Console viewer
 - Central Scope viewer
 - Event Generation Service
 - IM Configuration Management
 - IM Configuration Management viewer
 - Intelligent Integrated Management Base

Contents

Notices 2

Summary of amendments 8

Preface 9

1 Installation and Setup (for Windows) 27

- 1.1 Installation and setup procedures (for Windows) 28
- 1.2 Preparations required before installation (for Windows) 31
 - 1.2.1 Designing the JP1/IM setup details (for Windows) 31
 - 1.2.2 Configuring the system environment (for Windows) 31
 - 1.2.3 Installing the prerequisite program (for Windows) 31
- 1.3 Installing JP1/IM - Manager, JP1/IM - View, and JP1/IM - Agent (for Windows) 32
 - 1.3.1 Installation procedure (for Windows) 32
 - 1.3.2 Settings required immediately after installation (for Windows) 43
 - 1.3.3 Notes about installing (for Windows) 44
 - 1.3.4 How to collect data in installing (for Windows) 48
 - 1.3.5 How to link with the auto scale function (for Windows) 49
 - 1.3.6 Cloning a Virtual Machine (for Windows) 50
- 1.4 Creating IM databases (for Windows) 52
 - 1.4.1 Preparations for creating IM databases (for Windows) 52
 - 1.4.2 Setting up the integrated monitoring database (for Windows) 53
 - 1.4.3 Setting up the IM Configuration Management database (for Windows) 55
 - 1.4.4 Settings for using the functions of IM Configuration Management (for Windows) 56
 - 1.4.5 Updating IM databases (for Windows) 56
- 1.5 Construction of Intelligent Integrated Management Database (for Windows) 58
 - 1.5.1 Preparations for Building Intelligent Integrated Management Database (for Windows) 58
 - 1.5.2 Settings of Intelligent Integrated Management Database (for Windows) 58
 - 1.5.3 Excluding settings in security product(for Windows) 58
- 1.6 Setting the startup sequence for services (for Windows) 60
- 1.7 Setting up user authentication and user mapping (for Windows) 61
 - 1.7.1 Specifying the authentication server (for Windows) 61
 - 1.7.2 Registering JP1 users (for Windows) 62
 - 1.7.3 Setting operation permissions for the JP1 users (for Windows) 62
 - 1.7.4 Copying the primary authentication server settings (for Windows) 62
 - 1.7.5 Setting user mapping (for Windows) 63
- 1.8 Specifying settings for handling JP1/Base failures (for Windows) 64
- 1.9 Setting the system hierarchy (when IM Configuration Management is used) (for Windows) 65
 - 1.9.1 Using IM Configuration Management - View to set the system hierarchy (for Windows) 65

1.9.2	Using the export and import functions to set the system hierarchy (for Windows)	67
1.9.3	Settings for managing and monitoring a virtualization system configuration (for Windows)	67
1.10	Setting the system hierarchy (when IM Configuration Management is not used) (for Windows)	68
1.10.1	Setting the configuration definition information (for Windows)	68
1.10.2	Deleting the configuration definition information (for Windows)	69
1.10.3	Changing the configuration definition information (for Windows)	69
1.10.4	Notes about setting the configuration definition information (for Windows)	69
1.11	Setting up Event Service (for Windows)	71
1.12	Setting JP1 event forwarding when IM Configuration Management is used (for Windows)	72
1.13	Setting JP1 event forwarding when IM Configuration Management is not used (for Windows)	73
1.14	Collecting and distributing Event Service definition information when IM Configuration Management is used (for Windows)	74
1.15	Collecting and distributing Event Service definition information when IM Configuration Management is not used (for Windows)	75
1.16	Setting up a command execution environment (for Windows)	76
1.16.1	Setting up the command execution function for managed hosts (for Windows)	76
1.16.2	Setting up a client application execution environment (for Windows)	77
1.17	Specifying settings for using the source host name of Event Service in the FQDN format (for Windows)	78
1.17.1	Prerequisites (for Windows)	78
1.17.2	Setting method (for Windows)	78
1.17.3	Startup method (for Windows)	78
1.18	Specifying settings for monitoring logs on remotely monitored hosts (for Windows)	80
1.18.1	Configuring WMI (for Windows)	80
1.18.2	NetBIOS settings (NetBIOS over TCP/IP) (for Windows)	86
1.18.3	Configuring SSH (for Windows)	87
1.18.4	Specifying the size of log information that can be collected per monitoring interval (for Windows)	94
1.19	Setting up JP1/IM - Manager (for Windows)	95
1.19.1	Editing Configuration file of JP1/IM - Manager (for Windows)	95
1.19.2	Settings for using the functions of the Intelligent Integrated Management Base (for Windows)	95
1.19.3	Setup When Using JP1/IM - Agent as an agent	96
1.19.4	Register JP1/IM - Agent package (for Windows)	108
1.19.5	Specifying settings for using the functions of Central Scope (for Windows)	109
1.19.6	Specifying settings for handling JP1/IM - Manager failures (for Windows)	110
1.19.7	Specifying settings for upgrading (for Windows)	113
1.20	Setting up JP1/IM - View (for Windows)	119
1.20.1	Specifying settings for handling JP1/IM - View failures (for Windows)	119
1.20.2	Customizing operation of JP1/IM - View (Central Console viewer and Central Scope viewer) (for Windows)	119
1.20.3	Setting up and customizing IM Configuration Management - View (for Windows)	120
1.21	Setup for JP1/IM - Agent (for Windows)	122
1.21.1	Setup for JP1/IM - Agent service	122

1.21.2	Settings of JP1/IM - Agent	126
1.22	Building Container Environments in JP1/IM - Agent (for Windows)	207
1.22.1	Creating container images	207
1.22.2	Upgrading JP1/IM - Agent	213
1.23	Building optional features for JP1/IM - Agent (for Windows)	215
1.23.1	Configuring OracleDB exporter	215
1.23.2	Setting up Node exporter for AIX	230
1.23.3	Configuring SAP system monitoring	242
1.23.4	Configuring SQL exporter	247
1.24	Saving manuals to a computer (for Windows)	257
1.25	Uninstallation (for Windows)	259
1.25.1	Uninstallation procedure (for Windows)	259
1.25.2	Notes on uninstallation (for Windows)	262
1.26	Notes about installation and setting up (for Windows)	267

2 Installation and Setup (for UNIX) 268

2.1	Installation and setup procedures (for UNIX)	269
2.2	Preparations required before installation (for UNIX)	271
2.2.1	Designing the JP1/IM setup details (for UNIX)	271
2.2.2	Configuring the system environment (for UNIX)	271
2.2.3	Installing the prerequisite program (for UNIX)	271
2.3	Installing JP1/IM - Manager (for UNIX)	272
2.3.1	Installation procedure (for UNIX)	272
2.3.2	How to use the Hitachi Program Product Installer (for UNIX)	275
2.3.3	Settings required immediately after installation (for UNIX)	277
2.3.4	Notes about installing (for UNIX)	279
2.3.5	How to collect data in installing (for UNIX)	282
2.3.6	How to link with the auto scale function (for UNIX)	282
2.3.7	Cloning a Virtual Machine (for UNIX)	283
2.4	Creating IM databases (for UNIX)	285
2.4.1	Preparations for creating IM databases (for UNIX)	285
2.4.2	Setting up the integrated monitoring database (for UNIX)	286
2.4.3	Setting up the IM Configuration Management database (for UNIX)	287
2.4.4	Settings for using the functions of IM Configuration Management (for UNIX)	289
2.4.5	Updating IM databases (for UNIX)	289
2.5	Construction of Intelligent Integrated Management Database (for UNIX)	291
2.5.1	Preparations for Building Intelligent Integrated Management Database (in UNIX)	291
2.5.2	Settings of Intelligent Integrated Management Database (for UNIX)	291
2.5.3	Excluding settings in security product (for UNIX)	292
2.6	Setting up user authentication and user mapping (for UNIX)	293
2.6.1	Specifying the authentication server (for UNIX)	294
2.6.2	Registering JP1 users (for UNIX)	294

2.6.3	Setting operation permissions for the JP1 users (for UNIX)	294
2.6.4	Copying the primary authentication server settings (for UNIX)	295
2.6.5	Setting user mapping (for UNIX)	295
2.7	Specifying settings for handling JP1/Base failures (for UNIX)	296
2.8	Setting the system hierarchy (when IM Configuration Management is used) (for UNIX)	297
2.8.1	Using IM Configuration Management - View to set the system hierarchy (for UNIX)	297
2.8.2	Using the export and import functions to set the system hierarchy (for UNIX)	299
2.8.3	Settings for managing and monitoring a virtualization system configuration (for UNIX)	299
2.9	Setting the system hierarchy (when IM Configuration Management is not used) (for UNIX)	300
2.9.1	Setting the configuration definition information (for UNIX)	300
2.9.2	Deleting the configuration definition information (for UNIX)	301
2.9.3	Changing the configuration definition information (for UNIX)	301
2.9.4	Notes about setting the configuration definition information (for UNIX)	301
2.10	Setting up Event Service (for UNIX)	303
2.11	Setting JP1 event forwarding when IM Configuration Management is used (for UNIX)	304
2.12	Setting JP1 event forwarding when IM Configuration Management is not used (for UNIX)	305
2.13	Collecting and distributing Event Service definition information when IM Configuration Management is used (for UNIX)	306
2.14	Collecting and distributing Event Service definition information when IM Configuration Management is not used (for UNIX)	307
2.15	Setting up a command execution environment (for UNIX)	308
2.15.1	Setting up the command execution function for managed hosts (for UNIX)	308
2.15.2	Setting up a client application execution environment (for UNIX)	309
2.16	Specifying settings for using the source host name of Event Service in the FQDN format (for UNIX)	310
2.16.1	Prerequisites (for UNIX)	310
2.16.2	Setting method (for UNIX)	310
2.16.3	Startup method (for UNIX)	310
2.17	Specifying settings for monitoring logs on remotely monitored hosts (for UNIX)	311
2.17.1	Configuring SSH (for UNIX)	311
2.17.2	Specifying the size of log information that can be collected per monitoring interval (for UNIX)	317
2.18	Setting up JP1/IM - Manager (for UNIX)	318
2.18.1	Executing the setup program (for UNIX)	318
2.18.2	Setting automatic startup and automatic stop (for UNIX)	318
2.18.3	Editing Configuration file of JP1/IM - Manager (for UNIX)	320
2.18.4	Specifying settings for using the functions of the Intelligent Integrated Management Base (for UNIX)	320
2.18.5	Setup When Using JP1/IM - Agent as an agent	321
2.18.6	Register JP1/IM - Agent package (for Windows) (for UNIX)	321
2.18.7	Specifying settings for using the functions of Central Scope (for UNIX)	323
2.18.8	Settings for SELinux (for UNIX)	323
2.18.9	Suppressing Message to be output to the system log (syslog)	326
2.18.10	Specifying settings for handling JP1/IM - Manager failures (for UNIX)	327

2.18.11	Specifying settings for upgrading (for UNIX)	332
2.19	Setup for JP1/IM - Agent (for UNIX)	338
2.19.1	Setup for JP1/IM - Agent servicing	338
2.19.2	Settings of JP1/IM - Agent	341
2.20	Building Container Environments in JP1/IM - Agent (for UNIX)	358
2.21	Building optional features for JP1/IM - Agent (for UNIX)	359
2.21.1	Configuring OracleDB exporter	359
2.21.2	Configuring the Node exporter for AIX	363
2.21.3	Configuring SAP system monitoring	363
2.22	Saving manuals to a computer (for UNIX)	364
2.23	Uninstallation (for UNIX)	365
2.23.1	Uninstallation procedure (for UNIX)	365
2.23.2	Notes on uninstallation (for UNIX)	368
2.24	Notes about installation and setting up (for UNIX)	374
3	Using IM Configuration Management to Set the System Hierarchy	375
3.1	Registering hosts	376
3.1.1	Registering hosts	376
3.1.2	Registering remotely monitored hosts	377
3.1.3	Collecting information from hosts	378
3.1.4	Displaying host information	379
3.1.5	Changing the attributes of host information	380
3.1.6	Deleting hosts	381
3.2	Setting the system hierarchy	382
3.2.1	Collecting the system hierarchy	382
3.2.2	Displaying the system hierarchy	383
3.2.3	Verifying the system hierarchy	383
3.2.4	Editing the system hierarchy	384
3.2.5	Synchronizing the system hierarchy	390
3.3	Setting a virtualization system configuration	391
3.3.1	Using IM Configuration Management to manage a virtualization configuration	391
3.3.2	Collecting virtualization system configuration information	405
3.3.3	Using Central Scope to monitor a virtualization configuration	407
3.3.4	Notes when collecting the virtualization configuration	409
3.4	Setting business groups	410
3.4.1	Creating business groups	411
3.4.2	Adding hosts to business groups	416
3.4.3	Deleting hosts from business groups	417
3.4.4	Using Central Scope to monitor business groups	417
3.5	Setting the profiles	419
3.5.1	Setting the profiles on hosts in an agent configuration	419
3.5.2	Setting the profiles on hosts in a remote monitoring configuration	432

3.6	Importing and exporting the management information in IM Configuration Management	442
4	Setting Up the Intelligent Integrated Management Base	443
4.1	Overview of configuring an environment for the Intelligent Integrated Management Base	444
4.1.1	Before configuring an environment for the Intelligent Integrated Management Base	444
4.2	Setting system configuration information	445
4.3	Settings for using the encryption function with the Intelligent Integrated Management Base	448
4.4	Creating a cluster environment for the Intelligent Integrated Management Base	449
4.5	Settings necessary to use the custom UI display function	450
4.6	Compatible setting of the repeated event viewing suppression function	452
4.7	Defining links	453
4.8	Setting work impact icons	454
4.9	Monitor startup setting for linked products	455
4.10	Setting up the suggestion function for response actions depending on the system status	456
4.11	Settings for linkage with an OpenID provider through single sign-on (linkage with external products)	457
4.11.1	Providing linkage with an OpenID provider through single sign-on	457
4.11.2	How to reload the single sign-on mapping definition file (imdd_sso_mapping.properties)	458
4.11.3	How to stop linkage with the OpenID provider	459
4.12	Setting up the direct access URL	460
4.12.1	Direct access URL	460
4.12.2	Getting the direct access URL for node selection	461
4.12.3	OpenID authentication direct access URL	462
4.12.4	Examples of specifying direct access URLs	463
4.13	Configuring the method for applying system configuration information	467
4.14	Migration procedure of the IM management node link definition file	468
4.15	Web browser setup procedure to use the integrated operation viewer	469
4.16	Dashboard Configuration	470
4.16.1	Customizing Auto-Generated Dashboards	470
4.16.2	Creating a new dashboard	470
4.16.3	Editing Dashboards	470
4.16.4	Shared the Dashboard window	471
4.16.5	Deleting a dashboard	471
5	Setting Up Central Console	472
5.1	Settings for the operations to be performed during JP1/IM event acquisition	473
5.1.1	Displaying events by specifying the event acquisition range at login	473
5.2	Setting JP1 event filtering	475
5.2.1	Settings for view filters	475
5.2.2	Settings for event receiver filters	477
5.2.3	Settings for severe events filters	479
5.2.4	Settings for event acquisition filters	481

5.3	Setting monitoring of repeated events to be prevented	488
5.4	Setting the display colors of JP1 events	489
5.5	Setting automated actions	490
5.5.1	Setting up an execution environment for the automated action function	490
5.5.2	Setting the execution conditions and details of automated actions	490
5.5.3	Settings for monitoring the automated action execution status	492
5.5.4	Setting suppression of automated action execution	493
5.5.5	Setting email transmissions	493
5.6	Settings for generating correlation events	498
5.6.1	Setting startup of the correlation event generation function	498
5.6.2	Setting the size and number of correlation event generation history files	498
5.6.3	Setting startup options	499
5.6.4	Creating and applying a correlation event generation definition	500
5.7	Setting memo entries	501
5.8	Editing event guide information	502
5.8.1	How to edit event guide information	502
5.9	Setting JP1 event issuance during action status change	504
5.10	Adding program-specific attributes	505
5.11	Setting the display and specification of program-specific extended attributes	506
5.12	How to display user-defined event attributes	508
5.12.1	Creating the definition files	510
5.12.2	Enabling the definition files	512
5.13	Setting the severity changing function	513
5.13.1	Setting the severity changing function from the Severity Change Definition Settings window	513
5.13.2	Setting the severity changing function by using the severity changing definition file	514
5.14	Setting the display message change function	516
5.14.1	Configuring from the Display Message Change Definition Settings window	516
5.14.2	Configuring from the display message change definition file	518
5.14.3	Procedure for issuing events after display messages have been changed	518
5.15	Setting event source host mapping	520
5.16	Setting JP1/IM - View for each login user	523
5.16.1	Settings for JP1/IM - View	523
5.16.2	Procedure for specifying JP1/IM - View settings	524
5.17	Setting monitor startup for linked products	525
5.17.1	How to open monitor windows	525
5.17.2	Determining the window to be used for opening monitor windows	526
5.17.3	Creating the definition files	526
5.18	Setting the Tool Launcher window	528
5.18.1	Settings for opening the GUI of linked products from the Tool Launcher window	528
5.18.2	How to add new menus	528
5.18.3	Determining a window to be opened from the Tool Launcher window	529

5.18.4	Creating the definition files	529
5.18.5	Settings for opening the Web page of a linked product from the Tool Launcher window	532
5.19	Setting reference and operation restrictions on business groups	533
6	Setting Up Central Scope	535
6.1	Overview of the Central Scope environment setup	536
6.1.1	Before starting Central Scope environment setup	536
6.2	Registering host information	537
6.3	Using the GUI to create a monitoring tree	538
6.3.1	Opening the Monitoring Tree (Editing) window	538
6.3.2	Acquiring an existing monitoring tree	539
6.3.3	Generating a monitoring tree automatically	540
6.3.4	Customizing a monitoring tree	542
6.3.5	Saving a customized monitoring tree at the local host	551
6.3.6	Applying a customized monitoring tree to the manager	551
6.4	Using the GUI to create a Visual Monitoring window	553
6.4.1	Opening an edit window for the Visual Monitoring window	553
6.4.2	Acquiring an existing Visual Monitoring window	554
6.4.3	Customizing a Visual Monitoring window	554
6.4.4	Saving a customized Visual Monitoring window at the local host	558
6.4.5	Applying a customized Visual Monitoring window to the manager	558
6.4.6	Editing the list of Visual Monitoring windows and deleting Visual Monitoring windows	559
6.5	Editing the saved CSV file to create the Monitoring Tree window	561
6.6	Editing guide information	562
6.6.1	How to edit guide information	562
6.7	Setting up a Central Scope operating environment	565
6.7.1	Setting for the maximum number of status change events	565
6.7.2	Setting the completed-action linkage function	565
6.7.3	Settings for automatically deleting status change events when JP1 event handling is completed	566
6.7.4	Settings for initializing monitoring objects when JP1 events are received	566
6.7.5	Setting the memory-resident status change condition function	567
6.7.6	Customizing the toolbar for the monitoring tree	567
6.7.7	Settings for suppressing the display of a monitoring node name and the icon margin	568
6.7.8	Settings of the status color of a monitoring node name and monitoring node	569
6.7.9	Settings for suppressing the movement of the icon of a monitoring node	571
6.8	Setting up for linked products	572
6.8.1	Setup for linkage with JP1/AJS	572
6.8.2	Setup for linkage with JP1/Cm2/SSO	573
6.8.3	Setup for linkage with JP1/PFM	575
6.8.4	Setup for linkage with HP NNM	576
6.8.5	Setup for linkage with JP1/Software Distribution	577
6.8.6	Setup for linkage with JP1/PAM	578

6.8.7	Setup for linkage with Cosminexus	578
6.8.8	Setup for linkage with HiRDB	579
6.8.9	Setup for linkage with JP1/ServerConductor	579
6.9	Examples of monitoring object creation	580
6.9.1	Example of creating system-monitoring objects (JP1/AJS jobnet monitoring)	580
6.9.2	Example of creating a general monitoring object (CPU monitoring by JP1/Cm2/SSO)	581
6.9.3	Example of creating a general monitoring object (HiRDB monitoring)	586
6.9.4	Example of creating a general monitoring object (Cosminexus resource monitoring by JP1/Cm2/SSO)	591
7	Operation and Environment Configuration in a Cluster System (for Windows)	597
7.1	Overview of cluster operation (for Windows)	598
7.1.1	Overview of a cluster system (for Windows)	598
7.1.2	Prerequisites for cluster operation (for Windows)	599
7.1.3	JP1/IM configuration in a cluster system (for Windows)	602
7.2	Environment setup procedure for cluster operation (for Windows)	606
7.3	Installing and setting up logical hosts (new installation and setup) (for Windows)	608
7.3.1	Newly installing JP1/Base and JP1/IM - Manager (for Windows)	608
7.3.2	Setting up the physical host environment during new installation of JP1/IM - Manager (for Windows)	609
7.3.3	Setting up the logical host environment (primary node) during new installation of JP1/IM - Manager (for Windows)	609
7.3.4	Copying the common definition information during new installation of JP1/IM - Manager (for Windows)	616
7.3.5	Setting up the logical host environment (secondary node) during new installation of JP1/IM - Manager (for Windows)	616
7.3.6	Newly installing JP1/IM - Agent with integrated agent host (for Windows)	621
7.3.7	Setting up the JP1/IM - Agent during new installation (for Windows)	622
7.4	Creating a cluster environment for the Intelligent Integrated Management Base (for Windows)	627
7.4.1	Creating a new cluster environment (For Windows)	627
7.4.2	Creating a cluster environment to which a corrected version is applied (For Windows)	629
7.4.3	Creating a cluster environment after upgrading (For Windows)	629
7.5	Registering into the cluster software during new installation and setup (for Windows)	633
7.5.1	Registering into the cluster software (for Windows)	634
7.5.2	Setting the resource start and stop sequence (for Windows)	635
7.5.3	Setting Cluster Soft Parameters (for Windows)	635
7.6	Upgrade installation and setup of logical hosts (for Windows)	637
7.6.1	Upgrade installation of JP1/Base and JP1/IM - Manager (for Windows)	637
7.6.2	Upgrade installation of JP1/IM - Agent (for Windows)	638
7.6.3	Setting up the physical host environment during upgrade installation (for Windows)	639
7.6.4	Setting up the logical host environment (primary node) during upgrade installation (for Windows)	639
7.6.5	Copying the common definition information during upgrade installation (for Windows)	640

7.7	Uninstalling logical hosts (for Windows)	641
7.7.1	Deleting logical hosts (for Windows)	641
7.7.2	Uninstalling JP1/IM - Manager and JP1/Base (for Windows)	643
7.7.3	Uninstall JP1/IM - Agent (for Windows)	643
7.8	Procedures for changing settings (for Windows)	645
7.8.1	Changing settings in files (for Windows)	645
7.8.2	Using commands to change settings (for Windows)	645
7.8.3	Updating IM databases in a cluster environment (for Windows)	646
7.9	Notes about cluster operation (for Windows)	649
7.10	Logical host operation and environment configuration in a non-cluster system (for Windows)	650
7.10.1	Evaluating the configuration for running logical hosts in a non-cluster system (for Windows)	650
7.10.2	Environment setup for running logical hosts in a non-cluster system (for Windows)	650
7.10.3	Notes about running logical hosts in a non-cluster system (for Windows)	651

8 Operation and Environment Configuration in a Cluster System (for UNIX) 652

8.1	Overview of cluster operation (for UNIX)	653
8.1.1	Overview of a cluster system (for UNIX)	653
8.1.2	Prerequisites for cluster operation (for UNIX)	653
8.1.3	JP1/IM configuration in a cluster system (for UNIX)	653
8.2	Environment setup procedure for cluster operation (for UNIX)	656
8.3	Installing and setting up logical hosts (new installation and setup) (for UNIX)	658
8.3.1	Newly installing JP1/Base and JP1/IM - Manager (for UNIX)	658
8.3.2	Setting up the physical host environment during new installation of JP1/IM - Manager (for UNIX)	659
8.3.3	Setting up the logical host environment (primary node) of JP1/IM - Manager during new installation (for UNIX)	659
8.3.4	Copying the common definition information during new installation of JP1/IM - Manager (for UNIX)	664
8.3.5	Setting up the logical host environment (secondary node) during new installation of JP1/IM - Manager (for UNIX)	665
8.3.6	Newly installing JP1/IM - Agent with integrated agent host (for UNIX)	668
8.3.7	Setting up the JP1/IM - Agent during new installation (for UNIX)	669
8.4	Setup for Intelligent Integrated Management Base's cluster environment (for UNIX)	674
8.4.1	Creating a new cluster environment (for UNIX)	674
8.4.2	Creating a cluster environment to which a corrected version is applied (for UNIX)	676
8.4.3	Creating a cluster environment after upgrading (for UNIX)	676
8.5	Registering into the cluster software during new installation and setup (for UNIX)	680
8.5.1	Creating a script to be registered into the cluster software (for UNIX)	681
8.5.2	Setting the resource start and stop sequence (for UNIX)	683
8.5.3	Setting Cluster Soft Parameters (for Linux)	684
8.6	Upgrade installation and setup of logical hosts (for UNIX)	685
8.6.1	Upgrade installation of JP1/Base and JP1/IM - Manager (for UNIX)	685
8.6.2	Upgrade installation of JP1/IM - Agent (for UNIX)	686

8.6.3	Setting up the physical host environment during upgrade installation (for UNIX)	687
8.6.4	Setting up the logical host environment (primary node) during upgrade installation (for UNIX)	687
8.6.5	Copying the common definition information during upgrade installation (for UNIX)	689
8.7	Uninstalling logical hosts (for UNIX)	690
8.7.1	Deleting logical hosts (for UNIX)	690
8.7.2	Uninstalling JP1/IM - Manager and JP1/Base (for UNIX)	692
8.7.3	Uninstalling JP1/IM - Agent (for UNIX)	692
8.8	Procedures for changing settings (for UNIX)	694
8.8.1	Changing settings in files (for UNIX)	694
8.8.2	Using commands to change settings (for UNIX)	694
8.8.3	Updating IM databases in a cluster environment (for UNIX)	695
8.9	Notes about cluster operation (for UNIX)	697
8.10	Logical host operation and environment configuration in a non-cluster system (for UNIX)	698
8.10.1	Evaluating the configuration for running logical hosts in a non-cluster system (for UNIX)	698
8.10.2	Environment setup for running logical hosts in a non-cluster system (for UNIX)	698
8.10.3	Notes about running logical hosts in a non-cluster system (for UNIX)	699

9 Operation and Environment Configuration Depending on the Network Configuration 700

9.1	Controlling communications by JP1/Base	701
9.2	Operating in multiple networks	702
9.2.1	Example 1 (non-cluster operation with JP1/IM - View connection)	702
9.2.2	Example 2 (non-cluster operation with command execution)	703
9.2.3	Example 3 (cluster operation with JP1/IM - View connection)	704
9.2.4	Example 4 (cluster operation with command execution)	705
9.3	Operating in a firewall environment	707
9.3.1	Basic information about firewalls	707
9.3.2	JP1/IM communication	712
9.3.3	Notes on Windows Firewall	717
9.4	Configuring encrypted communication	720
9.4.1	Newly using the communication encryption function	720
9.4.2	Changing configured certificates	724
9.4.3	Stopping using the communication encryption function	727
9.4.4	Configuring JP1/IM - Manager	729
9.4.5	Settings for JP1/IM - Agent (JP1/IM agent control base)	730
9.4.6	Checking whether the communication encryption function has been configured correctly	730

10 Settings for Linking to Other JP1 Products 732

10.1	Linking to JP1/Service Support	733
10.1.1	Enabling calling the JP1/Service Support window	733
10.2	Linking to JP1/Navigation Platform	734
10.3	Linking with JP1/AJS	735

10.3.1	Settings for launching a JP1/AJS window by monitor startup	735
10.3.2	Settings for launching a JP1/AJS window from the Tool Launcher window	735
10.3.3	Settings for displaying the monitor window from the event guide information	735
10.3.4	Settings for displaying the monitor window from an email sent by an automated action	735
10.3.5	Settings for checking the association between root jobnets and their configuration information by using the Intelligent Integrated Management Base	735
10.4	Linking with JP1/PFM	737
10.4.1	Settings for launching a JP1/PFM window by monitor startup	737
10.4.2	Settings for launching a JP1/PFM window from the Tool Launcher window	737
10.4.3	Settings for displaying event-source-host performance reports	737
10.4.4	Settings for checking operation information by using the Intelligent Integrated Management Base	737

Index 739

1

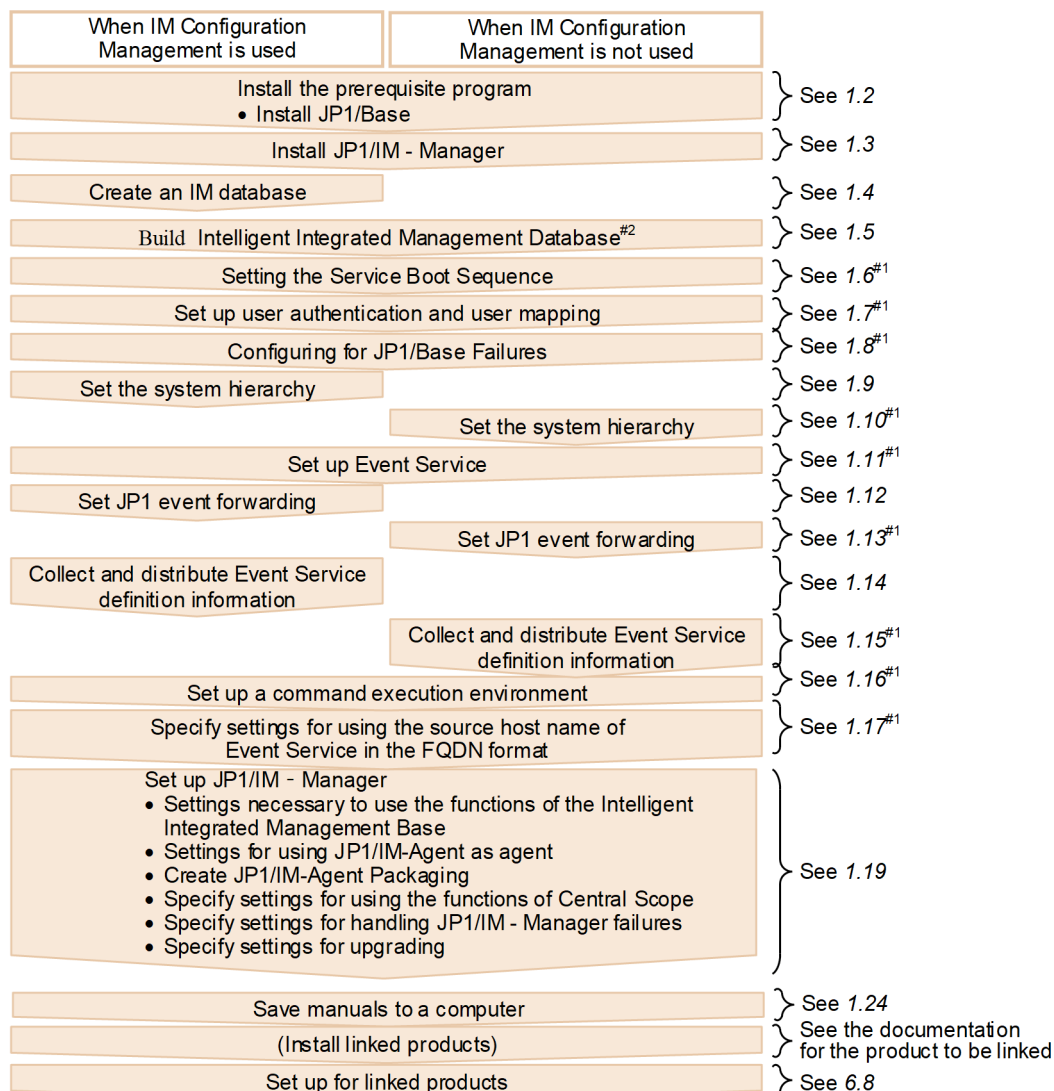
Installation and Setup (for Windows)

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 [1.25.1 Uninstallation procedure \(for Windows\)](#).

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



#1: For more information, see *JP1/Base Administration Guide documentation*.

#2: This is performed when Intelligent Integrated Management Database is used.

Figure 1–2: Installation and setup workflow (agent (JP1/IM - Agent))

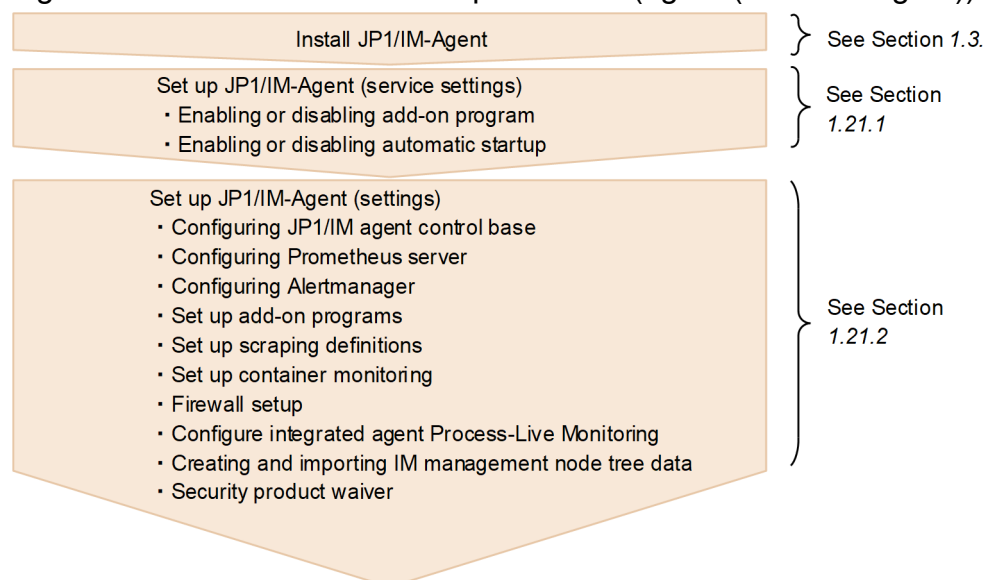
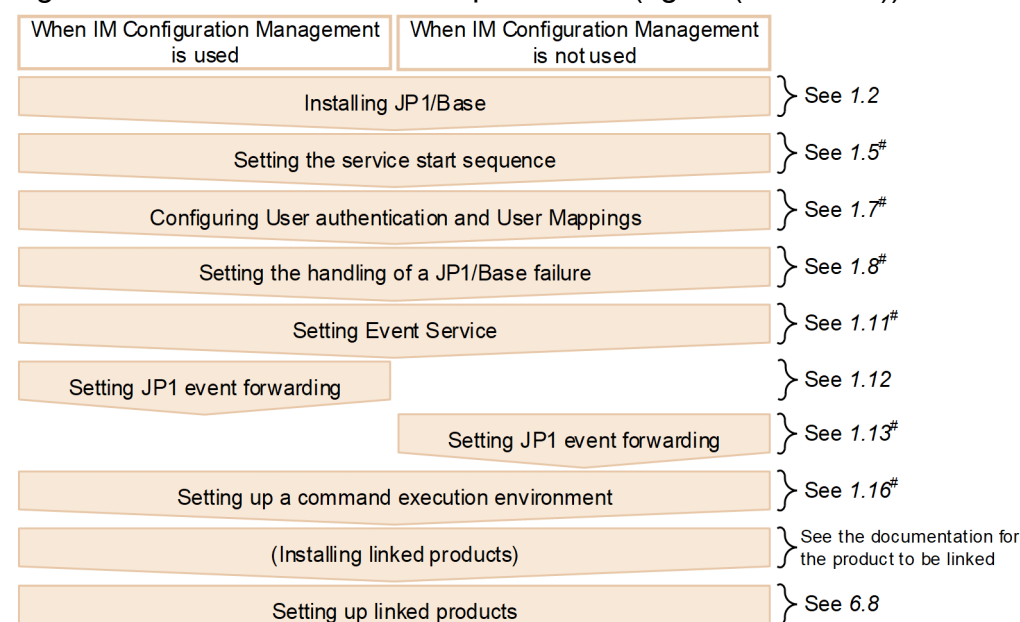
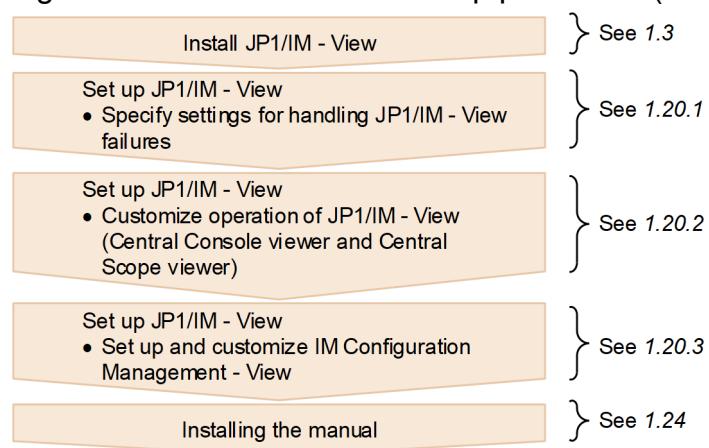


Figure 1–3: Installation and setup workflow (agent (JP1/Base))



[#]: For more information, see *JP1/Base Administration Guide* documentation.

Figure 1–4: Installation and setup procedure (viewer)



For details about the settings for monitoring logs on hosts that will be monitored remotely, see [1.18 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 [9.4 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 3 - 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.
- When IM databases are used, a host name must be a character string of not more than 32 characters consisting of only one-byte alphanumeric characters, -, and . (period).

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.

When you apply an OS patch, stop the product first, and then apply the patch while the product is stopped.

Important

- For installation, setup, and uninstallation, the administrator permission is required. Before a non-administrator user can perform any of these operations in an environment where Windows UAC (User Account Control) is enabled, the user must become an administrator. In an environment where UAC is unavailable, perform these operations as a user who belongs to the Administrators group.
- When you upgrade an OS where JP1/IM - Manager and JP1/IM - View has been installed, make sure to uninstall JP1/IM - Manager and JP1/IM - View before upgrading 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 3 - 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, JP1/IM - View, and JP1/IM - Agent (for Windows)

This section explains how to install JP1/IM - Manager, JP1/IM - View, and JP1/IM - Agent. 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, JP1/IM - View, and JP1/IM - Agent.

If you install JP1/IM - Manager, JP1/IM agent management base for using JP1/IM - Agent is also installed.

(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/IM3-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.
- Do not specify folders such as those below for the installation destination folder. If these kinds of folders are specified, operation cannot be guaranteed.
 - Folder names that contain symbols (such as a semicolon (;), hash mark (#), single quotation mark ('), or percent sign (%))
 - Folder names that contain character codes other than the SJIS character code (such as JIS Third and Forth Levels)
 - Folders for drives other than fixed disks or UNC paths
- When you install this product, make sure that the installation folder of this product (JP1IMM, JP1Cons, and JP1Scope) is not same as the installation folder of another product.
- The top-level folders (JP1IMM, JP1Cons, and JP1Scope), subfolders, and files created by JP1/IM - Manager inherit the permissions of the destination folder. For this reason, we recommend that you do not grant the following privileges to OS users without administrator privileges to the installation-destination folder:
 - Full control
 - Change
 - Write
 - Special access permissions
- For the volume on which JP1/IM - Manager will be installed and the volume on which the data of JP1/IM - Manager will be stored, it is necessary to create a short name (in 8.3 format). Before installing JP1/IM - Manager, check the OS settings to make sure short names can be created and they have not been removed, because creating short names may be disabled by default depending on the OS.
- Installations to virtual disks created in memory area pools of Windows Server 2016, Windows Server 2019, Windows Server 2022 or Windows Server 2025 are not supported.
- If you cancel installation during the installation process, some files may stay on the system, depending on the timing of the cancellation.

To perform encrypted communication with JP1/IM - Agent, perform the following steps related to JP1/IM agent management base.

1. Setup server certificate and its key file.

When performing cryptographic communication with integrated agent host, specify the full path of server certificate file to "tls_config.cert_file" of imbase common configuration file (`jpc_imbasecommon`), and the full path of the key file of server certificate in "tls_config.key_file".

For details, see *imbase common configuration file (jpc_imbasecommon.json)* in *Chapter 2. Definition Files* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

(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.
- Do not specify folders such as those below for the installation destination folder. If these kinds of folders are specified, operation cannot be guaranteed.
 - Folder names that contain symbols (such as a semicolon (;), hash mark (#), single quotation mark ('), or percent sign (%))
 - Folder names that contain character codes other than the SJIS character code (such as JIS Third and Forth Levels)
- It will not be possible to upgrade JP1/IM - View if it is installed anywhere other than on a fixed disk.

- Do not install JP1/IM - View (JP1CoView) and other products in the same folder.
- The top-level folders (JP1CoView), lower-level folders, and files created by JP1/IM - View inherit the permissions of the destination folder. For this reason, we recommend that you do not grant the following privileges to OS users without administrator privileges to the installation-destination folder:
 - Full control
 - Change
 - Write
 - Special access permissions
- To install to Windows 10(x86) or Windows 11, do not specify a directory under *system-drive:\Program Files\WindowsApps* as the installation destination. As an administrator user cannot write to the above folder, the installation fails.

(3) Procedure of JP1/IM - Agent installation

(a) Information required before installation

If you are installing JP1/IM - Agent newly, you need the following: Prepare before installation.

Table 1–3: Information required for a new installation

Item	Needing to specify	Description
Install destination folder	Optional	Specify the install destination folder. Specify a folder according to the following conditions: If it is installed in any other folders, it will not work properly. Characters can be specified in the following: single-byte alphanumeric characters, single-byte spaces, single-byte hyphens (-), single-byte underscores (_), single-byte backslash (\) ^{#1} , and single-byte colons (:) ^{#2} . #1: Indicates the characters used to separate folders. Cannot be used as a folder name. #2: Characters used to separate drives and folders. Cannot be used as a folder name.
Host name of the install destination JP1/IM - Manager	Required	Specifies the host name of the manager host that manages integrated agent to be installed. The name must be resolved to IP address.
Listen port for imbase processes	Optional	Specifies the listen port for imbase processes running on the manager host to connect, from 5001 to 65535. When this is omitted, imbase default port (20724) is used.
Listen port for imbaseproxy processes	Optional	Specifies the listen port for imbaseproxy processes running on the manager host to connect, from 5001 to 65535. When this is omitted, imbaseproxy default port (20725) is used.
Initial secret to connect to imbase for the first time	Required	Specifies initial secret to connect to imbase process running on the manager host to connect for the first time. Initial secret is issued from integrated operation viewer. If initial secret have been already issued and have been saved, prepare the value.
URL of proxy	Optional	If you are connecting to the manager host through a proxy server, specify the proxy URL in "http://host:port" format. The default for when this is omitted is an empty string.
User ID for proxy authentication	Optional	When connecting to the manager host, specify ID for authentication of the proxy server when passing through the proxy server. The characters that can be specified are the characters in ASCII encoding 0x20 to 0x7E. You can specify up to 1007-charaters-long string. The default for when this is omitted is an empty string.

Item	Needing to specify	Description
Password for proxy authentication	Optional	When connecting to the manager host, specify password for authentication of the proxy server when passing through the proxy server. The characters that can be specified are the characters in ASCII encoding 0x20 to 0x7E. You can specify up to 1007-charaters-long string. The default for when this is omitted is an empty string.
Functions to be used	Optional	Allows you to select the function that you use in JP1/IM - Agent. A new install setup the service for the feature you use to start automatically.

(b) Install instructions

Follow the procedure below to install.

1. Login agent host with administrator privileges.

You must have Administrators privilege to complete the install process.

2. Prepare a medium for installing JP1/IM - Agent.

There are two ways to install JP1/IM - Agent: Prepare the installation media according to the installation method to be used.

- To install by setting the offered media on the drive
Provide the offered media as an installation medium.
- To install by downloading JP1/IM - Agent packages registered to the manager host from Integrated Operation Viewer[#]
Download and extract JP1/IM - Agent packages to prepare them.

#

For the procedure for downloading JP1/IM - Agent package, see [1.19.4\(3\) How to Download JP1/IM - Agent Package](#).

3. Setup the environment variables for default settings for the host to be installed.

- For silent or remote installations (required)

The parameters required for installation must be setup in the environment variable [#] beforehand.

- For a typical installation (optional)

You can setup the values of parameters that you setup on the installer, except for user name, its membership, and install destination folder, by environment variable [#]in advance.

You do not need to setup the environment variables if you wish to enter it manually on the display of installer.

#

For details about environment variable, see [1.3.1\(3\)\(c\) Initialization environment variable used by the installer](#).

4. Terminate all programs.

Close all programs before installing.

Stop JP1/IM - Agent servicing before the version upgrade installing.

5. Install JP1/IM - Agent by executing the downloaded JP1/IM - Agent installer.

Follow the instructions in the installer that you launched.

Select the software to install, and then type the following: Select "Normal installation mode" for the installation mode.

- User Information

Enter this item only for a new installation.

If you upgraded from a previous Version of JP1/IM - Agent, it will inherit settings from the previous version.

- Installation destination folder

Do not install the software under "*System-drive*\Program Files (x86)\\" (Program files folders with x86). Mixing with 32-bit modules may cause operational problems.

When you install JP1/IM - Agent, the following installation folder is created:

Table 1–4: Folders created when installed

Product	Folders to be created ^{#1}	Description
JP1/IM - Agent	<i>Installation-destination-folder</i> \jp1ima ^{#2}	JP1/IM - Agent data is stored.

#1: The default value of the installation folder is "*system-drive*:\Program Files\Hitachi". In Windows, the notation "*system-drive*:\Program Files" is determined by OS environment variable when it was installed. Therefore, it may vary depending on the environment.

#2: If the old version of JP1/IM - Agent was installed in a different folder, the folder where the old version was installed is inherited. In this case, the folder shown above will not be created.

Note that only fixed-disk drives can be specified as JP1/IM - Agent installation destination folders.

■ When version upgrade installation is executed

If you are using the data distribution function to multiple manager hosts, perform [1.21.2\(2\)\(i\) Setting the data delivery function to multiple manager hosts \(for Windows\) \(optional\)](#) prior to starting JP1/IM - Agent service.

6. If restart is requested, restart Windows.

7. After the install completed, make the required setup changes.

Make the required setup change described in [1.21.2 Settings of JP1/IM - Agent](#). The mandatory setups should be performed for sure.

! Important

- Only fixed-disk drives can be specified as JP1/IM - Agent installation destination folders. It cannot be installed on removable disks, network drives, or UNC paths.
- For the folder where JP1/IM - Agent is installed, specify a folder according to the following criteria. If it is installed in any other folders, it will not work properly.
 - Characters can be specified in the following: single-byte alphanumeric characters, single-byte spaces, single-byte hyphens (-), single-byte underscores (_), single-byte backslash (\) ^{#1}, and single-byte colons (:)^{#2}.
 - #1: Indicates the characters used to separate folders. Cannot be used as a folder name.
 - #2: Indicates the characters used to separate drives and folders. Cannot be used as a folder name.
- The folder (jp1ima) where JP1/IM - Agent is installed should not be the same as the folder where other products are installed.
- The top-level folders (jp1ima), lower-level folders, and files created by JP1/IM - Agent inherit the permissions of the destination folder. For this reason, we recommend that you do not grant the following privileges to OS users without administrator privileges to the installation-destination folder:
 - Full control
 - Change
 - Write
 - Special access permissions

- Installing on a virtual disk created in Windows Server 2016, Windows Server 2019, Windows Server 2022, or Windows Server 2025 storage pools is not supported.
- If you cancel installing, files may remain depending on the timing.
- If you have changed initial secret after you installed JP1/IM agent control base on integrated agent host and before the first boot of JP1/IM agent control base, you must either update initial secret registered with integrated agent or uninstall and reinstall integrated agent. For details about updating initial secret registered in integrated agent, see step 4 in [1.21.2\(2\)\(a\) Change Integrated manager to connect to \(for Windows\) \(optional\)](#).

(c) Initialization environment variable used by the installer

The following are Environment variable for initial setup for installer of JP1/IM - Agent.

Table 1–5: List of Environment variables for initial setup used by JP1/IM - Agent installer

Item	Environment Variables	Whether or not to omit	Explanation of Value	Defaults value
JP1/IM - Agent installation mode	JP1IMAGENT_INSTALL_MODE	Not possible	• normal Normal installation mode Select this option when operating in an installed environment. • image Image creation mode Select in the following cases: - If you make an installed deployment virtual image and you want to operate with the new instance from the virtual machine image. - To create a base container image Notes You must complete the initial setup by using jimasetup command before starting operation. For details, see <i>jimasetup</i> in <i>Chapter 1. Commands in the JP1/Integrated Management 3 - Manager Command, Definition File and API Reference</i>.	None
Host name of the manager host to connect to	JP1IMAGENT_IM_MGR_HOST	Not possible	Specifies Host name of the manager host to connect that manages integrated agent to be newly installed.	None
Listen Port number for imbase	JP1IMAGENT_IM_MGR_IMBASE_PORT	Yes	Specifies the listen port number for imbase processes running on the manager host to connect, between 5001 and 65535. If this environment variable is omitted, the default value is assumed for the initial setup.	20724
Listen Port number for imbaseproxy	JP1IMAGENT_IM_MGR_IMBASEPROXY_PORT	Yes	Specifies the listen port number for imbaseproxy processes running on the manager host to connect, between 5001 and 65535. If this environment variable is omitted, the default Value is assumed for the initial setup.	20725
Initial secret	JP1IMAGENT_IM_MGR_INITIAL_SECRET	Not possible	Specifies initial secret to initially connect to imbase process running on the manager host to connect.	None

Item	Environment Variables	Whether or not to omit	Explanation of Value	Defaults value
			Check initial secret from integrated operation viewer.	
Proxy URL of connect destination	JP1IMAGENT_IMMGR_PROXY_URL	Yes	If you are connecting to the manager host through a proxy server, specify the proxy URL in "http://host:port" format. If this environment variable is omitted, default setup is performed assuming that the proxy is not used.	None
Proxy authentication customer ID	JP1IMAGENT_IMMGR_PROXY_USER	Yes	If you are connecting to the manager host through a proxy server, specify user ID for the proxy server's authentication. If the environment variable JP1IMAGENT_IMMGR_PROXY_URL is omitted, the system ignores this environment variable even if it is setup.	None
Proxy authentication password	JP1IMAGENT_IMMGR_PROXY_PASSWORD	Yes	If you are connecting to the manager host through a proxy server, specify Password for the proxy server's authentication. If the environment variable JP1IMAGENT_IMMGR_PROXY_URL or environment variable JP1IMAGENT_IMMGR_PROXY_USER is omitted, the system ignores this environment variable even if it is setup.	None
Enable or disable Setup of Prometheus server and Alertmanager	JP1IMAGENT_ADDON_PROMETHEUS_AND_ALERTMANAGER_ACTIVE	Yes	Specifies whether Prometheus server, Alertmanager are Enabled. - yes Turn Enable Prometheus server and Alertmanager - no Disable Prometheus server and Alertmanager If this environment variable is omitted, the default value is assumed and the initial setup is performed.	yes
Enable or disable Setup of Node exporter	JP1IMAGENT_ADDON_NODE_EXPORTER_ACTIVE	Yes	Specifies whether Node exporter is Enabled. - yes Enable Node exporter - no Disable Node exporter This environment variable is setup only for Linux. This is ignored when set in Windows. If this environment variable is omitted, the default value is assumed and the initial setup is performed.	yes
Enable or disable Setup of Windows exporter	JP1IMAGENT_ADDON_WINDOWS_EXPORTER_ACTIVE	Yes	Specifies whether Windows exporter is Enabled. - yes Enable Windows exporter - no Disable Windows exporter This environment-variable is setup only for Windows. This is ignored when set in Linux.	yes

Item	Environment Variables	Whether or not to omit	Explanation of Value	Defaults value
			If this environment variable is omitted, the default value is assumed and the initial setup is performed.	
Enable or disable Setup of Blackbox exporter	JPLIMAGENT_ADDON_BLACKBOX_EXPORTER_ACTIVE	Yes	Specifies whether Blackbox exporter is Enabled. - yes Enable Blackbox exporter - no Disable Blackbox exporter If this environment variable is omitted, the default value is assumed and the initial setup is performed.	no
Enable or disable Setup of Yet another cloudwatch exporter	JPLIMAGENT_ADDON_YA_CLOUDWATCH_EXPORTER_ACTIVE	Yes	Specifies whether Yet another CloudWatch exporter is Enabled. - yes Enable Yet another cloudwatch exporter - no Disable Yet another cloudwatch exporter If this environment variable is omitted, the default value is assumed and the initial setup is performed.	no
Enable or disable Setup of Fluentd	JPLIMAGENT_ADDON_FLUENTD_ACTIVE	Yes	Specifies whether Fluentd is Enabled. - yes Enable Fluentd - no Disable Fluentd If this environment variable is omitted, the default value is assumed and the initial setup is performed.	yes
Enable or disable Promitor	JPLIMAGENT_ADDON_PROMITOR_ACTIVE#	Yes	Specifies whether Promitor is Enabled. - yes Enable Promitor - no Disable Promitor	no
Enable or disable Process exporter	JPLIMAGENT_ADDON_PROCESS_EXPORTER_ACTIVE#	Yes	Specifies whether Process exporter is Enabled. - yes Enable Process exporter - no Disable Process exporter This environment variable is setup only for Linux. This is ignored when set in Windows.	yes
Enable or disable Script exporter	JPLIMAGENT_ADDON_SCRIPT_EXPORTER_ACTIVE#	Yes	Specifies whether Script exporter is Enabled. - yes Enable Script exporter - no Disable Script exporter	no
Enable or disable Web scenario monitoring	JPLIMAGENT_ADDON_WEB_EXPORTER_ACTIVE	Yes	Specifies whether Web scenario monitoring is Enabled.	no

Item	Environment Variables	Whether or not to omit	Explanation of Value	Defaults value
			• yes Enable Web scenario monitoring • no Disable Web scenario monitoring If this environment variable is omitted, the default value is assumed and the initial setup is performed.	
Enable or Disable VMware exporter	JP1IMAGENT_ADDON_VMWARE_EXPORTER_ACTIVE	Yes	Specifies whether VMware exporter is Enabled. • yes Enable VMware exporter • no Disable VMware exporter If this environment variable is omitted, the default value is assumed and the initial setup is performed.	no
Enabling/Disabling Hyper-V Monitor Feature	JP1IMAGENT_ADDON_WINDOWS_EXPORTER_HYPERV_ACTIVE	Yes	Enables or disables Hyper-V monitoring feature. • yes Enabling Hyper-V Monitor Feature • no Disable Hyper-V monitoring function If this environment variable is omitted, the default value is assumed and the initial setting is performed.	no

#

If the environment variable is omitted, the default value is assumed.

(4) 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 [14.2](#)

Upgrading from a previous version of JP1/IM in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

For notes on upgrading JP1/IM - Agent from version 13-00 or 13-01, see [1.3.3\(14\) Notes on upgrading JP1/IM - Agent from version 13-00 or 13-01](#) and [1.3.3\(15\) Notes on upgrading JP1/IM - Agent from version 13-00 to 13-10](#).

About the program folder displayed in the **Start** menu

- If you perform upgrade installation, the program folder for the product you are upgrading is retained without a change of name in the **Select Program Folder** window.
If you do not want to use the displayed program folder, enter a new program folder name in the **Select Program Folder** window.
- If you perform upgrade installation via JP1/Software Distribution, the program folder for the product you are upgrading is retained without a change of name. If you want to change the program folder name, manually change it after upgrade installation.
- If you manually changed the program folder for the product from which you perform a version upgrade install, the program folder is not deleted after performing the version upgrade install of JP1/IM - Manager, JP1/IM -

View, and JP1/IM - Agent. If you don't need the program folder, delete it manually after the version upgrade install has been completed.

If a shortcut is set in a program folder on the product before an upgrade

- If you changed the program folder name, the shortcut set on the product before the upgrade is not inherited. If you want to use the shortcut on the product before the upgrade, set a shortcut for the program folder after the upgrade. The shortcut remains for the program folder you used on the product before the upgrade. However, if the shortcut is no longer necessary, delete it.

Before performing a version upgrade install, follow these procedures:

- For JP1/IM - Manager
 - Stop the service (Service name: JP1_Console) of JP1/IM - Central Console.
 - If you have specified a logical host, stop the service(Service name: JP1_Console_Logical host name) of JP1/IM - Manger on the logical host.
 - Close the window if **Services** window or a service on **Manage Computer** window is displayed.
- For JP1/IM - Agent
 - If Logical host service is running, stop the service and then execute the version upgrade installation. If you execute the version upgrade installation while Logical host service is running, file used by Logical host service may be deleted and the service may terminate abnormally.

After performing a version upgrade install, make sure you restart the computer.

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. The following remote installation methods are available:

- Update installation

- For JP1/IM - Manager

The product is installed in the same folder as that of a JP1/IM - Manager instance that has already been installed. The setting information of the JP1/IM - Manager instance that has already been installed is inherited. If JP1/IM - Manager is not installed, updating installation cannot be performed.

- For JP1/IM - Agent

Install it in the same folders as the installed JP1/IM - Agent. Setup of the installed JP1/IM - Agent is inherited. If JP1/IM - Agent is not installed, updating installation cannot be performed.

- For JP1/IM - View

Install it in the same folders as the installed JP1/IM - View. Setup of the installed JP1/IM - View is inherited. If JP1/IM - View is not installed, updating installation cannot be performed.

- New installation

When using the default value for the drive and folder, the product is newly installed.

- For JP1/IM - Manager

- "system-drive:\Program Files\HITACHI\JP1IMM" folder
- " system-drive:\Program Files\HITACHI\JP1Cons" folder
- " system-drive:\Program Files\HITACHI\JP1Scope" folder

- For JP1/IM - Agent

- "system-drive:\Program Files\HITACHI\jp1ima" folder

- For JP1/IM - View

- "system-drive:\Program Files\HITACHI\JP1CoView" folder

When specifying only the drive, the product is installed on the specified drive directly.

When specifying the folder, JP1/IM - Manager is installed in the specified folder.

For details about the actual method and operation, see the manual of JP1/NETM/DM, JP1/IT Desktop Management 2, or Job Management Partner 1/Software Distribution. When you package this software product, you must use the packager of JP1/NETM/DM 09-00 or later, Job Management Partner 1/Software Distribution 09-00 or later, or JP1/IT Desktop Management 2. Note that JP1/NETM/DM is only sold 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 1–6: Windows encoding

OS	Language	Encoding
Windows	Japanese	SJIS
	Chinese	GB18030
	English	C

Important

If you change the system locale while using JP1/IM - View, the behavior of JP1/IM cannot be guaranteed. When you want to change the system locale, you have to first uninstall JP1/IM, change the system locale, and then install JP1/IM again.

(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)

(1) 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.

(2) About Hitachi Network Objectplaza Trace Library (HNTRLib2)

- When you install JP1/IM - View, JP1/IM - Agent, 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 or JP1/IM - Agent, 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.

(3) About the 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 3 - 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.

(4) 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.

(5) About the files and the registry

- Do not perform the following operations, because JP1/IM - Manager and JP1/IM - View manages such information as program information, configuration information, and maintenance information in files and in the registry. If you perform the following operations, JP1/IM - Manager and JP1/IM - View may not work properly.
 - Use an application such as Explorer to delete or change files and folders for JP1/IM - Manager. Or, change the access permissions.
 - Use Registry Editor to delete or change the information on JP1/IM - Manager, or change the access permissions.
- Do not create a file or a folder named *system-drive*: \Program. If a file or folder has the name described above, some problems occur, such as the `jcodbsetup` or `jcfdbsetup` command outputting the following message and terminating abnormally:

```
KNAN11053-E An attempt to read a file failed. (file name = instdb.log)
```

In addition, if a file or folder has the name described above, various programs, including JP1/IM - Manager, might not work normally.

(6) About reinstallation

When JP1/IM - Manager, JP1/IM - View, and JP1/IM - Agent 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, JP1/IM - View, and JP1/IM - Agent, 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.

(7) About downgrade installation

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

(8) About antivirus software

- If antivirus software scans the installation destination while you are installing JP1/IM - Manager, the installation might fail. In this case, there is a conflict between the installer and the antivirus software, which causes an application error. Make sure you terminate antivirus software before performing the installation.
- Before performing installation of JP1/IM - View, be sure to close applications that lock the JP1/IM - View files such as anti-virus software. If you do not close such applications, the installation might fail.
- Before performing a version upgrade installation of JP1/IM - View, be sure to close applications that lock the JP1/IM - View files such as anti-virus software. If you do not close such applications, the installation might fail.
- After upgrading the version of JP1/IM - View, if a message such as the following is output to the event log (application) and JP1/IM - View does not start, restart the OS and then reinstall JP1/IM - View.

```
Windows Installer requires a system restart.  
Product Name: JP1/Integrated Management - View. Product Version: <XXXX>.  
Product Language: XXXX. Manufacturer: Hitachi, Ltd..  
Type of System Restart: X. Reason for Restart: X.
```

(9) About silent installation

JP1/IM - Manager can be installed by using the silent installation functionality. Execute the following command:

```
<DVD-R-media>\_OWNEXE\HPPSINST.BAT /<full-path-of-DISK1-of-target-product> /  
<full-path-of-installation-destination>
```

JP1/IM - View can be installed by using the silent installation functionality. Execute the following command:

```
<DVD-R-media>\_OWNEXE\HPPSINST.BAT /<full-path-of-DISK1-of-target-product> /  
<full-path-of-installation-destination>
```

The silent installation feature provides an installation method for JP1/IM - Agent.

Command

- Case of the offering medium:

```
<DVD-R-media>\_OWNEXE\HPPSINST.BAT /<DVD-R-media>\_PPDIR\PCC2A2C9GDL\DISK  
1 /<full-path-of-installation-destination>
```

- For JP1/IM - Agent packages downloaded from integrated operation viewer:

```
msiexec /i JP1/IM - Agent-Package\DISK1\JP1IMAgent.msi /qn STARTFROM=NETM
```

- To execute the contents of DVD-R media directly from a hard drive, copy the contents of the DVD-R media to a directory on the hard drive whose path does not include any spaces. Then, compare the copied files to the original files (at the binary level, for example) to ensure that they are the same.
- Check the return value of the execution result to verify that the installation ended successfully. For details about the return values, see the JP1 website.
- If you install JP1/IM - Manager, JP1/IM - View, and JP1/IM - Agent with the silent install feature, you can not specify user information. To specify user information, install software product in the installation procedure described in the [1.3.1 Installation procedure \(for Windows\)](#).
- JP1/IM - Agent must be set in setx command prior to installing with the silent install feature.
After silent installation, execute setx command again to clear the user environment variables.

(10) About Windows Defender

If you install JP1/IM - Manager while Windows Defender is enabled, a Windows Defender warning event might be output to the Windows Defender history or event viewer Windows log (system log). This warning can be safely ignored.

(11) About restarting after performing an overwrite installation

When you perform an overwrite installation without using JP1/NETM/DM, you can operate JP1/IM - Manager and JP1/IM - View without restarting your computer, by performing the following procedure.

1. Close the following programs before performing the overwrite installation.
 - JP1/IM - Manager and JP1/IM - View
 - Applications that lock the files in the installation folder for JP1/IM - Manager and JP1/IM - View (such as applications that check for viruses)
 - All services of JP1/Base
 - All services of the products that require JP1/Base
 - Services of the integrated trace function
2. After installing the JP1/IM - Manager and JP1/IM - View, select "No" if you are asked to restart the computer.

(12) When using ReFS

If you install JP1/IM - Manager on Windows Server 2016, Windows Server 2019, Windows Server 2022 or Windows Server 2025 ReFS, performance might decrease compared to installations on NTFS. Therefore, if you use ReFS, conduct sufficient testing of actual operations to make sure that there is no problem with performance. If the performance requirements are not satisfied, consider using NTFS instead of ReFS.

(13) About JP1/IM - View

- Do not apply Windows Server 2016, Windows Server 2019, Windows Server 2022, and Windows Server 2025 data deduplication on the volume on which JP1/IM - View is installed.
- If you attempt to perform an overwrite installation while JP1/IM - View is being used, a dialog box appears. In this case, click the **Cancel** button to abort the overwrite installation, stop all running JP1/IM - View instances, and then retry the overwrite installation of JP1/IM - View.

(14) Notes on upgrading JP1/IM - Agent from version 13-00 or 13-01

- The following vulnerable cipher suites are not supported for certificates required when encrypting communication between JP1/IM agent management base and JP1/IM agent control base:
 - "TLS_RSA_WITH_AES_128_CBC_SHA" up to TLS1.2
 - "TLS_RSA_WITH_AES_256_CBC_SHA" up to TLS1.2
 - "TLS_RSA_WITH_AES_128_GCM_SHA256" (TLS1.2 only)
 - "TLS_RSA_WITH_AES_256_GCM_SHA384" (TLS1.2 only)

If you are using the cipher suites above, change the certificate to use the cipher suites that you want to support. For supported cipher suites, see *Supported Cipher Suites* in 3.15.7(1)(c) *Encrypted communication* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

- If you are using Yet another cloudwatch exporter, make sure that the service-name specified in exportedTagsOnMetrics parameter of Yet another cloudwatch exporter configuration file (jpc_ya_cloudwatch_exporter.yml) is also specified in type of jobs parameter. If not specified, JP1/IM - Agent 13-10 or later Yet another cloudwatch exporter might fail to start this service.

(15) Notes on upgrading JP1/IM - Agent from version 13-00 to 13-10

When JP1/IM - Agent is upgraded, executable row is updated and the first arguments row is added to service definition file shown in the following tables in order to apply OSS wrapper to OSS corresponding to the add-on management function. In JP1/IM - Agent installer log, verify that KAVB9447-I messaging is displayed for the respective service definition file. For details about JP1/IM - Agent installer log, see 12.2.2(8) *Installer Log* in the *JP1/Integrated Management 3 - Manager Administration Guide*.

Add-on program	Service definition file Name	Backup file name
Prometheus server	jpc_prometheus_server_service.xml	jpc_prometheus_server_service.xml.bk
Alertmanager	jpc_alertmanager_service.xml	jpc_alertmanager_service.xml.bk
Windows exporter	jpc_windows_exporter_service.xml	jpc_windows_exporter_service.xml.bk
Blackbox exporter	jpc_blackbox_exporter_service.xml	jpc_blackbox_exporter_service.xml.bk
Yet another cloudwatch exporter	jpc_ya_cloudwatch_exporter_service.xml	jpc_ya_cloudwatch_exporter_service.xml.bk

Add-on program	Service definition file Name	Backup file name
Promitor	jpc_promitor_resource_discovery_service.xml	jpc_promitor_resource_discovery_service.xml.bk
	jpc_promitor_scraper_service.xml	jpc_promitor_scraper_service.xml.bk
Script exporter	jpc_script_exporter_service.xml	jpc_script_exporter_service.xml.bk
Fluentd	jpc_fluentd_service.xml	jpc_fluentd_service.xml.bk
Web exporter	jpc_web_exporter_service.xml	jpc_web_exporter_service.xml.bk
VMware exporter	jpc_vmware_exporter_service.xml	jpc_vmware_exporter_service.xml.bk

If KAVB9448-W and KAVB9450-W messages are displayed, manually edit the appropriate service definition file to update executable line and add the first line of arguments line. For descriptions of executable line and arguments line, see *Service definition file (jpc_program-name_service.xml)* in *Chapter 2. Definition Files* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

(16) Notes on upgrading JP1/IM - Manager from version 13-00 to 13-11 to 13-50 or later

When JP1/IM - Manager is upgraded, the recommended settings for log output of the Intelligent Integrated Management Database are not reflected.

Check the setting values of the following parameters of Intelligent Integrated Management Database configuration file (postgresql.conf). If there are no parameters or the settings are different from those listed below, set them as shown below.

Parameters	Set value
log_min_messages	fatal
log_error_verbosity	terse
log2	on
log2_rotation_count	5
log2_rotation_max_size	70M

For details about the parameters of Intelligent Integrated Management Database configuration file and for information about reflecting changed settings, see *Intelligent Integrated Management Database configuration file (postgresql.conf)* in *Chapter 2. Definition Files* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

1.3.4 How to collect data in installing (for Windows)

(1) How to collect documentation when installing JP1/IM - Manager

The following describes how to collect data if an error occurs during installation.

1. Login to the manager host.
2. Collect the following File manually.
 - **Files under "System-drive:\Windows\Temp\HCDINST\"**

(2) How to collect documentation when installing JP1/IM - Agent

The following describes how to collect data if an error occurs during installation.

1. Login to integrated agent host.
 2. Collect the following File manually.
 - When installed on the provided media:
Files under "System-drive \Window \Temp\HCDINST\"
 - If you installed with a JP1/IM - Agent package downloaded from integrated operation viewer
%TEMP%#\Logfile that was output when installing (MSI*.LOG)
- #: %TEMP% indicates the path specified in the environment-variable TEMP.

1.3.5 How to link with the auto scale function (for Windows)

(1) How to link with the auto-scale function in JP1/IM - Agent

(a) Prerequisite services and conditions

The prerequisite services and conditions for operation corporate with the auto-scale function are as follows:

Prerequisite services

- Amazon EC2
- Amazon EC2 Auto Scaling

Prerequisite conditions

The following describes the prerequisites for operation corporate with the auto-scale function.

- It is not possible to target Logical host in a clustered environment.
- The system should not exceed 2500 units including the manager host.
- After scale-out or scale-in, you must create and reflect system configuration information. For details, see [1.21.2\(19\) Creation and import of IM management node tree data \(for Windows\) \(required\)](#).

(b) Creating a Virtual Machine Image (AMI)

Following are the steps to create a virtual machine image (AMI).

1. Install JP1/IM - Agent.
In this case, select the installation mode **Image creation mode**. For details, see [1.3.1\(3\)\(c\) Initialization environment variable used by the installer](#).
2. Creating a virtual machine image (AMI).
For details about creating a virtual machine image (AMI), see the official Amazon Web Services website.

(c) Creating an Auto Scaling Boot Setup

Following are the steps to create an Auto Scaling boot setup.

1. Open the [Amazon EC2] console from [AWS Management Console].

2. Click [Boot settings].of [Auto Scaling]in the left navigation pane.
3. Click [Create a boot settings].
4. Select the virtual machine image (AMI) created in step 1 from the [Select AMI] window.
5. In the [Detailed settings] window, select [by Text] from [Advanced details] - [User data] and write the following in the text box.
IN Windows

```
<script>
Install-destination\jplima\tools\jimasetup phost
Install-destination\jplima\tools\jpc_service_start -s all
</script>
```

1.3.6 Cloning a Virtual Machine (for Windows)

On the following virtualization platforms, you can clone a virtual machine from a virtual machine template in an integrated agent host deployment where you installed JP1/IM - Agent in imaging mode.

- VMware ESX
- Hyper-V
- SCVMM

(1) Prerequisites

The following are the prerequisites for replicating agent:

- You can only clone virtual machines on agent hosts. Also, it cannot target logical hosts in a cluster environment.
- Agent configuration can have up to 2500 hosts, including manager hosts.
- When creating a virtual machine template, select Image creation mode for JP1/IM - Agent install mode.

(2) How to Create a Virtual Machine Template

The following describes how to create a VM template.

1. Install JP1/IM - Agent on the virtual machine.

Select [Image creation mode] as the installation mode during installation.

For details about how to install the software, see [1.3.1\(3\) Procedure of JP1/IM - Agent installation](#).

Important

JP1/IM - Agent is not initialized.

(3) How to Clone a Virtual Machine

The following shows how to clone a virtual machine.

1. Clone a new virtual machine from a virtual machine template.

See virtualization software documentation for details about the replication features provided by virtualization platforms.

Check OS specifications for the tasks required by OS for duplication.

2. Start a new virtual machine.

3. Change the host name of the new virtual machine.

If necessary, change the host name of the virtual machine.

4. Change IP of the new virtual machine.

Change IP addressing of the virtual machine as needed.

For the procedure to be performed when IP address is changed, see *2.3.1(3) Tasks to be performed when IP address for agent is changed* in the *JP1/Integrated Management 3 - Manager Administration Guide*.

5. Perform JP1/IM - Agent initialization.

Run initial setting command of JP1/IM - Agent.

```
JP1/IM-Agent-Installation-destination-folder\jplima\tools\jimasetup phost
```

6. Refresh the tree of IM managed nodes on JP1/IM - Manager to which JP1/IM - Agent is connected.

For details, see *1.21.2(19) Creation and import of IM management node tree data (for Windows) (required)*.

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 or the Intelligent Integrated Management Base are 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 *2.6 Functions provided by the IM database* in the *JP1/Integrated Management 3 - 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/IM3 - Manager Service. See *3.1.1 In Windows* in the *JP1/Integrated Management 3 - Manager Administration Guide* to use the startup control function to set it.

JP1 events obtained from the event database after the JP1/IM3-Manager service has started are stored in the integrated monitoring database. For details, see *4.1.3(2) JP1 event control when using the integrated monitoring database* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

This section explains how to create an IM database.

Important

In operation in Amazon EC2 instance environment, host name can be longer than 32 characters (e.g., ip-xx-xx-xx-xx.ap-northeast-1.compute.internal(xx-xx-xx-xx means IP address). When setting up IM database, if host name of IM database exceeds the maximum (32 characters), the setup fails with an KNAN11141-E error message. Therefore, change it to a host name that does not exceed the 32-character limit according to how you permanently assign a static host name to Amazon EC2 instance that AWS exposes.

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
IMDBENVDIR=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 JP1/Integrated Management 3 - Manager Command, Definition File and API 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 IMDBENVDIR and IMDBDIR.

3. In case of existing the Application Experience service, verify that the startup type of the Application Experience service is not disabled.

If you specify Disabled for the service, executing the `jcodbsetup` command or `jcfdbsetup` command might result in the IM database setup failing with the following message:

KNAN11141-E An error occurred during the creation of a system database area. (Error code: -1073741811)

Important

- Do not specify a path of 200 or more bytes for the system environment variable TEMP. If a path is 200 bytes or more, a setup or unsetup of the IM database might fail. If setup fails, revise the value of the system environment variable TEMP, and then unsetup the integrated monitoring database and the IM Configuration Management database. Then, set them up again. If unsetup fails, revise the value of system environment variable TEMP, and then perform unsetup for the integrated monitoring database and the IM Configuration Management database.
- Make sure that there are sufficient disk space allocated under *Manager-path* while executing the `jcodbsetup` or `jcfdbsetup` command. If disk space is not enough, the `jcodbsetup` or `jcfdbsetup` command outputting the following message and terminating abnormally:
KNAN11053-E An attempt to read a file failed. (file name = instdb.log)

1.4.2 Setting up the integrated monitoring database (for Windows)

Create an integrated monitoring database and use the Intelligent Integrated Management Base or 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/IM3-Manager Service. The following are the setup procedures for the two cases.

- To stop JP1/IM3-Manager Service and set up the integrated monitoring database:
 1. Check if the IM database service (JP1/IM3-Manager DB Server) is running.
 2. Stop the following services:
 - JP1/IM3-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/IM3-Manager Service.

- To set up the integrated monitoring database without stopping JP1/IM3-Manager Service:

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

```
jcoimdef -cf OFF
```

2. Restart JP1/IM3-Manager Service.

3. Check if the IM database service (JP1/IM3-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/IM3-Manager Service.

For details about the `jcodbsetup` command, see *jcodbsetup* in *Chapter 1. Commands in the JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

For details about the `jcoimdef` command, see *jcoimdef* in *Chapter 1. Commands in the JP1/Integrated Management 3 - Manager Command, Definition File and API 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/IM3-Manager Service.

For details about the `jcodbsetup` command, see *jcodbsetup* in *Chapter 1. Commands in the JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

For details about the `jcoimdef` command, see *jcoimdef* in *Chapter 1. Commands* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API 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/IM3-Manager Service. The following are the setup procedures for the two cases.

- To stop JP1/IM3-Manager Service and set up the IM Configuration Management database:
 1. Check if the IM database service (JP1/IM3-Manager DB Server) is running.
 2. Stop the following services:
 - JP1/IM3-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/IM3-Manager Service:
 1. Execute the `jcoimdef` command to disable the integrated monitoring database.
`jcoimdef -db OFF`
 2. Restart JP1/IM3-Manager Service.
 3. Check if the IM database service (JP1/IM3-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 *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

For details about the `jcoimdef` command, see *jcoimdef* in *Chapter 1. Commands in the JP1/Integrated Management 3 - Manager Command, Definition File and API 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 JP1/Integrated Management 3 - Manager Command, Definition File and API 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 (`jcfmain`).

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

For details about the `jcoimdef` command, see *jcoimdef* in *Chapter 1. Commands in the JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

For details about the `jco_spmc_status` command, see *jco_spmc_status* in *Chapter 1. Commands in the JP1/Integrated Management 3 - Manager Command, Definition File and API 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:

If the status are different from the following status, start or stop the services to create the following status.

- If JP1/IM - MO is being used, the JP1/IM - Message Optimizer service of JP1/IM - MO is stopped at the connection source.
- If JP1/OA is receiving JP1 event from JP1/IM3 - Manager, JP1/OA is stopped at the connection source.
- JP1/IM3-Manager DB Server Service is running.

- JP1/IM3-Manager Service is stopped.
2. Execute the `jimdbupdate` command to check if the IM databases have been updated.
 - 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 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.`
`KNAN11211-I An update of the configuration files 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. Stop the following service:
 - JP1/IM3-Manager DB Server Service
 6. Start the following service:
 - JP1/IM3-Manager DB Server Service
 7. Start the following services:
 - JP1/IM3-Manager Service
 8. If the following services were stopped in step 1, start the services.
 - JP1/IM - Message Optimizer service of JP1/IM - MO on the connection source (If using JP1/IM - MO)
 - JP1/OA on the connection source (If JP1/OA is receiving JP1 event from JP1/IM3 - 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.

1.5 Construction of Intelligent Integrated Management Database (for Windows)

If you are using Intelligent Integrated Management Database, execute the setup command (jimgndbsetup command) manually after installing JP1/IM - Manager.

By constructing Intelligent Integrated Management Database, you can create a DB for managing the various types of information shown in 2.7.1(1)(a) *Database configuration* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*. This enables you to manage the data used by the various functions.

The procedure for building the Intelligent Integrated Management Database is described below.

1.5.1 Preparations for Building Intelligent Integrated Management Database (for Windows)

Prepare an *Intelligent Integrated Management Database setup information file* that contains the definitions required to build the Intelligent Integrated Management Database.

See *Intelligent Integrated Management Database setup information file (jimgndbsetupinfo.conf)* in *Chapter 2. Definition Files* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*, for editing Intelligent Integrated Management Database setup information file.

1.5.2 Settings of Intelligent Integrated Management Database (for Windows)

Create an Intelligent Integrated Management Database and configure the Intelligent Integrated Management Base to use the Intelligent Integrated Management Database. If you are not using the Intelligent Integrated Management Database, this step is not required.

Here are the steps to set it up:

1. Run the jimgndbsetup command to create the Intelligent Integrated Management Database.

```
jimgndbsetup -f Intelligent-Integrated-Management-Database-setup-information-file
```

For details of jimgndbsetup command, see *jimgndbsetup* in *Chapter 1. Commands* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

1.5.3 Excluding settings in security product(for Windows)

If you want to perform a virus check during JP1/IM - Manager is operating, exclude the following files and folders from scanning: Also, if you perform a virus check on outage and restart JP1/IM - Manager, make sure that the virus check is completed to the following files and folders:

Files and Folders in JP1/IM - Manager (for Windows)

- All files and folders under "*Storage destination of execution file of storage Intelligent Integrated Management Database*\".#
- All files and folders under "*Storage destination of data file of storage Intelligent Integrated Management Database*\".#
- All files and folders under "*Storage destination of associated library of storage Intelligent Integrated Management Database*\".#
- All files and folders under "*Storage destination of setting file of storage Intelligent Integrated Management Database*\".#
- All files and folders under "*Storage destination of operation command of storage Intelligent Integrated Management Database*\".#
- All files and folders under "*Storage destination of individual log of operation command of storage Intelligent Integrated Management Database*\".#
- All files and folders under "*Storage destination of Trend Data Management Service log*\".#

For details of the above storage destinations, see (1)(d) *Where related files are stored* in 2.7.1 *Intelligent Integrated Management Database* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

For Logical host, you should also exclude files and folders under shared folders from scanning:

- All files and folders under "*Shared Folders*\JP1\IMm\"
- All files and folders under "*Storage destination of Logical host's Intelligent Integrated Management Database data files*\"

#

Exclude if you are setting up the Intelligent Integrated Management database.

1.6 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 3 - Manager Administration Guide*.

1.7 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 1–7: 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 1–8: 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 `jpladmin` is registered by default. For `jpladmin`, operation permissions whose JP1 resource group is `*` and JP1 authority level is `JP1_Console_Admin` have been set (JP1 resource group `*` can access all JP1 resource groups).

1.7.1 Specifying the authentication server (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*.

1.7.2 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.

1.7.3 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 *9.4.1 Managing JP1 users* and *Appendix E. Operating Permissions* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

1.7.4 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.

1.7.5 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*.

1.8 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*.

1.9 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 [1.10 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.

1.9.1 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 [8.2.1 Hierarchical configurations managed by IM Configuration Management](#) in the *JP1/Integrated Management 3 - 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](#).

1.9.2 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](#).

1.9.3 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](#).

1.10 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 [1.9 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 [9.4.3 Managing the system hierarchy in the JP1/Integrated Management 3 - Manager Overview and System Design Guide](#).

1.10.1 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 `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.

1.10.2 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*.

1.10.3 Changing the configuration definition information (for Windows)

If you change the configuration definition information, follow the same procedure as in [1.10.1 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 [1.10.2 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 [1.10.1 Setting the configuration definition information \(for Windows\)](#).

1.10.4 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*.

1.11 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` and `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 `SYSTEM` and `root`. If `SYSTEM` and `root` are 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.

1.12 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 [1.9 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](#).

1.13 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 [1.10 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*.

1.14 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](#).

1.15 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*.

1.16 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.

1.16.1 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 the chapter that environment variable file in the *JPI/Base User's Guide*.
- Host group definition
See the chapter that Host group definition file in the *JPI/Base User's Guide*.
- Creation of a command button definition file
See *Command button definition file (cmdbtn.conf)* in *Chapter 2. Definition Files* in the *JPI/Integrated Management 3 - Manager Command, Definition File and API 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 *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

1.16.2 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 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 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 *JP1/Integrated Management 3 - Manager Command, Definition File and API 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 *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

1.17 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.

1.17.1 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.

1.17.2 Setting method (for Windows)

You must release the dependencies between JP1/IM3-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/IM3-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 *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

1.17.3 Startup method (for Windows)

Because no dependencies are set between JP1/IM3-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/IM3-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/IM3-Manager Service.

1.18 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 *13.5.2 Managing the remote monitoring configuration* in the *JP1/Integrated Management 3 - 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 *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

1.18.1 Configuring WMI (for Windows)

This subsection describes how to configure WMI.

WMI connections require the following:

- WMIC enabling

If the JP1/IM - Manager host or remotely monitored host is running Windows Server 2025, WMIC must be enabled on that host.

- 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) Enabling WMIC

If the JP1/IM - Manager host or remotely monitored host is running Windows Server 2025, WMIC must be enabled on that host.

Please follow the steps below to enable WMIC.

1. Log in to the Windows Server 2025 host using an account with Administrator privileges.
2. Open the Command Prompt with Administrator privileges and run the following command to install WMIC.

```
Dism /Online /Add-Capability /CapabilityName:WMIC~~~~
```

The installation process may take some time.

3. Display the WMIC status by executing the following command.

```
Dism /Online /Get-CapabilityInfo /CapabilityName:WMIC~~~~
```

If "State : Installed" is displayed, WMIC has been successfully enabled.

(2) 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**.

(3) 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.

(4) 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.

(5) Setting up UAC

In the monitoring-target settings, if a user who has administrator privileges other than Administrator privileges is specified, 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**.

(6) 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 `ntlm: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 `ntlm domain:`.

- 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.

1.18.2 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.

1.18.3 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 or AIX: `/etc/ssh/sshd_config`
3. Set `yes` for `PubkeyAuthentication`^{#1}.
4. Set `no` for `UseDNS`^{#1, #2}.
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 9 example)
`systemctl restart sshd.service`
 - For AIX (AIX 7.3 example)
`stopsrc -s sshd`
`startsrc -s sshd`

#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.

1. Installation and Setup (for Windows)

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`.

(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 [1.18.3\(2\) 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. Grant appropriate access permissions so that the placed private key file is not accessed by OS users without administrator privileges. 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 [5.20 System Common Settings window](#) in the *JP1/Integrated Management 3 - 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 [1.18.3\(2\) 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 [1.18.3\(2\) 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 [1.18.3\(2\) 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 Linux) `wc -l monitored-log-file-path`

Example of executing the command:

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

Example of execution result:

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

- `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 AIX) `/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
```

1.18.4 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 (`jplcf_remote_logtrap.conf`).

Manager-path\conf\imcf

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

`jbssetcnf Manager-path\conf\imcf\jplcf_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 (`jplcf_remote_logtrap.conf`)

For details, see *Remote log trap environment definition file (jplcf_remote_logtrap.conf)* in *Chapter 2. Definition Files* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

1.19 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.

1.19.1 Editing Configuration file of JP1/IM - Manager (for Windows)

There are two ways to change configuration files:

- The way to use integrated operation viewer
- The way to Login the host and setup

For configuration file that can be edited when integrated operation viewer is used, see the notes of the definition file for JP1/IM - Manager in *List of definition files* in *Chapter 2. Definition Files* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*. If you want to Login and Setup the host, all configuration files can be edited.

The following are the steps for setting:

- How to use integrated operation viewer

1. Download configuration files from integrated operation viewer.
If you add File, it does not need to be downloaded.
2. Edit the downloaded File.
3. Use integrated operation viewer to upload the edited File.
Setup is automatically reflected when uploaded.

- How to Login and Setup the Hosts

1. Login to the manager host.
2. Stop JP1/IM - Manager services.
3. To edit the configuration files.
4. Start the service.

1.19.2 Settings for using the functions of the Intelligent Integrated Management Base (for Windows)

When you install JP1/IM - Manager for the first time, the functions of the Intelligent Integrated Management Base are disabled by default.

To use the functions of the Intelligent Integrated Management Base, perform the following steps:

1. Set the integrated monitoring database.
2. Setup Intelligent Integrated Management Database.

3. Enable event source host mapping.

Execute `jcoimdef -hostmap ON`.

4. Enable the Intelligent Integrated Management Base service (`jddmain`).

Execute `jcoimdef -dd ON`.

5. Start JP1/IM - Manager.

6. Confirm that the Intelligent Integrated Management Base service is up and running.

Execute the `jco_spmdd_status` command. Confirm that `jddmain` is displayed as an active process.

For details about the integrated monitoring database, see [1.4.2 Setting up the integrated monitoring database \(for Windows\)](#).

For details about Intelligent Integrated Management Database, see [1.5.2 Settings of Intelligent Integrated Management Database \(for Windows\)](#).

For details about the `jcoimdef` command, see `jcoimdef` in *Chapter 1. Commands in the JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

Important

Once you configure the Intelligent Integrated Management Base, it will take longer for the JP1/IM3-Manager service to start. If your clustering software monitors the start-up time of the JP1/IM3-Manager service or the startup control of JP1/Base is used to start the JP1/IM3-Manager service, you need to check and, if necessary, revise the timeout value of the software. After configuring the Intelligent Integrated Management Base, check the start-up time of the service and adjust the timeout value.

1.19.3 Setup When Using JP1/IM - Agent as an agent

(1) Changing the settings of JP1/IM agent management base

(a) Common way to setup

■ To edit the configuration files (for Windows)

Configuration file is located in the following directories:

OS	Storage destination
Windows	<code>Manager-path\conf\imdd\plugin\jplpccs\</code> <code>Manager-path\conf\imdd\imagent\</code>
Linux	<code>/etc/opt/JPlimm/conf/imdd/plugin/jplpccs/</code> <code>/etc/opt/JPlimm/conf/imdd/imagent/</code>

There are two ways to change configuration file:

- The way to use integrated operation viewer
- The way to Login the host and Setup

For configuration file that can be edited when integrated operation viewer is used, see the notes of the definition file for JP1/IM - Manager in *List of definition files* in *Chapter 2. Definition Files* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*. If you want to Login and Setup the host, all configuration files can be edited.

The following are the steps for setting:

- How to use integrated operation viewer

1. Download configuration file from integrated operation viewer.
If you add File, it does not need to be downloaded.

2. Edit the downloaded File.

3. Use integrated operation viewer to upload the edited File.
Setup is automatically reflected when uploaded.

- How to Login and Setup the Hosts

1. Login to the Integration Manager host.

2. Stop JP1/IM - Manager servicing.

For details about how to stop the service, see *3.2 Stopping JP1/IM - Manager* in the *JP1/Integrated Management 3 - Manager Administration Guide*.

3. To edit the configuration file

4. Start the service.

For details about how to start the service, see *3.1 Starting JP1/IM - Manager* in the *JP1/Integrated Management 3 - Manager Administration Guide*.

(b) Change settings of JP1/IM agent management base (for Windows)

The following describes how to change setup of JP1/IM agent management base (imbase,imbaseproxy).

■ Change configuration file of JP1/IM agent management base

JP1/IM agent management base's configuration file are imbase configuration file (jpc_imbase.json) and imbaseproxy configuration file (.json).

For configuration file editing procedure, see *1.19.3(1)(a) Common way to setup*.

■ Changing JP1/IM agent management base ports

Perform the following steps:

1. Stop JP1/IM - Manager.

2. Change the listen port number of JP1/IM agent management base.

The listen port number is set to JP1/IM agent management base's imbase configuration file (jpc_imbase.json) and imbaseproxy configuration file (jpc_imbaseproxy.json) port member. Change this to the new port number.

For details on imbase configuration file and imbaseproxy configuration file, see the description of the appropriate file in *Chapter 2. Definition Files* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

3. Starts JP1/IM - Manager.

If the listen Port number of the JP1/IM agent management base is changed in an environment that is already in operation, the destination port number of the JP1/IM agent control base must also be changed.

■ Setup the certificate

To encrypt communication between JP1/IM3-Manager and JP1/IM3-Agent, perform the following steps:

1. Stop JP1/IM - Manager.

2. Change Server certificate and keying File for JP1/IM agent management base.

The listen port number is set to a member of the cert_file or key_file of imbase shared configuration file (jjpc_imbasecommon.json).

Updates Setup Value of cert_file or key_file, or File that you set itself.

For details of imbase shared configuration file, see the explanation of appropriate file in *Chapter 2. Definition Files* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

3. Starts JP1/IM - Manager.

■ Setup event-forwarding relay function (optional)

If you use event-forwarding relay function, JP1/IM - Manager must be 13-01 or later.

The following describes how to configure JP1/IM - Manager to enable event-forwarding relay function.

1. Stop JP1/IM - Manager servicing.

For a cluster configuration, stop the service from the cluster software.

2. Open imbase configuration file (jpc_imbase.json) and set the jp1base_forward_send items.

- When JP1/IM - Manager 13-10 or later is newly installed

The jp1base_forward_send items are listed in imbase configuration file, but because they are commented like `"/jp1base_forward_send"`, remove the leading `"/"`.

- Upgrading from a version earlier than JP1/IM - Manager 13-10

Imbase configuration file refers to imbase configuration file model file, because the jp1base_forward_send items are not listed. When writing, remove the leading `"/"`.

3. Set port below the jp1base_forward_send items in imbase configuration file.

Specifies the port for event-forwarding for JP1/Base that reside together.

If you specify a service name, set the service name and TCP in services file.

4. Start JP1/IM - Manager servicing.

For a cluster configuration, start the service from the cluster software.

To disable the event forwarding function, follow the same steps as above and comment out the jp1base_forward_send items as `"/jp1base_forward_send"` or remove the jp1base_forward_send items in step 2.

(c) Creation and import of IM management node tree data (for Windows) (required)

Follow the steps below to create and import IM management node tree.

1. Perform the steps in integrated agent host.

Follow steps 1 to 4 in *1.21.2(19) Creation and import of IM management node tree data (for Windows) (required)*.

2. Run JP1/IM - Manager's `jddcreatetree` command/create IM managed node-related API.

If the execution fails, follow the instructions in Message and execute again.

3. If add-on program or user-defined Prometheus or Fluentd configuration changes or deletions are made and trend data saved in Trend data Management Database is not required prior to the configuration change, delete the trend data and then execute `jddcreatetree` command or IM control node-related information generation API of JP1/IM - Manager.

Deleting trend data deletes all trend data saved by Prometheus and Fluentd (including user-defined Prometheus and user-defined Fluentd) on the specified host. If you want to retain trend data for add-on program that has not made any configuration changes, run `jddcreatetree` command in JP1/IM - Manager or the Generate IM Administration Node-related Information API without deleting trend data.

If execution fails, take corrective action according to the contents of the message and re-execute.

For details on how to delete trend data, see the following sections:

- *2.2.1 List of Integrated Agents window in the JP1/Integrated Management 3 - Manager GUI Reference*
- *5.11.4 Delete Trend Data and 5.18.2 Delete integrated agent info in the JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*

4. When add-on program or user-defined Prometheus or Fluentd configuration is changed or deleted, IM management node-related files described in "*Editing IM management node-related files*" below is edited (it is not necessary to perform it when building a new system).

5. Execute `jddupdatetree` command of JP1/IM - Manager (configuration change mode) or the import API of IM control node-related information.

If the execution fails, follow the instructions in Message and execute again.

6. Display integrated operation viewer and verify that IM management node is created correctly.

If it is not created correctly, review settings in integrated agent, add-on program, user-defined Prometheus or Fluentd that was not created, and then repeat the procedure from step 2.

- Editing IM management node-related files

If add-on program, or user-defined Prometheus or Fluentd configuration changes (configuration changes or deletions) are made, a pre-configuration IM management node is created until those sample are removed from Trend data Management Database. For the timing when trend data is deleted, see *2.7.2 Trend data Management Database in the JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

If you do not want to create a pre-configuration IM management node, you can modify IM management node file and IM management node tree file output by `jddcreatetree` command. For details on IM management node tree file, see *3.5.3 IM management node-related files in the JP1/Integrated Management 3 - Manager Overview and System Design Guide*. Copy the file to make a backup before editing.

- Editing IM management node Files

`Jddcreatetree` command-generated IM management node file (filename: `imdd_node_HITACHI_JP1_JPCCS_CONFINFO_JP1 hostname.json`) also displays /IM-Manager's pre-configuration OOE. When the setting is changed, SID of the configuration information is the same before and after the change, and SID of the second and subsequent configuration information is output with the suffix "-xx"(xx are numbered from 01 to 99).

If you do not need IM management node prior to the configuration change, remove IM management node object from `jddcreatetree` before the configuration change by editing IM management node file. The format of IM management node file is shown below.

```
{
  "meta": {
    ...
  },

```

```

"simtData": [
  Objects in IM management node,
  ...
]
}

```

An object of IM management node is an element of an array of simtData in the following format:

- IM management node Object-Format

```

{
  "sid": "SID Configuration",
  "value": {
    ...
    "property": {
      Displayed in IM management node Properties,
    },
    "jplim_TrendData_labels": {
      Values for identifying trend data
    },
    ...
  }
}

```

Review the values that you want to see in the properties of IM management node and the values to identify the trend data. Remove the objects in IM management node prior to the configuration change. For the values displayed in the properties of IM management node, see *3.15.6(1)(f) Property display* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*. The values shown in the following table are set as values for identifying trend data.

Key	Value Description
jpl_pc_prome_hostname	Hostname of Prometheus server This is the setting for the jpl_pc_prome_hostname of Prometheus configuration file. For log-monitored SID, this key/value is not displayed.
job	Scrape job name This is the setting for job_name in Prometheus configuration file. For log-monitored SID, or SID of kubernetes, this key/value is not printed.
instance	Instance Name This is specified in targets of the discovery configuration file.
jpl_pc_nodelabel	Label-name of IM management node This is the scrape_configs or metrics_scrape_configs of Prometheus configuration file or the jpl_pc_nodelabel tag for AWS resource.

When deleting an object of IM management node that does not have "-xx" at the end of SID of the configuration information and leaving an object of IM management node that has "-xx" at the end, delete and save the "-xx" at the end of SID of the configuration information to be left.

The following shows an example of editing when Node exporter port number is changed.

In this example, the port number before the change is 20716 and the port number after the change is 29999.

- Sample Pre-Edit IM management node Files

```

{
  "meta":{
    ...
  },
  "simtData": [

```



```

...
{
  "sid": "_JP1PC-IMB_MHOST/_JP1PC-M_AHOST/_JP1PC-AHOST_AHOST/_HOST_AHOST/_JP1PC-A_Linux%20metric%20collector%28Node%20exporter%29",
  "value": {
    "component": "/HITACHI/JP1/JPCCS/CONFINFO",
    "category": "platform",
    "visible": true,
    "label": "Linux metric collector(Node exporter)",
    "property": {
      "jpl_pc_prome_hostname": "ahost",
      "job": "jpc_node",
      "jpl_pc_exporter": "JPC Node exporter",
      "jpl_pc_trendname": "node_exporter"
    },
    "jplim_TrendData_labels": {
      "jpl_pc_prome_hostname": "ahost",
      "job": "jpc_node",
      "instance": "ahost:20716",
      "jpl_pc_nodelabel": "Linux metric collector(Node exporter)"
    },
    "methods": [
      "__metricListGet",
      "__timeSeriesDataGet"
    ]
  }
},
{
  "sid": "_JP1PC-IMB_MHOST/_JP1PC-M_AHOST/_JP1PC-AHOST_AHOST/_HOST_AHOST/_JP1PC-A_Linux%20metric%20collector%28Node%20exporter%29-01",
  "value": {
    "component": "/HITACHI/JP1/JPCCS/CONFINFO",
    "category": "platform",
    "visible": true,
    "label": "Linux metric collector(Node exporter)",
    "property": {
      "jpl_pc_prome_hostname": "ahost",
      "job": "jpc_node",
      "jpl_pc_exporter": "JPC Node exporter",
      "jpl_pc_trendname": "node_exporter"
    },
    "jplim_TrendData_labels": {
      "jpl_pc_prome_hostname": "ahost",
      "job": "jpc_node",
      "instance": "ahost:29999",
      "jpl_pc_nodelabel": "Linux metric collector(Node exporter)"
    },
    "methods": [
      "__metricListGet",
      "__timeSeriesDataGet"
    ]
  }
},
...
]
}

```

Deletes IM management node object whose instance is set to ahost:20716, and removes-xx at the end of the configuration SID that you want to keep. The edited IM management node filename is shown below.

- Sample IM management node Files After Editing

```
{
  "meta":{
    ...
  },
  "simtData": [
    ...
    {
      "sid": "_JP1PC-IMB_MHOST/_JP1PC-M_AHOST/_JP1PC-AHOST_AHOST/_HOST_AHOST/_JP1PC-A_Linux%20metric%20collector%28Node%20exporter%29",
      "value": {
        "component": "/HITACHI/JP1/JPCS/CONFINFO",
        "category": "platform",
        "visible": true,
        "label": "Linux metric collector(Node exporter)",
        "property": {
          "jpl_pc_prome_hostname": "ahost",
          "job": "jpc_node",
          "jpl_pc_exporter": "JPC Node exporter",
          "jpl_pc_trendname": "node_exporter"
        },
        "jplim_TrendData_labels": {
          "jpl_pc_prome_hostname": "ahost",
          "job": "jpc_node",
          "instance": "ahost:29999",
          "jpl_pc_nodelabel": "Linux metric collector(Node exporter)"
        },
        "methods": [
          "__metricListGet",
          "__timeSeriesDataGet"
        ]
      }
    },
    ...
  ]
}
```

- Editing IM management node tree file

IM management node tree file output by jddcreatetree command. is edited.

If you delete the configuration, delete the description of the tree object of the deleted IM management node.

When the setting is changed, the description of SID of the configuration information to which "-xx" is added at the end of SID of the configuration information is deleted from target array.

The following shows an example of editing when Node exporter setting is changed.

- Pre-Edit IM management node tree file Sample

```
{
  "meta":{
    ...
  },
  "simtData": [
    ...
    {
```

```

        "sid": "_ROOT_AllSystems/_HOST_AHOST/_CATEGORY_platform/_OBJECT_JP1P
C-A_Linux%20metric%20collector%28Node%20exporter%29",
        "value": {
            "target": [
                "_JP1PC-IMB_MHOST/_JP1PC-M_AHOST/_JP1PC-AHOST_AHOST/_HOST_AHOST/
_JP1PC-A_Linux%20metric%20collector%28Node%20exporter%29"
            ],
            "label": "Linux metric collector(Node exporter)"
        }
    },
    {
        "sid": "_ROOT_AllSystems/_HOST_AHOST/_CATEGORY_platform/_OBJECT_JP1P
C-A_Linux%20metric%20collector%28Node%20exporter%29-01",
        "value": {
            "target": [
                "_JP1PC-IMB_MHOST/_JP1PC-M_AHOST/_JP1PC-AHOST_AHOST/_HOST_AHOST/
_JP1PC-A_Linux%20metric%20collector%28Node%20exporter%29-01"
            ],
            "label": "Linux metric collector(Node exporter)"
        }
    },
    ...
]
}

```

- Sample IM management node tree file After Editing

```

{
  "meta":{
    ...
  },
  "simtData": [
    ...
    {
      "sid": "_ROOT_AllSystems/_HOST_AHOST/_CATEGORY_platform/_OBJECT_JP1P
C-A_Linux%20metric%20collector%28Node%20exporter%29",
      "value": {
        "target": [
            "_JP1PC-IMB_MHOST/_JP1PC-M_AHOST/_JP1PC-AHOST_AHOST/_HOST_AHOST/
_JP1PC-A_Linux%20metric%20collector%28Node%20exporter%29"
        ],
        "label": "Linux metric collector(Node exporter)"
      }
    },
    ...
  ]
}

```

- What happens when IM management node-related files is not edited

If you do not edit IM management node-related files, IM management node are created until the old sample is removed from Trend data Management Database. For configuration changes, JP1 events issued by add-on program, or user-defined Prometheus and Fluentd are mapped to IM management node without "-xx" at the end of the configuration SID.

(d) Settings of product plugin (for Windows)

This section explains how to set product plugin.

■ Define metric to Trend (optional)

Define metric to be displayed in the [Trend] tabbed page of integrated operation viewer in metric Defined File. The primary metric is initially setup. For details about the metric definition file, see the description of each metric definition file in *Chapter 2. Definition Files in the JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

To use the service monitoring function, configure the following settings. However, if you do not want to add metrics to display in the Trends tab, this setting is not required.

- When monitoring service with the Windows version of JP1/IM - Agent

Edit the Windows exporter (service monitoring) metric definition file (`metrics_windows_exporter_service.conf`). For details about the Windows exporter (service monitoring) metric definition file, see *Windows exporter (service monitoring) metric definition file (metrics_windows_exporter_service.conf)* in *Chapter 2. Definition Files in the JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*. For the initial value of this metric definition file, see *Model file settings (initial status) in Windows exporter (service monitoring) metric definition file (metrics_windows_exporter_service.conf)*.

- When monitoring service with the Linux version of JP1/IM - Agent

Edit the Node exporter (service monitoring) metric definition file (`metrics_node_exporter_service.conf`). For details about the Node exporter (service monitoring) metric definition file, see *Node exporter (service monitoring) metric definition file (metrics_node_exporter_service.conf)* in *Chapter 2. Definition Files in the JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*. For the initial value of this metric definition file, see *Model file settings (initial status) in Node exporter (service monitoring) metric definition file (metrics_node_exporter_service.conf)*. If you newly installed JP1/IM - Manager 13-50 or later, promql range vector selector in metric definition-file (value specified in square brackets []) is set to `"$stepTime{minSeconds="minimum-seconds"}"`.

When upgrading JP1/IM - Manager from versions 13-00 to 13-11 to version 13-50 or later, the range vector selector in promql of metric definition file does not have `"$stepTime{minSeconds="minimum-seconds"}"`. The values set in JP1/IM - Manager 13-00 to 13-11 are inherited (the default is "2m"). In this case, if you want to specify `"$stepTime{minSeconds="minimum-seconds"}"` as the promql range vector selector in the metric definition file, you must edit the metric definition file to specify it.

For details about the value of the range vector selector specified in promql of metric definition file, see *3.15.6(4)(c) About Performance Data to Retrieve in the JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

■ Setup AWS definition file (optional)

When monitoring with Yet another cloudwatch exporter, specify the mapping between the account ID of AWS that you want to use monitoring with Yet another cloudwatch exporter, and the account strings that setup to SID and IM management node properties by editing AWS definition file.

For details about AWS definition file, see *AWS definition file (aws_settings.conf)* in *Chapter 2. Definition Files in the JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

■ Edit system node definition file (imdd_systemnode) (Required only when using Yet another cloudwatch exporter)

If you want to monitor using Yet another cloudwatch exporter of add-on program and create a system node, setup system node definition file (imdd_systemnode) of JP1/IM - Manager.

This setup is mandatory if you want to monitor it using add-on program's Yet another cloudwatch exporter.

When creating system node shown in 3.15.6(1)(i) *Tree Format* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*, specify the following settings by editing system node definition file (imdd_systemnode). For setting items not listed here, specify an arbitrary value.

Item nam	Description
displayName	Specifies the name [#] of the service that publishes Amazon CloudWatch metric.
type	The slash (/) must be changed to a hyphen (-).
name	Specify the following string: [{"*":"regexp"}]

#

Indicates what is on Web of Amazon CloudWatch.

When configuring a system-managed node for AWS namespace monitored by Yet another cloudwatch exporter metric definition file (metrics_ya_cloudwatch_exporter).conf default settings, the following is a sample of the values to be set for the items in system node definition file.

displayName	type	name
Amazon Simple Storage Service	JP1PC-AWS-S3	[{"*":"regexp"}]
AWS Lambda	JP1PC-AWS-LAMBDA	
Amazon DynamoDB	JP1PC-AWS-DYNAMODB	
AWS Step Functions	JP1PC-AWS-STATES	
Amazon Simple Queue Service	JP1PC-AWS-SQS	
Amazon Elastic Container Service	JP1PC-AWS-ECS	
Amazon Elastic Block Store	JP1PC-AWS-EBS	
Amazon Elastic File System	JP1PC-AWS-EFS	
FSx File System	JP1PC-AWS-FSX	
Simple Notification Service	JP1PC-AWS-SNS	
Relational Database Service	JP1PC-AWS-RDS	

If you set the above content to system node definition file, it will be as follows.

```
{
  "meta":{
    "version":"2"
  },
  "allSystem":[
    {
      "id":"strageSystem",
      "displayName":"Amazon Simple Storage Service",
      "objectRoot":[
        {
          "type":"JP1PC-AWS-S3",
          "name":[{"*":"regexp"}]
        }
      ]
    }
  ],
}
```

```

{
  "id": "lambda",
  "displayName": "AWS Lambda",
  "objectRoot": [
    {
      "type": "JP1PC-AWS-LAMBDA",
      "name": [{".*": "regexp"}]
    }
  ]
},
{
  "id": "dynamodb",
  "displayName": "Amazon DynamoDB",
  "objectRoot": [
    {
      "type": "JP1PC-AWS-DYNAMODB",
      "name": [{".*": "regexp"}]
    }
  ]
},
{
  "id": "states",
  "displayName": "AWS Step Functions",
  "objectRoot": [
    {
      "type": "JP1PC-AWS-STATES",
      "name": [{".*": "regexp"}]
    }
  ]
},
{
  "id": "sqs",
  "displayName": "Amazon Simple Queue Service",
  "objectRoot": [
    {
      "type": "JP1PC-AWS-SQS",
      "name": [{".*": "regexp"}]
    }
  ]
},
{
  "id": "ecs",
  "displayName": "Amazon Elastic Container Service",
  "objectRoot": [
    {
      "type": "JP1PC-AWS-ECS",
      "name": [{".*": "regexp"}]
    }
  ]
},
{
  "id": "ebs",
  "displayName": "Amazon Elastic Block Store",
  "objectRoot": [
    {
      "type": "JP1PC-AWS-EBS",
      "name": [{".*": "regexp"}]
    }
  ]
}

```

```

    ]
  },
  {
    "id": "efs",
    "displayName": "Amazon Elastic File System",
    "objectRoot": [
      {
        "type": "JP1PC-AWS-EFS",
        "name": [{".*": "regexp"}]
      }
    ]
  },
  {
    "id": "fsx",
    "displayName": "FSx File System",
    "objectRoot": [
      {
        "type": "JP1PC-AWS-FSX",
        "name": [{".*": "regexp"}]
      }
    ]
  },
  {
    "id": "sns",
    "displayName": "Simple Notification Service",
    "objectRoot": [
      {
        "type": "JP1PC-AWS-SNS",
        "name": [{".*": "regexp"}]
      }
    ]
  },
  {
    "id": "rds",
    "displayName": "Relational Database Service",
    "objectRoot": [
      {
        "type": "JP1PC-AWS-RDS",
        "name": [{".*": "regexp"}]
      }
    ]
  }
]
}

```

After configuring system node definition file, if you run JP1/IM - Manager's `jddcreatetree` command to create a CloudWatch other than EC2, JP1/IM - Manager displays IM managed node under system node in the **Operating status** area of the integrated operation viewer, depending on AWS namespace name.

For details about the system node definition file, see *System node definition file (imdd_systemnode.conf)* in *Chapter 2. Definition Files* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

■ Placing the credential file

When monitoring with the add-on program Yet another cloudwatch exporter, place the credentials file under `"C:\Windows\System32\config\systemprofile\.aws\"` written in [1.21.2\(7\) Setup in Yet another cloudwatch exporter](#), [\(b\) Modify Setup to connect to CloudWatch \(for Windows\) \(required\)](#).

■ Editing category name definition file for IM management nodes (imdd_category_name.conf) (optional)

To use the service monitoring function, configure the following settings. However, if you newly installed JP1/IM - Manager 13-01 or later, this setting is not required because it was set at the time of installation.

In category name definition file for IM management nodes (imdd_category_name.conf), add the definitions shown in the following table. IM management node of agent SID created by the service-monitoring feature is displayed as the displayed category name shown in this table. If no definitions are added, IM management node category is "service" (the value of specified category ID). This setting is not required if "service" is already set for the specified category ID.

Table 1–9: Service monitoring function categories

Display category name	Specified category ID
Service	service

For details about this definition file, see *Category name definition file for IM management nodes (imdd_category_name.conf)* in Chapter 2. Definition Files in the JP1/Integrated Management 3 - Manager Command, Definition File and API Reference.

1.19.4 Register JP1/IM - Agent package (for Windows)

You can add JP1/IM - Agent package (hereinafter it is called as JP1/IM - Agent package) to JP1/IM - Manager host. You can also add JP1/IM - Agent packages of more than one Version.

You can install JP1/IM - Agent on agent host by downloading JP1/IM - Agent packages registered on JP1/IM - Manager host without using JP1/IM - Agent offered media.

To add JP1/IM - Agent packages is optional.

(1) How to register JP1/IM - Agent Package

When you install JP1/IM - Manager on JP1/IM - Manager host, the included JP1/IM - Agent packages are registered automatically.



Important

To be able to download JP1/IM - Agent package registered to the manager host, you need to setup Intelligent Integrated Management Base.

If you upgrade and install JP1/IM - Manager on the manager host, any previous versions of JP1/IM - Agent packages that are already installed will be removed.

(2) How to delete JP1/IM - Agent Packages

If you want to delete JP1/IM - Agent package registered on the manager host, delete files of register place for JP1/IM - Agent packages as follows:

Table 1–10: Register place for JP1/IM - Agent Packages (Integrated manager hosts (for Windows))

OS	JP1/IM - Agent packages		
	Register place	File Name	Product name
Windows	<i>Manager-path\public\download\ima gent\</i>	<i>jpl_pc_agent_windows_version-number-of- JP1/IM-Agent(in VVRRSS format) . zip</i>	JP1/IM - Agent(Windows version)
		<i>jpl_pc_agent_linux_version-number-of- JP1/IM-Agent(in VVRRSS format) . tar . gz</i>	JP1/IM - Agent(Linux version)

(3) How to Download JP1/IM - Agent Package

To download JP1/IM - Agent package, follow these steps:

- Prerequisites

- JP1/IM - Agent package is registered on the manager host.
- Setup of Intelligent Integrated Management Base is Completed.
- The JP1 user used to log in has been assigned the necessary permissions.

- Steps

1. Execute REST API of File downloads to download JP1/IM - Agent package.

<Description example>

```
GET http://JP1/IM-Manager(Intelligent-Management-base)-host-name:20703/download/imaget/the-file-name-of-JP1/IM-Agent-Package
```

To obtain a distribution from a JP1/IM - Manager (File downloading), you need JP1 user's authentication. For details, see *5.2.8 Authentication methods for REST API* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

2. Unzip the downloaded JP1/IM - Agent package.

- For Windows version

Use PowerShell to execute the following command:

```
Expand-Archive -Path jpl_pc_agent_windows_version-number-of-JP1/IM-Agent(in  
VVRRSS format) . zip
```

- For Linux version

Using a shell, run the following command:

```
tar -zxvf jpl_pc_agent_linux_version-number-of-JP1/IM-Agent(in VVRRSS format) . tar . gz
```

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

tougouscopekinou

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_spmd_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 *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

For details about the `jcoimdef` command, see `jcoimdef` in *Chapter 1. Commands* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

Important

About reconfiguration of the central scope database

After you uninstall JP1/IM - Manager and then re-install it or execute the `jcsdbsetup` command, if you connect JP1/IM - View, the [Monitoring Tree] window may display the information that exists before re-installation or execution of the command. If old information is displayed, stop JP1/IM - View, delete the following folder, and then

restart JP1/IM - View:

`system-drive:\ProgramData\HITACHI\JP1\JP1_DEFAULT\JP1CoView\log\output`

1.19.6 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 *12.3 Data that needs to be collected when a problem occurs* in the *JP1/Integrated Management 3 - Manager Administration Guide*.

About the data collection tool

- About `jim_log.bat`

See *jim_log.bat (Windows only)* in *Chapter 1. Commands* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API 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.
- Settings for immediately obtaining a problem investigation report in case of abnormal termination By setting the following registry before starting JP1/IM - Manager, you can immediately obtain a user mode process dump for a problem investigation report when JavaVM terminates abnormally: Take sufficient care when setting registry values, because registry values influence the entire system.

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Windows
Error Reporting\LocalDumps

Set the following registry value for the registry key above:

DumpFolder: REG_EXPAND_SZ <folder-name-of-dump-destination>

(The folder requires access authorization.)

DumpCount: REG_DWORD <number-of-dumps-saved>

DumpType: REG_DWORD 2

(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:

Console-path\conf\jplco_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_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 *JP1/Integrated Management 3 - Manager Command, Definition File and API 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 (`jplco_param_v7.conf`):

`Console-path\conf\jplco_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 *JP1/Integrated Management 3 - Manager Command, Definition File and API 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_spmc_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 JP1/Integrated Management 3 - Manager Command, Definition File and API Reference.

- About the `jcohctest` command

See *jcohctest* in Chapter 1. Commands in the JP1/Integrated Management 3 - Manager Command, Definition File and API 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 JP1/Integrated Management 3 - Manager Command, Definition File and API Reference.

3. Start JP1/IM - Manager.

1.19.7 Specifying settings for upgrading (for Windows)

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

If you are using IM database, you must update IM database by referring to [1.4.5 Updating IM databases \(for Windows\)](#).

(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 1–11: 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 `jplcsverup.bat` command

See *jplcsverup.bat (Windows only)* in *Chapter 1. Commands* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API 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*\jplcons\conf\action\actdef.conf

4. Start JP1/IM - Manager.

- About the automated action function

See *Chapter 6. Command Execution by Automated Action (JP1/Base linkage)* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

- About the `jcadefconv` command

See `jcadefconv` in *Chapter 1. Commands* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

(3) 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 *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

(4) 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 (`jplcf_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 (jplcf_profile_manager.conf)* in *Chapter 2. Definition Files* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

(5) 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 (`jplcf_profile_manager.conf`) to specify the enable/disable setting for the updated agent profile

notification function. For details, see *Profile management environment definition file (jplcf_profile_manager.conf)* in *Chapter 2. Definition Files* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

(6) 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 (`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 *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

(7) Upgrading the Intelligent Integrated Management Base (for Windows)

If you are using the Intelligent Integrated Management Base, you can upgrade it as follows:

When upgrading a linked product at the same time, upgrade the linked product prior to do step 5.

1. Terminate JP1/IM - Manager.
2. When upgrading JP1/IM - Manager from version 12-50 or earlier, construct the Intelligent Integrated Management Database.

For details, see [1.5 Construction of Intelligent Integrated Management Database \(for Windows\)](#).

3. Add new settings.

Add new settings corresponding to the new functions you are going to use.[#]

Note #

When upgrading JP1/IM - Manager from 13-00 or 13-01 to 13-10 or later, add three lines ("web-enable-admin-api: true", "db-connections-max: 50", "db-writer-connection-concurrency: 1" (underlined part of "after change" below) to the end of the following file in a text editor.

- For a physical host: `Manager-pass\conf\imgndb\config.yml`

- For a logical host: `shared-folder\jplimm\conf\imgndb\config.yml`

<Example of change>

- Before change

`db-host: localhost`

`db-name: imgndb`

`db-user: imuser`

`db-password: rCKsdJ8vSQn2`

`db-port: 20705`

`web-listen-address: localhost:20706`

`log-level: info`

`db-ssl-mode: allow`

`promql-max-points-per-ts: 30001`

- After change

`db-host: localhost`

`db-name: imgndb`


```
db-user: imuser
db-password: rCKsdJ8vSQn2
db-port: 20705
web-listen-address: localhost:20706
log-level: info
db-ssl-mode: allow
promql-max-points-per-ts: 30001
web-enable-admin-api: true
db-connections-max: 50
db-writer-connection-concurrency: 1
```

If you do not add a "web-enable-admin-api: true" line, deleting the trend data and deleting integrated agent info will fail.

For details on deleting trend data and integrated agent information, see *2.2.1 List of Integrated Agents window* in the *JP1/Integrated Management 3 - Manager GUI Reference* and *5.11.4 Delete Trend Data* and *5.18.2 Delete integrated agent info* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

If you do not add the "db-connections-max: 50" and "db-writer-connection-concurrency: 1" rows, the following events may occur when collecting a large amount of performance data (when the sum of sample collected by integrated agent in the system (in the system of lower manager in a multi-stage configuration) exceeds 10,000 seconds):

- Performance data is not saved in Intelligent Integrated Management Database and cannot be displayed and retrieved
- Trend data management service memory usage increases

4. Start JP1/IM - Manager.

5. Execute the `jddcreatetree` command.

6. Execute the `jddupdatetree` command in new and rebuilding mode.

- `jddcreatetree` command

For details, see `jddcreatetree` in *Chapter 1. Commands* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

- `jddupdatetree` command

For details, see `jddupdatetree` in *Chapter 1. Commands* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

Unless you upgrade the Intelligent Integrated Management Base, you cannot use the functionality provided by Intelligent Integrated Management Base 13-00.

(8) Upgrading Intelligent Integrated Management Database version (for Windows)

This section describes the setting at the time of version upgrade when using Intelligent Integrated Management Database.

If you have upgraded JP1/IM - Manager from version 13-11 or earlier and you are using Intelligent Integrated Management Database, you must execute `jimgndbupdate` command.

If you want to see the current version of the Intelligent Integrated Management Database, you must execute `jimgndbsetup` command with the `"-display"` parameter. Also, when the Intelligent Integrated Management Database is versioned as "No Data" or "131100", `jimgndbupdate` command must be executed.

For details about `jimgndbsetup` command and `jimgndbupdate` command, see *jimgndbsetup* in *Chapter 1. Commands* and *jimgndbupdate* in *Chapter 1. Commands* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

(9) Updating extended startup process definition file

If you upgraded from JP1/IM - Manager version 11 or earlier, add `jddmain`, `imbase`, `imbaseproxy` process-definition to extended startup process definition file (`jp1co_service.conf`).

When upgrading from version 12, add `imbase`, `imbaseproxy` process-definition.

For details about the extended startup process definition file, see *Extended startup process definition file (jp1co_service.conf)* in *Chapter 2. Definition Files* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

1.20 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.

1.20.1 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 *12.3 Data that needs to be collected when a problem occurs in the JP1/Integrated Management 3 - Manager Administration Guide*.

About the data collection tool

- About `jcoview_log.bat`

See `jcoview_log.bat` (Windows only) in *Chapter 1. Commands in the JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

Specify the settings that enable output of a memory dump and crash dump by referencing *1.19.6(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 JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

1.20.2 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 *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*

1.20.3 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 3 - View**. The name is **Configuration Management**.

For details about the `jcovcfsetup` command, see *jcovcfsetup (Windows only)* in *Chapter 1. Commands* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

Note:

If you have changed the location or name of **JP1_Integrated Management 3 - 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 *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*

1.21 Setup for JP1/IM - Agent (for Windows)

1.21.1 Setup for JP1/IM - Agent service

(1) Enable or disable add-on program

This section explains how to enable or disable add-on program. JP1/IM - Agent contains more than one add-on programs and can only start services that are enabled.

Note that the log metrics feature itself cannot be started or stopped because it is a Fluentd plug-in. The log metrics feature starts or stops as Fluentd starts or stops.

(a) Enable add-on programs

- To setup when installing

In initial setting command to use when installing, select add-on program that you want to Enable.

For details, see *3.15.9 Initial setting command* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

During the version upgrade installation, the existing settings are inherited. However, add-on programs that is newly added in new Version are in the disabled Status.

- To setup after installing

The following are the steps to Enable add-on program services for a JP1/IM - Agent:

1. If the service is running, execute the following command to terminate.

```
Agent-path\tools\jpc_service_stop -s all
```

2. Execute the following command to Enable the service.

```
Agent-path\tools\jpc_service -on Service-key-of-JP1/IM - Agent
```

3. Move the discovery configuration file corresponding to the service.

Move the discovery configuration file corresponding to the following services from *Agent-path\conf\jpc_file_sd_config_off* folder to *Agent-path\conf* folder.

Service	Discovery configuration file
prometheus_server	None
alertmanager	None
windows_exporter	jpc_file_sd_config_windows.yml
blackbox_exporter	• jpc_file_sd_config_blackbox_http.yml • jpc_file_sd_config_blackbox_icmp.yml
ya_cloudwatch_exporter	jpc_file_sd_config_cloudwatch.yml
fluentd	None
promitor	jpc_file_sd_config_promitor.yml

Service	Discovery configuration file
script_exporter	None
web_exporter	jpc_file_sd_config_web.yml
vmware_exporter	jpc_file_sd_config_vmware.yml

4. Verify that the service is Enabled.

At the command prompt, execute "services.msc" to see the service in management console. If the service exists, the service is Enabled.

5. Execute "*1.21.2(19) Creation and import of IM management node tree data (for Windows) (required)*".

(b) Disable add-on program

The following are the steps to disable service of add-on program for a JP1/IM - Agent:

1. If the service is running, execute the following command to terminate.

```
Agent-path\tools\jpc_service_stop -s all
```

2. Disable the service by execute the following command:

```
Agent-path\tools\jpc_service -off Service-key-of-JP1/IM - Agent
```

3. Move the discovery configuration file corresponding to the service.

Move the discovery configuration file corresponding to the following services from *Agent-path\conf* folder to *Agent-path\conf\jpc_file_sd_config_off* folder.

Service	Discovery configuration file
prometheus_server	None
alertmanager	None
windows_exporter	jpc_file_sd_config_windows.yml
blackbox_exporter	- jpc_file_sd_config_blackbox_http.yml - jpc_file_sd_config_blackbox_icmp.yml
ya_cloudwatch_exporter	jpc_file_sd_config_cloudwatch.yml
fluentd	None
promitor	jpc_file_sd_config_promitor.yml
script_exporter	None
web_exporter	jpc_file_sd_config_web.yml
vmware_exporter	jpc_file_sd_config_vmware.yml

4. Verify that the service is disabled.

At the command prompt, execute "services.msc" to see the service in management console. If the service does not exist, the service is disabled.

(2) Enable and Disable of Auto-start

(a) Enable for Auto-start

To Enable the service-auto-start when OS starts, follow these steps:

1. Execute the following command to Enable all the auto-start of services on JP1/IM - Agent.

```
jpc_service_autostart -on
```

(b) Disable for Auto-start

To disable the service-auto-start when OS starts, follow these steps:

1. Execute the following command to Disable all the auto-start of services on JP1/IM - Agent.

```
jpc_service_autostart -off
```

(c) How to Check Automatic Start and Stop

At the command prompt, execute "services.msc" to see the service in management console.

Open the properties of the applicable service and it is enabled if the "Startup Type" is "Automatic" or "Automatic (Delayed)". Otherwise, it is disabled. For details about the service name, see *2.9 Service of JP1/IM - Agent* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

(d) Notes on Auto-stop in OS Shutdown

Manually shut down all integrated agent services prior to shutting down Windows. Shutting down Windows does not wait for the service outage completed, so if you shut down Windows while the service is running, the service may not be able to terminate normally. If this happens, Error or Warnings may be output in the event log, and the contents of integrated agent logs around OS shutdown may be incorrect. In addition, it may take a while for the next service to start.

(3) How to start and stop manually

To start or stop JP1/IM - Agent manually, use the following command:

Table 1–12: Start/Stop Command

Command	Description
jpc_service_start	Start agent service.
jpc_service_stop	Stop agent service.

For details of the command, see *Chapter 1. Commands* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

(4) How to check Startup status of a service

At the command prompt, execute "services.msc" to see the service in management console. Check Status of the target service.

(5) Location of configuration file

When installing, place imagent, imagentproxy, imagentaction, and service definition file for each add-on program in the following location:

For details about the service definition file, see *Service definition file (jpc_program-name_service.xml)* in *Chapter 2. Definition Files* in the *JPI/Integrated Management 3 - Manager Command, Definition File and API Reference*.

Table 1–13: Location of service definition file for add-on program

Location (path)	Typical Uses	Layout method
<i>Agent-path</i> \conf\ (for physical hosts)	Model file (service definition file template) Do not edit the model file.	Place in the installer.
<i>Shared-disk</i> \JP1ima\conf\ (for logical hosts)	Model file (service definition file template) Do not edit the model file.	Manually place.
<i>Agent-path</i> \bin\ 	Service definition file main unit Do not edit the model file.	Place by initial setting command for Physical host and by manually for Logical host.

(6) Edit Configuration file

If you want to change setup of a service, edit service definition file. If you have edited service definition file, reflection method of the definition depends on the parameter you have changed, and going to be one of the following:

- Uninstall the service (Execute the `jpc_service disable` command) and reinstall it (Execute the `jpc_service enable` command).
- Restart the service
- Save Service definition file

For details, see *When the definitions are applied* in *Service definition file (jpc_program-name_service.xml)* in *Chapter 2. Definition Files* in the *JPI/Integrated Management 3 - Manager Command, Definition File and API Reference*.

(7) Notes on changing Setup of service-auto-start

<startmode> in service definition file enables you to setup the service-auto-start. However, because the `jpc_service_autostart` command or Windows service's setup can be directly changed to change setup of the service-auto-start, setup of the <startmode> specified in service definition file and current setup of the service-auto-start do not always match.

(8) Notes on disabling services

If you Execute the `jpc_service disable` command to disable the service, the invalidation may fail if service definition file does not exist or service definition file content is incorrect. If this happens, Execute the following command with administrator privileges.

```
SC Delete Service name
```

1.21.2 Settings of JP1/IM - Agent

(1) Common way for Setting

(a) Edit the configuration files (for Windows)

Configuration file is stored in conf directory. There are two ways to modify the content of configuration file:

- The way to use integrated operation viewer
- The way to Login and Setup the Hosts

About setting files that can be edited when you are using integrated operation viewer, see the notes of the definition file about JP1/IM - Agent (JP1/IM agent control base) in *List of definition files* in *Chapter 2. Definition Files* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*. If you Login host and Setup, All configuration files can be edited.

■ How to use integrated operation viewer

1. Download configuration file from integrated operation viewer.

Select file you want to edit from integrated operation viewer and download it.

If you want to add a defined file that you can optionally create, do the following:

1. Download user-created definition file list definition file.
 2. Write information about definition file you want to add in user-created definition file list definition file
 3. Upload user-created definition file list definition file.
 4. Upload definition file that you want to add.
2. Edit the downloaded file.



Note

Because format check can be done for Prometheus server defined file with `promtool` command, it is recommended to be checked at this point.

`promtool` command is included with Prometheus server. Prometheus server can be downloaded from GitHub website. Use the same version as Prometheus server that came with your JP1/IM - Agent.

Version of add-on program of JP1/IM - Agent can be checked in the add-on function list in the List of Integrated Agents window of integrated operation viewer or in the `addon_info.txt` file stored in "*Agent-path*\addon_management*add-on-name*".

3. Upload the edited file with integrated operation viewer.

Setup is automatically reflected when uploaded.

■ How to Login and Setup the Hosts

1. Login to integrated agent host.
2. Stop JP1/IM - Agent servicing.
3. Edit the configuration files.



Note

Because format check can be done for Prometheus server defined file with `promtool` command, it is recommended to be checked at this point.

4. Start JP1/IM - Agent service.

(b) Changing service definition file (for Windows)

Service definition file storage destination and file name are as follows:

- Storage destination: *Installation-destination-folder*\jplima\bin\
- File name: `jpc_service_name_service.xml`



Important

- If you make changes to service definition file items, you will need to restart the service or reinstall the service[#] to apply the changes. For details about what you need to do to import each items, see *When the definitions are applied in Service definition file (jpc_program-name_service.xml) in Chapter 2. Definition Files in the JP1/Integrated Management 3 - Manager Command, Definition File and API Reference.*
- If you change any of the items that require service reinstallation[#], you must disable registration of the service and enable again after that. For details about how to enable or disable registration of service, see *1.21.1(1) Enable or disable add-on program.*

#

Reinstalling a service means that you delete the service and then create the service again (using the `jpc_service` command.).

To change service definition file, follow these steps:

1. Login to integrated agent host.
2. Stop JP1/IM - Agent service.
3. Edit service definition file.
4. Start JP1/IM - Agent service.

(c) Change command-line options (for Windows)

Change the command-line options in service definition file `<arguments>` tag.

For how to edit, see *1.21.2(1)(b) Changing service definition file (for Windows).*

(2) Setup for JP1/IM agent control base

(a) Change Integrated manager to connect to (for Windows) (optional)

1. Stop JP1/IM - Agent service.

2. Change Integrated manager to connect to.

Change the destination Integration Manager defined in imagent common configuration file (jpc_imagentcommon.json) to the new destination.

For details on how to change configuration file, see [1.21.2\(1\)\(a\) Edit the configuration files \(for Windows\)](#).

If you want to change the target Integration Manager from the secondary JP1/IM agent control base using the multi-manager host data delivery feature, change the definition under the immgr_add.secondary instead of immgr.

3. Remove integrated agent host

In the integrated operation viewer **List of Integrated Agents** window, select the checkbox next to integrated agent host whose access point name you want to change, and then click the **Remove** button.

For details, see [2.2.1 List of Integrated Agents window](#) in the *JP1/Integrated Management 3 - Manager GUI Reference*.

4. Check initial secret.

Check initial secret (secret for first-time connection) with integrated operation viewer in Integrated manager hosting.

For details, see [2.2.3 Show Initial Secret window](#) in the *JP1/Integrated Management 3 - Manager GUI Reference*.

5. Obfuscate and register initial secret.

In the Secret Manager command, obfuscate initial secret and register it.[#]

```
jimasecret -add -key immgr.initial_secret -s " initial secret "
```

6. Delete Individual secret.

In the Secret Management command, Delete Individual secrets.[#]

```
jimasecret -rm -key immgr.client_secret
```

7. Modify a certificate

For details on how to change CA certificate, see [1.21.2\(2\)\(c\) Place CA certificate \(for Windows\) \(optional\)](#).

This step is not required if authentication station that issued the server certificate for Integrated manager to which the old connection was made and imbase to which the new connection was made are the same.

8. Start JP1/IM - Agent.

#

If you want to change the Integration Manager to which the secondary JP1/IM agent control base connects with the multi-manager host, see [3.15.7\(5\)\(e\) Keys for initial secret, client secret, and HTTP Proxy Passwords](#) in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide* for details about what to specify for-key option.

(b) Change the port (for Windows) (optional)

The listen port that JP1/IM agent control base uses is specified in imagent configuration file (jpc_imagent.json) and imagentproxy configuration file (jpc_imagent_proxy.json).

For details on how to change configuration file, see [1.21.2\(1\)\(a\) Edit the configuration files \(for Windows\)](#).

For details about the default port number, see [Appendix C.1\(2\) Port numbers used by JP1/IM - Agent](#) in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

! Important

- If you have changed the listen port of event-forwarding relay function, see [1.21.2\(2\)\(g\) Configuring the event-forwarding relay function \(for Windows\) \(optional\)](#) and review the event-forwarding setting of event-forwarding relay source JP1/Base.
- If you change the port of imagentproxy process, you must change Remote Write destination of Prometheus, the alert notification destination of Alertmanager, and the alert notification destination of Fluentd. For details for each change, see below.
 - Prometheus remote write destination: [1.21.2\(3\)\(e\) Changing Remote Write destination \(for Windows\) \(optional\)](#).
 - Alertmanager alert notification destination: [1.21.2\(4\)\(b\) Changing the alert notification destination \(for Windows\) \(optional\)](#).
 - Fluentd alert notification destination: [1.21.2\(9\)\(a\) Changing Setup of Common Definition file for Log Monitor \(for Windows\) \(optional\)](#).
- When configuring secondary JP1/IM agent control base settings for the multi-manager host data delivery feature, configure members with the same name under listen_add.secondary instead of the top-level port and jp1base_forward_receive for imagent configuration file (jpc_imagent) and imagentproxy configuration file (.json).

! Important

If you change port number, you must also review setup for the firewall. For details, see [1.21.2\(17\) Firewall's Setup \(for Windows\) \(required\)](#).

(c) Place CA certificate (for Windows) (optional)

To encrypt the communication between JP1/IM agent management base and JP1/IM agent control base, specify the `tls_config` of imagent shared configuration file (`jpc_imagentcommon`), and then configure the following settings. When configuring secondary JP1/IM agent control base settings for the multi-manager host data delivery feature, set the `immgr_add.secondary` instead of the top-level `tls_config`.

If you do not want to encrypt, this setup is not required.

For instructions on deploying a CA certificate, see [9.4.5 Settings for JP1/IM - Agent \(JP1/IM agent control base\)](#).

■ To verify the server certificate of JP1/IM agent management base

1. Place CA certificate.

Place CA certificate of authentication station that issued the server certificate of imbase you are connecting to in the following directory:

- In Windows
`Agent-path\conf\user\cert\`
- In Linux
`/opt/jplima/conf/user/cert/`

2. Provide CA certificate path in imagent Common configuration file (`jpc_imagentcommon.json`).

3. Restart imagent and imagentproxy.

■ Not to verify the server certificate of JP1/IM agent management base

1. Set "true" in the `tls_config.insecure_skip_verify` of imagent shared configuration file (`jpc_imagentcommon.json`) `tls_config.insecure_skip_verify`.

(d) Modify settings related to Action Execution (for Windows) (optional)

Setup for Action Execution is defined in imagent configuration file (`jpc_imagent.json`).

For details about how to set, see [1.21.2\(1\)\(a\) Edit the configuration files \(for Windows\)](#).

(e) Setup the proxy authentication's authentication ID and Password (for Windows) (optional)

If there is a proxy server between agent host and manager host that requires Basic authentication, authentication ID and Password must be setup.

Set authentication ID to the `immgr.proxy_user` of imagent shared configuration file (`jpc_imagentcommon.json`). For details about Setting of each definition files, see [1.21.2\(1\)\(a\) Edit the configuration files \(for Windows\)](#).

You set Password in the following ways: For details, see the explanation for each item.

- Secret management command
For details, see `jimasecret` in *Chapter 1. Commands* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.
- List of Secrets dialog box of integrated operation viewer
For details, see [2.2.2\(4\) List of Secrets dialog box](#) in the *JP1/Integrated Management 3 - Manager GUI Reference*.
- Integrated operation viewer Secret Management REST API
For details, see [5.4.3 Initial secret issue](#) in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

(f) Change the user of Action Execution (for Windows) (required)

Change `action.username` and `action.domainname` in imagent configuration file (`jpc_imagent.json`). For setup procedure, see [1.21.2\(1\)\(a\) Edit the configuration files \(for Windows\)](#). Furthermore, the password of the defined user is necessary to be registered using the `jimasecret` command.

(g) Configuring the event-forwarding relay function (for Windows) (optional)

If you use event-forwarding relay function, JP1/IM - Agent must be 13-01 or later.

Before configuring JP1/IM - Agent settings, configure JP1/IM - Manager settings for event-forwarding relay function settings. After completing JP1/IM - Manager settings, configure JP1/IM - Agent settings, and then configure JP1/Base settings. Finally, the tree should be updated in JP1/IM - Manager.

For details on JP1/IM - Manager setting, see *Setup event-forwarding relay function (optional)* in [1.19.3\(1\)\(b\) Change settings of JP1/IM agent management base \(for Windows\)](#).

The following steps describe how to configure JP1/IM - Agent and JP1/Base:

■ Setup of JP1/IM - Agent

1. Stop JP1/IM - Agent service.
For a cluster configuration, stop the service from the cluster software.

2. Open imagent configuration file (jpc_imagent.json) and set the jp1base_forward_recieve items.
 - When JP1/IM - Agent 13-10 or later is newly installed
The jp1base_forward_recieve items are listed in imagent configuration file, but because they are commented like "//jp1base_forward_recieve", remove the leading "//".
 - Upgrading from a version earlier than JP1/IM - Agent 13-10
Imagent configuration file refers to imagent configuration file model file, because the jp1base_forward_recieve items are not listed. When writing, remove the leading "//".
3. Set port below the jp1base_forward_recieve items in imagent configuration file.
4. Start JP1/IM - Agent service.
For a cluster configuration, start the service from the cluster software.

■ Setup of JP1/IM - Base

1. Stop JP1/Base.
For a cluster configuration, stop from the cluster software.
2. Register imagent in remote-server of the event server configuration file (conf).
Select and define the following

```
remote-server Event server name Communication type Address Port designati  
on
```

Event server name

Fixed value Specify "imagent".

Communication type

Fixed value Specify "keep-alive".

Address

Specify the host name (physical host name or logical host name) or IP address of the local host.
If the hostname cannot be resolved by a jp1hosts or jp1hosts2, specify IP address.

Port designation

Specify the port number specified in *Setup of JP1/IM - Agent*.

3. Sets the forwarding configuration file (forward).
Select and define the following

```
to imagent  
Event Filter  
end-to
```

4. Start JP1/Base.
For a cluster configuration, start from the cluster software.

■ Updating the tree

1. Refresh Intelligent Integrated Management Base tree in JP1/IM - Manager.
If event-forwarding relay source IM management node is not displayed when the tree is refreshed, check that jima_message.log of event relay source imagent is not erroneous.

(h) Releasing event-forwarding relay function (for Windows)

Configure JP1/Base settings, then configure JP1/IM - Agent settings. Finally, the tree should be updated in JP1/IM - Manager.

■ Setup of JP1/IM - Base

1. Stop JP1/Base.
For a cluster configuration, stop from the cluster software.
2. Editing the forwarding configuration file (forward) to release forwarding events to imagent.
3. Start JP1/Base.
For a cluster configuration, start from the cluster software.

■ Setup of JP1/IM - Agent

1. Stop JP1/IM - Agent service.
For a cluster configuration, stop the service from the cluster software.
2. Open imagent configuration file (jpc_imagent.json) and comment or remove jplbase_forward_recieve items.
3. Start JP1/IM - Agent service.
For a cluster configuration, start the service from the cluster software.

■ Updating the tree

1. Refresh Intelligent Integrated Management Base tree in JP1/IM - Manager.
If event-forwarding relay source IM management node is not displayed when the tree is refreshed, check that jima_message.log of event relay source imagent is not erroneous.

(i) Setting the data delivery function to multiple manager hosts (for Windows) (optional)

■ New setting

1. Shut down JP1/IM - Agent servicing.
The service key of the service to be stopped is shown below.
 - jpc_imagent
 - jpc_imagentaction
 - jpc_imagentproxy
 - jpc_alertmanager
 - jpc_prometheus_server
 - jpc_fluentd
2. Create folders for JP1/IM agent management base secondary.
Create the following folders as secondary folders for JP1/IM agent management base:
 - *Agent-path*\tmp\download-imagent-group-identifier
 - *Agent-path*\tmp\upload-imagent-group-identifier
 - *Agent-path*\tmp\jbsfwd-imagent-group-identifier

- *Agent-path\tmp\imagent-imagent-group-identifier*
- *Agent-path\logs\imagentproxy-imagent-group-identifier*
- *Agent-path\logs\imagentaction-imagent-group-identifier*

To create the above folder, use the following command:

```
mkdir folders
```

3. Create a file for JP1/IM agent management base secondary.

Copy the source file in *Agent-path\bin* and rename it to the destination file name.

Source file name	Destination file name
jpc_imagent_service.exe	jpc_imagent-imagent-group-identifier_service.exe
jpc_imagent_service.xml	jpc_imagent-imagent-group-identifier_service.xml
jpc_imagentproxy_service.exe	jpc_imagentproxy-imagent-group-identifier_service.exe
jpc_imagentproxy_service.xml	jpc_imagentproxy-imagent-group-identifier_service.xml
jpc_imagentaction_service.exe	jpc_imagentaction-imagent-group-identifier_service.exe
jpc_imagentaction_service.xml	jpc_imagentaction-imagent-group-identifier_service.xml

4. Configure settings for JP1/IM agent control base secondary.

See 3.15.7(5)(d) *configuration file of JP1/IM agent control base* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

5. Register a secret for the secondary of JP1/IM agent control base.

Obtain and register initial secret of JP1/IM - Manager to which the secondary JP1/IM agent control base connects. If you connect to JP1/IM - Manager through a HTTP proxy server that requires password-based HTTP authentication (Basic authentication), register HTTP proxy password as secret.

For the keys of initial secret to register and the keys of HTTP proxy password, see 3.15.7(5)(e) *Keys for initial secret, client secret, and HTTP Proxy Passwords* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

6. Perform settings other than JP1/IM agent control base.

See 3.15.7(5)(f) *Send settings for programs other than JP1/IM agent control base* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

7. Configure the service startup settings.

See 3.15.7(5)(c) *Configuring Secondary Service Startup* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

8. Run the following command to enable the service:

```
Agent-path\tools\jpc_service -on service-key
```

For the service key, use the service key of JP1/IM - Agent with *-imagent-group-identifier* in Windows described in 10.1 *JP1/IM - Agent Service* in the *JP1/Integrated Management 3 - Manager Administration Guide*.

9. Start JP1/IM - Agent servicing.

The service keys of the service to be started are shown below.

- jpc_imagent

- jpc_imagentaction
 - jpc_imagentproxy
 - jpc_imagent-*imagent-group-identifier*
 - jpc_imagentaction-*imagent-group-identifier*
 - jpc_imagentproxy-*imagent-group-identifier*
 - jpc_alertmanager
 - jpc_prometheus_server
- jpc_fluentd

10. Set auto start at OS startup.

For details about enabling auto start, see [1.21.1\(2\)\(a\) Enable for Auto-start](#).

■ Setting at version upgrade

If you are upgrading from a version that has data delivery function to multiple manager hosts enabled, perform the steps below.

Perform the following procedure after step 5 (before step 6) of [1.3.1\(3\)\(b\) Install instructions](#) at the time of version upgrade installation.

1. Create a file for JP1/IM agent management base secondary.

Copy the source file in *Agent-path*\bin and rename it to the destination file name.

Source file name	Destination file name
jpc_imagent_service.exe	jpc_imagent- <i>imagent-group-identifier</i> _service.exe
jpc_imagentproxy_service.exe	jpc_imagent- <i>imagent-group-identifier</i> _service.exe
jpc_imagentaction_service.exe	jpc_imagent- <i>imagent-group-identifier</i> _service.exe

(j) Deactivating the data delivery function to multiple manager hosts (for Windows) (optional)

The following describes the procedure for configuring the data delivery to multiple manager hosts when the data delivery function is no longer used.

Perform one of the following depending on your operating environment.

- Remove only the data delivery function to multiple manager hosts without uninstalling JP1/IM - Agent
- Uninstall JP1/IM - Agent itself.

■ To remove only the data delivery function to multiple manager hosts without uninstalling JP1/IM - Agent

1. Stop all JP1/IM - Agent servicing.

If the service is running, execute the following command to stop it.

```
Agent-path\tools\jpc_service_stop -s all
```

2. Disable the secondary service.

Disable the secondary services for JP1/IM agent control base by running the following command:

```
Agent-path\tools\jpc_service -off Service-Key
```

For details on how to disable the service, see step 2 and step 4 in [1.21.1\(1\)\(b\) Disable add-on program](#).

For service keys, the service key of JP1/IM - Agent in Windows described in [10.1 JP1/IM - Agent Service](#) in the *JP1/Integrated Management 3 - Manager Administration Guide* with *-imagent group identifier* is applicable.

3. Delete the secret that you created to use the data delivery to multiple manager hosts feature.

Remove the secret for the secondary JP1/IM agent control base that you registered in step 5 of [1.21.2\(2\)\(i\) Setting the data delivery function to multiple manager hosts \(for Windows\) \(optional\)](#).

For the key of the secret to be deleted, see [3.15.7\(5\)\(e\) Keys for initial secret, client secret, and HTTP Proxy Passwords](#) in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

This step is not necessary for secrets that have already been deleted.

4. The settings for using the data delivery function to multiple manager hosts.

Restore the settings for JP1/IM agent control base secondary set in step 4 of [1.21.2\(2\)\(i\) Setting the data delivery function to multiple manager hosts \(for Windows\) \(optional\)](#).

5. Delete the files copied to use the data delivery function to multiple manager hosts.

Remove the files for the secondary JP1/IM agent management base that you copied in step 3 of [1.21.2\(2\)\(i\) Setting the data delivery function to multiple manager hosts \(for Windows\) \(optional\)](#).

6. Delete the folder created to use the data delivery function to multiple manager hosts.

After saving the log and other required files, delete the folders for the secondary JP1/IM agent management base created in step 2 of [1.21.2\(2\)\(i\) Setting the data delivery function to multiple manager hosts \(for Windows\) \(optional\)](#).

7. Deletes integrated agent registered on JP1/IM - Manager to which the disabled secondary service is connected.

For details on deleting integrated agent data, see [2.2.1 List of Integrated Agents window](#) in the *JP1/Integrated Management 3 - Manager GUI Reference*.

■ When uninstalling JP1/IM - Agent

Follow the procedure from step 3 to step 6 in *To remove only the data delivery function to multiple manager hosts without uninstalling JP1/IM - Agent* above between steps 1 and 2 in [1.25.1\(5\) How to uninstall JP1/IM - Agent](#).

Follow step 7 in *To remove only the data delivery function to multiple manager hosts without uninstalling JP1/IM - Agent* above.

(3) Setup of Prometheus server

(a) Changing Ports (For Windows) (optional)

The listen port used by Prometheus server is specified in `--web.listen-address` option of `prometheus` command.

For details about how to change `prometheus` command options, see [1.21.2\(1\)\(c\) Change command-line options \(for Windows\)](#). For details of `--web.listen-address` option, see *prometheus command options* in *Service definition file (jpc_program-name_service.xml)* in *Chapter 2. Definition Files* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

The default port is "20713". If port number is changed, review setup of the firewall and prohibit accessing from outside. However, if you want to monitor Prometheus server with external shape monitoring by Blackbox exporter in other host, allow it to be accessed. In such cases, consider security measures such as limiting the source IP address as required.

(b) To Add the alert definition (for Windows) (optional)

Alert definitions are defined in alert configuration file (`jpc_alerting_rules.yml`).

For details on how to edit alert configuration file, see [1.21.2\(1\)\(a\) Edit the configuration files \(for Windows\)](#).

For details about the items that require setup in the alert definition, see *Alert rule definition for converting to JPI events* in [3.15.1\(3\)\(a\) Alert evaluation function](#) in the *JPI/Integrated Management 3 - Manager Overview and System Design Guide*. For details of the individual items and sample for the alert definitions, see *Alert configuration file (`jpc_alerting_rules.yml`)* in *Chapter 2. Definition Files* in the *JPI/Integrated Management 3 - Manager Command, Definition File and API Reference*.



Note

The following are the points for when you create an alert definition:

- Monitoring performance function on JPI/IM - Agent allows you to specify a duration (for). If the alert condition is met continuously during the specified period, it is judged as a firing.
- If you want to detect that metric is present, use `absent()` function in the alerting criteria.
`absent (metric { label } )`
- If you want the alert to be enabled for a certain duration, use PromQL for the alert criteria to setup it.
(Example) When monitoring from 8 o'clock to 12 o'clock in Japan time
`alert-condition and ON() (23 <= hour() or 0 <= hour() < 3)`
Note that "hour()" returns UTC time, so you need to consider UTC.
- Monitoring performance function on JPI/IM - Agent notifies you of the firing and resolved. If you want to be notified in two stages: Warning and abnormal, create alerts for Warning and alerts for abnormal.
- Message that is displayed when an alert occurs can include the following:
 - Message at firing
 - Message on resolved
- For details about the variables that can be embedded in alert Message, see [3.15.1\(3\)\(a\) Alert evaluation function](#) in the *JPI/Integrated Management 3 - Manager Overview and System Design Guide*.



Important

Please set alert definitions so that total number of time-series data sets that each alert definitions assesment is less than 150.

For example, when 3 alerts of Windows network interfaces are defined and there are 4 network interfaces on Windows host, 4 time-series data sets collected by Windows exporter are generated.

Therefore, it means 4 time-series data sets are assesmented by 3 alerts, total number of time-series data comes to $4 \times 3 = 12$.

(c) Add Blackbox exporter scrape job (for Windows) (optional)

Prior to Add a Blackbox exporter scrape job, you must add the module to configuration file on Blackbox exporter. For details, see [1.21.2\(6\)\(b\) Add, change, and delete modules \(for Windows\) \(optional\)](#).

After you Add the module, perform the following steps to setup a scrape job that scrape the newly created module:

1. Create a discovery configuration file for your Blackbox exporter.

Copy the original model File shown below and rename it to the definition File of Copy destination to create a discovery configuration file for Blackbox exporter.

- When performing HTTP/HTTPS monitoring

- For Windows:

Copy source: *Agent-path*\conf\jpc_file_sd_config_blackbox_http.yml.model

Copy to: *Agent-path*\conf\file_sd_config_blackbox_*module-name-begins-with-http*.yml

- For Linux:

Copy source: /opt/jplima/conf/jpc_file_sd_config_blackbox_http.yml.model

Copy to: /opt/jplima/conf/file_sd_config_blackbox_*module-name-begins-with-http*.yml

- When performing ICMP monitoring

- For Windows:

Copy source: *Agent-path*\conf\jpc_file_sd_config_blackbox_icmp.yml.model

Copy to: *Agent-path*\conf\file_sd_config_blackbox_*module-name-begins-with-icmp*.yml

- For Linux:

Copy source: /opt/jplima/conf/jpc_file_sd_config_blackbox_icmp.yml.model

Copy to: /opt/jplima/conf/file_sd_config_blackbox_*module-name-begins-with-icmp*.yml

The module name indicates the module that was added by [1.21.2\(6\)\(b\) Add, change, and delete modules \(for Windows\) \(optional\)](#).

2. Edit the discovery configuration files in Blackbox exporter.

- For monitoring HTTP/HTTPS Discovery configuration file

For descriptions, see *Blackbox exporter (HTTP/HTTPS monitoring) discovery configuration file (jpc_file_sd_config_blackbox_http.yml)* in *Chapter 2. Definition Files in the JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

- For monitoring ICMP Discovery configuration file

For descriptions, see *Blackbox exporter (ICMP monitoring) discovery configuration file (jpc_file_sd_config_blackbox_icmp.yml)* in *Chapter 2. Definition Files in the JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

3. Use integrated operation viewer to add definition File.

For instructions on how to add a definition File, see [1.21.2\(1\)\(a\) Edit the configuration files \(for Windows\)](#).

4. Add a scrape job to Prometheus configuration file.

- When performing HTTP/HTTPS monitoring

In Prometheus configuration file (jpc_prometheus_server.yml), Copy the Definition of Scrape Job with Job Name "jpc_blackbox_http" to add a new scrape job.

- When performing ICMP monitoring

In Prometheus configuration file (jpc_prometheus_server.yml), Copy definition of Scrape Job with Job Name "jpc_blackbox_icmp" to Add a new scrape job.

<Sample Setup>

```
scrape_configs:
  - job_name: any-scrape-job-name
    metrics_path: /probe
```

```

params:
  module: [module-name]
file_sd_configs:
  - files:
    - 'discovery-configuration-file-name'
relabel_configs:
  (Omitted)
metric_relabel_configs:
  (Omitted)

```

any-scrap-job-name

Specify any name that does not overlap with any other scrape job name, in the range of 1 to 255 characters, except for control characters.

module-name

Specify the module name that was added in [1.21.2\(6\)\(b\) Add, change, and delete modules \(for Windows\) \(optional\)](#).

discovery-configuration-file-name

Specify File that you created in step 1.

For descriptions of Prometheus configuration file, see `<scrape_config>` in *Prometheus configuration file (jpc_prometheus_server.yml)* in *Chapter 2. Definition Files in the JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

For details about editing Prometheus configuration file, see [1.21.2\(1\)\(a\) Edit the configuration files \(for Windows\)](#).

(d) Add user-defined Exporter scrape job (for Windows) (optional)

To scrape user-defined Exporter, you need the following setup:

- Add for user-specific discovery configuration file
- Editing Prometheus configuration file (jpc_prometheus_server.yml)

For details about how to Add and edit File each definition files, see [1.21.2\(1\)\(a\) Edit the configuration files \(for Windows\)](#).

1. Add user-specific discovery configuration file.

Specify user-defined Exporter that you want to scrape to user-specific discovery configuration file.

For descriptions, see *User-specific discovery configuration file (user_file_sd_config_any-name.yml)* in *Chapter 2. Definition Files in the JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

2. Add a scrape job to Prometheus configuration file.

In Prometheus configuration file (jpc_prometheus_server.yml), add the scrape job to scrape user-defined Exporter. Scrape jobs are listed in `scrape_configs`.

<Sample Setup>

```

scrape_configs:
  - job_name: scrape-job-name

    file_sd_configs:
      - files:
        - discovery-configuration-file-name

    relabel_configs:
      - target_label: jpl_pc_nodelabel
        replacement: label-name-of-IM-management-node

```

```
metric_relabel_configs:
- source_labels: ['__name__']
  regex: 'metric-1|metric-2|metric-3'
  action: 'keep'
```

scrape-job-name

Specify an arbitrary string. This value is setup on job label of metric.

discovery-configuration-file-name

Specify file of user-specific discovery configuration file created in step 1 above.

label-name-of-IM-management-node

Specify the character string that integrated operation viewer displays on IM management node label. This is not a control character.

When URL is encoded, the character string must be within 234 bytes (the upper limit for multibyte characters is 26). The *label-name* that overlap with *label-name* of the IM management nodes created by JP1/IM - Agent cannot be specified. Specify the character string that is not already specified in same host. If the character string that is already specified, the configuration information SIDs become same, IM management nodes are not created properly.

metric-1, metric-2, metric-3

Specify metric that you want to collect. If there is more than one metric to be collected, separate them with |. If you want to collect all metrics, you do not need to include "metric_relabel_configs". However, if a large amount of metric is present, the amount of data will be large. Therefore, we recommend that you list "metric_relabel_configs" and limit it to metric to be monitored.

3. Add metric definition file.

Add metric definition file for user-defined Exporter.

For descriptions, see *User-specific metric definition file (metrics_any-Prometheus-trend-name.conf)* in *Chapter 2. Definition Files in the JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

(e) Changing Remote Write destination (for Windows) (optional)

Specifies URL and ports of imagentproxy processes running on the same host in the remote_write.url of Prometheus configuration file (jpc_prometheus_server.yml) for Remote Write destination. You need to change it only if you want to change imagentproxy process port.

<Sample Setup>

```
remote_write:
- url: http://localhost:20727/ima/api/v1/proxy/service/promscale/write
```

For instructions on how to change configuration file, see [1.21.2\(1\)\(a\) Edit the configuration files \(for Windows\)](#).

(f) Configuring service monitoring settings (For Windows) (optional)

To use the service monitoring function in an environment where the version is upgraded and installed from JP1/IM - Agent 13-00 to 13-01 or later, configure the following settings. This setting is not required if JP1/IM - Agent 13-01 or later is newly installed.

■ Editing Prometheus configuration file (jpc_prometheus_server.yml)

If "windows_service_state" is not set to keep metric in the metric_relabel_configs settings of the jpc_windows scrape job, add the settings. Also, if the same metric_relabel_configs setting does not set a relabel config for "windows_service_.*" metric, add the setting. Add the underlined settings as follows:

```
(Omitted)
scrape_configs:
(Omitted)
  - job_name: 'jpc_windows'
(Omitted)
    metric_relabel_configs:
      - source_labels: ['__name__']
        regex: 'windows_cs_physical_memory_bytes|windows_cache_copy_read_hits_total|(Omitted)|windows_process_working_set_peak_bytes|windows_process_working_set_bytes|windows_service_state'
        action: 'keep'
      - source_labels: ['__name__']
        regex: 'windows_process_.*'
        target_label: 'jpl_pc_trendname'
        replacement: 'windows_exporter_process'
      - source_labels: ['__name__', 'process']
        regex: 'windows_process_.*;(.*)'
        target_label: 'jpl_pc_nodelabel'
        replacement: '${1}'
      - source_labels: ['__name__']
      - regex: 'windows_service_.*'
      - target_label: 'jpl_pc_trendname'
      - replacement: 'windows_exporter_service'
      - source_labels: ['__name__']
      - regex: 'windows_service_.*'
      - target_label: 'jpl_pc_category'
      - replacement: 'service'
      - source_labels: ['__name__', 'name']
      - regex: 'windows_service_.*;(.*)'
      - target_label: 'jpl_pc_nodelabel'
      - replacement: '${1}'
      - regex: jpl_pc_multiple_node
        action: labeldrop
```

■ Editing Windows exporter discovery configuration file (jpc_file_sd_config_windows.yml)

If "windows_service_state" is not set in the jpl_pc_multiple_node settings, add the underlined settings as shown below.

```
- targets:
  - host name:20717
    labels:
      jpl_pc_exporter: JPC Windows exporter
      jpl_pc_category: platform
      jpl_pc_trendname: windows_exporter
      jpl_pc_multiple_node: "{__name__=~'windows_process_.*|windows_service_.*'}"
  }
```


(g) Configure the settings when the label name (jp1_pc_nodelabel value) of the IM management node exceeds the upper limit (for Windows) (optional)

IM management node label-name (jp1_pc_nodelabel value) can be up to 234 bytes of URL encoded text (If all are multibyte characters, the limit is 26 characters). If the limit is exceeded, you must change the jp1_pc_nodelabel value in the metric_relabel_configs of the Prometheus configuration file (jpc_prometheus_server.yml). If you do not change the value, IM management node with that value is not created when you create IM management node.

If you want to change the value, add the following underlined settings to the metric_relabel_configs settings for Prometheus configuration file (jpc_prometheus_server.yml) scrape job: When changing the value of multiple targets, add the setting only for the number of monitored targets.

■ Editing Prometheus configuration file (jpc_prometheus_server.yml)

```
(Omitted)
scrape_configs:
(Omitted)
  - job_name: 'scrape-job-name'
(Omitted)
    metric_relabel_configs:
(Omitted)
      - source_labels: ['jp1_pc_nodelabel']
        regex: 'regular-expression-to-match-the-value-before-the-jp1_pc_node
label-change'
        target_label: 'jp1_pc_nodelabel'
        replacement: 'value-after-jp1_pc_nodelabel-change'
```

(h) Setting for executing the SAP system log extract command using Script exporter (for Windows) (optional)

Perform the following steps:

1. Edit the scrape definition in the Prometheus configuration file.

To execute SAP system log extract command using the http_sd_config method of Script exporter, change scrape definition of Script exporter as shown below.

- Editing Prometheus configuration file (jpc_prometheus_server.yml)

```
(Omitted)
scrape_configs:
(Omitted)
  - job_name: 'jpc_script'

    http_sd_configs:
      - url: 'http://installation-host-name:port/discovery'
(Omitted)

    metric_relabel_configs:
      - source_labels: ['__name__']
        regex: 'script_success|script_duration_seconds|script_exit_code'
        action: 'keep'
      - source_labels: [jp1_pc_script]
        target_label: jp1_pc_nodelabel
      - source_labels: [jp1_pc_script]
        regex: '.*jr3slget.*|.*jr3alget.*'
        target_label: 'jp1_pc_category'
```

```

      replacement: 'enterprise'
    - regex: (jpl_pc_script|jpl_pc_multiple_node|jpl_pc_agent_create_flag)
      action: labeldrop

```

(i) Add a Web exporter scrape job (for Windows) (optional)

1. Add a default scrape job to Prometheus configuration file.

If JP1/IM - Agent 13-10 or later is newly installed, it does not need to be executed.

If you upgrade JP1/IM - Agent from a version earlier than 13-10 to 13-10 or later, Prometheus configuration file model files stored in *JP1/IM-Agent-Installation-destination-folder\jplima\conf* are updated. Add the following content of Prometheus configuration file model file (*jpc_prometheus_server.yml.model*) to Prometheus configuration file (*jpc_prometheus_server.yml*) *scrape_configs*.

For logical host operation, refresh the *shared-folder\jplima\conf\jpc_prometheus_server.yml*.

<What to append>

```

scrape_configs:
- job_name: 'jpc_web_probe'
  scrape_interval: 6m
  scrape_timeout: 5m
  metrics_path: /probe
  file_sd_configs:
    - files:
      - 'jpc_file_sd_config_web.yml'
  relabel_configs:
    (Omitted)
  metric_relabel_configs:
    (Omitted)

```

2. Add a Web exporter discovery configuration file (optional).

For Web scenario monitoring, when you add a new scrape job, you create a new discovery configuration file.

Copy the following Web exporter discovery configuration file model file as a template, rename it to the copy destination definition file name, and create a discovery configuration file.

Copy source: *Agent-path\conf\jpc_file_sd_config_web.yml.model*

Copy destination: *Agent-path\conf\user\file_sd_config_web_any-name.yml*

For details about Web exporter discovery configuration file format, see *Web exporter discovery configuration file (jpc_file_sd_config_web)* in *Chapter 2. Definition Files* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

For details about editing Web exporter discovery configuration file, see [1.21.2\(1\)\(a\) Edit the configuration files \(for Windows\)](#).

3. Add a new scrape job to Prometheus configuration file (optional).

If you are monitoring Web scenarios, when you add a new scrape job, in Prometheus configuration file (*jpc_prometheus_server.yml*), add a new scrape job by copying the scrape job definition with the value of "jpc_web_probe".

<Setting example>

```

scrape_configs:
- job_name: any-scrape-job-name
  scrape_interval: scrape-request-interval
  scrape_timeout: timeout-period-for-scrape-request
  metrics_path: /probe

```

```

file_sd_configs:
- files:
- 'user/discovery-configuration-file-name'
relabel_configs:
(Omitted)
metric_relabel_configs:
(Omitted)

```

any-scrape-job-name

Specify any name that does not overlap with any other scrape job name, in the range of 1 to 255 characters, except for control characters.

For details on Prometheus configuration file, see *<scrape_config>* in *Prometheus configuration file (jpc_prometheus_server.yml)* in *Chapter 2. Definition Files in the JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

For details about editing Prometheus configuration file, see [1.21.2\(1\)\(a\) Edit the configuration files \(for Windows\)](#).

(j) Add a VMware exporter scrape job (for Windows only) (optional)

1. Add a default scrape job to Prometheus configuration file.

If JP1/IM - Agent 13-10 or later is newly installed, it does not need to be executed.

If you upgrade JP1/IM - Agent from a version earlier than 13-10 to 13-10 or later, Prometheus configuration file model files stored in *JP1/IM-Agent-Installation-destination-folder\jplima\conf* are updated. Add the following content of Prometheus configuration file model file (*jpc_prometheus_server.yml.model*) to Prometheus configuration file (*jpc_prometheus_server.yml*) *scrape_configs*.

For logical host operation, refresh the *shared-folder\jplima\conf\jpc_prometheus_server.yml*.

<What to append>

```

scrape_configs:
- job_name: 'jpc_vmware'
  params:
    section: ['section']
  file_sd_configs:
    - files:
      - 'jpc_file_sd_config_vmware.yml'
  relabel_configs:
    (Omitted)
  metric_relabel_configs:
    - source_labels: [vm_name]
      regex: '(.*)'
      target_label: instance
      action: replace
    - source_labels: ['ds_name']
      regex: '(.*)'
      target_label: instance
      replacement: ${1}
    - source_labels: ['ds_name']
      regex: '(.*)_(.*)'
      target_label: instance
      replacement: ${1}
    - source_labels: ['vm_name', '__name__']
      regex: '(.*)vmware_vm_.*'
      target_label: instance
      replacement: ${1}
      action: replace
    - source_labels: ['host_name', '__name__']

```

```

    regex: '(.*);vmware_host_.*'
    target_label: instance
    replacement: ${1}
    action: replace
- source_labels: ['__name__']
  regex: 'vmware_host_.*|vmware_datastore_.*'
  target_label: jpl_pc_trendname
  replacement: vmware_exporter_host
- source_labels: ['__name__']
  regex: 'vmware_vm_.*'
  target_label: jpl_pc_trendname
  replacement: vmware_exporter_vm
(Omitted)

```

2. Add a scrape job to Prometheus configuration file.

Prior to adding a VMware exporter scrape job, you must add a section to configuration file of VMware exporter. For details, see [1.21.2\(14\)\(b\) Add, change, or remove sections \(for Windows\) \(mandatory\)](#).

After adding the section, perform the following steps to set up a scrape job to scrape the newly created section.

If you want to monitor VMware ESXi, in Prometheus configuration file (jpc_prometheus_server.yml), add a new scrape job by copying the scrape job definition with the job name "jpc_vmware".

Also, if you want to monitor the new section additionally, in Prometheus configuration file (jpc_prometheus_server.yml), add a new scrape job by copying the scrape job definition with the job name "jpc_vmware". In this scenario, the section name in params is the section name set by VMware exporter configuration file (jpc_vmware_exporter.yml).

<Setting example>

```

scrape_configs:
- job_name: any-scrape-job-name
  params:
    section: ['section-name']
  file_sd_configs:
    - files:
        - 'jpc_file_sd_config_vmware.yml'
  relabel_configs:
    (Omitted)
  metric_relabel_configs:
    - source_labels: [vm_name]
      regex: '(.*)'
      target_label: instance
      action: replace
    - source_labels: ['ds_name']
      regex: '(.*)'
      target_label: instance
      replacement: ${1}
    - source_labels: ['ds_name']
      regex: '(.*)_(.*)'
      target_label: instance
      replacement: ${1}
    - source_labels: ['vm_name', '__name__']
      regex: '(.*);vmware_vm_.*'
      target_label: instance
      replacement: ${1}
      action: replace
    - source_labels: ['host_name', '__name__']
      regex: '(.*);vmware_host_.*'
      target_label: instance

```

```

replacement: ${1}
action: replace
- source_labels: ['__name__']
  regex: 'vmware_host_.*|vmware_datastore_.*'
  target_label: jpl_pc_trendname
  replacement: vmware_exporter_host
- source_labels: ['__name__']
  regex: 'vmware_vm_.*'
  target_label: jpl_pc_trendname
  replacement: vmware_exporter_vm
(Omitted)

```

any-scrape-job-name

Add an underscore () without changing the first "jpc_vmware", followed by any name that does not overlap with any other scrape job name, ranging from 1 to 255 characters, except for control characters.

section-name

Specify the section name added in [1.21.2\(14\)\(b\) Add, change, or remove sections \(for Windows\) \(mandatory\)](#).

Enclose the section name in single quotation marks (') or double quotation marks (").

For details on Prometheus configuration file, see `<scrape_config>` in *Prometheus configuration file (jpc_prometheus_server.yml)* in *Chapter 2. Definition Files* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

For details about editing Prometheus configuration file, see [1.21.2\(1\)\(a\) Edit the configuration files \(for Windows\)](#).

(k) Add a Windows exporter (Hyper-V Monitor scrape job (for Windows only) (optional)

1. Add a default scrape job to Prometheus configuration file.

If JP1/IM - Agent 13-11 or later is newly installed, it does not need to be executed.

If you upgrade JP1/IM - Agent from a version earlier than 13-11 to 13-11 or later, Prometheus configuration file model files stored in *JP1/IM-Agent-Installation-destination-folder\jplima\conf* are updated. Add the following content of Prometheus configuration file model file (jpc_prometheus_server) (.yml.model) to Prometheus configuration file (jpc_prometheus_server) scrape_configs.

For logical hosts, refresh *shared-folder\jplima\conf\jpc_prometheus_server.yml*.

<What to append>

```

scrape_configs:
- job_name: 'jpc_hyperv'

  file_sd_configs:
  - files:
    - 'jpc_file_sd_config_windows_hyperv.yml'

  metric_relabel_configs:
  - source_labels: ['__name__']
    regex: 'windows_hyperv_vm_cpu_total_run_time|windows_hyperv_vm_device_bytes_written|windows_hyperv_vm_device_bytes_read|windows_hyperv_host_cpu_total_run_time|windows_hyperv_vswitch_bytes_received_total|windows_hyperv_vswitch_bytes_sent_total|windows_cs_logical_processors|windows_hyperv_vm_cpu_hypervisor_run_time'
    action: 'keep'
  - source_labels: ['__name__']
    regex: 'windows_hyperv_host_.*|windows_hyperv_vswitch_.*|windows_h

```

```

yperv_vm_cpu_.*|windows_cs_.*'
  target_label: jpl_pc_nodelabel
  replacement: Hyperv metric collector(Hypervisor)
- source_labels: ['__name__', 'instance']
  regex: 'windows_hyperv_vm_device_.*;([[::]]+):?.*'
  target_label: jpl_pc_nodelabel
  replacement: 'Hyperv metric collector(VM) Hypervisor:${1}'
- source_labels: ['__name__', 'instance']
  regex: 'windows_hyperv_vm_cpu_total_run_time;([[::]]+):?.*'
  target_label: jpl_pc_nodelabel
  replacement: 'Hyperv metric collector(VM) Hypervisor:${1}'
- source_labels: ['vm', '__name__']
  regex: '(.*)windows_hyperv_vm_cpu_total_run_time'
  target_label: instance
  replacement: ${1}
  action: replace
- source_labels: ['vm_device']
  regex: '^(.*)-([[::]]+)(?:_[[::]]+)?\.[[::]]+*$'
  target_label: instance
  replacement: ${2}
  action: replace
- source_labels: ['__name__']
  regex: 'windows_hyperv_host_.*|windows_hyperv_vswitch_.*|windows_h
yperv_vm_cpu_hypervisor_.*|windows_cs_.*'
  target_label: jpl_pc_trendname
  replacement: windows_exporter_hyperv_host
- source_labels: ['__name__']
  regex: 'windows_hyperv_host_.*|windows_hyperv_vswitch_.*|windows_h
yperv_vm_cpu_hypervisor_.*|windows_cs_.*'
  target_label: jpl_pc_category
  replacement: VirtualMachine Host
- source_labels: ['__name__']
  regex: 'windows_hyperv_vm_device_.*|windows_hyperv_vm_cpu_total_ru
n_time'
  target_label: jpl_pc_trendname
  replacement: windows_exporter_hyperv_vm
- source_labels: ['__name__']
  regex: 'windows_hyperv_vm_device_.*|windows_hyperv_vm_cpu_total_ru
n_time'
  target_label: 'jpl_pc_remote_monitor_instance'
  replacement: 'installation-host-name:Hyperv metric collector(VM) '
  action: 'replace'

```

(4) Setup of Alertmanager

(a) Changing Ports (For Windows) (optional)

The listen port used by Alertmanager is specified in `--web.listen-address` option of `alertmanager` command.

For details about how to change `alertmanager` command options, see [1.21.2\(1\)\(c\) Change command-line options \(for Windows\)](#). For details of `--web.listen-address` option, see `alertmanager` command options in *Service definition file (jpc_program-name_service.xml)* in *Chapter 2. Definition Files in the JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

The default port is "20714". If port number is changed, review setup of the firewall and prohibit accessing from outside. However, if you want to monitor Alertmanager with external shape monitoring by Blackbox exporter in other host, allow it to be accessed. In such cases, consider security measures such as limiting the source IP address as required.

(b) Changing the alert notification destination (for Windows) (optional)

To specify Alert destinations, write the URL and port of imagentproxy processes running on the same host to `recieivers.webhook_config.url` in Alertmanager configuration file (`jpc_alertmanager.yml`). You need to change it only if you want to change imagentproxy process port.

For instructions on how to change configuration file, see [1.21.2\(1\)\(a\) Edit the configuration files \(for Windows\)](#).

(c) Setup silence (for Windows) (optional)

Execute the command from JP1/IM - Manager to the host where Alertmanager whose silence you want to setup is running. Use curl command to call REST API that setup silence.

For REST API on how to setup silence, see [5.22.4 Silence creation of Alertmanager](#) in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

Settings in silence to be specified in message body of the request is passed in curl command argument.

(5) Setup of Windows exporter

(a) Change Port (optional)

The listen port used by Windows exporter is specified in `--telemetry.addr` option of the `windows_exporter` command.

For details about how to change `windows_exporter` command options, see [1.21.2\(1\)\(c\) Change command-line options \(for Windows\)](#). For details of `--telemetry.addr` option, see `windows_exporter command options` in *Service definition file (jpc_program-name_service.xml)* in *Chapter 2. Definition Files* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

The default port is "20717". If port number is changed, review setup of the firewall and prohibit accessing from outside.

(b) Modify metric to Collect (optional)

1. Add metric to Prometheus configuration file.

In the `metric_relabel_configs` of Prometheus configuration file (`jpc_prometheus_server.yml`), metric to be collected are defined separated by "|". Delete metric that you do not need to collect and Add metric that you want to collect.

For instructions on updating configuration file, see [1.21.2\(1\)\(a\) Edit the configuration files \(for Windows\)](#).

<Sample Setup>

```
- job_name: 'jpc_windows'
  :
  metric_relabel_configs:
    - source_labels: ['__name__']
      regex: 'windows_cache_copy_read_hits_total| Windows_cache_copy_read_hits_total| Windows_cpu_time_total| Windows_logical_disk_free_bytes| Windows_logical_disk_idle_seconds_total| Windows_logical_disk_read_bytes_total|...|windows_net_packets_sent_total| Windows_net_packets_received_total| Windows_system_context_switches_total| Windows_system_processor_queue_length| Windows_system_system_calls_total [Add metric here]'
```


2. If required, define a trend view in metric Definition file.

In Windows exporter and Windows exporter (process monitoring) metric definition files, you define a trend view. For descriptions, see *Windows exporter metric definition file (metrics_windows_exporter.conf)* and *Windows exporter (process monitoring) metric definition file (metrics_windows_exporter_process.conf)* in Chapter 2. *Definition Files in the JP1/Integrated Management 3 - Manager Command, Definition File and API Reference.*

3. Configure the service monitor settings.

- Editing Windows exporter configuration file (jpc_windows_exporter.yml)

When performing service monitoring, Windows exporter configuration file (jpc_windows_exporter.yml) is edited as shown below.

```
collectors:
  enabled: cache,cpu,logical_disk,memory,net,system,cs,process,service
collector:
  logical_disk:
    volume-whitelist: ".+"
    volume-blacklist: ""
  net:
    nic-whitelist: ".+"
    nic-blacklist: ""
  process:
    whitelist: ""
    blacklist: ""
  service:
    services-where: "WQL's-Where-phrase"
scrape:
  timeout-margin: 0.5
```

If "service" is not set for "enabled" of "collectors", add the "service" setting.

If "service" of "collector" is not set, add "service" and "services-where" lines. The value of "services-where" is Where phrase of WQL and sets the service name of the service to be monitored in the format "Name='service-name'". If the service name is set to exact match and you want to monitor more than one service, connect them with a OR and set them in the format "Name='service-name' OR Name='service-name' OR ...".

- Sample definitions of Windows exporter configuration file (jpc_windows_exporter.yml)

The following is a sample definition for monitoring jpc_imagent and jpc_imagentproxy servicing:

```
collectors:
  enabled: cache,cpu,logical_disk,memory,net,system,cs,process,service
collector:
  logical_disk:
    volume-whitelist: ".+"
    volume-blacklist: ""
  net:
    nic-whitelist: ".+"
    nic-blacklist: ""
  process:
    whitelist: ""
    blacklist: ""
  service:
    services-where: "Name='jpc_imagent' OR Name='jpc_imagentproxy'"
scrape:
  timeout-margin: 0.5
```


(c) Specifying monitored processes (required)

- Edit the Windows exporter configuration file (jpc_windows_exporter.yml)

Edit the Windows exporter configuration file (jpc_windows_exporter.yml) to define which processes are to be monitored.

By default, no process is to be monitored, and therefore you will specify the processes you want to monitor in the Windows exporter configuration file.

For details on the Windows exporter configuration file, see *Windows exporter configuration file (jpc_windows_exporter.yml)* in *Chapter 2. Definition Files* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

(6) Setup of Blackbox exporter

(a) Changing Ports (For Windows) (optional)

The listen port used by Blackbox exporter is specified in `--web.listen-address` option of the `blackbox_exporter` command.

For details about how to change `blackbox_exporter` command options, see [1.21.2\(1\)\(c\) Change command-line options \(for Windows\)](#). For details of `--web.listen-address` option, see *blackbox_exporter command options* in *Service definition file (jpc_program-name_service.xml)* in *Chapter 2. Definition Files* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

The default port is "20715". If port number is changed, review setup of the firewall and prohibit accessing from outside.

(b) Add, change, and delete modules (for Windows) (optional)

For each target (host or URL), it must be defined monitoring methods, such as protocols and authentication data in Blackbox exporter.

The following modules are defined in the default setup:

Table 1–14: Modules Defined in the Initial Setup

Module name	Feature
http	- Monitor http/https. - The method is "GET" and the headers are not setup. - Client authentication, Server authentication, and HTTP authentication (Basic authentication) are not performed. - When http/https's URL is accessed and a status code in 200-299 is returned, 1 is setup to the <code>probe_success</code> (metric). - If communication to URL is not possible or if the status code is not in 200-299, 0 is setup to metric. - If the target is redirected, it depends on the status code of the redirected target.
icmp	- Monitor icmp. - Authentication is not performed. - If icmp communication can be performed for the host or IP address to be monitored, 1 is setup to metric. If communication is not possible, 0 is setup.

If monitoring is possible with the module of the default setup, there is no need to define a new one. If there are requirements that cannot be monitored by the module in the initial setup, as shown below, the module definition must be added.

- When authentication is required

- To change the judgment based on the content of the response

Modules are defined in Blackbox exporter configuration file. For descriptions, see *Blackbox exporter configuration file (jpc_blackbox_exporter.yml)* in *Chapter 2. Definition Files* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

The following shows description rules:

- Setup the new module-name as follows:
 - When performing HTTP/HTTPS monitoring
Setup the name starting with http.
 - For ICMP monitoring
Setup the name starting with icmp.
- If you are creating a client-side authentication, a Server authentication, or a HTTP authentication (Basic authentication) module, you will need a certificate and a setup of password.

For the location of the certificate, see the list of files/directories in the *Appendix A.4 JP1/IM - Agent* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

For details about HTTP authentication (Basic authentication) Password's Setting method, see *1.21.2(6)(e) Setup the proxy authentication ID and Password (for Windows) (optional)* and *1.21.2(6)(f) Setup authentication ID, Password, and Bearer tokens for accessing the monitored Web Server (for Windows) (optional)*.

Table 1–15: Monitoring requirements and required setup

Monitoring conditions	Required File	Required Setup
Server authentication	Place CA certificate of authentication station that issued the server certificate of the target in <i>Agent-path</i> \conf\user\cert.	Setup the contents below to <code>tls_config</code> of Blackbox exporter configuration file. • Setup <code>ca_file</code> for CA certificate path • Setup <code>false</code> to the <code>insecure_skip_verify</code>
No server authentication	None.	Setup the contents below to the <code>tls_config</code> of Blackbox exporter configuration file. • Setup <code>true</code> to <code>insecure_skip_verify</code>
Client authentication	• Place the client certificate in <i>Agent-path</i>\conf\cert. • Place the client certificate key File in <i>Agent-path</i>\conf\user\secret.	Setup the contents below to <code>tls_config</code> of Blackbox exporter configuration file. • Setup the client certificate path to <code>cert_file</code> • Setup the client certificate key File to <code>key_file</code>
No client authentication	None.	None.
Basic authentication	None.	Setup the contents below to <code>basic_auth</code> of Blackbox exporter configuration file. • Setup User name used for Basic authentication in <code>username</code> For details about Basic authentication's Password's Setup, see <i>1.21.2(6)(f) Setup authentication ID, Password, and Bearer tokens for accessing the monitored Web Server (for Windows) (optional)</i>.

For instructions on updating Blackbox exporter configuration file and deploying the certificate File, see *1.21.2(1)(a) Edit the configuration files (for Windows)*.

If it needs to from Blackbox exporter to access the monitored Web Server through a proxy server, the proxy server's setup is required. See [1.21.2\(6\)\(d\) Monitoring HTTP through proxy \(for Windows\) \(optional\)](#)".

If you Add the module definition, you will need to define a scrape job to scrape with the newly created module from Prometheus server. For details about setup on Prometheus server, see [1.21.2\(3\)\(c\) Add Blackbox exporter scrape job \(for Windows\) \(optional\)](#).

(c) Add, change, or Delete the monitoring target (for Windows) (required)

Monitoring targets of Blackbox exporter are listed in definition file in the following tables.

After you Add the targets, you must refresh IM management node tree. For details, see [1.21.2\(19\) Creation and import of IM management node tree data \(for Windows\) \(required\)](#).

- Blackbox exporter (HTTP/HTTPS monitoring) discovery configuration file

Item	Description
File Name	• <code>jpc_file_sd_config_blackbox_http.yml</code> • <code>file_sd_config_blackbox_module-name-begins-with-http.yml</code>
Setup target	Define the monitoring target of HTTP/HTTPS.
Format	See <i>Blackbox exporter (HTTP/HTTPS monitoring) discovery configuration file</i> (<code>jpc_file_sd_config_blackbox_http.yml</code>) in <i>Chapter 2. Definition Files</i> in the <i>JP1/Integrated Management 3 - Manager Command, Definition File and API Reference</i> .
Update procedure	See 1.21.2(1)(a) Edit the configuration files (for Windows) .

- Blackbox exporter (ICMP monitoring) discovery configuration file

Item	Description
File Name	• <code>jpc_file_sd_config_blackbox_icmp.yml</code> • <code>file_sd_config_blackbox_module-name-begins-with-icmp.yml</code>
Setup target	Define the monitoring target of ICMP.
Format	See <i>Blackbox exporter (ICMP monitoring) discovery configuration file</i> (<code>jpc_file_sd_config_blackbox_icmp.yml</code>) in <i>Chapter 2. Definition Files</i> in the <i>JP1/Integrated Management 3 - Manager Command, Definition File and API Reference</i> .
Update procedure	See 1.21.2(1)(a) Edit the configuration files (for Windows) .

(d) Monitoring HTTP through proxy (for Windows) (optional)

Setup "proxy_url" to Blackbox exporter configuration file (`jpc_blackbox_exporter.yml`).

For details about the Blackbox exporter configuration file, see *Blackbox exporter configuration file* (`jpc_blackbox_exporter.yml`) in *Chapter 2. Definition Files* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

For details on updating Blackbox exporter configuration file, see [1.21.2\(1\)\(a\) Edit the configuration files \(for Windows\)](#).

Note that authentication ID and Password must be setup when authentication is routed through the required proxies. For setting method of authentication ID and Password, see [1.21.2\(6\)\(e\) Setup the proxy authentication ID and Password \(for Windows\) \(optional\)](#).

When you skip DNS resolution and change of URL performed by Blackbox exporter, it is necessary to set `skip_resolve_phase_with_proxy` true in Blackbox exporter configuration file (`jpc_blackbox_exporter.yml`). For details and the example of case that setting of `skip_resolve_phase_with_proxy` is necessary, see *Blackbox exporter*

configuration file (`jpc_blackbox_exporter.yml`) in *Chapter 2. Definition Files in the JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

(e) Setup the proxy authentication ID and Password (for Windows) (optional)

When performing HTTP/HTTPS monitoring, if there is a proxy server that requires a Basic authentication between Blackbox exporter and the monitored Web Server, authentication ID and Password must be setup.

Authentication ID is specified in "modules. module-name. http.proxy_user" of Blackbox exporter configuration file (`jpc_blackbox_exporter.yml`). For details about Setting method of Blackbox exporter configuration file, see [1.21.2\(1\)\(a\) Edit the configuration files \(for Windows\)](#).

Set Password in the following ways: For details, refer to the explanation for each item.

- Secret management command
- List of Secrets dialog box of integrated operation viewer
- REST API of Secret Management of integrated operation viewer

(f) Setup authentication ID, Password, and Bearer tokens for accessing the monitored Web Server (for Windows) (optional)

When you perform HTTP/HTTPS monitoring, you must setup authentication ID, Password, and Bearer tokens if Basic authentication is required for accessing the monitored Web Server.

Authentication ID is specified in "modules. module-name. http.basic_auth.username" of Blackbox exporter configuration file (`jpc_blackbox_exporter.yml`). For details about setting method of Blackbox exporter configuration file, see [1.21.2\(1\)\(a\) Edit the configuration files \(for Windows\)](#).

Password and Bearer tokens are setup in the following ways: For details, refer to the explanation for each item.

- Secret management command
- List of Secrets dialog box of integrated operation viewer
- REST API of Secret Management of integrated operation viewer

(7) Setup in Yet another cloudwatch exporter

(a) Changing Ports (For Windows) (optional)

The listen port used by Yet another cloudwatch exporter is specified in `-listen-address` option of `yet-another-cloudwatch-exporter` command.

For details about how to change the options of `yet-another-cloudwatch-exporter` command, see [1.21.2\(1\)\(c\) Change command-line options \(for Windows\)](#). For details of `-listen-address` option, see *yet-another-cloudwatch-exporter command options in Unit definition file (`jpc_program-name.service`) in Chapter 2. Definition Files in the JP1/Integrated Management 3 - Manager, Command Definition File and API Reference*.

The default port is "20718". If port number is changed, review setup of the firewall and prohibit accessing from outside.

(b) Modify Setup to connect to CloudWatch (for Windows) (required)

There are two ways to connect to CloudWatch from Yet another cloudwatch exporter: using an access key (hereinafter referred to as the access key method) and using an IAM role (hereinafter referred to as the IAM role method). If you

install Yet another cloudwatch exporter on a host other than AWS/EC2, you can only use the access key method. If you are installing Yet another cloudwatch exporter on AWS/EC2, you can use the access key method or the IAM role method.

The procedure for connecting to CloudWatch is described in the following four patterns.

- Access Key Method (Part 1)
Connect to CloudWatch as an IAM user in your AWS account
- Access Key Method (Part 2)
Create multiple IAM users in your AWS account with the same role, and connect to CloudWatch with IAM users in this role
- IAM Role Method (Part 1)
Connect to CloudWatch with an AWS account for which you have configured an IAM role
- IAM Role Method (Part 2)
Connect to CloudWatch with multiple AWS accounts with the same IAM role

- When connecting to CloudWatch with access method (part 1)

1. Create an IAM policy "yace_policy" in your AWS account (1) and set the following JSON format information.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "CloudWatchExporterPolicy",
      "Effect": "Allow",
      "Action": [
        "tag:GetResources",
        "cloudwatch:ListTagsForResource",
        "cloudwatch:GetMetricData",
        "cloudwatch:ListMetrics"
      ],
      "Resource": "*"
    }
  ]
}
```

2. Create an IAM group "yace_group" in the AWS account (1) and assign the IAM policy "yace_policy" created in step 1.
3. Create IAM user "yace_user" in AWS account (1) and belong to the IAM group "yace_group" created in step 2.
4. On the host of the monitoring module, create a credentials file in the "/root/.aws/" directory, and set the access key and secret access key of the IAM user "yace_user" created in step 3 in the [default] section of the credentials file.

- When connecting to CloudWatch with access method (part 2)

1. Create IAM policy "yace_policy" in AWS account (2) and set the same JSON format information as in step 1 of *Access method (Part 1)*.
2. Create the IAM role "cross_access_role" in AWS account (2), select "Another AWS account" for [Select trusted entity type], and specify the account ID of AWS account (1) as the account ID.
3. Assign the IAM policy "yace_policy" created in step 1 to the IAM role "cross_access_role" created in step 2.

4. Create IAM policy "yace_policy" in AWS account (1) and set the same JSON format information as in step 1 of *Access method (Part 1)*.
5. Create IAM policy "account2_yace_policy" in AWS account (1) and set the following JSON format information.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "sts:AssumeRole",
      "Resource": "arn:aws:iam::AWS-account(2):role/cross_access_role"
    }
  ]
}
```

The underlined "cross_access_role" is the name of IAM role created in step 2.

6. Create an IAM group "yace_group" in your AWS account (1), and assign the IAM policy "yace_policy" created in step 1 and the IAM policy "account2_yace_policy" created in step 5.
7. Create IAM user "yace_user" in AWS account (1) and belong to the IAM group "yace_group" created in step 6.
8. On the host of the monitoring module, create a credentials file in the "/root/.aws/" directory, and set the access key and secret access key of the IAM user "yace_user" created in step 7 in the [default] section of the credentials file.
9. Add the following definition[#] of AWS account (2) to the Yet another cloudwatch exporter configuration file (ya_cloudwatch_exporter.yml).

```
discovery:
  exportedTagsOnMetrics:
    AWS/S3:
      - jpl_pc_nodelabel
  jobs:
    - type: AWS/S3
      regions:
        - us-east-2
      metrics:
        - name: BucketSizeBytes
          statistics:
            - Sum
          period: 300000
          length: 400000
          nilToZero: true

    - type: AWS/S3
      regions:
        - us-east-2
      roles:
        - roleArn: "arn:aws:iam::AWS-account(2):role/cross_access_role"
      metrics:
        - name: BucketSizeBytes
          statistics:
            - Sum
          period: 300000
```

```
length: 400000
nilToZero: true
```

#

Lines 1 to 15 show the collection settings of AWS account (1), and lines 17 and later show the collection settings of AWS account (2).

In the collection settings of AWS account (2), "roles.roleArn" must be specified. You can specify up to two AWS accounts for "roles.roleArn", but if you want to specify two or more accounts, please contact Hitachi Sales.

- When connecting to CloudWatch using the IAM role method (Part 1)

1. Create IAM policy "yace_policy" in AWS account (1) and set the same JSON format information as in step 1 of *Access method (Part 1)*.
2. Create an IAM role "yace_role" in your AWS account (1), and select AWS service for [Select trusted entity type] and EC2 for [Select use case].
3. Assign the IAM policy "yace_policy" created in step 1 to the IAM role "yace_role" created in step 2.
4. Assign the IAM role "yace_role" created in steps 2~3 to the EC2 instance where the monitoring module of AWS account (1) is installed[#].

#

Open the EC screen of the AWS console and execute it in the menu of [Action] - [Security] - [Change IAM Role].

- When connecting to CloudWatch using the IAM role method (part 2)

1. Create IAM policy "yace_policy" in AWS account (2) and set the same JSON format information as in step 1 of *Access method (Part 1)*.
2. Create the IAM role "cross_access_role" in AWS account (2), select "Another AWS account" for [Select trusted entity type], and specify the account ID of AWS account (1) as the account ID. Also, specify an external ID if necessary.
3. Create IAM policy "account2_yace_policy" in AWS account (1) and set the following JSON format information.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "sts:AssumeRole",
      "Resource": "arn:aws:iam::AWS-account (2):role/cross_access_role"
    }
  ]
}
```

The underlined "cross_access_role" is the name of IAM role created in step 2.

4. Create an IAM role "yace_role" in your AWS account (1), and select AWS service for [Select trusted entity type] and EC2 for [Select use case].
5. Assign the IAM policy "account2_yace_policy" created in step 3 to the IAM role "yace_role" created in step 4.

6. Assign the IAM role "yace_role" created in step 4 to the EC2 instance where the monitoring module of the AWS account (1) is installed.[#]

Open the EC screen of the AWS console and execute it in the menu of [Action] - [Security] - [Change IAM Role].

7. Add the following definition[#] of AWS account (2) to the Yet another cloudwatch exporter configuration file (ya_cloudwatch_exporter.yml).

```
discovery:
  exportedTagsOnMetrics:
    AWS/S3:
      - jpl_pc_nodelabel
  jobs:
    - type: AWS/S3
      regions:
        - us-east-2
      roles:
        - roleArn: "arn:aws:iam::AWS-account(2):role/cross_access_role"
          externalId: "External-ID"
      metrics:
        - name: BucketSizeBytes
          statistics:
            - Sum
          period: 300000
          length: 400000
          nilToZero: true
```


Lines 9~11 show the collection settings for AWS account (2).

In the collection settings of AWS account (2), "roles.roleArn" must be specified. You can specify up to two AWS accounts for "roles.roleArn", but if you want to specify two or more accounts, please contact Hitachi Sales.

Specify "externalId" in the collection settings of your AWS account (2) only if you specified an external ID in step 2.

(c) Connect to CloudWatch through a proxy (for Windows) (optional)

If you need to connect to CloudWatch through a proxy, use the environment variable HTTPS_PROXY (the environment variable HTTP_PROXY is not available).

The format of value specified in the environment-variable HTTPS_PROXY is shown below.

```
http://proxy-user-name:password@proxy-server-host-name:port-number
```

Important

Note that value begins with "http://" in HTTPS_PROXY of the environment variable-name.

■ For Windows

1. Stop Yet another cloudwatch exporter.
2. Open the System Properties dialog from [Setup] - [System] - [Detailed Information] - [Related settings] - [System Detail settings].

3. Click the [Environment Variable] to display the Environment Variables dialog box.

4. Setup the system environment as follows.

Variable Name	Value
HTTPS_PROXY	<code>http://proxy-user-name:password@proxy-server-host-name:port-number</code>

5. Start Yet another cloudwatch exporter.

Important

- Because the environment variable HTTPS_PROXY is setup to the system environment variable, it is reflected in all processes running on that host.
- It is important to note that system environment variables can be displayed by anyone who can Login them. When Password is specified in the environment-variable HTTPS_PROXY, measures such as limiting the number of users who can login the system are required.

■ For Linux

1. Stop Yet another cloudwatch exporter.

2. Create any File and describe it as follows:

```
HTTPS_PROXY=http://proxy-user-name:Password@proxy-server-host-name:port-number
```

For details of what to write, execute `man systemd.exec` and check value that has been Setup to "EnvironmentFile=".

3. Add EnvironmentFile to unit definition file and write file path created in step 2.

```
:
[Service]
EnvironmentFile = "path-of-file-created-in-step-2"
WorkingDirectory = ....
ExecStart = ....
:
```

4. Refresh systemd.

Execute the following command:

```
systemctl daemon-reload
```

5. Start Yet another cloudwatch exporter.

(d) Add AWS Services to be Monitored (optional)

The following AWS services are monitored by default: If you want to monitor other AWS services, follow the steps here.

- AWS/EC2
- AWS/Lambda
- AWS/S3
- AWS/DynamoDB

- AWS/States
- AWS/SQS
- AWS/EBS
- AWS/ECS
- AWS/EFS
- AWS/FSx
- AWS/RDS
- AWS/SNS
- ECS/ContainerInsights

1. Add AWS service definition in Yet another cloudwatch exporter configuration file.

For details about editing, see [1.21.2\(1\)\(a\) Edit the configuration files \(for Windows\)](#).

Add AWS service definition to the underlined sections below.

- discovery.exportedTagsOnMetrics

- Description

```
discovery:
  exportedTagsOnMetrics:
    AWS-service-name:
      - jpl_pc_nodelabel
```

- Sample Setup

```
discovery:
  exportedTagsOnMetrics:
    AWS/EC2:
      - jpl_pc_nodelabel
```

- discovery.jobs

- Description

```
discovery:
  :
  jobs:
    - type: AWS-service-name
      regions:
        - AWS-region
      period: 0
      length: 600
      delay: 120
      metrics:
```

- Sample Setup

```
discovery:
  :
  jobs:
    - type: AWS/EC2
      regions:
        - ap-northeast-1
      period: 0
      length: 600
```

```
delay: 120
metrics:
```

2. Add metric you want to collect.

See [1.21.2\(7\)\(f\) Modify metric to Collect \(optional\)](#).

(e) Monitoring AWS Resources (required)

For AWS resource to be monitored by Yet another cloudwatch exporter, the `jp1_pc_nodelabel` tag must be setup to AWS resource that you want to monitor. See AWS documentation for how to set the tags for AWS resource.

For `jp1_pc_nodelabel` tag, setup the following value: Specify an alphanumeric character or hyphen within the range of 1 to 255 characters.

- For EC2
Specify the host name.
- Other than EC2
Specifies the text that is labeled in IM management node.

Important

- Setup a string that is unique within AWS services. You can setup the same string for different services - for example, EC2 and Lambda.
- Accounts with different Yet another cloudwatch exporter monitoring destinations must be different string. Even in different regions, for the same service, use different strings.
- If a string is duplicated, only one IM management node is created.

The value set in `jp1_pc_nodelabel` tags is added as the value of `jp1_pc_nodelabel` label of samples collected by Yet another cloudwatch exporter.

(f) Modify metric to Collect (optional)

1. Verify metric collected on CloudWatch.

Verify that metric that you want to collect is collected on CloudWatch.

In addition, you must have verified setup for CloudWatch metric name and CloudWatch statistic types in preparation for setup in the following steps.

For details about CloudWatch metric name and CloudWatch statistical types, see "Amazon CloudWatch User Guide" in AWS documentation.

2. Add definition of CloudWatch metric to Yet another cloudwatch exporter configuration file.

The underlined sections of `discovery.jobs.metrics` below describe CloudWatch metric definitions.

```
discovery:
  :
  jobs:
  - type: AWS-service-name
    regions:
      - AWS-region
    period: 0
    length: 600
    delay: 120
    metrics:
```

```

- name: CloudWatch-metric-name-1#1
  statistics:
    - CloudWatch-statistic-types#2
- name: CloudWatch-metric-name-2#3
  statistics:
    - CloudWatch-statistic-types#4
- name: CloudWatch-metric-name-3#5
  statistics:
    - CloudWatch-statistic-types#6
:

```

#1 Example of 1 CloudWatch metric name1: CPUUtilization

#2 Sample 2 CloudWatch statistical types: Average

#3 Example of 3 CloudWatch metric name2: DiskReadBytes

#4 Sample 4 CloudWatch statistical types: Sum

#5 Example of 5 CloudWatch metric name3: DiskWriteBytes

#6 Sample 6 CloudWatch statistical types: Sum

3. Add metric to Prometheus configuration file.

Value of metric `relabel_configs` lists metric to collect, separated by |. Add metric that you want to collect. Also, Delete metric that does not need to be collected. For the naming conventions for metric names, see *Naming conventions for Exporter metrics* in 3.15.1(1)(g) *Yet another cloudwatch exporter (Azure Monitor performance data collection capability)* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

For details on editing Prometheus configuration file, see [1.21.2\(1\)\(a\) Edit the configuration files \(for Windows\)](#).

<Sample Setup>

```

- job_name: 'jpc_cloudwatch'
  :
  metric_relabel_configs:
    - regex: 'tag_(jpl_pc_.*)'
      replacement: ${1}
      action: labelmap
    - regex: 'tag_(jpl_pc_.*)'
      action: 'labeldrop'
    - source_labels: ['__name__', 'jpl_pc_node_label']
      regex: '(aws_ec2_cpuutilization_average|aws_ec2_disk_read_bytes_sum|aws_ec2_disk_write_bytes_sum|aws_lambda_errors_sum|aws_lambda_duration_average|aws_s3_bucket_size_bytes_sum|aws_s3_5xx_errors_sum|aws_dynamodb_consumed_read_capacity_units_sum|aws_dynamodb_consumed_write_capacity_units_sum|aws_states_execution_time_average|aws_states_executions_failed_sum|aws_sqs_approximate_number_of_messages_delayed_sum|aws_sqs_number_of_messages_deleted_sum [Add metrics here as "|" separated by]);. +$'
      action: 'keep'

```

4. If required, define a trend view in metric definition file.

For descriptions, see *Yet another cloudwatch exporter metric definition file (metrics_ya_cloudwatch_exporter.conf)* in Chapter 2. *Definition Files* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

(8) Set up of Promitor

If you use Promitor for monitoring, configure the following settings.

(a) Configuring the settings for establishing a connection to Azure (required)

- Modify the service definition file (for Windows) or the unit definition file (for Linux)

You specify the storage location of the Promitor configuration file with an absolute path in the `PROMITOR_CONFIG_FOLDER` environment variable. Modify this environment variable, which is found in the service definition file (for Windows) or the unit definition file (for Linux). For details on the service definition file (for Windows) and the unit definition file (for Linux), see the sections describing the applicable files under *Chapter 2. Definition Files in the JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

- Modify the Promitor Scraper runtime configuration file (runtime.yaml)

In the Promitor Scraper runtime configuration file (runtime.yaml), specify the path to the Promitor Scraper configuration file (metrics-declaration.yaml) in `metricsConfiguration.absolutePath`. For details on the Promitor Scraper runtime configuration file (runtime.yaml), see the section describing the applicable file under *Chapter 2. Definition Files in the JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

- Configure information for connecting to Azure

Configure authentication information used for Promitor to connect to Azure. For details on how to configure it, see [1.21.2\(8\)\(b\) Configuring authentication information for connecting to Azure](#).

(b) Configuring authentication information for connecting to Azure

Promitor can connect to Azure through the service principal method or the managed ID method. Only the service principal method is available when Promitor is installed in hosts other than Azure Virtual Machines. Both the service principal method and the managed ID method are available when Promitor is installed in Azure Virtual Machines.

The following describes three procedures for connecting to Azure.

- Service principal method
This uses a client secret to connect to Azure.
- Managed ID method (system-assigned)
This uses a system-assigned managed ID to connect to Azure.
- Managed ID method (user-assigned)
This uses a user-assigned managed ID to connect to Azure.

- Using the service principal method to connect to Azure

Perform steps 1 to 3 in Azure Portal and then perform steps 4 to 6 on a host where Promitor has been installed.

1. Create an application and issue a client secret.
2. Obtain an application (client) ID in **Overview** for the application.
3. Select a resource group (or subscription) to be monitored, execute **Access control (IAM) - Add role assignment**, and specify **Monitor Viewer**.
4. Add the client secret value under the **Value** column issued in step 1 to JP1/IM - Agent.
Specify the values in the table below for keys used to register the secret.

Secret registration key	Value
Promitor Resource Discovery key	<code>Promitor.resource_discovery.env.AUTH_APPKEY</code>
Promitor Scraper key	<code>Promitor.scraper.env.AUTH_APPKEY</code>

For details on how to register the secrets, see the description in *3.15.10(2) Adding, changing, or deleting a secret in the JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

Important

When building in a container environment, you cannot perform this step before you create a container image. Create a container, and then perform this step.

5. In the Promitor Scraper runtime configuration file (runtime.yaml) and the Promitor Resource Discovery runtime configuration file (runtime.yaml), specify `ServicePrincipal` for `authentication.mode`.

6. In the Promitor Scraper configuration file (metrics-declaration.yaml) and the Promitor Resource Discovery configuration file (resource-discovery-declaration.yaml), specify the information on the Azure instance to connect to.

- Promitor Scraper configuration file (metrics-declaration.yaml)
Specify the information on the Azure instance to connect to for `azureMetadata`.
- Promitor Resource Discovery configuration file (resource-discovery-declaration.yaml)
Specify the information on the Azure instance to connect to for `azureLandScape`.

- Using the managed ID method (system-assigned) to connect to Azure

Perform steps 1 to 3 in Azure Portal and then perform steps 4 to 6 on a host where Promitor has been installed.

1. In **Virtual Machines**, select the Azure Virtual Machine where Promitor has been installed.
2. Go to **Identity** and then **System assigned**, and change **Status** to **On**.
3. In **Identity - System assigned**, under **Permissions**, select **Azure role assignments** and specify **Monitoring Reader**.
4. In the Promitor Scraper runtime configuration file (runtime.yaml) and the Promitor Resource Discovery runtime configuration file (runtime.yaml), specify `SystemAssignedManagedIdentity` for `authentication.mode`.
5. In the Promitor Scraper configuration file (metrics-declaration.yaml) and the Promitor Resource Discovery configuration file (resource-discovery-declaration.yaml), specify the information on the Azure instance to connect to.
 - Promitor Scraper configuration file (metrics-declaration.yaml)
Specify the information on the Azure instance to connect to for `azureMetadata`.
 - Promitor Resource Discovery configuration file (resource-discovery-declaration.yaml)
Specify the information on the Azure instance to connect to for `azureLandScape`.

- Using the managed ID method (user-assigned) to connect to Azure

Perform steps 1 to 5 in Azure Portal and then perform steps 6 and 7 on a host where Promitor has been installed.

1. In the service search, select **Managed Identities** and then **Create Managed Identity**.
2. Specify a resource group, name, and other information to create a managed ID.
3. In **Azure role assignments**, assign **Monitoring Reader**.
4. In **Virtual Machines**, select the Azure Virtual Machine where Promitor has been installed.

5. Select **Identity**, **User assigned**, and then **Add**, and add the managed ID you created in step 2.
6. In the Promitor Scraper runtime configuration file (runtime.yaml) and the Promitor Resource Discovery runtime configuration file (runtime.yaml), specify `UserAssignedManagedIdentity` for `authentication.mode`.
7. In the Promitor Scraper configuration file (metrics-declaration.yaml) and the Promitor Resource Discovery configuration file (resource-discovery-declaration.yaml), specify the information on the Azure instance to connect to.
 - Promitor Scraper configuration file (metrics-declaration.yaml)
Specify the information on the Azure instance to connect to for `azureMetadata`.
 - Promitor Resource Discovery configuration file (resource-discovery-declaration.yaml)
Specify the information on the Azure instance to connect to for `azureLandScape`.

(c) Configuring a proxy-based connection to Azure (optional)

If your connection to Azure must be established via a proxy, use the `HTTPS_PROXY` environment variable. For details on how to set it up, see [2.19.2\(8\)\(c\) Connect to CloudWatch through a proxy \(for Linux\) \(optional\)](#) in [2.19 Setup for JP1/IM - Agent \(for UNIX\)](#). For `NO_PROXY`, specify the value of `resourceDiscovery.host` in the Promitor Scraper runtime configuration file (runtime.yaml).

(d) Configuring scraping targets (required)

- Configure monitoring targets that must be specified separately (required)

Monitoring targets can be detected automatically by default; however, some of the services, like the ones described below, must be detected manually. For these services to be detected, edit the Promitor Scraper configuration file (metrics-declaration.yaml) to specify your monitoring targets separately.

- Services you must specify separately as monitoring targets
These services are found as the ones with automatic discovery disabled in the table listing the services Promitor can monitor of [3.15.1\(1\)\(h\) Promitor \(Azure Monitor performance data collection capability\)](#) in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.
- How to specify monitoring targets separately
Uncomment a monitoring target in the Promitor Scraper configuration file (metrics-declaration.yaml) and add it to the resources section.

- Change monitoring targets (optional)

In Promitor, monitoring targets can be specified in the following two ways:

- Specifying monitoring targets separately
If you want to separately specify Azure resources to be monitored, add them to the Promitor Scraper configuration file (metrics-declaration.yaml).
- Detecting monitoring targets automatically
If you want to detect resources in your tenant automatically and monitor Azure resources in them, add them to the Promitor Scraper configuration file (metrics-declaration.yaml) and the Promitor Resource Discovery configuration file (resource-discovery-declaration.yaml).

- Change monitoring metrics (optional)

To change metrics to be collected or displayed:

1. Confirm that Azure Monitor has collected the metric.
Confirm that Azure Monitor has collected the metric you want to collect. As preparation for the settings in the next step, check the metric name and the aggregation type.

For the metric name, see "Metric" in "Reference > Supported metrics > Resource metrics" in the Azure Monitor documentation. For the aggregation type, see "Aggregation Type" in "Reference > Supported metrics > Resource metrics" in the Azure Monitor documentation.

2. Edit the settings in the Prometheus configuration file (`jpc_prometheus_server.yml`).

If you want to change metrics to be collected, modify the `metric_relabel_configs` setting in the Prometheus configuration file (`jpc_prometheus_server.yml`).

For details on the Prometheus configuration file, see *Prometheus configuration file (jpc_prometheus_server.yml)* of JP1/IM - Agent in *Chapter 2. Definition Files* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

3. Edit the settings in the Promitor metric definition file (`metrics_promitor.conf`).

If you want to change metrics displayed in the **Trends** tab of the integrated operation viewer, edit the settings in the Promitor metric definition file (`metrics_promitor.conf`).

For details on the Promitor metric definition file, see *Promitor metric definition file (metrics_promitor.conf)* in *Chapter 2. Definition Files* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

(e) Configuring labels for tenant information (optional)

Add labels for the tenant ID and subscription ID of a monitoring target to the property label definition file (`property_labels.conf`). Otherwise, the tenant and subscription show default in the property of an IM management node and an extended attribute of a JP1 event.

For details on the property label definition file, see *Property label definition file (property_labels.conf)* in *Chapter 2. Definition Files* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

(f) Configuring the system node definition file (`imdd_systemnode.conf`) (required)

To create a system node described in 3.15.6(1)(i) *Tree format* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*, edit the system node definition file (`imdd_systemnode.conf`) to configure the setting items listed in the table below. You can specify any values to the items that are not listed in the table.

Table 1–16: Settings in the system node definition file (`imdd_systemnode.conf`)

Item	Value
<code>displayname</code>	Specify the name of the service that publishes metrics for Azure Monitor.
<code>type</code>	It must be specified in uppercase characters as follows: <code>Azure-Azure-service-name</code> <code>Azure-service-name</code> is equivalent to one of the names under the <i>Promitor resourceType name</i> column in the table listing the services Promitor can monitor, in 3.15.1(1)(h) <i>Promitor (Azure Monitor performance data collection capability)</i> in the <i>JP1/Integrated Management 3 - Manager Overview and System Design Guide</i> .
<code>name</code>	This is specified as: <code>[{ ". * " : "regex" }]</code>

The following table shows a setting example of the system node definition file when you create system management nodes for Azure services that are found by default as monitoring targets in the Promitor metric definition file (`metrics_promitor.conf`).

Table 1–17: Setting example of the system node definition file (imdd_systemnode.conf)

Item		
displayName	type	name
Azure Function App	JP1PC-AZURE-FUNCTIONAPP	[{"*":"regex"}]
Azure Container Instances	JP1PC-AZURE-CONTAINERINSTANCE	[{"*":"regex"}]
Azure Kubernetes Service	JP1PC-AZURE-KUBERNETESSERVICE	[{"*":"regex"}]
Azure File Storage	JP1PC-AZURE-FILESTORAGE	[{"*":"regex"}]
Azure Blob Storage	JP1PC-AZURE-BLOBSTORAGE	[{"*":"regex"}]
Azure Service Bus Namespace	JP1PC-AZURE-SERVICEBUSNAMESPACE	[{"*":"regex"}]
Azure Cosmos DB	JP1PC-AZURE-COSMOSDB	[{"*":"regex"}]
Azure SQL Database	JP1PC-AZURE-SQLDATABASE	[{"*":"regex"}]
Azure SQL Server	JP1PC-AZURE-SQLSERVER	[{"*":"regex"}]
Azure SQL Managed Instance	JP1PC-AZURE-SQLMANAGEDINSTANCE	[{"*":"regex"}]
Azure SQL Elastic Pool	JP1PC-AZURE-SQLELASTICPOOL	[{"*":"regex"}]
Azure Logic Apps	JP1PC-AZURE-LOGICAPP	[{"*":"regex"}]

The following shows how the items in the above table can be defined in the system node definition file.

```
{
  "meta":{
    "version":"2"
  },
  "allSystem":[
    {
      "id":"functionApp",
      "displayName":"Azure Function App",
      "objectRoot":[
        {
          "type":"JP1PC-AZURE-FUNCTIONAPP",
          "name":["*":"regex"]
        }
      ]
    },
    {
      "id":"containerInstance",
      "displayName":"Azure Container Instances",
      "objectRoot":[
        {
          "type":"JP1PC-AZURE-CONTAINERINSTANCE",
          "name":["*":"regex"]
        }
      ]
    }
  ]
}
```

```

    ]
  },
  {
    "id": "kubernetesService",
    "displayName": "Azure Kubernetes Service",
    "objectRoot": [
      {
        "type": "JP1PC-AZURE-KUBERNETESSERVICE",
        "name": [{".*": "regexp"}]
      }
    ]
  },
  {
    "id": "fileStorage",
    "displayName": "Azure File Storage",
    "objectRoot": [
      {
        "type": "JP1PC-AZURE-FILESTORAGE",
        "name": [{".*": "regexp"}]
      }
    ]
  },
  {
    "id": "blobStorage",
    "displayName": "Azure Blob Storage",
    "objectRoot": [
      {
        "type": "JP1PC-AZURE-BLOBSTORAGE",
        "name": [{".*": "regexp"}]
      }
    ]
  },
  {
    "id": "serviceBusNamespace",
    "displayName": "Azure Service Bus Namespace",
    "objectRoot": [
      {
        "type": "JP1PC-AZURE-SERVICEBUSNAMESPACE",
        "name": [{".*": "regexp"}]
      }
    ]
  },
  {
    "id": "cosmosDb",
    "displayName": "Azure Cosmos DB",
    "objectRoot": [
      {
        "type": "JP1PC-AZURE-COSMOSDB",
        "name": [{".*": "regexp"}]
      }
    ]
  },
  {
    "id": "sqlDatabase",
    "displayName": "Azure SQL Database",
    "objectRoot": [
      {
        "type": "JP1PC-AZURE-SQLDATABASE",

```

```

        "name": [{".*": "regexp"}]
    }
]
},
{
    "id": "sqlServer",
    "displayName": "Azure SQL Server",
    "objectRoot": [
        {
            "type": "JP1PC-AZURE-SQLSERVER",
            "name": [{".*": "regexp"}]
        }
    ]
},
{
    "id": "sqlManagedInstance",
    "displayName": "Azure SQL Managed Instance",
    "objectRoot": [
        {
            "type": "JP1PC-AZURE-SQLMANAGEDINSTANCE",
            "name": [{".*": "regexp"}]
        }
    ]
},
{
    "id": "sqlElasticPool",
    "displayName": "Azure SQL Elastic Pool",
    "objectRoot": [
        {
            "type": "JP1PC-AZURE-SQLELASTICPOOL",
            "name": [{".*": "regexp"}]
        }
    ]
},
{
    "id": "logicApp",
    "displayName": "Azure Logic Apps",
    "objectRoot": [
        {
            "type": "JP1PC-AZURE-LOGICAPP",
            "name": [{".*": "regexp"}]
        }
    ]
}
]
}

```

With the system node definition file configured, an IM management node is displayed under the system node that has the corresponding Azure service name, when the `jddcreatetree` is run and PromitorSID other than VirtualMachine is created. For PromitorSID of VirtualMachine, an IM management node is displayed under the node that represents the host, without the need for listing the name in the system node definition file.

For details on the system node definition file, see *System node definition file (imdd_systemnode.conf)* in *Chapter 2. Definition Files in the JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

(g) Changing Ports (optional)

■ Specifying a port number of scrape used by Promitor Scraper

The listen port that the Promitor Scraper uses is specified in the Promitor Scraper runtime configuration file (`runtime.yaml`).

For details on how to change configuration file, see [1.21.2\(1\)\(a\) Edit the configuration files \(for Windows\)](#).

The default port is "20719". If port number is changed, review setup of the firewall and prohibit accessing from outside.

Notes:

It is changed in the Promitor Scraper runtime configuration file (`runtime.yaml`), not the command line option. If you change this configuration file, you must also change the Promitor discovery configuration file (`jpc_file_sd_config_promitor.yaml`).

For details, see *Promitor Scraper runtime configuration file (runtime.yaml)* in *Chapter 2. Definition Files* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

■ Specifying a port number of scrape used by Promitor Resource Discovery

The listen port that the Promitor Resource Discovery uses is specified in the Promitor Resource Discovery runtime configuration file (`runtime.yaml`).

For details on how to change configuration file, see [1.21.2\(1\)\(a\) Edit the configuration files \(for Windows\)](#).

The default port is "20720". If port number is changed, review setup of the firewall and prohibit accessing from outside.

Notes:

It is changed in the Promitor Resource Discovery runtime configuration file (`runtime.yaml`), not the command line option. If you change this configuration file, you must also change the Promitor Scraper runtime configuration file (`runtime.yaml`).

For details, see *Promitor Resource Discovery runtime configuration file (runtime.yaml)* in *Chapter 2. Definition Files* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

(9) Setup of Fluentd

(a) Changing Setup of Common Definition file for Log Monitor (for Windows) (optional)

If you want to change the following setup, change setup of log monitoring common definition file:

- Port number of JP1/IM agent control base
- Settings of buffer plugin

For details about the log monitoring common definition file, see *Log monitoring common definition file (jpc_fluentd_common.conf)* in *Chapter 2. Definition Files* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

For details on how to change configuration file, see [1.21.2\(1\)\(a\) Edit the configuration files \(for Windows\)](#).

(b) Monitoring the text-formatted log file (for Windows) (required)

If you want to monitor a new text-formatted log file, perform the following steps:

1. Create a text-formatted log file monitoring definition file.

Create a text-formatted log file monitoring definition file by copying the original template shown below and renaming it to file that you want to copy.

Copy source: *Agent-path\conf\fluentd_@@trapname@@_tail.conf.template*

Copy destination: *Agent-path\conf\user\fluentd_log-monitoring-name_tail.conf*

Copy the template (*fluentd_@@trapname@@_tail.conf.template*) to create text-formatted log file monitoring definition file. Rename the copy destination file to "*fluentd_log-monitoring-name_tail.conf*".

For descriptions of the monitoring text-formatted log file definition file, see *Monitoring text-formatted log file definition file (fluentd_@@trapname@@_tail.conf.template)* in *Chapter 2. Definition Files* in the *JPI/Integrated Management 3 - Manager Command, Definition File and API Reference*.

For details on how to change configuration file, see *1.21.2(1)(a) Edit the configuration files (for Windows)*.

2. Edit the Log Monitor Target Definition File (*jpc_fluentd_common_list.conf*).

If you want to temporarily stop the logging monitoring of some monitoring definitions File, define by enumerating monitoring definition Files in the log monitoring target definition File.

For details about the log monitoring target definition File, see *Log monitoring target definition file (jpc_fluentd_common_list.conf)* in *Chapter 2. Definition Files* in the *JPI/Integrated Management 3 - Manager Command, Definition File and API Reference*. If the log monitoring target definition File is not being edited, no editing is required.

For details on how to change configuration file, see *1.21.2(1)(a) Edit the configuration files (for Windows)*.

3. Apply in integrated operation viewer tree.

For details about Application method, see *1.21.2(19) Creation and import of IM management node tree data (for Windows) (required)*.

Note

If you change the monitoring setup of the textual log file when, for example, the log file trap name of the monitoring definition file is changed, perform steps 2 and 3 above.

(c) Modifying the monitoring settings of the text-formatted log file (for Windows) (optional)

If you want to change the monitoring setup for a text-formatted log file, perform the following steps:

1. Change text-formatted log file monitoring definition file.

Modify the created monitor definition file (*fluentd_log-monitoring-name_tail.conf*).

For descriptions of the monitoring text-formatted log file definition file, see *Monitoring text-formatted log file definition file (fluentd_@@trapname@@_tail.conf.template)* in *Chapter 2. Definition Files* in the *JPI/Integrated Management 3 - Manager Command, Definition File and API Reference*.

For details on how to change configuration file, see *1.21.2(1)(a) Edit the configuration files (for Windows)*.

2. Edit the log monitoring target definition file (*jpc_fluentd_common_list.conf*).

In the log monitoring target definition file, define by listing files of the monitoring definition file:

- When the log monitoring name of the monitoring definition file is changed
- If you are performing operations that temporarily stop logging for some monitoring definition file

For details about the log monitoring target definition file, see *Log monitoring target definition file (jpc_fluentd_common_list.conf)* in *Chapter 2. Definition Files* in the *JPI/Integrated Management 3 - Manager*

Command, Definition File and API Reference. If the log monitoring target definition File is not being edited, no editing is required.

For details on how to change configuration file, see [1.21.2\(1\)\(a\) Edit the configuration files \(for Windows\)](#).

3. Reflect in integrated operation viewer tree.

If value in the [Metric Settings] section is changed, the changes are reflected in integrated operation viewer tree. For details about reflection method, see [1.21.2\(19\) Creation and import of IM management node tree data \(for Windows\) \(required\)](#).

(d) Deleting the monitoring settings of the text-formatted log file (for Windows) (optional)

To Delete monitoring settings in text-formatted logfile, perform the following steps:

1. Delete monitoring text-formatted log file definition file.

Delete the created monitoring definition file (`fluentd_log-monitoring-name_tail.conf`).

For details about how to delete configuration file, see [1.21.2\(1\)\(a\) Edit the configuration files \(for Windows\)](#).

2. Edit the log monitoring target definition file (`jpc_fluentd_common_list.conf`)

To temporarily stop log monitoring for some monitoring definition files, delete the file names of monitoring definition files defined in the log monitoring target definition file.

3. Reflect in integrated operation viewer tree.

For details about reflection method, see [1.21.2\(19\) Creation and import of IM management node tree data \(for Windows\) \(required\)](#).

(e) Monitor Windows Event Log (required)

To monitor a new Windows event log, perform the following steps:

1. Create a Windows event log monitoring definition file.

Create a Windows event log monitoring definition file by copying the following source template and renaming it to the destination definition file:

Copy source: `Agent-path\conf\fluentd_@@trapname@@_wevt.conf.template`

Copy to: `Agent-path\conf\user\fluentd_log-monitoring-name_wevt.conf`

Copy the template (`fluentd_@@trapname@@_wevt.conf.template`) to create Windows event log monitoring definition file. Rename file of copy destination to "`fluentd_log-monitoring-name_wevt.conf`".

For descriptions of Windows event log monitoring definition file, see *Windows event log monitoring definition file (fluentd_@@trapname@@_wevt.conf.template)* in *Chapter 2. Definition Files in the JPI/Integrated Management 3 - Manager Command, Definition File and API Reference*.

For details on how to change configuration file, see [1.21.2\(1\)\(a\) Edit the configuration files \(for Windows\)](#).

2. Edit Windows event log monitoring definition file.

If you want to temporarily stop the logging monitoring of some monitoring definitions file, you must define by listing filenames of the monitoring definition files in Windows event log monitoring definition file.

For details about the log monitoring target definition file, see *Log monitoring target definition file (jpc_fluentd_common_list.conf)* in *Chapter 2. Definition Files in the JPI/Integrated Management 3 - Manager Command, Definition File and API Reference*. If the log monitoring target definition file is not being edited, no editing is required.

For details on how to change configuration file, see [1.21.2\(1\)\(a\) Edit the configuration files \(for Windows\)](#).

3. Reflect in integrated operation viewer tree.

For details about reflection method, see [1.21.2\(19\) Creation and import of IM management node tree data \(for Windows\) \(required\)](#).



Note

If you change the monitoring setup of the textual log file when, for example, the log file trap name of the monitoring definition file is changed, perform steps 2 and 3 above.

(f) Modify the Monitor Setup for Windows Event Log (optional)

If you want to change monitoring settings of Windows event log, perform the following steps:

1. Change Windows event log monitoring definition file.

Change the monitoring definition file (`fluentd_log-monitoring-name_wevt.conf`) that has been created.

For descriptions of Windows event log monitoring definition file, see *Windows event log monitoring definition file (fluentd_@@trapname@@_wevt.conf.template)* in *Chapter 2. Definition Files* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

For details on how to change configuration file, see [1.21.2\(1\)\(a\) Edit the configuration files \(for Windows\)](#).

2. Edit the Log Monitor Target Definition File (`jpc_fluentd_common_list.conf`)

Define by listing filenames of monitoring definition files in log monitor target definition file in the following condition:

- When the log file trap name of the monitor-definition file is changed
- If you are performing operations that temporarily stop monitoring logs for some monitor-definition file

For details about the log monitoring target definition file, see *Log monitoring target definition file (jpc_fluentd_common_list.conf)* in *Chapter 2. Definition Files* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*. If the log monitoring target definition file is not being edited, no editing is required.

For details on how to change configuration file, see [1.21.2\(1\)\(a\) Edit the configuration files \(for Windows\)](#).

3. Apply in integrated operation viewer tree.

If value in the [Metric Settings] section is changed, the changes are reflected in integrated operation viewer tree. For details about reflection method, see [1.21.2\(19\) Creation and import of IM management node tree data \(for Windows\) \(required\)](#).

(g) Delete Monitoring settings of Windows Event Logs (optional)

To delete monitoring settings of Windows event logs, perform the following steps:

1. Delete Windows event log monitoring definition file.

Delete the monitoring definition file (`fluentd_log-monitoring-name_wevt.conf`) that has been created.

For descriptions of Windows event log monitoring definition file, see *Windows event log monitoring definition file (fluentd_@@trapname@@_wevt.conf.template)* in *Chapter 2. Definition Files* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

For details about how to delete configuration file, see [1.21.2\(1\)\(a\) Edit the configuration files \(for Windows\)](#).

2. Edit the log monitoring target definition file (`jpc_fluentd_common_list.conf`)

To temporarily stop log monitoring for some monitoring definition files, delete the filenames of monitoring definition files defined in log monitoring target definition file.

3. Apply in integrated operation viewer tree.

For details about reflection method, see *1.21.2(19) Creation and import of IM management node tree data (for Windows) (required)*.

(h) Setup of the log metrics definition (optional)

If you want to use the log metrics feature, configure the settings of Fluentd of JP1/IM - Agent in the procedure for enabling the add-on programs and then configure the following settings.

■ Editing a log metrics definition file (defining log metrics)

Create a log metrics definition file (fluentd_*any-name*_logmetrics.conf) to define input and output plug-in features.

In addition, the log metric to be monitored is specified in the output plug-in function definition of the log metric definition file.

- When adding log metrics to be monitored:
Add a new <metric> definition in parallel with the existing <metric> definition.
- When changing the log metrics to be monitored:
Change the appropriate <metric> definition.
- When deleting monitored log metrics
Delete or comment out all relevant definitions in the log metrics definition file.

For details on sample log metrics definition files, see the section describing the applicable file under *3.15.1(1)(l) Log metrics* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

■ Editing the log monitoring target definition file (adding include statements)

To enable logs to be monitored as defined in the log metrics definition file, add a row that starts with @include to the log monitoring target definition file (jpc_fluentd_common_list.conf), followed by the name of the log metrics definition file you edited in *Editing a log metrics definition file (defining log metrics)*.

For details on sample log monitoring target definition files, see the section describing the applicable file under *3.15.1(1)(l) Fluentd (Log metrics)* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

■ Restarting Fluentd

To apply the definitions specified in *Editing a log metrics definition file (defining log metrics)* and *Editing the log monitoring target definition file (adding include statements)*, restart Fluentd.

For details on starting and stopping services before the restart, see *Chapter 10. Starting and stopping JP1/IM - Agent* in the *JP1/Integrated Management 3 - Manager Administration Guide*.

■ Setting up log metrics definition in JP1/IM - Manager

If you want to show time-series data on log metrics when trend information of nodes is displayed in the **Trends** tab of the integrated operation viewer of JP1/IM - Manager through the log metrics feature, define log metrics to be shown in JP1/IM - Manager.

Use user-specific metric definitions for the log metrics definitions here.

For descriptions, see *User-specific metric definition file (metrics_*any-Prometheus-trend-name*.conf)* in *Chapter 2. Definition Files* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

(i) Changing Ports (optional)

■ Specifying the port number for scraping used by Fluentd

Specify the port number for scraping used by the fluent-plugin-prometheus plug-in in the log metrics definition file.

Specify the *listening-port-number*[#] for port in <source> described in the following example of changes.

Example of changes:

```
## Input
<worker worker-id-used-for-the-log-metrics-feature>
  <source>
    @type prometheus
    bind 0.0.0.0
    port listening-port-number
    metrics_path /metrics
  </source>
</worker>

<worker worker-id>
<source>
(Omitted)
</source>

(Omitted below)
```

#:

The actual Listen port used by Fluentd (log metrics feature) depends on the `worker_id` of worker used by log metrics feature (the value specified in "worker-id" in log metrics definition file (`fluentd_any-name_logmetrics.conf`)), and is the port number as shown in the following formula.

$24820 + \text{worker\_id}$

If log metrics feature uses 129 worker, the default port number is a sequence number from 24820 to 24948.

■ Changing the port number for scraping used by Prometheus

Change the port number for scraping defined in the Prometheus discovery configuration file to the *listening-port-number+worker-id* specified in *Specifying the port number for scraping used by Fluentd*.

Change the *listening-port-number* for targets in the following example of changes.

```
- targets:
  - name-of-monitored-host:listening-port-number+worker-id
(Omitted)
  labels:
(Omitted)
```

(j) Monitoring SAP system logging (optional)

To monitor SAP system's system log information newly, perform Fluentd setting procedure described below along with Script exporter setting procedure described in [1.21.2\(12\)\(d\) Setting when executing SAP system log extract command \(optional\)](#).

Perform the following steps to newly monitor the system log information of SAP system.

1. Creates the system log information monitoring definition file for SAP system.

Create a text-formatted log file monitoring definition file by copying sample file (fluentd_sap_syslog_tail.conf). Refer to the *File/Directory list* in the *Appendix A.4 JPI/IM - Agent* in the *JPI/Integrated Management 3 - Manager Overview and System Design Guide*. Change the destination file name to "fluentd_log-monitoring_name_tail.conf".

For details about text-formatted log file monitoring definition file descriptions, see *text-formatted log file monitoring definition file (fluentd_@@trapname@@_tail.conf.template)* in *Chapter 2. Definition Files* in the *JPI/Integrated Management 3 - Manager Command, Definition File and API Reference*.

For details about how to change configuration file, see [1.21.2\(1\)\(a\) Edit the configuration files \(for Windows\)](#).

2. Edits the log monitoring target definition file (jpc_fluentd_common_list.conf).

If you want to temporarily stop log monitoring of some monitor definition files, list the names of the monitor definition files in the log monitor target definition file and define them.

For details about the log monitor target definition file descriptions, see *Log monitoring target definition file (jpc_fluentd_common_list.conf)* in *Chapter 2. Definition Files* in the *JPI/Integrated Management 3 - Manager Command, Definition File and API Reference*. You do not need to edit the log monitoring target definition file if you have not already done so.

For details about how to change configuration file, see [1.21.2\(1\)\(a\) Edit the configuration files \(for Windows\)](#).

3. Reflect in integrated operation viewer tree.

For details on how to reflect, see [1.21.2\(19\) Creation and import of IM management node tree data \(for Windows\) \(required\)](#).

(k) Modify SAP system logging monitoring configuration (optional)

For details about how to change the monitoring settings of SAP system's system log information, see [1.21.2\(9\)\(c\) Modifying the monitoring settings of the text-formatted log file \(for Windows\) \(optional\)](#).

(l) Remove SAP system logging monitoring configuration (optional)

For details about deleting the monitoring configuration for SAP system's system log information, see [1.21.2\(9\)\(d\) Deleting the monitoring settings of the text-formatted log file \(for Windows\) \(optional\)](#).

(m) Monitoring CCMS alerting for SAP system (optional)

To newly monitor CCMS alert information in the SAP system, perform the following steps.

1. Creates a CCMS alert-information monitoring definition file for SAP system.

Create a text-formatted log file monitoring definition file by copying sample file (fluentd_sap_alertlog_tail.conf). Refer to the *File/Directory list* in the *Appendix A.4 JPI/IM - Agent* in the *JPI/Integrated Management 3 - Manager Overview and System Design Guide*. Change the destination file name to "fluentd_log-monitoring_name_tail.conf".

For details about text-formatted log file monitoring definition file descriptions, see *text-formatted log file monitoring definition file (fluentd_@@trapname@@_tail.conf.template)* in *Chapter 2. Definition Files* in the *JPI/Integrated Management 3 - Manager Command, Definition File and API Reference*.

For details about how to change configuration file, see [1.21.2\(1\)\(a\) Edit the configuration files \(for Windows\)](#).

2. Edits the log monitoring target definition file (jpc_fluentd_common_list.conf).

If you want to temporarily stop log monitoring of some monitor definition files, list the names of the monitor definition files in the log monitor target definition file and define them.

For details about the log monitor target definition file descriptions, see *Log monitoring target definition file (jpc_fluentd_common_list.conf)* in *Chapter 2. Definition Files* in the *JPI/Integrated Management 3 - Manager*

Command, Definition File and API Reference. You do not need to edit the log monitoring target definition file if you have not already done so.

For details about how to change configuration file, see [1.21.2\(1\)\(a\) Edit the configuration files \(for Windows\)](#).

3. Reflect in integrated operation viewer tree.

For details on how to reflect, see [1.21.2\(19\) Creation and import of IM management node tree data \(for Windows\) \(required\)](#).

(n) Modify SAP system CCMS alert information monitoring settings (optional)

For details about how to change the SAP system CCMS alert information monitoring settings, see [1.21.2\(9\)\(c\) Modifying the monitoring settings of the text-formatted log file \(for Windows\) \(optional\)](#).

(o) Remove SAP system CCMS alert information monitoring settings (optional)

For details about how to delete SAP system CCMS alert information monitoring settings, see [1.21.2\(9\)\(d\) Deleting the monitoring settings of the text-formatted log file \(for Windows\) \(optional\)](#).

(10) Setting up scraping definitions

If you want features provided by the add-on programs to be scraped, provide the scraping definitions listed in the following table.

Table 1–18: Scraping definitions for the features provided by the add-on programs

Feature provided by the add-on programs	OS that the add-on runs on	Exporter or target	Scraping definition
Windows performance data collection	Windows	Windows exporter	Definitions are not required.
Linux process data collection	Linux	Process exporter	
AWS CloudWatch performance data collection	Windows and Linux	Yet another cloudwatch exporter	
Azure Monitor performance data collection		Promitor	
Log metrics		Fluentd	The definition must be provided to use the log metrics feature. For details on what definition is needed, see 1.21.2(10)(a) Scraping definition for the log metrics feature .
UAP monitoring		Script exporter	A monitoring target script must be set up. For details on what settings are needed, see 1.21.2(10)(b) Scraping definition for Script exporter .

(a) Scraping definition for the log metrics feature

A user-defined Exporter scrapes logs based on the scraping definition of the log metrics feature.

- Create a user-specific discovery configuration file (required)

Create a user-specific discovery configuration file (`user_file_sd_config_<any-name>.yaml`) and define what should be monitored.

For details on the user-specific discovery configuration file, see the section describing the applicable file in *Chapter 2. Definition Files* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

For details on what should be defined for the log metrics feature, see the section describing sample files for the applicable file under 3.15.1(1)(l) *Fluentd (Log metrics)* in the *JPI/Integrated Management 3 - Manager Overview and System Design Guide*.

- Set up `scrape_configs` in the Prometheus configuration file (required)

Add the `scrape_configs` setting in the Prometheus configuration file (`jpc_prometheus_server.yml`).

For details on the Prometheus configuration file, see the section describing the applicable file in *Chapter 2. Definition Files* in the *JPI/Integrated Management 3 - Manager Command, Definition File and API Reference*.

For details on what should be defined for the log metrics feature, see the section describing sample files for the applicable file under 3.15.1(1)(l) *Fluentd (Log metrics)* in the *JPI/Integrated Management 3 - Manager Overview and System Design Guide*.

(b) Scraping definition for Script exporter

You can specify a scraping definition by using the `http_sd_config` method by which you run all scripts defined in the Script exporter configuration file (`jpc_script_exporter.yml`) or the `file_sd_config` method by which you specify one of the scripts defined in the Script exporter configuration file (`jpc_script_exporter.yml`) as a `params` element of `scrape_configs` in the Prometheus configuration file (`jpc_prometheus_server.yml`). The default is the `http_sd_config` method.

For details on the Script exporter configuration file and the Prometheus configuration file, see the section describing the applicable file in *Chapter 2. Definition Files* in the *JPI/Integrated Management 3 - Manager Command, Definition File and API Reference*.

The following shows scraping definition examples.

- Example of a scraping definition with the `http_sd_config` method

```
scrape_configs:
  - job_name: jpc_script_exporter
    http_sd_configs:
      - url: http://installation-host-name:port/discovery
    relabel_configs:
      - source_labels: [__param_script]
        target_label: jpl_pc_script
      - target_label: jpl_pc_exporter
        replacement: JPC Script Exporter
      - target_label: jpl_pc_category
        replacement: any-category-name
      - target_label: jpl_pc_trendname
        replacement: script_exporter
      - target_label: jpl_pc_multiple_node
        replacement: jpl_pc_exporter="{job='jpc_script.*',jpl_pc_multiple_no
de=''}"
      - target_label: jpl_pc_nodelabel
        replacement: Script metric collector(Script exporter)
      - target_label: jpl_pc_agent_create_flag
        replacement: false
    metric_relabel_configs:
      - source_labels: [jpl_pc_script]
        target_label: jpl_pc_nodelabel
      - regex: (jpl_pc_multiple_node|jpl_pc_script|jpl_pc_agent_create_flag)
        action: labeldrop
```

installation-host-name

Specify the name of the host where Script exporter has been installed, with 1 to 255 characters other than control characters.

port

Specify the port number Script exporter is going to use.

any-category-name

Specify a category ID of the IM management node for the agent SID, with 1 to 255 characters other than control characters.

- Example of a scraping definition with the `file_sd_config` method

```
scrape_configs:
# Example of running a script in a configuration file
- job_name: any-scraping-job-name-1
  file_sd_configs:
    - files:
        - 'path-to-the-Script-exporter-discovery-configuration-file'
  metrics_path: /probe
  params:
    script: [scripts.name-in-the-Script-exporter-configuration-file]
  relabel_configs:
    - source_labels: [__param_script]
      target_label: jpl_pc_script
    - target_label: jpl_pc_category
      replacement: any-category-name
    - target_label: jpl_pc_nodelabel
      replacement: Script metric collector(Script exporter)
  metric_relabel_configs:
    - source_labels: [jpl_pc_script]
      target_label: jpl_pc_nodelabel
    - regex: (jpl_pc_multiple_node|jpl_pc_script|jpl_pc_agent_create_flag)
      action: labeldrop

# Example of running a script in a configuration file with additional arguments 1 and 2 added to the script
- job_name: any-scraping-job-name-2
  file_sd_configs:
    - files:
        - 'path-to-the-Script-exporter-discovery-configuration-file'
  metrics_path: /probe
  params:
    script: [scripts.name-in-the-Script-exporter-configuration-file]
    argument-name-1: [argument-name-1-value]
    argument-name-2: [argument-name-2-value]
  relabel_configs:
    - source_labels: [__param_script]
      target_label: jpl_pc_script
    - target_label: jpl_pc_category
      replacement: any-category-name
    - target_label: jpl_pc_nodelabel
      replacement: Script metric collector(Script exporter)
  metric_relabel_configs:
    - source_labels: [jpl_pc_script]
      target_label: jpl_pc_nodelabel
```

```
- regex: (jpl_pc_multiple_node|jpl_pc_script|jpl_pc_agent_create_flag)
  action: labeldrop
```

any-scraping-job-name

Specify a given scraping job name that is unique on the host, with 1 to 255 characters other than control characters.

path-to-the-Script-exporter-discovery-configuration-file

Specify the path to the Script exporter discovery configuration file (jpc_file_sd_config_script.yml).

any-category-name

Specify a category ID of the IM management node for the agent SID, with 1 to 255 characters other than control characters.

(11) Setting up container monitoring

You use different features and setup procedures to monitor different monitoring targets. The following table lists what feature you will use and where you can see the setup procedure for each monitoring target.

Monitoring target	Feature you use	See the setup procedure in
Red Hat OpenShift	User-defined Prometheus	Subsections following this table.
Kubernetes		
Amazon Elastic Kubernetes Service (EKS)		
Azure Kubernetes Service (AKS)	Azure's monitoring feature (Promitor) AKS can be monitored by default.	1.21.2(8) Set up of Promitor

- Setting the Authentication Method for User-Specific Prometheus (Required)

1. See the following reference and instruction to obtain the secret:

- Reference

When registering or acquiring IM client secret for use with your own OSS in 3.7.2 IM client secret in the JP1/Integrated Management 3 - Manager Overview and System Design Guide

- Instruction

Click **Add/Delete IM Clients** from the **Option** menu of Integrated Operation Viewer window to display the List of IM Clients window, and when you click the **Add** button, enter the IM client ID from the Add IM Client dialog box to obtain the secret.

2. Create a secret in Red Hat OpenShift or similar environments so that the obtained secret is set in the Authorization header of the remote write configuration as shown below. For the remote write configuration itself, see *remote_write* section in [1.21.2\(11\)\(b\)Configuring the settings for a connection \(required\)](#).

- Authorization Header Configuration for remote write

- When specifying Basic as the authentication method:

"Basic " + *Client-ID : Base64-encoded-ASCII-string-of-Client-Secret*

- When specifying basic_auth as the authentication method:

"basic_auth " + *Client-ID : Base64-encoded-ASCII-string-of-Client-Secret*

Below is an example definition of a secret created in Red Hat OpenShift. For the creation method, see the manual or documentation of the Red Hat OpenShift you are using.

- Example Definition of Secret

The following is an example of the definition when the Client ID obtained in *Step 1* is `openshift_prometheus` and the secret is `secret`.

Note: Depending on Red Hat OpenShift specifications, non-Base64-encoded ASCII strings may be set for the Client ID and secret.

```
kind: Secret
apiVersion: v1
metadata:
  name: jpl-basic-auth
  namespace: openshift-monitoring
data:
  username: b3BlbnNoaWZ0X3Byb21ldGhldXM=
  password: c2VjcjcmV0
type: kubernetes.io/basic-auth
```

(a) Configuring the settings of scraping through user-defined Prometheus (required)

- Red Hat OpenShift

Settings are not required.

An openshift-monitoring project is installed and a scraping setting is added during installation.

- Kubernetes and Amazon Kubernetes Service (EKS)

When Prometheus is not installed, or when Prometheus is installed but the scraping targets listed in the following table are not configured, add a scraping setting.

Scraping target	Data you can retrieve	Metric you can collect
kube-stat-metrics	Status data on nodes, pods, and workloads	See the section describing <i>Key metric items</i> of 3.15.4(2)(a) <i>Red Hat OpenShift</i> in the <i>JP1/Integrated Management 3 - Manager Overview and System Design Guide</i> .
node_exporter	Node's performance data	
kubelet	Pod's performance data	

The subsequent steps are common to Red Hat OpenShift, Kubernetes, and Amazon Kubernetes Service (EKS).

(b) Configuring the settings for a connection (required)

Configure the remote write setting to collect information from user-defined Prometheus.

For details on how to modify the settings for each monitoring target, see [1.21.2\(11\)\(c\) Modifying the Prometheus settings \(Red Hat OpenShift\)](#) and [1.21.2\(11\)\(d\) Modifying the Prometheus settings \(Amazon Elastic Kubernetes Service \(EKS\)\)](#).

To comply with the specifications of Red Hat OpenShift, configuration items must be written in camel case notation. Therefore, the settings in the following sections must be written using camel case notation.

- `global.external_labels` section
- `remote_write` section

- Examples of notation changes

Snake Case Notation	Camel Case Notation
<code>source_labels</code>	<code>sourceLabels</code>
<code>target_label</code>	<code>targetLabel</code>

- global.external_labels section

- `jpl_pc_prome_hostname` (required)
Specify the name of the Prometheus host.
- `jpl_pc_prome_clustername` (optional)
Specify the name of the cluster.
When this label is omitted, the system does not create an IM management node for the cluster.

(Example)

```
global:
external_labels:
  jpl_pc_prome_hostname: promHost
  jpl_pc_prome_clustername: myCluster
```

- remote_write section

- Configure a connection destination
Specify an endpoint of JP1/IM - Manager (Intelligent Integrated Management Base) as a remote write destination. Specify one endpoint and, in each section, enter (1) and (2) of the settings of the label required for container monitoring. When creating the cluster nodes, specify another endpoint and enter (3).
- Configure labels necessary for container monitoring
To give labels necessary for container monitoring, add the statement shown below to the `write_relabel_configs` section. It does not affect any local storage for user-defined Prometheus because it is relabeled during remote writing.
When you monitor Red Hat OpenShift, add the following settings at the beginning of (1) Basic settings and (2) Settings for creating the pod nodes.

```
- source_labels: ['__name__']
  regex: 'kube_.*'|container_.*
  target_label: instance
  replacement: any-value-that-is-unique-within-the-cluster#
```

#: The value specified here is displayed in the tree as the host on which Kubernetes metric collector runs.

(1) Basic settings

```
- source_labels: ['__name__']
  regex: 'kube_job_status_failed_addlabel|kube_job_owner|kube_pod_status_phase|kube_daemonset_status_desired_number_scheduled|kube_daemonset_status_current_number_scheduled|kube_deployment_spec_replicas|kube_deployment_status_replicas_available|kube_replicaset_spec_replicas|kube_replicaset_status_ready_replicas|kube_replicaset_owner|kube_statefulset_replicas|kube_statefulset_status_replicas_ready|kube_node_status_condition|container_cpu_usage_seconds_total|container_fs_reads_bytes_total|container_fs_writes_bytes_total|container_memory_working_set_bytes|container_spec_memory_limit_bytes|node_boot_time_seconds|node_context_switches_total|node_cpu_seconds_total|node_disk_io_now|node_disk_io_time_seconds_total|node_disk_read_bytes_total|node_disk_read_time_seconds_total|node_disk_reads_completed_total|node_disk_write_time_seconds_total|node_disk_writes_completed_total|node_disk_written_bytes_total|node_filesystem_avail_bytes|node_filesystem_files|node_filesystem_files_free|node_filesystem_free_bytes|node_filesystem_size_bytes|node_intr_total|node_load1|node_load15|node_load5|node_memory_Active_file_bytes|node_memory_Buffers_bytes|node_memory_Cached_bytes|node_memory_Inactive_file_bytes|node_memory_MemAvailable_bytes|node_memory_MemFree_bytes|node_memory_MemTotal_bytes|node_memory_SReclaimable_bytes|node_memory_SwapFree_bytes|node_memory_SwapTotal_bytes|node_netstat_Icmp6_InMsgs|node_ne
```



```

tstat_Icmp_InMsgs|node_netstat_Icmp6_OutMsgs|node_netstat_Icmp_OutMsgs|nod
e_netstat_Tcp_InSegs|node_netstat_Tcp_OutSegs|node_netstat_Udp_InDatagrams
|node_netstat_Udp_OutDatagrams|node_network_flags|node_network_iface_link|
node_network_mtu_bytes|node_network_receive_errs_total|node_network_receiv
e_packets_total|node_network_transmit_colls_total|node_network_transmit_er
rs_total|node_network_transmit_packets_total|node_time_seconds|node_uname_
info|node_vmstat_pswpin|node_vmstat_pswpout'
  action: 'keep'
- source_labels: ['__name__']
  target_label: __name__
  regex: "kube_job_status_failed_addlabel"
  replacement: "kube_job_status_failed"
  action: replace
- source_labels: ['__name__', 'name']
  regex: '(container_cpu_usage_seconds_total|container_memory_working_se
t_bytes|container_spec_memory_limit_bytes);'
  action: drop
- source_labels: ['__name__', 'pod']
  regex: '(container_fs_reads_bytes_total|container_fs_writes_bytes_tota
l);'
  action: drop
- source_labels: ['__name__', 'namespace']
  regex: '(kube_pod_|kube_job_|container_).*;(.*)'
  target_label: jpl_pc_nodelabel
  replacement: ${2}
- source_labels: ['__name__', 'node']
  regex: 'kube_node_.*;(.*)'
  target_label: jpl_pc_nodelabel
- source_labels: ['__name__', 'daemonset']
  regex: 'kube_daemonset_.*;(.*)'
  target_label: jpl_pc_nodelabel
- source_labels: ['__name__', 'deployment']
  regex: 'kube_deployment_.*;(.*)'
  target_label: jpl_pc_nodelabel
- source_labels: ['__name__', 'replicaset']
  regex: 'kube_replicaset_.*;(.*)'
  target_label: jpl_pc_nodelabel
- source_labels: ['__name__', 'statefulset']
  regex: 'kube_statefulset_.*;(.*)'
  target_label: jpl_pc_nodelabel
- source_labels: ['__name__', 'owner_kind', 'owner_name']
  regex: '(kube_job_status_failed|kube_job_owner);CronJob;(.*)'
  target_label: jpl_pc_nodelabel
  replacement: $2
- source_labels: ['__name__']
  regex: 'node_.*'
  target_label: jpl_pc_nodelabel
  replacement: Linux metric collector(Node exporter)
- source_labels: ['__name__']
  regex: '(kube_pod_|kube_job_|container_).*'
  target_label: jpl_pc_module
  replacement: kubernetes/Namespace
- source_labels: ['__name__']
  regex: 'kube_node_.*'
  target_label: jpl_pc_module
  replacement: kubernetes/Node
- source_labels: ['__name__']
  regex: 'kube_daemonset_.*'

```

```

target_label: jpl_pc_module
replacement: kubernetes/DaemonSet
- source_labels: ['__name__']
  regex: 'kube_deployment.*'
  target_label: jpl_pc_module
  replacement: kubernetes/Deployment
- source_labels: ['__name__']
  regex: 'kube_replicaset.*'
  target_label: jpl_pc_module
  replacement: kubernetes/ReplicaSet
- source_labels: ['__name__']
  regex: 'kube_statefulset.*'
  target_label: jpl_pc_module
  replacement: kubernetes/StatefulSet
- source_labels: ['__name__', 'owner_kind']
  regex: '(kube_job_status_failed|kube_job_owner);CronJob'
  target_label: jpl_pc_module
  replacement: kubernetes/CronJob
- source_labels: ['__name__']
  regex: 'kube_.*|container.*'
  target_label: jpl_pc_trendname
  replacement: kubernetes
- source_labels: ['__name__']
  regex: 'node.*'
  target_label: jpl_pc_trendname
  replacement: node_exporter
- source_labels: ['__name__']
  regex: 'kube.*'
  target_label: jpl_pc_exporter
  replacement: JPC Kube Exporter
- source_labels: ['__name__']
  regex: 'node.*'
  target_label: jpl_pc_exporter
  replacement: JPC Node exporter
- source_labels: ['__name__']
  regex: 'container.*'
  target_label: jpl_pc_exporter
  replacement: JPC Kube Exporter
- source_labels: ['__name__']
  regex: 'kube.*'
  target_label: job
  replacement: jpc_kube_exporter
- source_labels: ['__name__']
  regex: 'node.*'
  target_label: job
  replacement: jpc_kube_node
- source_labels: ['__name__']
  regex: 'container.*'
  target_label: job
  replacement: jpc_kube_exporter
- source_labels: ['__name__']
  regex: 'node.*'
  target_label: jpl_pc_category
  replacement: platform
- source_labels: ['job', 'instance']
  regex: 'jpc_kube_exporter;([^:]+):?(.*)'
  target_label: jpl_pc_remote_monitor_instance
  replacement: ${1}:Kubernetes metric collector

```

```

- source_labels: ['job','jpl_pc_prome_hostname','jpl_pc_remote_monitor_instance']
  regex: 'jpc_kube_exporter;(.*);'
  target_label: jpl_pc_remote_monitor_instance
  replacement: ${1}:Kubernetes metric collector
- regex: '__.+_|jpl_pc_prome_hostname|jpl_pc_prome_clustername|jpl_pc_nodelabel|jpl_pc_trendname|jpl_pc_module|jpl_pc_exporter|jpl_pc_remote_monitor_instance|instance|job|cronjob|namespace|schedule|concurrency_policy|daemonset|deployment|condition|status|job_name|owner_kind|owner_name|owner_is_controller|reason|replicaset|statefulset|revision|phase|node|kernel_version|os_image|container_runtime_version|kubelet_version|kubeproxy_version|pod_cidr|provider_id|system_uuid|internal_ip|key|value|effect|resource|unit|pod|host_ip|pod_ip|created_by_kind|created_by_name|uid|priority_class|host_network|ip|ip_family|image_image_id|image_spec|container_id|container_type|persistentvolumeclaim|label_+_LABEL|id|name|device|major|minor|operation|cpu|mode|failure_type|scope'
  action: 'labelkeep'

```

(2) Settings for creating the pod nodes

```

- source_labels: ['__name__']
  regex: 'kube_pod_owner|kube_pod_status_phase|container_cpu_usage_seconds_total|container_fs_reads_bytes_total|container_fs_writes_bytes_total|container_memory_working_set_bytes|container_spec_memory_limit_bytes'
  action: 'keep'
- source_labels: ['__name__', 'name']
  regex: '(container_cpu_usage_seconds_total|container_memory_working_set_bytes|container_spec_memory_limit_bytes);'
  action: drop
- source_labels: ['__name__', 'pod']
  regex: '(container_fs_reads_bytes_total|container_fs_writes_bytes_total);'
  action: drop
- source_labels: ['pod']
  target_label: jpl_pc_nodelabel
- target_label: jpl_pc_module
  replacement: kubernetes/Pod
- target_label: jpl_pc_trendname
  replacement: kubernetes
- target_label: jpl_pc_exporter
  replacement: JPC Kube Exporter
- target_label: job
  replacement: jpc_kube_exporter
- source_labels: ['instance']
  regex: '([^\:]+):?(.*)'
  target_label: jpl_pc_remote_monitor_instance
  replacement: ${1}:Kubernetes metric collector
- source_labels: [jpl_pc_prome_hostname,jpl_pc_remote_monitor_instance]
  regex: '(.*);'
  target_label: jpl_pc_remote_monitor_instance
  replacement: ${1}:Kubernetes metric collector
- regex: '__.+_|jpl_pc_prome_hostname|jpl_pc_prome_clustername|jpl_pc_nodelabel|jpl_pc_trendname|jpl_pc_module|jpl_pc_exporter|jpl_pc_remote_monitor_instance|instance|job|cronjob|namespace|schedule|concurrency_policy|daemonset|deployment|condition|status|job_name|owner_kind|owner_name|owner_is_controller|reason|replicaset|statefulset|revision|phase|node|kernel_version|os_image|container_runtime_version|kubelet_version|kubeproxy_version|pod_cidr|provider_id|system_uuid|internal_ip|key|value|effect|resource|unit

```

```
|pod|host_ip|pod_ip|created_by_kind|created_by_name|uid|priority_class|host_network|ip|ip_family|image_image_id|image_spec|container_id|container_type|persistentvolumeclaim|label_._+_LABEL|id|name|device|major|minor|operation|cpu|mode|failure_type|scope'|
    action: labelkeep
```

(3) Settings for creating the cluster nodes

```
- source_labels: ['__name__', 'jpl_pc_prome_clustername']
    regex: '(container_cpu_usage_seconds_total|container_fs_reads_bytes_total|container_fs_writes_bytes_total|container_memory_working_set_bytes|container_spec_memory_limit_bytes);(.*)'
    action: 'keep'
- source_labels: ['__name__', 'name']
    regex: '(container_cpu_usage_seconds_total|container_memory_working_set_bytes|container_spec_memory_limit_bytes);'
    action: drop
- source_labels: ['__name__', 'pod']
    regex: '(container_fs_reads_bytes_total|container_fs_writes_bytes_total);'
    action: drop
- source_labels: ['jpl_pc_prome_clustername']
    target_label: jpl_pc_nodelabel
- target_label: jpl_pc_module
    replacement: kubernetes/Cluster
- target_label: jpl_pc_trendname
    replacement: kubernetes
- target_label: jpl_pc_exporter
    replacement: JPC Kube Exporter
- target_label: job
    replacement: jpc_kube_exporter
- source_labels: ['instance']
    regex: '([^.:]+):?(.*)'
    target_label: jpl_pc_remote_monitor_instance
    replacement: ${1}:Kubernetemetric collector
- source_labels: [jpl_pc_prome_hostname, jpl_pc_remote_monitor_instance]
    regex: '(.*)';'
    target_label: jpl_pc_remote_monitor_instance
    replacement: ${1}:Kubernetes metric collector
- regex: '__.+_|jpl_pc_prome_hostname|jpl_pc_prome_clustername|jpl_pc_nodelabel|jpl_pc_trendname|jpl_pc_module|jpl_pc_exporter|jpl_pc_remote_monitor_instance|instance|job|cronjob|namespace|schedule|concurrency_policy|daemonset|deployment|condition|status|job_name|owner_kind|owner_name|owner_is_controller|reason|replicaset|statefulset|revision|phase|node|kernel_version|os_image|container_runtime_version|kubelet_version|kubeproxy_version|pod_cidr|provider_id|system_uid|internal_ip|key|value|effect|resource|unit|pod|host_ip|pod_ip|created_by_kind|created_by_name|uid|priority_class|host_network|ip|ip_family|image_image_id|image_spec|container_id|container_type|persistentvolumeclaim|label_._+_LABEL|id|name|device|major|minor|operation|cpu|mode|failure_type|scope'|
    action: labelkeep
```

- Configuring PrometheusRule

Register the following settings in PrometheusRule. When you register this setting in PrometheusRule, a new metric named `kube_job_status_failed_addlabel` is saved. If you are referencing metric for container monitoring outside of JP1/IM, ensure that this metric is not RemoteWrite to anything other than JP1/IM.

```
spec:
  groups:
  - name: any-name
    rules:
    - expr: kube_job_status_failed * on(job_name, namespace) group_left(ow
ner_kind,owner_name) kube_job_owner
      record: kube_job_status_failed_addlabel
```

(c) Modifying the Prometheus settings (Red Hat OpenShift)

- Prerequisites

- As a user with the cluster-admin role, you can access the cluster.
- OpenShift CLI (oc) has been installed.

- Procedure

1. Check whether a ConfigMap object is created.

```
$ oc -n openshift-monitoring get configmap cluster-monitoring-config
```

2. If the ConfigMap object is not created, create a new file.

```
$ vi cluster-monitoring-config.yaml
```

3. If the ConfigMap object is created, edit a cluster-monitoring-config object in the openshift-monitoring project.

```
$ oc -n openshift-monitoring edit configmap cluster-monitoring-config
```

4. Add the settings in camel case to data/config.yaml/prometheusK8s.

Please define the secret obtained in *Setting the Authentication Method for User-Specific Prometheus (Required)* after the `url` field. Below is an example of how to write it, based on the *Example Definition of Secret* (Example where the Client ID obtained is `openshift_prometheus` and the secret is `secret`) in *Setting the Authentication Method for User-Specific Prometheus (Required)*.

(Example)

```
apiVersion: v1
kind: ConfigMap
metadata:
  name: cluster-monitoring-config
  namespace: openshift-monitoring
data:
  config.yaml: |
    prometheusK8s:
      externalLabels:
        jp1_pc_prome_hostname: promHost
        jp1_pc_prome_clustername: myCluster
      remoteWrite:
        - url: "http://host-name-of-JP1/IM - Manager (Intelligent Integrate
d Management Base):20703/im/api_system/v1/trendData/write"
          basicAuth:
            username:
              name: jp1-basic-auth
              key: username
            password:
```

```

        name: jpl-basic-auth
        key: password
writeRelabelConfigs:
- sourceLabels: ['__name__']
  regex: 'kube_.*|container_.*'
  targetLabel: instance
  replacement: any-value-that-is-unique-within-the-cluster
- sourceLabels: ['__name__']
  regex: 'kube_job_status_failed_addlabel|kube_job_owner|kube_pod_
status_phase|kube_daemonset_status_desired_number_scheduled|kube_daemonset
_status_current_number_scheduled|kube_deployment_spec_replicas|kube_deploy
ment_status_replicas_available|kube_replicaset_spec_replicas|kube_replicas
et_status_ready_replicas|kube_replicaset_owner|kube_statefulset_replicas|k
ube_statefulset_status_replicas_ready|kube_node_status_condition|container
_cpu_usage_seconds_total|container_fs_reads_bytes_total|container_fs_write
s_bytes_total|container_memory_working_set_bytes|container_spec_memory_lim
it_bytes|node_boot_time_seconds|node_context_switches_total|node_cpu_secon
ds_total|node_disk_io_now|node_disk_io_time_seconds_total|node_disk_read_b
ytes_total|node_disk_read_time_seconds_total|node_disk_reads_completed_tot
al|node_disk_write_time_seconds_total|node_disk_writes_completed_total|nod
e_disk_written_bytes_total|node_filesystem_avail_bytes|node_filesystem_fil
es|node_filesystem_files_free|node_filesystem_free_bytes|node_filesystem_s
ize_bytes|node_intr_total|node_load1|node_load15|node_load5|node_memory_Ac
tive_file_bytes|node_memory_Buffers_bytes|node_memory_Cached_bytes|node_me
memory_Inactive_file_bytes|node_memory_MemAvailable_bytes|node_memory_MemFre
e_bytes|node_memory_MemTotal_bytes|node_memory_SReclaimable_bytes|node_mem
ory_SwapFree_bytes|node_memory_SwapTotal_bytes|node_netstat_Icmp6_InMsgs|n
ode_netstat_Icmp_InMsgs|node_netstat_Icmp6_OutMsgs|node_netstat_Icmp_OutMs
gs|node_netstat_Tcp_InSegs|node_netstat_Tcp_OutSegs|node_netstat_Udp_InDat
agrams|node_netstat_Udp_OutDatagrams|node_network_flags|node_network_iface
_link|node_network_mtu_bytes|node_network_receive_errs_total|node_network_
receive_packets_total|node_network_transmit_colls_total|node_network_trans
mit_errs_total|node_network_transmit_packets_total|node_time_seconds|node_
uname_info|node_vmstat_pswpin|node_vmstat_pswpout'
  action: 'keep'
- sourceLabels: ['__name__']
  targetLabel: __name__
  regex: "kube_job_status_failed_addlabel"
  replacement: "kube_job_status_failed"
  action: replace
- sourceLabels: ['__name__', 'name']
  regex: '(container_cpu_usage_seconds_total|container_memory_work
ing_set_bytes|container_spec_memory_limit_bytes);'
  action: drop
- sourceLabels: ['__name__', 'pod']
  regex: '(container_fs_reads_bytes_total|container_fs_writes_byte
s_total);'
  action: drop
- sourceLabels: ['__name__', 'namespace']
  regex: '(kube_pod_|kube_job_|container_).*;(.*)'
  targetLabel: jpl_pc_nodelabel
  replacement: $2
- sourceLabels: ['__name__', 'node']
  regex: 'kube_node_.*;(.*)'
  targetLabel: jpl_pc_nodelabel
- sourceLabels: ['__name__', 'daemonset']
  regex: 'kube_daemonset_.*;(.*)'
  targetLabel: jpl_pc_nodelabel

```

```

- sourceLabels: ['__name__', 'deployment']
  regex: 'kube_deployment.*;(.*)'
  targetLabel: jpl_pc_nodelabel
- sourceLabels: ['__name__', 'replicaset']
  regex: 'kube_replicaset.*;(.*)'
  targetLabel: jpl_pc_nodelabel
- sourceLabels: ['__name__', 'statefulset']
  regex: 'kube_statefulset.*;(.*)'
  targetLabel: jpl_pc_nodelabel
- sourceLabels: ['__name__', 'owner_kind', 'owner_name']
  regex: '(kube_job_status_failed|kube_job_owner);CronJob;(.*)'
  targetLabel: jpl_pc_nodelabel
  replacement: $2
- sourceLabels: ['__name__']
  regex: 'node_.*'
  targetLabel: jpl_pc_nodelabel
  replacement: Linux metric collector(Node exporter)
- sourceLabels: ['__name__']
  regex: '(kube_pod|kube_job|container_).*'
  targetLabel: jpl_pc_module
  replacement: kubernetes/Namespace
- sourceLabels: ['__name__']
  regex: 'kube_node_.*'
  targetLabel: jpl_pc_module
  replacement: kubernetes/Node
- sourceLabels: ['__name__']
  regex: 'kube_daemonset_.*'
  targetLabel: jpl_pc_module
  replacement: kubernetes/DaemonSet
- sourceLabels: ['__name__']
  regex: 'kube_deployment_.*'
  targetLabel: jpl_pc_module
  replacement: kubernetes/Deployment
- sourceLabels: ['__name__']
  regex: 'kube_replicaset_.*'
  targetLabel: jpl_pc_module
  replacement: kubernetes/ReplicaSet
- sourceLabels: ['__name__']
  regex: 'kube_statefulset_.*'
  targetLabel: jpl_pc_module
  replacement: kubernetes/StatefulSet
- sourceLabels: ['__name__', 'owner_kind']
  regex: '(kube_job_status_failed|kube_job_owner);CronJob'
  targetLabel: jpl_pc_module
  replacement: kubernetes/CronJob
- sourceLabels: ['__name__']
  regex: 'kube_.*|container_.*'
  targetLabel: jpl_pc_trendname
  replacement: kubernetes
- sourceLabels: ['__name__']
  regex: 'node_.*'
  targetLabel: jpl_pc_trendname
  replacement: node_exporter
- sourceLabels: ['__name__']
  regex: 'kube_.*'
  targetLabel: jpl_pc_exporter
  replacement: JPC Kube Exporter
- sourceLabels: ['__name__']

```

```

    regex: 'node_.*'
    targetLabel: jpl_pc_exporter
    replacement: JPC Node exporter
- sourceLabels: ['__name__']
  regex: 'container_.*'
  targetLabel: jpl_pc_exporter
  replacement: JPC Kube Exporter
- sourceLabels: ['__name__']
  regex: 'kube_.*'
  targetLabel: job
  replacement: jpc_kube_exporter
- sourceLabels: ['__name__']
  regex: 'node_.*'
  targetLabel: job
  replacement: jpc_kube_node
- sourceLabels: ['__name__']
  regex: 'container_.*'
  targetLabel: job
  replacement: jpc_kube_exporter
- sourceLabels: ['__name__']
  regex: 'node_.*'
  targetLabel: jpl_pc_category
  replacement: platform
- sourceLabels: ['job','instance']
  regex: 'jpc_kube_exporter;([^\:]+):?(.*)'
  targetLabel: jpl_pc_remote_monitor_instance
  replacement: ${1}:Kubernetes metric collector
- sourceLabels: ['job','jpl_pc_prome_hostname','jpl_pc_remote_moni
tor_instance']
  regex: 'jpc_kube_exporter;(.*);'
  targetLabel: jpl_pc_remote_monitor_instance
  replacement: ${1}:Kubernetes metric collector
- regex: '.__.+_|jpl_pc_prome_hostname|jpl_pc_prome_clustername|jpl
1_pc_nodelabel|jpl_pc_trendname|jpl_pc_module|jpl_pc_exporter|jpl_pc_remot
e_monitor_instance|instance|job|cronjob|namespace|schedule|concurrency_pol
icy|daemonset|deployment|condition|status|job_name|owner_kind|owner_name|o
wner_is_controller|reason|replicaset|statefulset|revision|phase|node|kerne
l_version|os_image|container_runtime_version|kubelet_version|kubeproxy_ver
sion|pod_cidr|provider_id|system_uid|internal_ip|key|value|effect|resourc
e|unit|pod|host_ip|pod_ip|created_by_kind|created_by_name|uid|priority_cla
ss|host_network|ip|ip_family|image_image_id|image_spec|container_id|contai
ner|type|persistentvolumeclaim|label_.__.+_LABEL|id|name|device|major|minor|o
peration|cpu|mode|failure_type|scope'
  action: 'labelkeep'

```

5. Save the file and apply the changes to the ConfigMap object.

```
$ oc apply -f cluster-monitoring-config.yaml
```

(d) Modifying the Prometheus settings (Amazon Elastic Kubernetes Service (EKS))

- Procedure

1. Create a yaml file with a given name (example: my_prometheus_values.yaml) and add the settings to the server section.

- Settings in external_labels

Add them to the global.external_labels section.

- Settings in remote_write

Add them to the remoteWrite section.

(Example)

```
server:
  global:
    external_labels:
      jpl_pc_prome_hostname: promHost
      jpl_pc_prome_clustername: myCluster
  remoteWrite:
    - url: http://host-name-of-JP1/IM - Manager (Intelligent Integrated Ma
      nagement Base):20703/im/api/v1/trendData/write
      write_relabel_configs:
        - source_labels: ['__name__']
          regex: 'kube_job_status_failed|kube_job_owner|kube_pod_status_ph
            ase|kube_daemonset_status_desired_number_scheduled|kube_daemonset_status_c
            urrent_number_scheduled|kube_deployment_spec_replicas|kube_deployment_stat
            us_replicas_available|kube_replicaset_spec_replicas|kube_replicaset_status
            _ready_replicas|kube_replicaset_owner|kube_statefulset_replicas|kube_state
            fulset_status_replicas_ready|kube_node_status_condition|container_cpu_usag
            e_seconds_total|container_fs_reads_bytes_total|container_fs_writes_bytes_t
            otal|container_memory_working_set_bytes|container_spec_memory_limit_bytes|
            node_boot_time_seconds|node_context_switches_total|node_cpu_seconds_total|
            node_disk_io_now|node_disk_io_time_seconds_total|node_disk_read_bytes_tota
            l|node_disk_reads_completed_total|node_disk_writes_completed_total|node_di
            sk_written_bytes_total|node_filesystem_avail_bytes|node_filesystem_files|n
            ode_filesystem_files_free|node_filesystem_free_bytes|node_filesystem_size_
            bytes|node_intr_total|node_load1|node_load15|node_load5|node_memory_Active
            _file_bytes|node_memory_Buffers_bytes|node_memory_Cached_bytes|node_memory
            _Inactive_file_bytes|node_memory_MemAvailable_bytes|node_memory_MemFree_by
            tes|node_memory_MemTotal_bytes|node_memory_SReclaimable_bytes|node_memory
            _SwapFree_bytes|node_memory_SwapTotal_bytes|node_netstat_Icmp6_InMsgs|node_
            netstat_Icmp_InMsgs|node_netstat_Icmp6_OutMsgs|node_netstat_Icmp_OutMsgs|n
            ode_netstat_Tcp_InSegs|node_netstat_Tcp_OutSegs|node_netstat_Udp_InDatagra
            ms|node_netstat_Udp_OutDatagrams|node_network_flags|node_network_iface_lin
            k|node_network_mtu_bytes|node_network_receive_errs_total|node_network_rece
            ive_packets_total|node_network_transmit_colls_total|node_network_transmit_
            errs_total|node_network_transmit_packets_total|node_time_seconds|node_unam
            e_info|node_vmstat_pswpin|node_vmstat_pswpout'
          action: keep
        - source_labels: ['__name__', 'namespace']
          regex: '(kube_pod_|kube_job_|container_).*; (.*)'
          target_label: jpl_pc_nodelabel
          replacement: $2
        - source_labels: ['__name__', 'node']
          regex: 'kube_node_.*; (.*)'
          target_label: jpl_pc_nodelabel
        - source_labels: ['__name__', 'daemonset']
          regex: 'kube_daemonset_.*; (.*)'
          target_label: jpl_pc_nodelabel
        - source_labels: ['__name__', 'deployment']
          regex: 'kube_deployment_.*; (.*)'
          target_label: jpl_pc_nodelabel
        - source_labels: ['__name__', 'replicaset']
          regex: 'kube_replicaset_.*; (.*)'
          target_label: jpl_pc_nodelabel
        - source_labels: ['__name__', 'statefulset']
```

```

    regex: 'kube_statefulset_.*;(.*)'
    target_label: jpl_pc_nodelabel
- source_labels: ['__name__', 'owner_name']
  regex: 'kube_job_owner;(.*)'
  target_label: jpl_pc_nodelabel
- source_labels: ['__name__', 'instance']
  regex: 'node_.*;(.*)'
  target_label: jpl_pc_nodelabel
- source_labels: ['__name__']
  regex: 'kube_.*'
  target_label: jpl_pc_trendname
  replacement: kube_state_metrics
- source_labels: ['__name__']
  regex: 'node_.*'
  target_label: jpl_pc_trendname
  replacement: node_exporter
- source_labels: ['__name__']
  regex: 'container_.*'
  target_label: jpl_pc_trendname
  replacement: kubelet
- source_labels: ['__name__']
  regex: 'kube_.*'
  target_label: jpl_pc_exporter
  replacement: JPC Kube state metrics
- source_labels: ['__name__']
  regex: 'node_.*'
  target_label: jpl_pc_exporter
  replacement: JPC Node exporter
- source_labels: ['__name__']
  regex: 'container_.*'
  target_label: jpl_pc_exporter
  replacement: JPC Kubelet
- source_labels: ['__name__']
  regex: 'kube_.*'
  target_label: job
  replacement: jpc_kube_state
- source_labels: ['__name__']
  regex: 'node_.*'
  target_label: job
  replacement: jpc_node
- source_labels: ['__name__']
  regex: 'container_.*'
  target_label: job
  replacement: jpl_kubelet

```

2. Apply the changes.

```

helm upgrade prometheus-chart-name prometheus-community/prometheus -n prometheus-namespace -f my_prometheus_values.yaml

```

(e) Configuring scraping targets (optional)

- Change monitoring targets

If you want to monitor only a part of the monitoring targets in a user environment with JP1/IM, specify the monitoring targets in the `write_relabel_configs` section. See the following examples.

(Example 1) Specifying a whitelist of specific resources

```
- source_labels: ['__name__', 'pod']
  regex: '(kube_pod_|container_).*;coredns-.*|prometheus'
  action: 'keep'
```

(Example 2) Specifying a blacklist of all resources

```
- source_labels: ['jp1_pc_nodelabel']
  regex: 'coredns-.*|prometheus'
  action: 'drop'
```

In addition, to monitor metrics that have already been collected in a different aggregation type, add the `remote_write` section and define it as the type to be monitored.

- Change monitoring metrics

If you want to change metrics displayed in the **Trends** tab of the integrated operation viewer, edit the metric definition files.

The files you need to edit are as follows:

- Node exporter metric definition file (`metrics_node_exporter.conf`)
- Container monitoring metric definition file (`metrics_kubernetes.conf`)

For details on these metric definition files, see the sections describing the applicable files in the *JPI/Integrated Management 3 - Manager Command, Definition File and API Reference*.

(f) Configuring the system node definition file (`imdd_systemnode.conf`) (required)

To create a system node described in (e) *Tree format* in the *JPI/Integrated Management 3 - Manager Overview and System Design Guide 3.15.6(1)(i) Creating IM management nodes (__configurationGet method)*, edit the system node definition file (`imdd_systemnode.conf`) to configure the setting items listed in the table below. You can specify any values to the items that are not listed in the table.

Table 1–19: Settings in the system node definition file (`imdd_systemnode.conf`)

Item	Value
<code>displayname</code>	This specifies the name of the Kubernetes component.
<code>type</code>	It must be specified in uppercase characters as follows: <code>Kubernetes-Kubernetes-component-name</code> <code>Kubernetes-component-name</code> is equivalent to one of the names under the <i>Component name</i> column of the section describing the <i>component names monitored by Kubernetes</i> in 3.15.4(2)(b) <i>Kubernetes</i> in the <i>JPI/Integrated Management 3 - Manager Overview and System Design Guide</i> .
<code>name</code>	This is specified as: [{"*":"regex"}]

The following table shows a setting example of the system node definition file when you create system management nodes for Kubernetes components that are found by default as monitoring targets in the container monitoring metric definition file.

Table 1–20: Setting example of the system node definition file (`imdd_systemnode.conf`)

Item		
<code>displayName</code>	<code>type</code>	<code>name</code>
Clusters	JP1PC-KUBERNETES-CLUSTER	[{"*":"regex"}]
Nodes	JP1PC-KUBERNETES-NODE	[{"*":"regex"}]

Item		
displayName	type	name
Namespaces	JP1PC-KUBERNETES-NAMESPACE	[{"*":"regex"}]
Deployments	JP1PC-KUBERNETES-DEPLOYMENT	[{"*":"regex"}]
DaemonSets	JP1PC-KUBERNETES-DAEMONSET	[{"*":"regex"}]
ReplicaSets	JP1PC-KUBERNETES-REPLICASET	[{"*":"regex"}]
StatefulSets	JP1PC-KUBERNETES-STATEFULSET	[{"*":"regex"}]
CronJobs	JP1PC-KUBERNETES-CRONJOB	[{"*":"regex"}]
Pods	JP1PC-KUBERNETES-POD	[{"*":"regex"}]

The following shows how the items in the above table and Kubernetes at a higher level can be defined in the system node definition file.

```

{
  "meta":{
    "version":"2"
  },
  "allSystem":[
    {
      "id":"kubernetes",
      "displayName":"Kubernetes",
      "children":[
        {
          "id":"cluster",
          "displayName":"Clusters",
          "objectRoot":[
            {
              "type":"JP1PC-KUBERNETES-CLUSTER",
              "name":[{"*":"regex"}]
            }
          ]
        },
        {
          "id":"namespace",
          "displayName":"Namespaces",
          "objectRoot":[
            {
              "type":"JP1PC-KUBERNETES-NAMESPACE",
              "name":[{"*":"regex"}]
            }
          ]
        },
        {
          "id":"node",
          "displayName":"Nodes",
          "objectRoot":[
            {
              "type":"JP1PC-KUBERNETES-NODE",
              "name":[{"*":"regex"}]
            }
          ]
        }
      ]
    }
  ],
}
```

```

{
  "id": "deployment",
  "displayName": "Deployments",
  "objectRoot": [
    {
      "type": "JP1PC-KUBERNETES-DEPLOYMENT",
      "name": [{".*": "regex"}]
    }
  ]
},
{
  "id": "daemonset",
  "displayName": "DaemonSets",
  "objectRoot": [
    {
      "type": "JP1PC-KUBERNETES-DAEMONSET",
      "name": [{".*": "regex"}]
    }
  ]
},
{
  "id": "replicaset",
  "displayName": "ReplicaSets",
  "objectRoot": [
    {
      "type": "JP1PC-KUBERNETES-REPLICASET",
      "name": [{".*": "regex"}]
    }
  ]
},
{
  "id": "statefulset",
  "displayName": "StatefulSets",
  "objectRoot": [
    {
      "type": "JP1PC-KUBERNETES-STATEFULSET",
      "name": [{".*": "regex"}]
    }
  ]
},
{
  "id": "cronjob",
  "displayName": "CronJobs",
  "objectRoot": [
    {
      "type": "JP1PC-KUBERNETES-CRONJOB",
      "name": [{".*": "regex"}]
    }
  ]
},
{
  "id": "pod",
  "displayName": "Pods",
  "objectRoot": [
    {
      "type": "JP1PC-KUBERNETES-POD",
      "name": [{".*": "regex"}]
    }
  ]
}

```

```

    ]
  }
]
}
]
}
}

```

With the system node definition file specified, an IM management node is displayed under the system node that has the corresponding Kubernetes component name, when the `jddcreatetree` is run.

For details on the system node definition file, see *System node definition file (imdd_systemnode.conf)* of JP1/IM - Manager in *Chapter 2. Definition Files* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

(12) Editing the Script exporter definition file

(a) Specifying scripts as monitoring targets (required)

- Edit the Script exporter configuration file (jpc_script_exporter.yml)

Edit the Script exporter configuration file (`jpc_script_exporter.yml`) to define which scripts are to be monitored.

For details on the Script exporter configuration file, see *Script exporter configuration file (jpc_script_exporter.yml)* in *Chapter 2. Definition Files* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

(b) Modifying monitoring metrics (optional)

- Edit the Prometheus configuration file (jpc_prometheus_server.yml)

If you want to add metrics collected from the scripts, add them to the `metric_relabel_config` section in the Prometheus configuration file (`jpc_prometheus_server.yml`).

For details on the Prometheus configuration file, see *Prometheus configuration file (jpc_prometheus_server.yml)* in *Chapter 2. Definition Files* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

```

scrape_configs:
  - job_name: jpc_script_exporter
    ...
    metric_relabel_configs:
      - source_labels: ['__name__']
        regex: 'script_success|script_duration_seconds|script_exit_code [Ad
d metrics here]'

```

- Edit the Script exporter metric definition file (metrics_script_exporter.conf)

If you want to change metrics displayed in the **Trends** tab of the integrated operation viewer, edit the settings in the Script exporter metric definition file (`metrics_script_exporter.conf`).

For details on the Script exporter metric definition file, see *Script exporter metric definition file (metrics_script_exporter.conf)* in *Chapter 2. Definition Files* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

(c) Changing Ports (optional)

The listen port used by Script exporter is specified in `--web.listen-address` option of the `script_exporter` command.

For details about how to change the options of `script_exporter` command, see [1.21.2\(1\)\(c\) Change command-line options \(for Windows\)](#), [2.19.2\(1\)\(c\) Change command-line options \(for Linux\)](#). For details about `--web.listen-address` option, see *If you want to change command line options in Unit definition file (jpc_program-name.service) in Chapter 2. Definition Files in the JP1/Integrated Management 3 - Manager Command, Definition File and API Reference.*

The default port is "20722". If port number is changed, review setup of the firewall and prohibit accessing from outside.

Notes:

- When specifying the host name for this option, the same host name must be set for `targets` in the Script exporter discovery configuration file (`jpc_file_sd_config_script.yml`) on the same host. If you specify with `http_sd_config`, also change `url`.
- When specifying an IP address for this option, the host name that is resolved to the IP address specified for this option must be set for `targets` in the Process exporter discovery configuration file (`jpc_file_sd_config_process.yml`) on the same host. If you specify with `http_sd_config`, also change `url`.

(d) Setting when executing SAP system log extract command (optional)

If you use Script exporter to execute the SAP system log extract command, configure Script exporter configuration file settings using sample file (`jpc_script_exporter_sap.yml`) of SAP system monitoring.

For details about sample file of Script exporter configuration file for *Sample file of Script exporter configuration file for SAP system monitoring (jpc_script_exporter_sap.yml)* in *Chapter 2. Definition Files in the JP1/Integrated Management 3 - Manager Command, Definition File and API Reference.*

For details on how to configure the settings, see *Sample file of Script exporter configuration file for SAP system monitoring (jpc_script_exporter_sap.yml)* in *Chapter 2. Definition Files in the JP1/Integrated Management 3 - Manager Command, Definition File and API Reference* and [1.21.2\(12\) Editing the Script exporter definition file](#).

(13) Setting up Web scenario monitoring function

This section explains how to configure Web exporter when using Web scenario monitoring function.

(a) Setting up JP1/IM - Agent

Set up JP1/IM - Agent to use Web scenario monitoring function.

■ Browser settings on agent host

- Installing the browser

Install a browser that runs Web scenario file using Playwright and Web scenario creation function.

If the browser is already installed, installation is not required.

- Setting the browser language

The language used to display the browser must be available in the browser.

Check whether the language to be used has been added in the setting window of the browser to be used. If not, run Codegen and add the language to be used because monitoring by Playwright may not work properly.

■ Configuring authentication

When a Playwright accesses a monitored Web application, a client authentication or HTTP authentication (Basic authentication) requires settings such as a certificate/password.

Table 1–21: Monitor Conditions and Required Settings

Monitoring conditions	Required file	Required Settings
Client authentication	Place the client certificate file in PKCS#12 format in any folder on the client host.	- Import the certificate file into the browser on the client host. - Run the following command to register the registry key to use: - When using Google chrome <pre>reg add "HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome\AutoSelectCertificateForUrls" /v <i>an-integer-of-1-or-more</i> /t "REG_SZ" /d "{ \"pattern\": \"client-authentication-required-web-site-URL\", \"filter\": { \"ISSUER\": { \"CN\": \"CN-of-CA-certificate\" } } }"</pre> - When using Microsoft Edge <pre>reg add "HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Edge\AutoSelectCertificateForUrls" /v <i>an-integer-of-1-or-more</i> /t "REG_SZ" /d "{ \"pattern\": \"client-authentication-required-web-site-URL\", \"filter\": { \"ISSUER\": { \"CN\": \"CN-of-CA-certificate\" } } }"</pre> - Change the following options in Playwright configuration file: <pre><Before change> headless true <After change> headless false</pre>
Basic authentication	None	In Web scenario file, define a username and password. For Web Scenario-creation feature, enter the username/ password as follows when entering Web website where you want to log in with URL: <pre>http://Username:Password@domain-name:Port/Path...</pre>

■ Setting up the environment variables

Set the environment variables so that JP1/IM - Agent hosts can execute npx playwright test commands from the Web exporter, and also use the Web scenario creation support function and trace viewer function. Perform the following steps:

1. Display the System Properties dialog from **Settings - System - About - Related Settings - Advanced System Settings**.
2. Click the **Environment Variables** button to display the Environment Variables dialog.
3. Set the system variables as follows.

Variable name	Variable value
Path	<i>JP1/IM-Agent-Installation-destination-folder\jplima\lib\nodejs</i>

If you have already installed nodejs separately, or if you install nodejs in the future, please configure the settings so that the nodejs of JP1/IM - Agent is prioritized.

■ Setting up Web exporter

You must also register a password for the person who runs Web scenarios that you specify for Web exporter configuration file(jpc_web_exporter.yml). For details on registering a password, see *jimasecret* in *Chapter 1. Commands* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

Web exporter configuration file (jpc_web_exporter.yml) and secret key are reflected only when Web exporter is started. A Web exporter restart is required to reflect the Web exporter configuration file (jpc_web_exporter.yml) or secret changes after Web exporter starts.

■ Creating a New Web Scenario File

If you want to create a new Web scenario file, do the following:

1. Stop Web exporter.

If Web exporter is already running, it will be stopped.

2. Create a Web scenario file.

You use Web Scenario Creation Assistant feature to create Web scenario files. For details on Web scenario creation support function, see the section describing *Web Scenario Creation Support Function* in *3.15.1(1)(m) Web scenario monitoring function* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

Outputs the code generated by Web scenario creation support function to Web scenario file. If an operation is mistakenly recorded during operation recording and an incorrect code is generated, exit codegen and record the operation again.

Place the created Web scenario file in the following folders:

- For physical hosts

JP1/IM-Agent-Installation-destination-folder\jplima\lib\playwright\tests

- For logical hosts

shared-folder\jplima\lib\playwright\tests

For the codes recorded by Codegen operation, see *Operation and operation of browsers that can be recorded and measured as Web scenario* described in *Web Scenario Creation Function (playwright codegen)* in *3.15.1(1)(m) Web scenario monitoring function* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

For the format of Web scenario file, see *Web scenario file (any name.spec.ts)* in *Chapter 2. Definition Files* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

For details about configuration file editing procedure, see *To edit the configuration files (for Windows)* in *1.19.3(1)(a) Common way to setup*.

■ Setting up Playwright configuration file

Add the definition to Playwright configuration file (jpc_playwright.config.ts) that runs Web scenario file that you created. If a file other than the one stored during installation is used as Playwright configuration file (including when a model file or the original configuration file is copied and created), set the file access privilege to Administrators only.

For details about Playwright configuration file, see *Playwright configuration file (jpc_playwright.config.ts)* in *Chapter 2. Definition Files* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

For details about configuration file editing procedure, see *To edit the configuration files (for Windows)* in *1.19.3(1)(a) Common way to setup*.

■ Configuring Web exporter Discovery configuration file

1. Editing Web exporter Discovery configuration file.

Edits Web exporter discovery configuration file (`jpc_file_sd_config_web.yml`) and defines Web scenario filename to perform.

For details about the settings, see *Web exporter discovery configuration file (`jpc_file_sd_config_web.yml`)* in *Chapter 2. Definition Files* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

2. Create a new Web exporter discovery configuration file (optional).

Create a new discovery configuration file if you want to configure additional scrape jobs that are defined by defaults in Prometheus configuration file, for example, if you want to run scrape on more than one Web exporter with a different timeout.

For details on how to create it, see *Add a Web exporter discovery configuration file (optional)* in *1.21.2(3)(i) Add a Web exporter scrape job (for Windows) (optional)*.

■ **Setting up Web exporter Scrape Jobs**

See Section *1.21.2(3)(i) Add a Web exporter scrape job (for Windows) (optional)*.

■ **Starting Web exporter**

Start Web exporter.

(14) Setting up VMware exporter

(a) Changing ports (for Windows) (optional)

The listen port used by VMware exporter is specified in `--port` option of the `vmware_exporter` command. The changed port is reflected at the timing when VMware exporter service is restarted.

For details about how to change `vmware_exporter` command options, see *1.21.2(1)(c) Change command-line options (for Windows)*. For details of `--port` option, see *vmware_exporter command options* in *Service definition file (`jpc_program-name_service.xml`)* in *Chapter 2. Definition Files* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

The default port is 20732. If you change the port number, review the firewall settings and prohibit external access.

(b) Add, change, or remove sections (for Windows) (mandatory)

For each target (VMware ESXi), VMware exporter must define its connectivity in VMware exporter configuration file (`jpc_vmware_exporter.yml`). This definition is called a section.

The following sections are defined by default for sample:

Table 1–22: Sections defined in Initial Settings

Section name	Feature
Default	• This section sets the first monitoring target. • Rewrite the value to use (you must set the host name and port). • The section-name "default" is subject to presence checking and should not be deleted or modified.

If you add a target, you must copy default section and configure the section definitions for the number of monitored targets.

If you change the settings, you must restart VMware exporter and Prometheus server services.

Sections are defined in VMware exporter configuration file (`jpc_vmware_exporter.yml`). For details about VMware exporter configuration file, see *VMware exporter configuration file (`jpc_vmware_exporter.yml`)* in *Chapter 2. Definition Files* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

Set the section name of the new section to the same name as the section name of the parameter to be set to Prometheus configuration file (`jpc_prometheus_server.yml`). For details, see *1.21.2(3)(j) Add a VMware exporter scrape job (for Windows only) (optional)*.

When adding a new section, make sure that there are no duplicate VM names for each section before adding the section.

For the user used to connect to VMware ESXi, use a role other than No Access or Non-Encrypted Administrator.

For details about registering the password used to connect to VMware ESXi, see *jimasecret* in *Chapter 1. Commands* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*. The length of the password at the time of secret registration follows the secret control commands (*jimasecret*). If VMware ESXi has changed the password length limit, set a password with up to 1024 characters.

For instructions on updating VMware exporter configuration file and deploying the certificate file, see *1.21.2(1)(a) Edit the configuration files (for Windows)*.

If you add a section definition, you need to define a scrape job to scrape using the newly created section from Prometheus server. For Prometheus server settings, see *1.21.2(3)(j) Add a VMware exporter scrape job (for Windows only) (optional)*.

VMware exporter configuration file (`jpc_vmware_exporter.yml`) and secret key are reflected only when VMware exporter is started. A VMware exporter restart is required to reflect any VMware exporter configuration file (`jpc_vmware_exporter.yml`) or secret changes that you have made since VMware exporter was launched.

(c) Registering secrets (mandatory)

Register the secret used to connect to default section of the monitoring target (VMware ESXi) and sections that you add.

Also, if you add any sections, you must register the corresponding secret.

For details on how to register a secret for the monitor target, see *jimasecret* in *Chapter 1. Commands* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

■ Note on Secret Registration

For notes on obfuscating passwords for VMware ESXi with the Secret Management Command (*jimasecret*), see *jimasecret* in *Chapter 1. Commands* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

(d) Certificate Settings (mandatory)

When SSL authentication is performed on a VMware exporter, certificates must be set up on the machine in the same way, regardless of whether they are physical or logical hosts.

One of the following certificates is required:

- Default certificate
The certificate that is created when VMware is built.
- vCenter Server certificate (certificate of the certificate authority)
A certificate issued by vCenter Server.
- Own certificate (self-signed server certificate)
Refers to a certificate issued by the user.

The procedure for each certificate is shown below.

- For default certificates

1. Set "ignore_ssl" of VMware exporter configuration file (jpc_vmware_exporter.yml) to True.
Make sure that there is no problem in operation even if this setting is made, and then perform the setting.

- For vCenter Server certificates or your own certificate[#]

Perform the following steps to import the certificate:

Note #: If an authentication error occurs in the original certificate, review the created certificate. If the connection cannot be established even after review, check in advance that there are no operational problems, and then refer to the procedure in "Default Certificate".

- For Windows

1. Select **Run** from the Windows **Start** menu.
2. In the **Run** dialog, type `mmc` and click the **OK** button.
3. In **Console 1**, select **File - Add or Remove Snap-ins**.
4. Select **Certificates** and click the **Add** button.
5. Choose **Computer account** and click the **Next** button.
6. Select **Local computer** and click the **Finish** button.
7. Confirm that **Certificates (Local Computer)** has been added to **Selected snap-ins**, and click the **OK** button.
8. Right-click on **Certificates (Local Computer) - Trusted Root Certification Authorities - Certificates**, and select the **All Tasks - Import** menu that appears.
9. Click the **Next** button.
10. In the **File name** text box, enter the filename of the certificate to be imported and click the **Next** button.
11. Select **Place all certificates in the following store** and click the **Next** button.
12. Click the **Finish** button and then click the **OK** button.

- For Linux

- for Linux 7 or Linux 8[#]

Note #: This assumes that ca-certificate packaging is installed on OS.

1. Run the following command to copy the certificate file.
`# cp certificate-file-path/etc/pki/ca-trust/source/anchors`

2. Update the truststore configuration.
<Example for updating the system-wide trust store settings>
`# update-ca-trust`

- For Linux 9

1. Place the certificate file on the server and run the following command:
`# PKICertImport -d . -n certificate-file-path -t "CT,C,C" -a-i ca_root.crt -u L`

- For Oracle Linux 7, Oracle Linux 8, or Oracle Linux 9

Refer to Linux 7 instructions.

- For SUSE Linux 12 or SUSE Linux 15

1. Specify the location of the certificate file in SSL environment variable.
`export CA_CERT = certificate-file-path`

```
export SERVER_KEY = key-file-path
export SERVER_CERT = server-certificate-path
```

2. Run SUSE Manager setup-command.

```
# yast susemanager_setup
```

- For Amazon Linux 2023

Refer to Linux 7 instructions.

(15) Setting Windows exporter (Hyper-V monitoring function)

(a) Changing ports (optional)

The listen port used by Windows exporter(Hyper-V Monitor) is specified in `--telemetry.addr` option of the `windows_exporter` command. It will.

For details about how to change `windows_exporter` command options, see [1.21.2\(1\)\(c\) Change command-line options \(for Windows\)](#). For details on `--telemetry.addr` options, see *windows_exporter command options (Hyper-V Monitoring)* in *Service definition file (jpc_program-name_service.xml)* in *Chapter 2. Definition Files* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

The default port is 20734. If you change the port number, review the firewall settings and prohibit external access.

(16) Specifying a listening port number and listening address (optional)

If you neither change the default port numbers nor limit IP addresses to listen to, you can skip this step.

For details on what you should modify if you want to change port numbers or IP addresses to listen to, see [1.21.2 Settings of JP1/IM - Agent](#) (for Windows) and [2.19.2 Settings of JP1/IM - Agent](#) (for Linux).

(17) Firewall's Setup (for Windows) (required)

You must setup the firewall to restrict external accessibility as follows:

Table 1–23: Firewall Setup

Port	Firewall Setup
Imagent port	Access from outside is prohibited.
Imagentproxy port	Access from outside is prohibited.
Imagentaction port	Access from outside is prohibited.
Alertmanager port	Access from outside is prohibited. However, if you want to monitor Alertmanager with external shape monitoring by Blackbox exporter in other host, allow it to be accessed. In this case, consider security measures such as limiting source IP address.
Prometheus_server port	Access from outside is prohibited. However, if you want to monitor Prometheus server with external shape monitoring by Blackbox exporter in other host, allow it to be accessed. In this case, consider security measures such as limiting source IP address.
Windows_exporter port	Access from outside is prohibited.
Node_exporter port	
Process_exporter port	

Port	Firewall Setup
Ya_cloudwatch_exporter port	
Promitor_scraper port	
Promitor_resource_discovery port	
Blackbox_exporter port	
Script_exporter port	
Fluentd port	

(18) Setup of integrated agent process alive monitoring (for Windows) (optional)

You monitor integrated agent processes in the following ways:

- External shape monitoring by other-host Blackbox exporter
- Alive monitoring processes by Windows exporter
- Monitoring with Prometheus server up metric

(a) External shape monitoring by other-host Blackbox exporter

Prometheus server and Alertmanager services monitors from Blackbox exporter of integrated agent running on other hosts. The following tables show URL to be monitored.

For details about how to add HTTP monitor of Blackbox exporter, see [1.21.2\(6\)\(c\) Add, change, or Delete the monitoring target \(for Windows\) \(required\)](#). For details about setting method of the alert definition, see [1.21.2\(3\)\(b\) To Add the alert definition \(for Windows\) \(optional\)](#).

Table 1–24: URL monitored by HTTP monitoring of Blackbox exporter

Service	URL to monitor
Prometheus server	<code>http://Host-name-of-integrated-agent:Port-number-of-Prometheus-server/-/healthy</code>
Alertmanager	<code>http://Host-name-of-integrated-agent:Port-number-of-Alertmanager/-/healthy</code>

The following is a sample alert-definition that you want to monitor with HTTP Monitor for Blackbox exporter.

```
groups:
- name: service_healthcheck
  rules:
- alert: jp1_pc_prometheus_healthcheck
  expr: probe_success{instance=~".*:20713/-/healthy"} == 0
  for: 3m
  labels:
    jp1_pc_product_name: "/HITACHI/JP1/JPCCS2"
    jp1_pc_component: "/HITACHI/JP1/JPCCS/CONFINFO"
    jp1_pc_severity: "Error"
    jp1_pc_metricname: "probe_success"
  annotations:
    jp1_pc_firing_description: "Communication to Prometheus server failed."
    jp1_pc_resolved_description: "Communication to Prometheus server was successful."
```

```

- alert: jpl_pc_alertmanager_healthcheck
  expr: probe_success{instance=~".*:20714/~/healthy"} == 0
  for: 3m
  labels:
    jpl_pc_product_name: "/HITACHI/JP1/JPCCS2"
    jpl_pc_component: "/HITACHI/JP1/JPCCS/CONFINFO"
    jpl_pc_severity: "Error"
    jpl_pc_metricname: "probe_success"
  annotations:
    jpl_pc_firing_description: "Communication to Alertmanager failed. "
    jpl_pc_resolved_description: "Communication to Alertmanager was successful. "

```

(b) Alive Monitoring Processes by Windows exporter

Windows servicing program are monitored by Windows exporter's process monitoring activity information. The processes to be monitored are described in the following table.

For details about Setting method of the alert definition, see [1.21.2\(3\)\(b\) To Add the alert definition \(for Windows\) \(optional\)](#).

Table 1–25: Processes monitored by the Windows exporter

Service	Processes to monitor	Monitored Name
jpc_imagent_service	<i>Agent-path</i> \bin\jpc_imagent_service.exe	Monitoring target 1:imagent Monitoring target 2:imagent
jpc_imagentproxy_service	<i>Agent-path</i> \bin\jpc_imagentproxy_service.exe	Monitoring target 1:imagentproxy Monitoring target 2:imagentproxy
jpc_imagentaction_service	<i>Agent-path</i> \bin\jpc_imagentaction_service.exe	Monitoring target 1:imagentaction Monitoring target 2:imagentaction
jpc_prometheus_server_service	<i>Agent-path</i> \bin\jpc_prometheus_server_service.exe	Monitoring target 1:prometheus Monitoring target 2:prometheus_server
jpc_alertmanager_service	<i>Agent-path</i> \bin\jpc_alertmanager_service.exe	Monitoring target 1:alertmanager Monitoring target 2:alertmanager
jpc_windows_exporter_service	<i>Agent-path</i> \bin\jpc_windows_exporter_service.exe	Monitoring target 1:Windows metric collector(Windows exporter) Monitoring target 2:windows_exporter
jpc_blackbox_exporter_service	<i>Agent-path</i> \bin\jpc_blackbox_exporter_service.exe	Monitoring target 1:RM Synthetic metric collector(Blackbox exporter) Monitoring target 2:blackbox_exporter
jpc_ya_cloudwatch_exporter_service	<i>Agent-path</i> \bin\jpc_ya_cloudwatch_exporter_service.exe	Monitoring target 1:RM AWS metric collector(Yet another cloudwatch exporter) Monitoring target 2:ya_cloudwatch_exporter
jpc_fluentd_service	<i>Agent-path</i> \bin\jpc_fluentd_service.exe	When to Use fluentd Monitoring target 1:fluentd_win Log trapper (Fluentd) Monitoring target 2:fluentd

Service	Processes to monitor	Monitored Name
		- When using only log metrics feature Monitoring target 1: fluentd_prome_win Log trapper (Fluentd) - Monitoring target 2: fluentd
jpc_script_exporter_service	Agent-path\bin\jpc_script_exporter_service.exe	- When using the UAP monitoring function Monitoring target 1: Script metric collector(Script exporter) Monitoring target 2: script_exporter - When using the job monitoring function Monitoring target 1: JP1/AJS3 metric collector(Script exporter) Monitoring target 2: script_exporter
jpc_promitor_scraper_service	Agent-path\bin\jpc_promitor_scraper_service.exe	Monitoring target 1: RM Promitor Monitoring target 2: promitor_scraper
jpc_promitor_resource_discovery_service	Agent-path\bin\jpc_promitor_resource_discovery_service.exe	Monitoring target 1: RM Promitor Monitoring target 2: promitor_resource_discovery

Here is a sample alert-definition that Windows exporter monitors:

```
groups:
- name: windows_exporter
  rules:
  - alert: jp1_pc_procmon_monitoring-target-1
    expr: absent (windows_process_start_time {instance="imahost:20717", job = "jpc_windows", jp1_pc_exporter= "JPC Windows exporter", jp1_pc_nodelabel = "jpc_monitoring-target-2_service", process = "jpc_monitoring-target-2_service"}) = 1.
    for: 3m
    labels:
      jp1_pc_product_name: "/HITACHI/JP1/JPCCS2"
      jp1_pc_component: "/HITACHI/JP1/JPCCS/CONFINFO"
      jp1_pc_severity: "Error"
      jp1_pc_metricname: "windows_process_start_time"
    annotations:
      jp1_pc_firing_description: "The number of processes was less than the threshold Value (1). "
      jp1_pc_resolved_description: "The number of processes exceeded the threshold Value (1). "
```

- Specify integrated agent host name in imahost part. Specify port number of Windows exporter in 20717 part
- For monitoring target 1 and monitoring target 2, specify the monitoring target name of *Table 1-25 Processes monitored by the Windows exporter*.
- If you specify more than one alert definition, repeat setup multiple times after the line starting with " - alert:".

(c) Monitoring with Prometheus server up metric

Windows exporter service, Blackbox exporter service, and Yet another cloudwatch exporter service are monitored through Prometheus server alert-monitoring. For details about setting method of the alert definition, see [1.21.2\(3\)\(b\) To Add the alert definition \(for Windows\) \(optional\)](#).

Here is a sample alert-definition that monitors up metric:

```
groups:
- name: exporter_healthcheck
  rules:
  - alert: jpl_pc_exporter_healthcheck
    expr: up{jpl_pc_remote_monitor_instance=""} == 0 or label_replace(sum
by (jpl_pc_remote_monitor_instance,jpl_pc_exporter) (up{jpl_pc_remote_monito
r_instance!=""}), "jpl_pc_nodelabel", "${1}", "jpl_pc_remote_monitor_instanc
e", "^[^:]*:([^:]*)$") == 0
    for: 3m
    labels:
      jpl_pc_product_name: "/HITACHI/JP1/JPCCS2"
      jpl_pc_component: "/HITACHI/JP1/JPCCS/CONFINFO"
      jpl_pc_severity: "Error"
      jpl_pc_metricname: "up"
    annotations:
      jpl_pc_firing_description: " Communication to Exporter failed. "
      jpl_pc_resolved_description: " Communication to Exporter was success
ful. "
```

(19) Creation and import of IM management node tree data (for Windows) (required)

Follow the steps below to create and import IM management node tree.

1. If you add a new integrated agent host or change hostname of integrated agent host, start service JP1/IM agent control base on that host.
2. Start add-on program and the integrated agent control base service in the same host, when you add an new add-on program or change program settings leads to configuration changes.
3. After all integrated agent host have started the corresponding service in steps 1 and 2, wait for one minute[#] after starting the service.

[#]: If value of the scrape_interval of Prometheus configuration file (jpc_prometheus_server.yml) has been changed, wait for that value time.

4. Perform the steps in Integrated manager host.

For details about the procedure, see steps 2 to 5 in [1.19.3\(1\)\(c\)Creation and import of IM management node tree data \(for Windows\) \(required\)](#).

(20) Security-product exclusion Setup (for Windows) (optional)

If you are deploying antivirus software or security products, setup the following directories to exclude them:

- In Windows
Agent-path\

- In Linux
/opt/jplima/

(21) Notes on updating the definition file (for Windows)

If you restart the service of JP1/IM - Agent to reflect the updated content of definition files, monitoring stops during restart of the service is ongoing.

1.22 Building Container Environments in JP1/IM - Agent (for Windows)

To create a container environment, do the following:

1. Create a container image
2. Start the container

1.22.1 Creating container images

(1) Conditions for the base container image

For details about the conditions for base container images for Docker image and Podman image, see *14.3.12(4)(c) Container image prerequisites* and *14.3.12(5)(b) Container image prerequisites* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*, respectively.

(2) How to create Docker and Podman image

1. Create a working directory on Docker host or Podman host where you want to create the image.
2. Prepare the following items under the working directory:
 - Dockerfile File
 - JP1/IM - Agent install package
 - Supervisord definition file (shown as using Supervisor)
 - Startup script
 - Credentials File (if Yet another cloudwatch exporter is used)
 - File to be placed in conf directory.

Here, the directory configuration is as follows.

Place files to be updated among JP1/IM - Agent definition files in conf directory.

```
Working-directory/#1
+ Dockerfile#2
+ JP1IMA/#3
|   + X64LIN/
|       + h_inst
|       + ppmanage
|       + setup
|       + PCC842C/
|           + 9GDL/
|               + ...
+ supervisord.conf#4
+ start.sh#5
+ credentials#6
+ conf/
    + jpc_imagentcommon.json.model#7
    + jpc_alerting_rules.yml.model#8
    + jpc_ya_cloudwatch_exporter.yml.model#9
    + jpc_blackbox_exporter.yml.model#10
```

1. Installation and Setup (for Windows)

```

+ jpc_file_sd_config_blackbox_http.yml.model#11
+ jpc_file_sd_config_blackbox_icmp.yml.model#12
+ jpc_process_exporter.yml#13
+ jpc_script_exporter.yml#14
+ promitor/#15
| + scraper/#16
| | + runtime.yml#17
| | + metrics-declaration.yml#18
| + resource-discovery/#19
|   + runtime.yml#20
|   + resource-discovery-declaration.yml#21
+ user/
  + cert/
    + XXXX.crt#22

```

#1: The working directory created in step 1

#2: Dockerfile File

#3: The directories and files where JP1/IM - Agent installation package was extracted

#4: supervisord definition file

#5: Start script

#6: AWS credential file (when Yet another cloudwatch exporter is used)

#7: imagent common configuration file

#8: alert configuration file (when defining alerts)

#9: Yet another cloudwatch exporter configuration file

#10: Blackbox exporter configuration file

#11: Blackbox (HTTP/HTTPS monitoring) discovery configuration file

#12: Blackbox (ICMP monitoring) discovery configuration file

#13: process exporter configuration file (If changing the settings)

#14: script exporter configuration file (If changing the settings)

#15: promitor configuration file directory (If changing the settings)

#16: promitor scraper configuration file directory (If changing the settings)

#17: promitor scraper configuration file (If changing the settings)

#18: promitor scraper configuration file (If changing the settings)

#19: promitor resource discovery configuration file directory (If changing the settings)

#20: promitor resource discovery configuration file (If changing the settings)

#21: promitor resource discovery configuration file (If changing the settings)

#22: CA certificates for connecting to Integrated manager host

The build procedure to connect to Azure with ServicePrincipal is as follows.

1. In the build procedure described in *Building a container environment for integrated agents* for JP1/IM - Agent, perform the steps other than step 4 in *1.21.2(8) Set up of Promitor > (b) Configuring authentication information for connecting to Azure* and then create the files under the working directory.

2. After starting the container, perform step 4 in *1.21.2(8) Set up of Promitor > (b) Configuring authentication information for connecting to Azure*.

3. Start the Promitor service. For details, see *Building a container environment for integrated agents* for service control.

- Notes on Definition file

Do not specify IP address for definition File. Also, do not include IP address in the certificate File. If you include IP address data, you cannot handle containers that dynamically change IP address.

- Sample of Dockerfile File

Set the installer environment variables as needed, as shown in the ENV line in the example below.

```
FROM oraclelinux:8

RUN mkdir /root/.aws
COPY credentials /root/.aws/credentials
COPY JP1IMA/X64LIN /tmp/X64LIN
COPY start.sh /opt/start.sh
COPY supervisord.conf /opt/supervisord.conf
RUN dnf install -y python3
RUN pip3 install supervisor
RUN dnf install -y cpio
RUN chmod a+x /opt/start.sh

ENV JP1IMAGENT_INSTALL_MODE "image"
ENV JP1IMAGENT_IMMGR_HOST "Set the host name of the destination manager"
ENV JP1IMAGENT_IMMGR_INITIAL_SECRET "Set the initial secret"
ENV JP1IMAGENT_ADDON_BLACKBOX_EXPORTER_ACTIVE "yes"
ENV JP1IMAGENT_ADDON_YA_CLOUDWATCH_EXPORTER_ACTIVE "yes"
ENV JP1IMAGENT_ADDON_PROMITOR_ACTIVE "no"#
ENV JP1IMAGENT_ADDON_PROCESS_EXPORTER_ACTIVE "yes"
ENV JP1IMAGENT_ADDON_SCRIPT_EXPORTER_ACTIVE "no"

RUN /tmp/X64LIN/setup -f -k P-CC842C-9GDL /tmp/
COPY conf /opt/jplima/conf

CMD [ "/bin/bash", "-c", "/opt/start.sh" ]
```

#

If "yes", the following log will be output after the container is started, and the service startup will fail. After setting the authentication information and restarting, it starts normally.

Validation failed: Azure authentication is not configured correctly - No identity secret was configured for service principle authentication

- Creation Sample of service definition file of supervisord

```
[unix_http_server]
file=/tmp/supervisor.sock ; the path to the socket file

[supervisord]
logfile=/tmp/supervisord.log
logfile_maxbytes=5MB
logfile_backups=10
loglevel=info
pidfile=/tmp/supervisord.pid
nodaemon=true

[program:imagent]
command=/opt/jplima/bin/imagent
directory=/opt/jplima/bin/
stopasgroup=true
autostart=true
stopwaitsecs=180
```

```

[program:imagentaction]
command=/opt/jplima/bin/imagentaction
directory=/opt/jplima/bin/
stopasgroup=true
autostart=true
stopwaitsecs=180

[program:imagentproxy]
command=/opt/jplima/bin/imagentproxy
directory=/opt/jplima/bin/
stopasgroup=true
autostart=true
stopwaitsecs=180

[program:prometheus]
command=command-line#1
directory=/opt/jplima/bin#2
autostart=true#3
stopasgroup=true
stopwaitsecs=180

[program:alertmanager]
command=command-line#1
directory=/opt/jplima/bin#2
autostart=true#3
stopasgroup=true
stopwaitsecs=180

[program:node_exporter]
command=command-line#1
directory=/opt/jplima/bin#2
autostart=true#3
stopasgroup=true
stopwaitsecs=180

[program:process_exporter]
command=command-line#1
directory=/opt/jplima/bin
autostart=true
stopwaitsecs=180

[program:program-name]
command= command-line#1
directory=/opt/jplima/bin#2
autostart=true#3
stopasgroup=true#4
stopwaitsecs=180

```

Note: No description is required for services that are not used.

#1: For *command-line*, use Value of ExecStart listed in `jpc_XXXXXX.service` stored in `/usr/lib/systemd/system` directory of Physical host. In this case, you need to replace "`@@installldir1@@`" and "`@@installldir2@@`" with `/opt`".

If ExecStart listed in the `jpc_XXXXXX.service` starts with `"/bin/sh-c 'XXXXXXXX'`, modify it as in `"/bin/sh-c 'trap "" 15; XXXXXXXX'`.

Sample for Alertmanager

```
/bin/sh -c 'trap "" 15; /opt/jplima/bin/osswrapper "/opt/
jplima/bin/alertmanager" ...
```

#2: When JP1/IM - Agent program is run from the service-management program, specify /opt/jplima/bin as the current directory#3: Select Enable for auto start.

#4: Set stopasgroup to true.

- Startup Script Example

```
#!/bin/bash
/opt/jplima/tools/jimasetup container#1
mv -f /opt/jplima/conf/jpc_file_sd_config_blackbox_http.yml \
/opt/jplima/conf/jpc_file_sd_config_off#2
mv -f /opt/jplima/conf/jpc_file_sd_config_blackbox_icmp.yml \
/opt/jplima/conf/jpc_file_sd_config_off#2
mv -f /opt/jplima/conf/jpc_file_sd_config_cloudwatch.yml \
/opt/jplima/conf/jpc_file_sd_config_off#2
mv -f /opt/jplima/conf/jpc_file_sd_config_process.yml \
/opt/jplima/conf/jpc_file_sd_config_off#2
mv -f /opt/jplima/conf/jpc_file_sd_config_promitor.yml \
/opt/jplima/conf/jpc_file_sd_config_off#2
exec /usr/local/bin/supervisord -c /opt/supervisord.conf#3
```

#1: Execute initial setting command of JP1/IM - Agent with container option-specification.

#2: For the following services, move the discovery configuration file corresponding to the unused services from /opt/jplima/conf directory to /opt/jplima/conf/jpc_file_sd_config_off directory:

Service	Discovery configuration file
prometheus_server	None
alertmanager	None
windows_exporter	jpc_file_sd_config_windows.yml
blackbox_exporter	- jpc_file_sd_config_blackbox_http.yml - jpc_file_sd_config_blackbox_icmp.yml
ya_cloudwatch_exporter	jpc_file_sd_config_cloudwatch.yml
fluentd	None
promitor	jpc_file_sd_config_promitor.yml
script_exporter	None

#3: Execute the service management tools.

- Example of imagent common configuration file

An example of the model file (jpc_imagentcommon.json.model) of the imagent common configuration file is as follows:

If you use TLS, set the path of the CA certificate to the ca_file. If you don't want to use TLS, delete the tls_config item.

```
{
  "JP1_BIND_ADDR": "ANY",
  "COM_LISTEN_ALL_ADDR": 0,
  "COM_MAX_LISTEN_NUM": 4,
  "JP1_CLIENT_BIND_ADDR": "ANY",
```

```

"http": {
  "max_content_length": 10,
  "client_timeout": 30
},
"immgr": {
  "host": "@@immgr.host@",
  "proxy_url": "@@immgr.proxy_url@",
  "proxy_user": "@@immgr.proxy_user@",
  "tls_config": {
    "ca_file": "/opt/jplima/conf/user/cert/XXXX.crt",
    "insecure_skip_verify": false,
    "min_version": "TLSv1_2"
  },
  "ibase": {
    "port": @@immgr.ibase_port@@
  },
  "ibaseproxy": {
    "port": @@immgr.ibaseproxy_port@@
  }
}
}

```

3. Navigate to the directory where the Dockerfile resides and launch a Docker or Podman build.

- For Docker

```
# docker build -t Docker-image-name:tag .
```

- For Podman

```
# podman build -t Podman-image-name:tag .
```

(3) How to Create Docker and Podman Containers

1. Launch Docker or Podman containers.

- For Docker

```
# docker container run --ulimit nofile=65536:65536 -add-host=Manager-Host
-name:IP-address -d -h Host-name-for-the-container Docker-Image-Name:Tag
```

- For Podman

```
# podman container run --ulimit nofile=65536:65536 -add-host=Manager-Host
-name:IP-address -d -h Host-name-for-the-container Podman-Image-Name:Tag
```

Important

Host name of the containers is displayed in integrated operation viewer tree. If you omit the -h option, we recommend that you specify Host name because it will automatically Setup Host name by Docker or Podman and that Host name will appear in integrated operation viewer tree.

2. Check the log of the service management tools and the log of JP1/IM - Agent to make sure that it is running in Normal. If Error is printed or if the process you want to run is not running, identify the reason and recreate Docker or Podman image.

3. Refresh IM management node tree.

For details, see [1.21.2\(19\) Creation and import of IM management node tree data \(for Windows\) \(required\)](#).

(4) How to delete Docker and Podman Containers

1. Stop Docker or Podman containers.

- For Docker

```
# docker container stop container-name
```

- For Podman

```
# podman container stop container-name
```

2. Delete a Docker or Podman container.

- For Docker

```
# docker container rm container-name
```

- For Podman

```
# podman container rm container-name
```

3. Refresh IM management node tree.

For details, see [1.21.2\(19\) Creation and import of IM management node tree data \(for Windows\) \(required\)](#).

(5) About the impact on kernel parameters

For the upper limit of the number of File descriptors, specify 65536 in `--ulimit` option when starting containers.

For details, see [1.22.1\(3\) How to Create Docker and Podman Containers](#).

1.22.2 Upgrading JP1/IM - Agent

Although you can upgrade JP1/IM - Agent on already created containers, we recommend that you use the new version of JP1/IM - Agent to create Docker and Podman images and recreate the containers from the new container images.

Follow the steps below to upgrade JP1/IM - Agent on the containers you have already created.

(1) When upgrading JP1/IM - Agent from a pre-13-11 version on a container that has already been created

- Stopping JP1/IM - Agent

Before upgrading JP1/IM - Agent on a container that you have already created, stop JP1/IM - Agent service in the service management tools.

- Updating service definition file

When you upgrade and install JP1/IM - Agent on a container from a version earlier than 13-11 to a version 13-11 or later, unit definition file model files that exist in `/opt/jplima/conf` folder are updated. Manually reconfigure the

command line that appears on ExecStart line of this model file as a command line that runs on the serviced management tools. Also replace "@@installldir1@" and "@@installldir2@" with "/opt".

If the command-line begins with "/bin/sh -c 'xxxxxxx'", modify it as in "/bin/sh -c 'trap "" 15; xxxxxxxx'".

This manual uses supervisord as a serviced management tools. Here is a sample command-line change for Prometheus server listed in service definition file of supervisord: Add the underlined text.

- Before change

```
[program:prometheus]
command=/bin/sh -c '/opt/jplima/bin/prometheus" --config.file="/opt/jplima/conf/jpc_prometheus_server.yml" --web.listen-address="0.0.0.0:20713" --web.read-timeout=5m --web.max-connections=10 --web.enable-lifecycle --storage.tsdb.path="/opt/jplima/data/prometheus_server/" --storage.tsdb.retention.time=1h --storage.tsdb.min-block-duration=1h --storage.tsdb.max-block-chunk-segment-size=32MB --storage.remote.flush-deadline=5s --rules.alert.for-outage-tolerance=1h --rules.alert.for-grace-period=10m --rules.alert.resend-delay=1m --alertmanager.notification-queue-capacity=10000 --log.level=debug --log.format=logfmt |& ( trap "" 15 && exec "/opt/jplima/bin/rotatelog" -n 8 "/opt/jplima/logs/prometheus_server/prometheus_service" 10240K) '
directory=/opt/jplima/bin
autostart=true
stopasgroup=true
stopwaitsecs=180
```

- After change

```
[program:prometheus]
command=/bin/sh -c '/opt/jplima/bin/ossrapper "/opt/jplima/bin/prometheus" --config.file="/opt/jplima/conf/jpc_prometheus_server.yml" --web.listen-address="0.0.0.0:20713" --web.read-timeout=5m --web.max-connections=10 --web.enable-lifecycle --storage.tsdb.path="/opt/jplima/data/prometheus_server/" --storage.tsdb.retention.time=1h --storage.tsdb.min-block-duration=1h --storage.tsdb.max-block-chunk-segment-size=32MB --storage.remote.flush-deadline=5s --rules.alert.for-outage-tolerance=1h --rules.alert.for-grace-period=10m --rules.alert.resend-delay=1m --alertmanager.notification-queue-capacity=10000 --log.level=debug --log.format=logfmt |& ( trap "" 15 && exec "/opt/jplima/bin/rotatelog" -n 8 "/opt/jplima/logs/prometheus_server/prometheus_service" 10240K) '
directory=/opt/jplima/bin
autostart=true
stopasgroup=true
stopwaitsecs=180
```

1.23 Building optional features for JP1/IM - Agent (for Windows)

1.23.1 Configuring OracleDB exporter

This section describes how to configure OracleDB exporter, an optional feature of integrated agent host.

(1) Preparing for OracleDB exporter configuration

This section describes how to prepare for configuring OracleDB exporter.

(a) Obtaining setup archive files

Retrieve the setup archive file to use OracleDB exporter. The setup archive file is in JP1/IM - Agent installation folder.

The file names for the setup archive files are as follows:

JP1/IM-Agent-Installation-destination-folder/jplima/options/

- *oracledb_exporter_windows_VVRRSS.zip* (Windows version)
- *oracledb_exporter_linux_VVRRSS.tar.gz* (Linux version)

(b) Setting up JP1/IM - Manager

If JP1/IM - Manager 13-01 or later is newly installed, it does not need to be executed.

Perform the following steps when upgrading from a version earlier than JP1/IM - Manager 13-01.

■ Placing metric definition files

Perform the following steps when upgrading from a version earlier than JP1/IM - Manager 13-01 in logical host operation.

1. Copy metric definition file of the following OracleDB exporter and rename it to the definition file name of the copy destination.
 - For Windows
Source filename: *JP1/IM-Manager-installation-folder\jplimm\conf\imdd\plugin\jplpccs\metrics_oracledb_exporter.conf.model*
Destination filename: *JP1/IM-Manager-installation-folder\jplimm\conf\imdd\plugin\jplpccs\metrics_oracledb_exporter.conf*
 - For Linux
Source filename: *JP1/IM-Manager-installation-directory/jplimm/conf/imdd/plugin/jplpccs/metrics_oracledb_exporter.conf.model*
Destination filename: *JP1/IM-Manager-installation-directory/jplimm/conf/imdd/plugin/jplpccs/metrics_oracledb_exporter.conf*

For Linux, set the permissions to 600.

For logical host operation, place this file in the following location:

- For Windows
shared-folder\jplimm\conf\imdd\plugin\jplpccs
- For Linux

shared-directory/jplimm/conf/imdd/plugin/jplpccs/

■ Updating IM manager updatable definition file list definition file

Perform the following steps when upgrading from a version earlier than JP1/IM - Manager 13-01 in logical host operation.

If the procedure for installing another optional function overwrites with "imdd_product_deffile_list.json.update" obtained from the most recent archived file, the procedure below is not necessary.

1. Copy the following IM manager updatable definition file list definition file and rename it to the destination definition file.

- For Windows

Source filename: *JP1/IM-Manager-installation-*

folder\jplimm\conf\imdd\system\fileoperation\imdd_product_deffile_list.json.update

Destination filename: *JP1/IM-Manager-installation-*

folder\jplimm\conf\imdd\system\fileoperation\imdd_product_deffile_list.json

- For Linux

Source filename: *JP1/IM-Manager-installation-directory/jplimm/conf/imdd/system/fileoperation/imdd_product_deffile_list.json.update*

Destination filename: *JP1/IM-Manager-installation-directory/jplimm/conf/imdd/system/fileoperation/imdd_product_deffile_list.json*

For logical host operation, place this file in the following location:

- For Windows

shared-folder\jplimm\conf\imdd\system\fileoperation

- For Linux

shared-directory/jplimm/conf/imdd/system/fileoperation/

(c) Setting up JP1/IM - Agent

If JP1/IM - Agent 13-01 or later is newly installed, it does not need to be executed.

Perform the following steps when upgrading from a version earlier than JP1/IM - Agent 13-01.

■ Stopping JP1/IM - Agent

Stop JP1/IM - Agent service.

For physical hosts

Stop JP1/IM - Agent servicing by running the following command.

```
jpc_service_stop -s all
```

For logical hosts

Stop from the cluster software.

■ Setting up OracleDB exporter scrape jobs

The model file of the Prometheus configuration file is updated when the version is upgraded. Write the following details of Prometheus configuration file model file (jpc_prometheus_server.yml.model) under scrape_configs of Prometheus configuration file (jpc_prometheus_server.yml).

For logical host operation, update the following files:

- For Windows

shared-folder\jplima\conf\jpc_prometheus_server.yml

- For Linux

shared-directory/jplima/conf/jpc_prometheus_server.yml

```
(Omitted)
:
scrape_configs:
  - job_name: 'jpc_oracledb'
    scrape_interval: 60s
    scrape_timeout: 30s
    metrics_path: /metrics
    file_sd_configs:
      - files:
        - 'jpc_file_sd_config_oracledb.yml'
    relabel_configs:
      - source_labels: [__address__]
        target_label: instance
        regex: ([^:]+):([^:]+):(.*)
        replacement: ${1}:${2}
      - source_labels: [__address__]
        target_label: jpl_pc_nodelabel
        regex: ([^:]+):([^:]+):(.*)
        replacement: ${2}
      - source_labels: [__address__]
        target_label: __address__
        regex: ([^:]+):([^:]+):(.*)
        replacement: @@hostname@@#:${3}
    metric_relabel_configs:
      - source_labels: ['__name__']
        regex: 'oracledb_sessions_value|oracledb_resource_current_utilizatio
n|oracledb_resource_limit_value|oracledb_asm_diskgroup_total|oracledb_asm_di
skgroup_free|oracledb_activity_execute_count|oracledb_activity_parse_count_t
otal|oracledb_activity_user_commits|oracledb_activity_user_rollbacks|oracled
b_activity_physical_reads_cache|oracledb_activity_consistent_gets_from_cache
|oracledb_activity_db_block_gets_from_cache|oracledb_process_count|oracledb_
wait_time_administrative|oracledb_wait_time_application|oracledb_wait_time_c
ommit|oracledb_wait_time_concurrency|oracledb_wait_time_configuration|oracle
db_wait_time_network|oracledb_wait_time_other|oracledb_wait_time_scheduler|o
racledb_wait_time_system_io|oracledb_wait_time_user_io|oracledb_tablespace_b
ytes|oracledb_tablespace_max_bytes|oracledb_tablespace_free|oracledb_tablesp
ace_used_percent|oracledb_exporter_last_scrape_duration_seconds|oracledb_exp
orter_last_scrape_error|oracledb_exporter_scrapes_total|oracledb_up'
        action: 'keep'
```

#

Specify the host name of JP1/IM - Agent (or logical host name for logical host operation).

■ Deploying OracleDB exporter discovery configuration file

If the procedure for installing another optional function overwrites with

"jpc_product_deffile_list.json.update" obtained from the most recent archived file, the procedure below is not necessary.

1. Copy the model file of the definition file that defines the monitoring target of the following OracleDB exporter, and rename it to the definition file name of the copy destination.

- For Windows

Source filename: *JP1/IM - Agent*

installation_folder\jplima\conf\jpc_file_sd_config_oracledb.yml.model

Destination filename: *JP1/IM - Agent*

installation_folder\jplima\conf\jpc_file_sd_config_oracledb.yml

- For Linux

Source filename: *JP1/IM - Agent installation directory/jplima/*

conf/jpc_file_sd_config_oracledb.yml.model

Destination filename: *JP1/IM - Agent installation directory/jplima/*

conf/jpc_file_sd_config_oracledb.yml

For Linux, set the permissions to 600.

For logical host operation, place this file in the following location.

- For Windows

shared_folder\jplima\conf

- For Linux

shared-directory/jplima/conf/

2. Open the jpc_file_sd_config_oracledb.yml file created in step 1 in a text editor, edit it as follows, and overwrite it.

```
- targets:
# - Oracle-Database-host-name:any-name:port-number-of-OracleDB-exporter
  labels:
    jpl_pc_exporter: JPC OracleDB exporter
    jpl_pc_category: database
    jpl_pc_trendname: oracledb_exporter
    jpl_pc_remote_monitor_instance: @@hostname@#:OracleDB collector(OracleDB exporter)
```

#

Specify the host name of JP1/IM - Agent (or logical host name for logical host operation).

■ Updating integrated agent updatable definition file list definition file

The following describes the steps for updating integrated agent updatable definition file list definition file.

If the procedure for installing another optional function overwrites with

"jpc_product_deffile_list.json.update" obtained from the most recent archived file, the procedure below is not necessary.

1. Copy the following integrated agent updatable definition file list definition file and rename it to the destination definition filename.

- For Windows

Source filename: *JP1/IM-Agent-installation-*

folder\jplima\conf\jpc_product_deffile_list.json.update

Destination filename: *JP1/IM-Agent-installation-*

folder\jplima\conf\jpc_product_deffile_list.json

- For Linux

Source filename: *JP1/IM-Agent-installation-directory/jplima/*

conf/jpc_product_deffile_list.json.update

Destination filename: *JP1/IM-Agent-installation-directory/jplima/*

conf/jpc_product_deffile_list.json

For logical host operation, place this file in the following location:

- For Windows

shared-folder\jplima\conf

- For Linux

shared-directory/jplima/conf/

■ Checking the settings

Prometheus server definition file is checked because the format can be checked by the `promtool` command.

The `promtool` command is stored in under *JP1/IM-Agent-installation-destination/jplima/tools*.

```
promtool check config jpc_prometheus_server.yml
```

If an error is displayed, review the error.

Note that there is no problem even if the following warning is displayed.

```
WARNING: file "../conf/jpc_file_sd_config_windows.yml" for file_sd in scrap
e job "jpc_windows" does not exist
```

■ Starting JP1/IM - Agent

Start JP1/IM - Agent servicing.

- For physical hosts

Run the following command to start JP1/IM - Agent services.

```
jpc_service_start -s all
```

- For logical hosts

Start from the cluster software.

(2) Installing OracleDB exporter

This section describes how to install OracleDB exporter.

(a) OracleDB exporter layout

Extract the setup archive file[#] obtained in *1.23.1(1)(a) Obtaining setup archive files* to any folder. Do not specify the folder where JP1/IM - Manager or JP1/IM - Agent is installed in the destination folder.

1. Installation and Setup (for Windows)

#

- For Windows
oracledb_exporter_windows_VVRRSS.zip
- For Linux
oracledb_exporter_linux_VVRRSS.tar.gz

When operating OracleDB exporter on a logical host, place it in shared folders.

(b) Creating the default metric files

1. Copies the model file of the following default metric definition file and renames it to the definition file name of the copy destination.

- For Windows
Source filename: *OracleDB-exporter-location*\oracledb_exporter_windows\jplima\conf\default-metrics.toml.model
Destination filename: *OracleDB-exporter-location*\oracledb_exporter_windows\jplima\conf\default-metrics.toml
- For Linux
Source filename: *OracleDB-exporter-location*/oracledb_exporter_linux/jplima/conf/default-metrics.toml.model
Destination filename: *OracleDB-exporter-location*/oracledb_exporter_linux/jplima/conf/default-metrics.toml

(c) Adding a monitoring target

For details on adding a monitoring target, see [1.23.1\(4\)\(a\) Adding a monitoring target \(required\)](#).

(3) Uninstalling OracleDB exporter

This section describes how to uninstall OracleDB exporter.

(a) Deleting a monitoring target

When uninstalling OracleDB exporter, remove all the monitoring targets and then remove OracleDB exporter. For details about deleting a monitoring target, see [1.23.1\(4\)\(d\) Deleting a monitoring target \(optional\)](#).

(b) Deleting OracleDB exporter

To delete OracleDB exporter, delete the folders that were placed in [1.23.1\(2\)\(a\) OracleDB exporter layout](#).

(4) Setting up OracleDB exporter

This section explains how to setup OracleDB exporter.

(a) Adding a monitoring target (required)

■ Preparing to add a monitoring target

1. Determine "instance name" that identifies the service for OracleDB exporter.
OracleDB exporter must be started for each target. If you have more than one target, you need to create more than one OracleDB exporter service. The name used to identify OracleDB exporter services is called "instance name".

- Instance name can contain only alphanumeric characters.
- The length of instance name is 32 bytes or less.

2. Determine the listen port for OracleDB exporter.

Determine the port number on which OracleDB exporter service listens. Use a port number that is not used by other services or other OracleDB exporter services.

3. Check the value to be set in the environment variable JP1IMADIR.

You must set the environment variable JP1IMADIR to service definition file, or unit definition file of OracleDB exporter. Depending on the type of host in the JP1/IM - Agent, the following values will occur.

- For Windows

Host type	Environment-variable JP1IMADIR
For physical host operation	<i>JP1/IM-Agent-installation-folder\jplima</i>
For logical host operation	<i>shared-folder\jplima</i>

- For Linux

Host type	Environment-variable JP1IMADIR
For physical host operation	<i>/opt/jplima</i>
For logical host operation	<i>shared-directory/jplima</i>

4. Check the value to be set in the environment variable DATA_SOURCE_NAME for the OracleDB exporter specified in the service definition file of OracleDB exporter.

In the environment variable DATA_SOURCE_NAME for the OracleDB exporter specified in the service definition file of OracleDB exporter, the connection user and connection destination information must be set.

The environment variable DATA_SOURCE_NAME for OracleDB exporter is specified in the following format.

- For Windows

```
oracle://user-name@host-name:port/service-name?connection timeout=10[&instance name=monitored-Oracle-instance-name]
```

- For Linux

```
oracle://user-name@host-name:port/service-name?connection timeout=10[&instance name=monitored-Oracle-instance-name]
```

user-name

Specifies the username of the user used to connect to Oracle Database.

Allowed characters are uppercase letters, numbers, underscores, dollar signs, pound signs, periods, and at signs. Specify within 30 characters.

host-name

Specifies the hostname of OracleDB host to monitor.

Characters that can be specified are uppercase letters, lowercase letters, numbers, -(hyphen), _ (underscore), . (period). Specify within 253 characters.

port

Specify the port number for connecting to Oracle listener.

service-name

Specifies the service name of Oracle listener.

Characters that can be specified are uppercase letters, lowercase letters, numbers, _ (underscore), - (hyphen), . (period). Specify within 64 characters.

Option

Specify the connection options. If you have more than one option, use "&" in Windows and "&" in Linux.

- connection timeout=*seconds*

Specifies the connection timeout in seconds. This option must be specified.

Be sure to specify 10.

If you specify a value other than 10 and do not specify this option, scrape of Prometheus server times out and up metric may be 0 even if OracleDB exporter is running.

- instance name=*monitored-Oracle-instance-name*

Specifies Oracle instance name to connect to. Specifying this option is optional.

The host name, port, service name can be checked with `lsnrctl service` command of Oracle Database. In the example below, the host name is ORAHOST, the port is 1521, the service name is orcl.local, and Oracle instance name is orcl.

```
$ lsnrctl service

LSNRCTL for 64-bit Windows: Version 19.0.0.0.0 - Production on 13-Dec-202
3 09:09:34

Copyright (c) 1991, 2019, Oracle. All rights reserved.

Connected to (DESCRIPTION=(ADDRESS=(PROTOCOL=TCP) (HOST=ORAHOST) (PORT=1521)
))
Service Summary...
:
:
The service "orcl.local" has one instance.
Instance "orcl", Status READY has one handler for this service...
Handler:
  "DEDICATED" Established:10674 Rejected:1 Status:ready
    LOCAL SERVER
:
:
```

In this case, the environment variable DATA_SOURCE_NAME for OracleDB exporter is as follows.

- For Windows

```
oracle://user-name@ORAHOST:1521/orcl.local?connection timeout=10&instance name=orcl
```

- For Linux

```
oracle://user-name@ORAHOST:1521/orcl.local?connection timeout=10&instance name=orcl
```

5. Determine the name of the monitoring target to be displayed in the tree of the Intelligent Integrated Management Base.

OracleDB exporter monitoring targets are displayed in Intelligent Integrated Management Base tree as follows.

Since any name can be specified for the monitoring target name, please decide an appropriate monitoring target name.

```
All Systems
  + Oracle-Database-host-name
```

```
+ Database
+ monitoring-target-name-1
+ monitoring-target-name-2
```

For the length of characters and strings that can be used, see *OracleDB exporter discovery configuration file (jpc_file_sd_config_oracledb.yml)* in *Chapter 2. Definition Files* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

6. Confirm whether to operate on a physical host or a logical host.

OracleDB exporter is also a physical host operation if scrape of the newly added JP1/IM - Agent is a physical host operation.

OracleDB exporter is also logical host operation if scrape of the newly added JP1/IM - Agent is logical host operation.

7. Make sure you can get the metrics you want to monitor.

We recommend that you run SQL statement for acquiring data directly with the person you use to connect to ensure that the required metric can be retrieved.

If you cannot get the metrics you want to monitor, contact Oracle Database support so that they can be retrieved.

■ Setting up OracleDB exporter

1. Copy the Windows serviced program and rename it to the destination program name.

Source filename: *OracleDB-exporter-*

location\oracledb_exporter_windows\jplima\bin\oracledb_exporter_@@instance@@_service.exe

Destination file name:

- For physical host operation

OracleDB-exporter-

location\oracledb_exporter_windows\jplima\bin\oracledb_exporter_instance-name-identifying-the-OracleDB-exporter-service#_service.exe

- For logical host operation

OracleDB-exporter-

location\oracledb_exporter_windows\jplima\bin\oracledb_exporter_instance-name-identifying-the-OracleDB-exporter-service#_logical-host-name_service.exe

#

For instance name, specify the name determined in - *Preparation for adding a monitoring target* in *1.23.1(4)(a) Adding a monitoring target (required)*.

2. Create a service definition file.

Copy the source service definition file and rename it to the destination program.

Source filename: *OracleDB-exporter-*

location\oracledb_exporter_windows\jplima\bin\oracledb_exporter_@@instance@@_service.xml.model

Destination file name:

- For physical host operation

OracleDB-exporter-

location\oracledb_exporter_windows\jplima\bin\oracledb_exporter_instance-name-identifying-the-OracleDB-exporter-service#_service.xml

- For logical host operation

OracleDB-exporter-
location\oracledb_exporter_windows\jplima\bin\oracledb_exporter_instance-name-
identifying-the-OracleDB-exporter-service#_logical-host-name_service.xml

#

For instance name, specify the name determined in - *Preparation for adding a monitoring target* in *1.23.1(4)(a) Adding a monitoring target (required)*.

3. Updating service definition file.

Modify the following for service definition file you created in step 2.

Value to be changed	Value to specify
<code>@@instance@@</code>	- For physical host operation Replace with the name determined in step 1 of <i>Preparing to add a monitoring target</i> in <i>1.23.1(4)(a) Adding a monitoring target (required)</i> . - For logical host operation Replace with the name determined in step 1 of <i>Preparing to add a monitoring target</i> in <i>1.23.1(4)(a) Adding a monitoring target (required)</i> with the name " <code>_logical-host-name</code> ".
<code>@@oracledb_exporter_installdir@@</code>	Replace with OracleDB exporter location.
<code>@@autostart@@</code>	- To start automatically at OS startup "Automatic" - To not start automatically "Manual" For logical hosts, substitute "Manual".
<code>@@port@@</code>	Replace with the port number determined in step 2 of <i>Preparing to add a monitoring target</i> in <i>1.23.1(4)(a) Adding a monitoring target (required)</i> . For a logical host, specify the logical host name, and replace it so that <code>--web.listen-address="logical-host-name:port-number"</code> .
<code>@@installdir2@@</code>	Replace with the directory confirmed in step 3 of <i>Preparing to add a monitoring target</i> in <i>1.23.1(4)(a) Adding a monitoring target (required)</i> .
<code>@@data_source_name@@</code>	Replace with the content confirmed in step 4 of <i>Preparing to add a monitoring target</i> in <i>1.23.1(4)(a) Adding a monitoring target (required)</i> .

4. Register the service.

Execute the command created in step 1 as follows.

- For physical host operation
`oracledb_exporter_instance-name-identifying-the-OracleDB-exporter-service#_service.exe install`
- For logical host operation
`oracledb_exporter_instance-name-identifying-the-OracleDB-exporter-service#_logical-host-name_service.exe install`
 For logical host operation, execute the command on both nodes that make up the cluster.

#

For instance name, specify the name determined in *Preparing to add a monitoring target* in *1.23.1(4)(a) Adding a monitoring target (required)*.

5. Register the password of the user used to connect to Oracle Database.

Register the password of the user used to connect to Oracle Database with the `jimasecret` command.

- For physical host operation

```
jimasecret -add -key OracleDB.user.user-name -s password
```

- For logical host operation

```
jimasecret -add -key OracleDB.user.user-name -s password -l shared-folder
```

If you want to register users with the same user name but different passwords, you can use a key that includes the host name and the service name.

For details about the `jimasecret` command, see `jimasecret` in *Chapter 1. Commands* in the *JPI/Integrated Management 3 - Manager Command, Definition File and API Reference*.

6. Register the service with the cluster software.

For a cluster configuration, register the service with the cluster software.

7. Start OracleDB exporter service.

Start OracleDB exporter service from the command line or from Windows Service Control Manager.

For a cluster configuration, start the service from the cluster software.

8. Confirm that OracleDB exporter can acquire the performance information.

The following URL can be accessed by using curl commands and browsers to check whether performance information can be obtained.

```
http://host-name:port/metrics
```

The hostname is the host on which OracleDB exporter is booting, and the port is the listen port of OracleDB exporter.

■ Configuring Prometheus

1. Add monitoring target to OracleDB exporter discovery configuration file.

Add a new entry under targets in the OracleDB exporter discovery configuration file (`jpc_file_sd_config_oracledb.yml`).

```
- targets:
#   - Oracle-Database-host-name:any-name:port-number-of-OracleDB-exporter

   - Oracle-Database-host-name: monitoring-target-name-1:port-number-1
   - Oracle-Database-host-name: monitoring-target-name-2:port-number-2
   - Oracle-Database-host-name: monitoring-target-name-3:port-number-3
   - Oracle-Database-host-name: monitoring-target-name-4:port-number-4  <-
Add here
  labels:
    jpl_pc_exporter: JPC OracleDB exporter
    jpl_pc_category: database
    jpl_pc_trendname: oracledb_exporter
    jpl_pc_remote_monitor_instance: installation-destination-host-name:OracleDB metric collector(OracleDB exporter)
```

Item	Value to specify
Oracle Database host name	Specify the hostname confirmed in step 4 of <i>Preparing to add a monitoring target</i> in 1.23.1(4)(a) Adding a monitoring target (required) .
Monitoring target name	Specify the monitoring target name determined in step 5 of <i>Preparing to add a monitoring target</i> in 1.23.1(4)(a) Adding a monitoring target (required) .
Port number	Specify the port number determined in step 2 of <i>Preparing to add a monitoring target</i> in 1.23.1(4)(a) Adding a monitoring target (required) .

2. Check the settings with the `promtool` command.

Verify that the settings are correct.

The `promtool` command is located in the *JPI/IM-Agent-installation-destination/jplima/tools* folder.

```
promtool check config jpc_prometheus_server.yml
```

If an error is displayed, review the error.

3. Restart Prometheus.

Restart Prometheus for the changes to take effect.

■ Configuring Intelligent Integrated Management Base

1. Refresh Intelligent Integrated Management Base tree a few minutes after all services have started.

Generate or import tree data from integrated operation viewer, or execute the `jddcreatetree` command or the `jddupdatetree` command to refresh the tree and check the following:

- Oracle Database targets are displayed in Intelligent Integrated Management Base tree.
- The monitoring target can be selected and displayed as a trend.

(b) Changing OracleDB exporter port (optional)

You must change the listen port on Oracle Database exporter and the port number that Prometheus will scrape.

The procedure for changing is as follows.

1. Stopping Prometheus service.

2. Stopping OracleDB exporter service.

3. Change the listen port for OracleDB exporter in the definition-file as shown in the following tables.

- For Windows

Host type	File to be changed
For physical host operation	<i>OracleDB-exporter-location\oracledb_exporter_windows\jplima\bin\oracledb_exporter_instance-name-identifying-the-OracleDB-exporter-service.xml</i>
For logical host operation	<i>OracleDB-exporter-location\oracledb_exporter_windows\jplima\bin\oracledb_exporter_instance-name-identifying-the-OracleDB-exporter-service_logical-host-name.xml</i>

- For Linux

Host type	File to be changed
For physical host operation	<i>/usr/lib/systemd/system/oracledb_exporter_instance-name-identifying-the-OracleDB-exporter-service.service</i>
For logical host operation	<i>/usr/lib/systemd/system/oracledb_exporter_instance-name-identifying-the-OracleDB-exporter-service_logical-host-name.service</i>

4. For Linux, run `systemctl daemon-reload` command.

5. Changes OracleDB exporter port number that scrape Prometheus in the definition-file shown in the following tables.

- For Windows

Host type	File to be changed
For physical host operation	<i>JP1/IM-Manager-installation-folder</i> \JP1IMM\conf\jpc_file_sd_config_oracledb.yml
For logical host operation	<i>Shared-folder</i> \jplimm\conf\jpc_file_sd_config_oracledb.yml

- For Linux

Host type	File to be changed
For physical host operation	/opt/jplima/conf/jpc_file_sd_config_oracledb.yml
For logical host operation	<i>Shared-directory</i> /jplima/conf/jpc_file_sd_config_oracledb.yml

6. Start OracleDB exporter service.

7. Start Prometheus service.

(c) Change the password for connecting (optional)

If you change the password for Oracle Database, you must refresh the password that OracleDB exporter uses to connect.

1. Stop OracleDB exporter.

2. Update the password.

Refresh the password of the user used to connect to Oracle Database with the `jimasecret` command.

- For physical host operation

```
jimasecret -add -key OracleDB.user.user-name -s password
```

- For logical host operation

```
jimasecret -add -key OracleDB.user.user-name -s password -l shared-folder
```

If you want to register users with the same username but different passwords, you can use a key that includes the host name and the service name.

3. Start OracleDB exporter.

(d) Deleting a monitoring target (optional)

■ Configuring Prometheus

1. Remove monitoring targets from OracleDB exporter discovery configuration

file (jpc_file_sd_config_oracledb.yml).

Deletes the monitoring targets listed in the targets of the OracleDB exporter discovery configuration file (jpc_file_sd_config_oracledb.yml).

2. Restart Prometheus.

Restart Prometheus for the changes to take effect.

■ Removing OracleDB exporter from Cluster Software

For logical host operation, remove OracleDB exporter from the cluster software. If necessary, stop the service, etc.

■ Setting up OracleDB exporter

1. Stop OracleDB exporter service for the monitoring target to be deleted.

Stop OracleDB exporter service from the command line or from Windows Service Control Manager.

2. Deregister a service.

Unregister the service by executing the following command.

- For physical host operation

```
oracledb_exporter_instance-name-identifying-the-OracleDB-exporter-  
service_service.exe uninstall
```

- For logical host operation

```
oracledb_exporter_instance-name-identifying-the-OracleDB-exporter-service_logical-host-  
name_service.exe uninstall
```

For logical host operation, execute the command on both nodes that make up the cluster.

3. Deletes the password for the user used to connect to Oracle Database.

If you are not using the same user in another OracleDB exporter, use `jimasecret` command to remove the registered password.

- For physical host operation

```
jimasecret -rm -key OracleDB.user.user-name
```

- For logical host operation

```
jimasecret -rm -key OracleDB.user.user-name -s password -l shared-folder
```

If you register by specifying a key that includes a host name or listener name, specify that key.

4. Delete the service definition file and the Windows servicing program.

Delete the following files in *OracleDB-exporter-location\oracledb_exporter_windows\jplima\bin* folder.

- For physical host operation

```
oracledb_exporter_instance-name-identifying-the-OracleDB-exporter-service_service.xml  
oracledb_exporter_instance-name-identifying-the-OracleDB-exporter-service_service.exe
```

- For logical host operation

```
oracledb_exporter_instance-name-identifying-the-OracleDB-exporter-service_logical-host-  
name_service.xml  
oracledb_exporter_instance-name-identifying-the-OracleDB-exporter-service_logical-host-  
name_service.exe
```

(e) Setting up OracleDB exporter life-and-death monitoring (optional)

Life-and-death monitoring of the OracleDB exporter service can be monitored with the `up` metric on the Prometheus server. The following is an example of how to monitor OracleDB exporter in the alert-definition.


```

groups:
- name: exporter_healthcheck
  rules:
  - alert: jpl_pc_exporter_healthcheck
    expr: up{jpl_pc_remote_monitor_instance=""} == 0 or label_replace(up{jpl_pc_exporter="JPC OracleDB exporter"}, "jpl_pc_nodelabel", "${1}", "jpl_pc_remote_monitor_instance", "^[^:]*:([^:]*)$") == 0 or label_replace(up{jpl_pc_remote_monitor_instance!="", jpl_pc_exporter!="JPC OracleDB exporter"}, "jpl_pc_nodelabel", "${1}", "jpl_pc_remote_monitor_instance", "^[^:]*:([^:]*)$") == 0
    for: 3m
    labels:
      jpl_pc_product_name: "/HITACHI/JP1/JPCCS2"
      jpl_pc_component: "/HITACHI/JP1/JPCCS/CONFINFO"
      jpl_pc_severity: "Error"
      jpl_pc_metricname: "up"
    annotations:
      jpl_pc_firing_description: "Communication to Exporter failed. instance={{ $labels.instance }}"
      jpl_pc_resolved_description: "Communication to Exporter failed. instance={{ $labels.instance }}"

```

(f) Modifying users for connections (optional)

1. Add a new person to Oracle Database.

2. Stop OracleDB exporter.

3. Delete the password of the user before the change.

Use `jimasecret` command to remove the password of the user used to connect to Oracle Database.

- For physical host operation

```
jimasecret -rm -key OracleDB.user.old-user-name
```

- For logical host operation

```
jimasecret -rm -key OracleDB.user.old-user-name -l shared-folder
```

If you want to register users with the same user name but different passwords, use a key that includes the host name and the service name.

4. Register the password of the user after change.

Register the password of the user used to connect to Oracle Database with the `jimasecret` command.

- For physical host operation

```
jimasecret -add -key OracleDB.user.new-user-name -s password
```

- For logical host operation

```
jimasecret -add -key OracleDB.user.new-user-name -s password -l shared-folder
```

If you want to register users with the same username but different passwords, you can use a key that includes the host name and the service name.

5. Modify the environment-variable `DATA_SOURCE_NAME` for the OracleDB exporter specified in the service definition file of OracleDB exporter.

Open the service definition file of OracleDB exporter in a text editor, change the username in the environment variable `DATA_SOURCE_NAME` for the OracleDB exporter to the new username, and save it.

6. Start OracleDB exporter.
7. Deletes the previous person from Oracle Database.
If the old user is not needed, remove the old user from Oracle Database.

(5) Cluster environment

If the JP1/IM - Agent scraping the OracleDB exporter is a logical host operation, the OracleDB exporter must also be a logical host operation.

1.23.2 Setting up Node exporter for AIX

This section describes how to configure Node exporter for AIX, an optional feature of integrated agent host.

(1) Preparing Node exporter for AIX setting

This section describes how to prepare for setting up Node exporter for AIX.

(a) Obtaining the setup archive file

Retrieve the setup archive file to use Node exporter for AIX. The setup archive file is located in JP1/IM - Agent installation folder.

The file names for the setup archive files are as follows.

JP1/IM-Agent-installation-folder/jplima/options/

- *node_exporter_aix_VVRRSS.tar.z* (AIX version)

(b) Setting up JP1/IM - Manager

If JP1/IM - Manager 13-01 or later is newly installed, it does not need to be executed.

Perform the following steps when upgrading from a version earlier than JP1/IM - Manager 13-01.

■ Placing the metrics definition file

If you are upgrading from a version prior to JP1/IM - Manager 13-01 to version 13-01 or later, perform the following steps.

1. Copy metric definition file of the following Node exporter for AIX and rename it to the definition file name of the copy destination.

A model file of metric definition file is generated during the version upgrade.

- For Windows

Source filename: *JP1/IM-Manager-installation-*

folder\jplimm\conf\imdd\plugin\jplpccs\metrics_node_exporter_aix.conf.model

Destination filename: *shared-*

folder\jplimm\conf\imdd\plugin\jplpccs\metrics_node_exporter_aix.conf

- For Linux

Source filename: *JP1/IM-Manager-installation-directory/jplimm/conf/imdd/plugin/*

jplpccs/metrics_node_exporter_aix.conf.model

Destination filename: *shared-directory*\jplimm/conf/imdd/plugin/
jplpccs/metrics_node_exporter_aix.conf

For Linux, set the permissions to 600.

■ Updating IM manager updatable definition file list definition file

For details about updating IM Manager updatable definition file list definition file, see *Updating IM manager updatable definition file list definition file* in [1.23.1\(1\)\(b\) Setting up JP1/IM - Manager](#).

(c) Setting up JP1/IM - Agent

If JP1/IM - Manager 13-01 or later is newly installed, it does not need to be executed.

Perform the following steps when upgrading from a version earlier than JP1/IM - Manager 13-01.

■ Stopping JP1/IM - Agent

Stopping JP1/IM - Agent service.

- For physical hosts

Stop JP1/IM - Agent servicing by running the following command.

```
jpc_service_stop -s all
```

- For logical hosts

Stop from the cluster software.

■ Setting up Node exporter for AIX scrape jobs

Configuration file model file of Prometheus is updated when upgrading. Write the following details of Prometheus configuration file model file (jpc_prometheus_server.yml.model) under scrape_configs of Prometheus configuration file (jpc_prometheus_server.yml).

For logical host operation, update the following files:

- For Windows

shared-folder\jplima\conf\jpc_prometheus_server.yml

- For Linux

shared-directory/jplima/conf/jpc_prometheus_server.yml

```
(Omitted)
:
scrape_configs:
:
- job_name: 'jpc_node_aix'

  file_sd_configs:
  - files:
    - 'jpc_file_sd_config_node_aix.yml'

  relabel_configs:
  - target_label: jpl_pc_nodelabel
    replacement: AIX metric collector(Node exporter for AIX)

  metric_relabel_configs:
  - source_labels: ['__name__']
```

```

    regex: 'node_context_switches|node_cpu|aix_memory_iomu|aix_cpu_wait|
aix_diskpath_wblks|aix_disk_rserv|aix_disk_rblks|aix_disk_wserv|aix_disk_wbl
ks|aix_diskpath_rblks|node_filesystem_avail_bytes|node_filesystem_files_avai
l|node_filesystem_free_bytes|node_filesystem_free_bytes|node_filesystem_size
_bytes|node_intr|node_load1|node_load15|node_load15|aix_netbuffer_inuse|aix_
memory_real_avail|aix_netinterface_mtu|aix_netinterface_oobytes|aix_netinterf
ace_ierrors|aix_netinterface_ipackets|aix_netadapter_tx_bytes|aix_netinterfa
ce_collisions|aix_netadapter_tx_errors|aix_netinterface_opackets|aix_memory_
pgspins|aix_memory_pgspouts'
    action: 'keep'

```

■ Deploying Node exporter for AIX discovery configuration file

1. Copy the model file of the discovery configuration file of the following Node exporter for AIX and rename it to the definition file name of the copy destination.

Model files for the discovery configuration file are generated during version upgrade.

- For Windows

Source filename: *JPI/IM-Agent-installation-*

folder\jplima\conf\jpc_file_sd_config_node_aix.yml.model

Destination filename: *JPI/IM-Agent-installation-*

folder\jplima\conf\jpc_file_sd_config_node_aix.yml

- For Linux

Source filename: *JPI/IM-Agent-installation-directory/jplima/*
conf/jpc_file_sd_config_node_aix.yml.model

Destination filename: *JPI/IM-Agent-installation-directory/jplima/*
conf/jpc_file_sd_config_node_aix.yml

For Linux, set the permissions to 600.

- For Windows

shared-folder\jplima\conf

- For Linux

shared-directory/jplima/conf/

When adding a monitor target setting, see [1.23.2\(4\)\(a\) Adding a monitoring target \(required\)](#).

■ Updating integrated agent updatable definition file list definition file

For details about updating integrated agent updatable definition file list definition file, see *Updating integrated agent updatable definition file list definition file* in [1.23.1\(1\)\(c\) Setting up JPI/IM - Agent](#).

■ Checking the settings

For details on how to check the settings, see *Checking the settings* in [1.23.1\(1\)\(c\) Setting up JPI/IM - Agent](#).

■ Starting JPI/IM - Agent

For details on how to check the settings, see *Checking the settings* in [1.23.1\(1\)\(c\) Setting up JPI/IM - Agent](#).

(2) Installing Node exporter for AIX

This section describes how to install Node exporter for AIX.

(a) Deploying the Node exporter for AIX

Extract `node_exporter_aix_VVRRSS.tar.z` obtained in [1.23.2\(1\)\(a\) Obtaining the setup archive file](#) to any directory on the monitored host (AIX). Do not specify the same directory configuration as JP1/IM - Manager or JP1/IM - Agent installation location in the destination directory.

When operating Node exporter for AIX on a logical host, place it in a shared directory.

(b) Output setting of system log

Set this item if the system log is not output.

Node exporter for AIX log is written to OS system log. Therefore, Node exporter for AIX logging settings are based on OS system logging settings. If you have not configured OS system logs to be printed, add the settings to `/etc/syslog.conf`.

The following shows an example configuration to add.

```
User.info /var/log/syslog.log rotate size 10m files 8
```

After adding the above settings, restart `syslogd` for the settings to take effect.

If you are using `user` for another application to output to the system log, the log is also output.

(c) Enabling service-registration for Node exporter for AIX

For details about enabling service registration for Node exporter for AIX, see [10.4.2\(1\) Enabling registering services](#) in the *JP1/Integrated Management 3 - Manager Administration Guide*.

(d) Node exporter for AIX service registration activation confirmation

For details on checking the activation of the service registration of Node exporter for AIX, see [10.4.2\(4\) Checking the status of services](#) in the *JP1/Integrated Management 3 - Manager Administration Guide*.

(e) Starting Node exporter for AIX

For details on starting Node exporter for AIX service, see [10.4.2\(6\) Starting the Service](#) in the *JP1/Integrated Management 3 - Manager Administration Guide*.

(f) Adding a monitoring target

For details on adding a monitoring target, see [1.23.2\(4\)\(a\) Adding a monitoring target \(required\)](#).

(3) Uninstalling Node exporter for AIX

This section describes how to uninstall Node exporter for AIX.

(a) Deleting a monitoring target host (AIX)

1. Deletes the monitoring target host (AIX)

Remove the monitored hosts (AIX) listed in the (`jpc_file_sd_config_node_aix.yml`) targets.

For details about Node exporter for AIX Discovery configuration file, see *Node exporter for AIX discovery configuration file (`jpc_file_sd_config_node_aix.yml`)* in *Chapter 2. Definition Files* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

When deleting multiple monitored target hosts (AIX), delete multiple monitored target hosts (AIX) listed in targets, restart Prometheus, and then execute [1.23.2\(3\)\(b\) Stopping Node exporter for AIX](#) and later for each of the deleted monitored hosts (AIX).

2. Restart Prometheus.

Restart Prometheus for the changes to take effect.

(b) Stopping Node exporter for AIX

For details on stopping the service of Node exporter for AIX, see [10.4.2\(7\) Stopping the service](#) in the *JP1/Integrated Management 3 - Manager Administration Guide*.

(c) Disabling Auto-Start for a Node exporter for AIX

If you have enabled auto-start of Node exporter for AIX, you must disable it.

For details on disabling auto-start of Node exporter for AIX, see [10.4.2\(10\) Disabling automatic startup](#) in the *JP1/Integrated Management 3 - Manager Administration Guide*.

(d) Disabling Auto-Stop for a Node exporter for AIX

If you have enabled Node exporter for AIX auto-stop, you must disable it.

For details on disabling auto-stop of Node exporter for AIX, see [10.4.2\(12\) Disabling Automatic Stop](#) in the *JP1/Integrated Management 3 - Manager Administration Guide*.

(e) Disabling service registration for Node exporter for AIX

If you have enabled service registration for the Node exporter for AIX, you must disable it.

For details on disabling the registration of Node exporter for AIX services, see [10.4.2\(2\) Disable registering service](#) in the *JP1/Integrated Management 3 - Manager Administration Guide*.

Make sure that Node exporter for AIX service registration is disabled after execution.

(f) Deleting Node exporter for AIX

To delete Node exporter for AIX, delete the directory that were placed in "[1.23.2\(2\)\(a\) Deploying the Node exporter for AIX](#)".

(4) Configuring the Node exporter for AIX

(a) Adding a monitoring target (required)

The procedure for adding a monitoring target is as follows.

■ Configuring Prometheus

1. Add monitoring targets to Node exporter for AIX Discovery configuration file.

Add a new entry under targets in the Node exporter for AIX discovery configuration file (`jpc_file_sd_config_node_aix.yml`).

```
- targets:
  - monitoring-target-host-name-1:port-number-1
  - monitoring-target-host-name-2:port-number-2
  - monitoring-target-host-name-3:port-number-3  <- Add here
```

```
labels:
  jpl_pc_exporter: JPC Node exporter for AIX
  jpl_pc_category: platform
  jpl_pc_trendname: node_exporter_aix
```

Item	Value to specify
Monitoring target host name	Specifies the host name of the monitoring target host (AIX).
Port number	Specifies Node exporter for AIX port number.

2. Checking the settings with the `promtool` command.

Verify that the settings are correct.

The `promtool` command is located in the `JP1/IM-Agent-installation-destination/jplima/tools` folder.

```
promtool check config jpc_prometheus_server.yml
```

If an error is displayed, review the error.

3. Restart Prometheus.

Restart Prometheus for the changes to take effect.

■ Configuring Intelligent Integrated Management Base

1. Refresh Intelligent Integrated Management Base tree a few minutes after all services have started.

Generate or import tree data from integrated operation viewer, or execute the `jddcreatetree` command or the `jddupdatetree` command to refresh the tree and check the following:

- Node exporter for AIX node is displayed in Intelligent Integrated Management Base tree.
- The ability to select and trend Node exporter for AIX nodes.

(b) Changing the port on Node exporter for AIX (optional)

You must change the listen port on Node exporter for AIX and the port number that Prometheus will scrape.

The procedure for changing is as follows.

1. Stopping Prometheus service.
2. Stopping Node exporter for AIX service.
3. Change the listen port for Node exporter for AIX registered to the service listed in the following tables.

OS	Host type	File to be changed
AIX	For physical host operation	Services with subsystem named "jpc_node_exporter_aix"
	For logical host operation	Services with subsystem named "jpc_node_exporter_aix_logical-host-name"

For details on changing the registration of a service, see *10.4.2(3) Registering the service changed* in the *JP1/Integrated Management 3 - Manager Administration Guide*.

4. Changes Node exporter for AIX port number that scrape Prometheus in the definition-file shown in the following tables.

OS	Host type	File to be changed
Windows	For physical host operation	<i>JPI/IM-Agent-installation-folder</i> \jplima\conf\jpc_file_sd_config_node_aix.yml
	For logical host operation	<i>JPI/IM-Agent-shared-folder</i> \jplima\conf\jpc_file_sd_config_node_aix.yml
Linux	For physical host operation	/opt/jplima/conf/jpc_file_sd_config_node_aix.yml
	For logical host operation	<i>JPI/IM-Agent-shared-directory</i> /jplima/conf/jpc_file_sd_config_node_aix.yml

5. Start Node exporter for AIX.

6. Start Prometheus service.

7. Perform the settings in steps 1 to 6 and wait a few minutes after all services have started.

8. Refresh IM management node tree.

Follow steps 2 to 5 in [1.19.3\(1\)\(c\) Creation and import of IM management node tree data \(for Windows\) \(required\)](#).

(c) Modify metric to collect (optional)

1. Add metric to Prometheus configuration file (jpc_prometheus_server.yml).

Modify the metrics listed in the metric_relabel_configs of the Prometheus configuration file (jpc_prometheus_server.yml).

For Prometheus configuration file editing procedure, see [1.21.2\(1\)\(a\) Edit the configuration files \(for Windows\)](#).

Note that the supported metric is set to be collected by default.

```
- job_name: 'jpc_node_aix'
  :
  metric_relabel_configs:
    - source_labels: ['__name__']
      regex: 'node_context_switches|node_cpu|aix_memory_iomu|aix_cpu_wait|aix_diskpath_wblks|aix_disk_rserv|aix_disk_rblks|aix_disk_wserv|.....|aix_netinterface_opackets|aix_memory_pgspins|aix_memory_pgspouts (Add here)'
      action: 'keep'
```

2. Define trend display in metric definition file

Optionally, define a metric in metric definition-file that you want to view in integrated operation viewer trend view. The primary metric is initially configured.

(d) Configuring Node exporter for AIX life-and-death monitoring (optional)

Node exporter for AIX processes are monitored by up metric of Prometheus server.

For details on how to configure monitoring with Prometheus server's up metric, see [1.21.2\(18\)\(c\) Monitoring with Prometheus server up metric](#).

(e) Monitoring processes on monitoring hosts (AIX) (optional)

Monitor the processes on the monitoring hosts (AIX) using the following script-results in Script exporter:

- Script that connects SSH to the monitored host (AIX) and executes ps command on the monitored host (AIX)

The following are configuration steps and examples of specific scripts and definition files.

In the following example, integrated operation viewer's tree chart format creates a node with the process name under Platform category node of AIX's host node and displays a graphical representation of only metric with the Process Status. Script exporter metrics other than Process Status, are graphically displayed on the "*monitoring-target-host-name(AIX):aix_process*" node under Other Applications category node of the agent host node on which Script exporter is installed, and Process Status metric is not graphically displayed.

1. Create a script that connects SSH to the monitored host (AIX) and executes ps command on the monitored host (AIX).

Create a script that connects to the monitoring host (AIX) with ssh command and executes ps command on the monitoring host (AIX). If you want to monitor multiple processes, create one script for each process you want to monitor.

It is necessary to enable SSH connection from the integrated agent host to the monitored host (AIX) in advance. You must also be able to connect SSH to anyone who runs the following scripts:

Environments under which Script exporter runs	User running the script
Windows	Users who run Script exporter services. (Local system account)
Linux	root

- When Script exporter runs in Windows

Create the following batch and text files:

- Batch file

```
@echo off
setlocal

rem Name of the process to be monitored on rem monitored host (AIX) (speci
fy with a space separator if you specify more than one)
set PROCESS=node_exporter_aix logger

rem Users who ssh connect to the monitoring target host (AIX)
set USER=user1

rem Private key file path in PuTTY format used to connect ssh to rem monit
ored host (AIX)
Set PUTTY_ID_RSA="C:\tmp\ScriptExporter\id_rsa.ppk"

rem Host name of the monitoring target host (AIX)
set AIX_HOST=aixhost1

rem ps command result output destination file (specify any location)
set FILE1="C:\tmp\ScriptExporter\ps.txt"

rem A file that outputs the contents to be read by the Script exporter (sp
ecify any location)
set FILE2="C:\tmp\ScriptExporter\ps_for_exporter.txt"
```

```

rem Specify rem plink.exe filepath
Set PLINK_EXE="C:\Program Files\PuTTY\plink.exe"

rem Specifies the text file path for rem (b)
Set CMD_LIST="C:\tmp\ScriptExporter\command.txt"

rem Destination file for plink.exe stderr (any location)
set LOG_FILE="C:\tmp\ScriptExporter\ssh_log.txt"

echo enter | %PLINK_EXE% %USER%%AIX_HOST% -i %PUTTY_ID_RSA% -m %CMD_LIST
% > %FILE1% 2>%LOG_FILE%

rem Output metrics
(echo # HELP script_aix_process AIX process status.&echo # TYPE script_aix
_process gauge)> %FILE2%

for %%i in (%PROCESS%) do call:findpsinfo %%i

type %FILE2%
endlocal
exit /b

:findpsinfo
for /f "tokens=1-3* usebackq" %%i in (`findstr %1 %FILE1%`) do (
    set PNAME=%1
    set STATE=%%j
    call:putinfo
    exit /b
)
set PNAME=%1
set STATE=
call:putinfo
exit /b

:putinfo
if "%STATE%"=="A" (
    echo script_aix_process{host="%AIX_HOST%",process="%PNAME%",state="A"}
1 >> %FILE2%
) else (
    echo script_aix_process{host="%AIX_HOST%",process="%PNAME%",state="A"}
0 >> %FILE2%
)
exit /b

```

-Text file

```
/usr/bin/ps -A -X -o comm,st,etime
```

- When Script exporter runs in Linux

Create the following shell script.

```

#!/bin/sh

# Process-name to be monitored on the monitored host (AIX) (specified by
a space separator if more than one is specified)
PROCESS=("node_exporter_aix" "logger")

# Private key file used to connect ssh to the monitoring target host (AIX)

```

```

ID_RSA=/temp/script_exporter/id_rsa

# Users ssh connecting to monitoring target host (AIX)
USER=guest

# Hostname of the monitoring target host (AIX)
AIX_HOST=aixhsot1

# ps command result output destination file (specify any location)
FILE1=/temp/script_exporter/ps.txt

#A file that outputs the contents to be read by the Script exporter (specify any location)
FILE2=/temp/script_exporter/ps_for_exporter.txt

# Destination file for ssh stderr (any location)
LOG_FILE=/temp/script_exporter/ssh_log.txt

/usr/bin/ssh -i $ID_RSA $USER@$AIX_HOST /usr/bin/ps -A -X -o comm,st,etime >$FILE1 2>$LOG_FILE

echo '# HELP script_aix_process AIX process status.'>$FILE2
echo '# TYPE script_aix_process gauge'>>$FILE2

for target in "${PROCESS[@]}" ; do
    psinfo=`grep -ml "$target" $FILE1`
    find_flag=$?
    if [ $find_flag = 0 ]; then
        psinfo=($psinfo)
        if [ "${psinfo[1]}" = "A" ]; then
            echo "script_aix_process{host=\"$AIX_HOST\",process=\"$target\",state=\"A\"} 1">>$FILE2
        else
            echo "script_aix_process{host=\"$AIX_HOST\",process=\"$target\",state=\"A\"} 0">>$FILE2
        fi
    else
        echo "script_aix_process{host=\"$AIX_HOST\",process=\"$target\",state=\"A\"} 0">>$FILE2
    fi
done

cat $FILE2

```

2. Editing Script exporter configuration file and Prometheus configuration file.

Edit the Script exporter configuration file and the Prometheus configuration file as follows.

For configuration file editing procedure, see [1.21.2\(1\)\(a\) Edit the configuration files \(for Windows\)](#).

- Editing Script exporter configuration file

Change the following:

```

scripts:
  - name: monitoring-target-host-name (AIX) :aix_process
    command: file-path-of-the-script-created-in-step-1
    timeout:
      max_timeout: 30
      enforced: true

```

- Editing Prometheus configuration file

Change the metric_relabel_configs of Script exporter as follows:

```
- job_name: 'jpc_script_exporter'
  :
  metric_relabel_configs:
    - source_labels: ['__name__']
      regex: 'script_success|script_duration_seconds|script_exit_code|script_aix_process'
      action: 'keep'
    - source_labels: [jpl_pc_script]
      target_label: jpl_pc_nodelabel
    - source_labels: ['__name__']
      target_label: jpl_pc_category
      regex: 'script_aix_process'
      replacement: platform
    - source_labels: ['__name__', 'process']
      regex: 'script_aix_process.*;(.*)'
      target_label: jpl_pc_nodelabel
      replacement: ${1}
    - source_labels: ['__name__', 'host']
      regex: 'script_aix_process.*;(.*)'
      target_label: instance
      replacement: ${1}
    - regex: (jpl_pc_script|jpl_pc_multiple_node|jpl_pc_agent_create_flag)
      action: labeldrop
```

3. Editing alert configuration file.

For an alert definition that alerts you when a monitoring target process stops, edit alert configuration file as follows.

For details on how to edit alert configuration file, see [1.21.2\(1\)\(a\) Edit the configuration files \(for Windows\)](#).

```
groups:
- name: script_exporter
  rules:
    - alert: process_state(Script exporter)
      expr: script_aix_process{state="A"} == 0
      for: 3m
      labels:
        jpl_pc_product_name: "/HITACHI/JP1/JPCCS2"
        jpl_pc_component: "/HITACHI/JP1/JPCCS/CONFINFO"
        jpl_pc_severity: "Error"
        jpl_pc_eventid: "1404"
        jpl_pc_metricname: "script_aix_process"
      annotations:
        jpl_pc_firing_description: "The status of the process is not running."
        jpl_pc_resolved_description: "The status of the process is now running."
```

4. Create and import tree information for IM management nodes.

Perform steps 1 to 3 and perform steps 2 to 5 in [1.19.3\(1\)\(c\) Creation and import of IM management node tree data \(for Windows\) \(required\)](#).

5. Editing Script exporter metric definition file.

Editing Script exporter metric definition file as follows.

For details on how to edit Script exporter metric definition file, see *To edit the configuration files (for Windows)* in *1.19.3(1)(a) Common way to setup*.

```
[
  :
  {
    "name": "script_exit_code",
    :
  },
  {
    "name": "script_aix_process",
    "default": true,
    "promql": "script_aix_process{state=\"A\"} and $jplim_TrendData_labels",
    "resource_en": {
      "category": "script_aix_process",
      "label": "Process status",
      "description": "Status of processes on AIX hosts.",
      "unit": "-"
    },
    "resource_ja": {
      "category": "script_aix_process",
      "label": "Processing status",
      "description": "The state of the process on the AIX host.",
      "unit": "-"
    }
  }
]
```

The monitored hosts (AIX) listed above have been tested with the following OS and packaging:

- OS
AIX7.2 TL3 SP2
- Package
Openssh.base.client 7.5.102.1500
Openssh.base.server 7.5.102.1500
Openssh.man.en_US 7.5.102.1500
Openssh.msg.en_US 7.5.102.1500

(f) Changing the log destination of Node exporter for AIX (optional)

Node exporter for AIX log is written to OS system log. To change Node exporter for AIX logging destination, use `syslogd` settings and `logger` command I will.

The following shows an example in which `local1.info` is specified in `-p` of `logger` command, the log output destination of the system log is set to `/var/log/jpc_node_exporter_aix/jpc_node_exporter_aix.log`, and the log size is changed to 8 10MB, log sectors. #

#

If you are using `local1` for other products to output to the system log, the output destination of the log is also changed. Note that the `jpc_stop_node_exporter_aix` command log destination is not changed.

1. Add the following to `/etc/syslog.conf`:

```
local1.info /var/log/jpc_node_exporter_aix/jpc_node_exporter_aix.log rotate size 10m files 8
```

2. Create a directory and file for the log output destination.

3. Restart `syslogd`.

4. Stop Node exporter for AIX.

5. Change the registration of a service.

Run the following command.

- For physical host operation

```
chssys -p /bin/sh -s jpc_node_exporter_aix -u root -S -f 9 -n 15
-a "-c \"'Node-exporter-for-AIX-installation-directory/jplima/bin/node_exporter_aix' -CcADmdiabf -p 20730 2>&1 | logger -p local1.info\""
```

- For logical host operation

```
chssys -p /bin/sh -s jpc_node_exporter_aix_logical host name -u root
-S -f 9 -n 15 -a "-c \"'Node-exporter-for-AIX-installation-directory/jplima/bin/
node_exporter_aix' -CcADmdiabf -p 20730 2>&1 | logger -p local1.info\""
```

6. Start Node exporter for AIX.

1.23.3 Configuring SAP system monitoring

This section explains how to set the SAP system log extract command, which is an optional integrated agent host function for SAP system monitoring.

The following describes how to set SAP system monitoring function other than the SAP system log extract command.

Function		Setting procedure
Script execution function (Script exporter)		To use this function, perform the setting steps described in the following sections after you have set up the SAP system log extract command. • 1.21.2(3)(h) Setting for executing the SAP system log extract command using Script exporter (for Windows) (optional) • 1.21.2(12)(d) Setting when executing SAP system log extract command (optional)
SAP system log extract command (jr3slget, jr3alget)		Follow the configuration procedures in this section.
Script execution result monitoring function		
	Script execution result monitoring function (Fluentd)	To use this function, perform the setting steps described in the following sections after you have set up the SAP system log extract command. • (j) Monitoring SAP system logging (optional) to (o) Remove SAP system CCMS alert information monitoring settings (optional) in 1.21.2(9) Setup of Fluentd
	Script execution result monitoring function (JP1/Base)	If you want to use this feature, see the description about JP1/Base log file traps in the <i>JP1/Base User's Guide</i> .
Metric transmission function		
	Metric output function (Script exporter)	This function can be used by executing the script execution function (Script exporter) setting procedure.

Function	Setting procedure
Metric output function (Fluentd)	This function can be used by executing the script execution function (Fluentd) setting procedure.

(1) Preparing for configuring SAP system monitoring

This section describes how to prepare for configuring SAP system monitoring.

(a) Obtaining setup archive files

Retrieve archived files for using SAP system monitoring. The archived files are located in JP1/IM - Agent installation folder.

The file names for the setup archive files are as follows:

JP1/IM-Agent-installation-destination/jplima/options/

- *sap_windows_VVRRSS.zip* (Windows version)
- *sap_linux_VVRRSS.tar.gz* (Linux version)

(b) Setting up SAP system log extract commands

The included SAP system log extract commands can be used only when JP1/PFM - Agent for EAP and JP1/IM - Agent do not coexist. For the procedure in an environment in which JP1/PFM - Agent for EAP and JP1/IM - Agent coexist, see [1.23.3\(1\)\(d\) Steps to build in an environment where JP1/IM - Agent and JP1/PFM - Agent for EAP coexist](#).

■ Installing the SAP system log extract command

- For Windows

1. Registers the registry used by the command.

Execute the following command at the command prompt.

```
reg add
"HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Hitachi\JP1PC\InstalledProduct"
/v "JP1PCAGTM" /t "REG_SZ" /d "1200"
reg add
"HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Hitachi\JP1PCAGTM\1200\PathName"
/v "Path00#" /t "REG_SZ" /d "C:\Program Files (x86)\Hitachi\jplpc"
#
```

The location of the command.

2. Place the unzipped agtm folder.

Extracting the *sap_windows_VVRRSS.zip* to *JP1/IM-Agent-installation-folder\jplima\options* generates a *sap_windows* folder,

Place *agtm* folder under *sap_windows\command* directly under the folder (where the command is placed) with the path set to *Path00*. If you executed the command in step 1, place it in the following path:

C:\Program Files (x86)\Hitachi\jplpc\tar

If the destination path of *agtm* folder does not exist, create a new destination folder.

- For Linux

1. Place the decompressed *agtm* directory.

Extracting the `sap_linux_VVRRSS.tar.gz` to `JP1/IM-Agent-installation-directory/jplima/options` generates a `sap_linux` directory, generates a `sap_linux` directory.

Place `agtm` directory under the `sap_linux/command` under the following directory.

`/opt/jplpc/`

If the destination path of `agtm` directory does not exist, create a new destination directory with the following owners and privileges:

Owner: root

Privileges: 755

■ Obtaining RFC libraries

For instructions on obtaining and deploying RFC library, see the *Release Notes* for JP1/IM - Agent as well.

1. Obtain SAP NW RFC SDK 7.50 from SAP Software Download Center.

- For Windows
SAP NW RFC SDK 7.50 (Windows on x64 64bit) (patch level 0 or higher)
- For Linux
SAP NW RFC SDK 7.50 (Linux on 64bit) (patch level 0 or higher)

2. Unzip the obtained compressed file according to SAP instructions.

The extracted folder has the following structure.

```
nwrfsdk
+ bin      : Executable sample programs
+ demo     : C source file of the sample program
+ include  : C header file
+ lib      : Shared libraries
```

The files required for the operation of SAP system log extract commands are stored in `lib` folders.

3. Store all files under the extracted "lib" folder in the following folder.

- For Windows
Where-the-command-is-placed[#]\agtm\lib\rfc
#: Location of the command specified in *Installing the SAP system log extract command* under [1.23.3\(1\)\(b\) Setting up SAP system log extract commands](#).
- For Linux
`/opt/jplpc/agtm/lib/rfc/`

If the above path does not have the same rights as the installation folder, grant the rights.

■ Obtaining CRT library (for Windows only)

Obtain and apply CRT libraries required for the operation of RFC library. You can find the required CRT library version in SAP Note 2573790.

■ Set Up the environment parameters file (optional)

1. Create the environmental parameters file.

Copy sample file (`jr3slget.ini.sample`, `jr3alget.ini.sample`) of the configuration parameter configuration file and change the file name of the copy destination to "any name.ini".

For the location of configuration file configuration parameter, see *Appendix A.4 (3) Integrated agent host (Windows)* and *Appendix A.4 (4) Integrated agent host (Linux)* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

For details about the settings of the environment parameters file, see *Environment parameters file for jr3slget command (jr3slget.ini)* and *Environment parameters file for jr3alget command (jr3alget.ini)* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference (2. Definition Files)*.

For details about sample file of environment parameters file, see *Sample file of environment parameters file for jr3slget command (jr3slget.ini.sample)* and *Sample file of environment parameters file for jr3alget command (jr3alget.ini.sample)* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference (2. Definition Files)*.

2. Creates a working directory for SAP system log extract command.

After editing the environment parameter configuration file, create a working directory for the SAP system log extract command. Create a directory of the path set in WORKDIR label of the environment parameter configuration file.

For a Linux, create it with the following owners and privileges:

Owner: root

Privilege: 777

(c) Uninstalling for SAP system log extract command

1. Stop the script execution result monitoring.

If the log data of the SAP system log extract command is being monitored using the script execution result monitoring function (Fluentd or JP1/Base), monitoring is stopped.

2. Stop script execution.

If the SAP system log extract command is executed using the script execution function (Script exporter) of SAP system monitoring or cron, the command execution is stopped.

3. Deletes the registry used by the command. (For Windows only)

Run the following commands at the command prompt.

```
reg delete "HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Hitachi\JP1PC\InstalledProduct" /v "JP1PCAGTM"
reg delete "HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Hitachi\JP1PCAGTM\1200\PathName" /v "Path00"
```

4. Deletes SAP system log extract command's working directory.

If you created a directory for the path specified in WORKDIR label of the environment parameters file in *Set Up the environment parameters file (optional)* under *1.23.3(1)(b) Setting up SAP system log extract commands*, delete the created directory.

5. Deletes the directory where SAP system log extract command is located.

Delete the following folders and subordinate files.

- For Windows

Where-the-command-is-placed[#]\agtm

[#]: Location of the command specified in *Installing the SAP system log extract command* under *1.23.3(1)(b) Setting up SAP system log extract commands*.

- For Linux

/opt/jp1pc/agtm

(d) Steps to build in an environment where JP1/IM - Agent and JP1/PFM - Agent for EAP coexist

■ Install a new JP1/IM - Agent from scratch in an environment where JP1/PFM - Agent for EAP is already installed

If JP1/IM - Agent and JP1/PFM - Agent for EAP coexist, you cannot use the SAP system log extract command that ships with JP1/IM - Agent.

■ Install a new JP1/PFM - Agent for EAP from scratch in an environment where JP1/IM - Agent is already installed

If the SAP system log extract command has already been set up

The SAP system log extract commands included with JP1/IM - Agent is not available and must be deleted.

1. Back up the SAP system log extract commands and definition file of SAP system bundled with JP1/IM - Agent.
Copy the destination folder specified in the installation command to get SAP system information and the files under it, and back it up to any folder.
2. Uninstall the SAP system log extract command.
For details about how to do this, see [1.23.3\(1\)\(c\) Uninstalling for SAP system log extract command](#).
3. Install and set up JP1/PFM - Agent for EAP.

When the SAP system log extract command has not been set up

You do not have to do it in advance.

■ Upgrading and installing JP1/PFM - Agent for EAP in an environment where JP1/IM - Agent and JP1/PFM - Agent for EAP coexist.

In this environment, you cannot use the SAP system log extract command that ships with JP1/IM - Agent, so there are no required steps.

■ Upgrading and installing JP1/IM - Agent in an environment where JP1/IM - Agent and JP1/PFM - Agent for EAP coexist.

In this environment, you cannot use the SAP system log extract command that ships with JP1/IM - Agent, so there are no required steps.

■ Uninstalling JP1/PFM - Agent for Enterprise Applications in an environment where JP1/IM - Agent and JP1/PFM - Agent for EAP coexist.

Back up the environment parameters files to use `jr3slget` and `jr3alget` commands that you created during JP1/PFM - Agent for EAP operation.

When using the SAP system log extract command bundled with JP1/IM - Agent, you can refer to the parameter of the environment parameters file of the backed up JP1/PFM - Agent for EAP as a reference.

■ Uninstalling JP1/IM - Agent in an environment where JP1/IM - Agent and JP1/PFM - Agent for EAP coexist.

In this environment, you cannot use the SAP system log extract command that ships with JP1/IM-Agent, so there are no required steps.

1.23.4 Configuring SQL exporter

This section describes how to configure SQL exporter, an optional feature of integrated agent host.

(1) Preparing for SQL exporter Configuration

This section describes how to prepare for setting up SQL exporter.

(a) Setting up JP1/IM - Manager

If JP1/IM - Manager 13-11 or later is newly installed, it does not need to be executed.

If you upgraded from a version earlier than JP1/IM - Manager 13-11, perform the following steps:

(b) Obtaining setup archive files

Retrieve the setup archive file to use SQL exporter. The setup archive file is located in the folder where JP1/IM - Agent is installed.

The file names for the setup archive files are as follows:

JP1/IM-Agent-installation-destination/jplima/options/

- *sql_exporter_windows_VVRRSS.zip*

■ Placing metric definition files

Perform the following steps when upgrading from a version earlier than JP1/IM - Manager 13-11 in logical host operation.

1. Copy the model file of metric definition file of the following SQL exporter and rename it to the definition file name of the copy destination.

Source filename: *JP1/IM-Manager-installation-*

folder\jplimm\conf\imdd\plugin\jplpccs\metrics_sql_exporter.conf.model

Destination filename: *JP1/IM-Manager-installation-*

folder\jplimm\conf\imdd\plugin\jplpccs\metrics_sql_exporter.conf

For logical host operation, place this file in the following location:

shared-folder\jplimm\conf\imdd\plugin\jplpccs

(c) Setting up JP1/IM - Agent

This step is not required if you are installing JP1/IM - Agent 13-11 or later.

If you upgraded from a version earlier than JP1/IM - Agent 13-11, perform the following steps:

Note that you do not need to install Microsoft SQL Server modules on JP1/IM - Agent hosts.

■ Stopping JP1/IM - Agent

Stop JP1/IM - Agent service.

- For physical hosts

Stop JP1/IM - Agent servicing by running the following command.

```
jpc_service_stop -s all
```

- For logical hosts
Stop from the cluster software.

■ Setting up SQL exporter scrape jobs

The model file of the Prometheus configuration file is updated when the version is upgraded. Write the following details of Prometheus configuration file model file (jpc_prometheus_server.yml.model) under scrape_configs of Prometheus configuration file (jpc_prometheus_server.yml).

For logical host operation, update the following files:

shared-folder\jpl1ma\conf\jpc_prometheus_server.yml

```
(Omitted)
:
scrape_configs:
:
- job_name: 'jpc_sql'
  scrape_interval: 60s
  scrape_timeout: 30s

  metrics_path: /metrics

  file_sd_configs:
  - files:
    - 'jpc_file_sd_config_mssql.yml'

  relabel_configs:
  - target_label: jpl_pc_nodelabel
    replacement: MSSQL metric collector(SQL exporter)

  metric_relabel_configs:
  - source_labels: ['__name__']
    regex: 'mssql_local_time_seconds|mssql_connections|mssql_deadlocks|mssql_user_errors|mssql_kill_connection_errors|mssql_page_life_expectancy_seconds|mssql_batch_requests|mssql_log_growths|mssql_buffer_cache_hit_ratio|mssql_checkpoint_pages_sec|mssql_io_stall_seconds|mssql_io_stall_total_seconds|mssql_resident_memory_bytes|mssql_virtual_memory_bytes|mssql_memory_utilization_percentage|mssql_page_fault_count|mssql_os_memory|mssql_os_page_file|mssql_database_detail_process_count|mssql_global_server_summary_perc_busy|mssql_global_server_summary_packet_errors|mssql_server_detail_blocked_processes|mssql_server_overview_cache_hit|mssql_transaction_log_overview_log_space_used'
    action: 'keep'
  - source_labels: [exported_job]
    target_label: instance
    replacement: ${1}
  - source_labels: [target]
    target_label: jpl_pc_nodelabel
    replacement: ${1}
```

■ Deploying SQL exporter discovery configuration file

1. Copy the model file of the definition file that defines the monitoring target of the following SQL exporter, and rename it to the definition file name of the copy destination.

Source filename: *JP1/IM - Agent*

installation folder\jplima\conf\jpc_file_sd_config_mssql.yml.model

Destination filename: *JP1/IM - Agent*

installation folder\jplima\conf\jpc_file_sd_config_oracledb.yml

For logical host operation, place this file in the following location:

shared-folder\jplima\conf

2. Open the `jpc_file_sd_config_oracledb.yml` file created in step 1 in a text editor, edit it as follows, and overwrite it.

```
- targets:
#-@@hostname@@#:SQL-exporter's-port-number
  labels:
    jpl_pc_exporter: JPC SQL exporter
    jpl_pc_category: database
    jpl_pc_trendname: sql_exporter
    jpl_pc_remote_monitor_instance: @@hostname@@:MSSQL metric collector(SQL
    exporter)
    jpl_pc_multiple_node: "{__name__=~'mssql_.*'}"
```

#

Specify the host name of JP1/IM - Agent (or logical host name for logical host operation).

■ Checking the settings

Prometheus server definition file is checked because the format can be checked by the `promtool` command.

The `promtool` command is stored in under *JP1/IM-Agent-installation-destination/jplima/tools*.

```
promtool check config jpc_prometheus_server.yml
```

If an error is displayed, review the error.

Note that there is no problem even if the following warning is displayed.

```
WARNING: file "../conf/jpc_file_sd_config_windows.yml" for file_sd in scrap
e job "jpc_windows" does not exist
```

■ Starting JP1/IM - Agent

Start JP1/IM - Agent servicing.

- For physical hosts

Run the following command to start JP1/IM - Agent services.

```
jpc_service_start -s all
```

- For logical hosts

Start from the cluster software.

(2) Installing SQL exporter

This section describes how to install SQL exporter.

(a) Preparing for Installation

1. Confirm the setting of JP1IMADIR.

You must set JP1IMADIR in service definition file for SQL exporter. Depending on the type of host in the JP1/IM - Agent, the following values will occur.

Host type	Environment variable JP1IMADIR
For physical host operation	<i>JP1/IM-Agent-installation-folder\jplima</i>
For logical host operation	<i>shared-folder\jplima</i>

2. Confirm whether to operate on a physical host or a logical host.

SQL exporter is also a physical host operation if scrape of the newly added JP1/IM - Agent is a physical host operation.

SQL exporter is also logical host operation if scrape of the newly added JP1/IM - Agent is logical host operation.

(b) Installing SQL exporter

1. Place SQL exporter.

Extract the setup archive file[#] obtained in [1.23.4\(1\)\(b\) Obtaining setup archive files](#) to a folder of your choice. Do not specify the folder where JP1/IM - Manager or JP1/IM - Agent will be installed in the destination folder.

#

`sql_exporter_windows_VVRRSS.zip`

To operate SQL exporter on a logical host, place it in shared-folder.

2. Create a defaulted metric definition-file.

Copies the model file of the following default metric definition file and renames it to the definition file name of the copy destination.

Source filename: *SQL exporter*

location\sql_exporter_windows\jplima\conf\mssql_standard.collector.yml.model

Destination filename: *SQL*

exporter location\sql_exporter_windows\jplima\conf\mssql_standard.collector.yml

3. Updating service definition file.

Verify that the following files exist:

SQL exporter location\sql_exporter_windows\jplima\bin\sql_exporter_service.exe

SQL

exporter location\sql_exporter_windows\jplima\bin\sql_exporter_service.xml.model

Modify the following service definition file settings:

Value to be changed	Value to specify
<code>@@sql_exporter_installdir@@</code>	Replace with SQL exporter location.
<code>@@autostart@@</code>	- To start automatically at OS startup Replace with "Automatic". - To not start automatically Replace with "Manual". For logical hosts, substitute "Manual".

4. Register the service.

Run the following command to register SQL exporter service with Windows:

- For physical host operation
`sql_exporter_service.exe install`
- For logical host operation
`sql_exporter_logical-host-name_service.exe install`
For logical host operation, execute the command on both nodes that make up the cluster.

5. Set the monitoring target in SQL exporter configuration file.

The target of SQL exporter is listed in SQL exporter configuration file (`jpc_sql_exporter.yml`).

For details about SQL exporter configuration file, see *SQL exporter configuration file (jpc_sql_exporter)* in *Chapter 2. Definition Files* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

6. Add a target.

For details on adding a target, see *1.23.4(4)(a) Adding monitoring targets (required)*.

7. Register the service with the cluster software.

For a cluster configuration, register the service with the cluster software.

(c) Configuring Prometheus

1. Configure monitoring targets for SQL exporter discovery configuration file.

SQL exporter targets are listed in SQL exporter Discovery configuration file (`jpc_file_sd_config_mssql`) targets.

For details about SQL exporter discovery configuration file, see *SQL exporter discovery configuration file (jpc_file_sd_config_mssql)* in *Chapter 2. Definition Files* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

2. Checking the settings with promtool command.

Verify that the settings are correct.

`promtool` command is located in *JP1/IM-Agent-installation-folder\jplima\tools* folder.

```
promtool check config jpc_prometheus_server.yml
```

If an error is displayed, review the error.

Note that there is no problem even if the following warning is displayed.

```
WARNING: file "../conf/jpc_file_sd_config_windows.yml" for file_sd in scrape job "jpc_windows" does not exist
```

3. Restart Prometheus.

Restart Prometheus for the changes to take effect.

(3) Uninstalling SQL exporter

1. Deletes SQL exporter.

To remove SQL exporter, delete the folders you placed in *1.23.4(2)(b) Installing SQL exporter*.

(4) Configuring SQL exporter

This section explains how to set SQL exporter.

(a) Adding monitoring targets (required)

■ Preparing to add a target

1. Set the monitoring target in SQL exporter configuration file.

The target of SQL exporter is listed in SQL exporter configuration file (`jpc_sql_exporter`) (`.yaml`).

For details about SQL exporter configuration file, see *SQL exporter configuration file (jpc_sql_exporter)* in Chapter 2. *Definition Files* in the *JPI/Integrated Management 3 - Manager Command, Definition File and API Reference*.

2. Verify that Microsoft SQL Server you are monitoring has the required permissions assigned to you.

For details about the privileges required, see "Prerequisites for monitoring Microsoft SQL Server in 3.15.1(1)(q) *SQL exporter (Microsoft SQL Server monitoring function)* in the *JPI/Integrated Management 3 - Manager Overview and System Design Guide*.

■ Configuring SQL exporter

1. Shut down SQL exporter servicing.

2. Register the password of the user used to connect to Microsoft SQL Server.

Use `jimasecret` command. Register the password of the user used to connect to Microsoft SQL Server.

- For physical host operation

```
jimasecret-add-key MSSQL.hostname.instance-name.username -s password
```

- For logical host operation

```
jimasecret-add-key MSSQL.hostname.instance-name.username -s password -l shared-folder
```

For details about `jimasecret` command, see `jimasecret` in Chapter 1. *Commands* in the *JPI/Integrated Management 3 - Manager Command, Definition File and API Reference*.

3. Start SQL exporter servicing.

Start SQL exporter service from Windows management tools service window, etc.

For a cluster configuration, start the service from the cluster software.

4. Confirm that SQL exporter can acquire the performance data.

The following URL can be accessed by using `curl` commands/browsers to check whether performance data can be obtained.

```
Http://hostname:20735/metrics
```

■ The hostname specifies the host on which SQL exporter is running. Configuring Intelligent Integrated Management Base

1. Refresh Intelligent Integrated Management Base tree a few minutes after all services have started.

Generate or import tree data from integrated operation viewer, or execute `jddcreatetree` command or `jddupdatetree` command to refresh the tree and check the following:

- Microsoft SQL Server targets are displayed in Intelligent Integrated Management Base tree.
- The monitoring target can be selected and displayed as a trend.

(b) Change password for connection (optional)

If you change the password for Microsoft SQL Server during operation, you must refresh the password that SQL exporter uses to connect.

1. Shut down SQL exporter.

2. Update the password.

Use `jimasecret` command to refresh the password of the user used to connect to Microsoft SQL Server.

- For physical host operation

```
jimasecret-add-key MSSQL.hostname.instance-name.username -s password
```

- For logical host operation

```
jimasecret-add-key MSSQL.hostname.instance-name.username -s password -l shared-folder
```

For details about `jimasecret` command, see `jimasecret` in *Chapter 1. Commands* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

3. Start SQL exporter.

(c) Delete a monitored target (optional)

■ Configuring SQL exporter

- To delete some monitoring targets

1. Shut down SQL exporter.

2. Delete a password.

Use `jimasecret` command to remove the password of the user used to connect to Microsoft SQL Server.

- For physical host operation

```
jimasecret-rm-key MSSQL.hostname.instance-name.username
```

- For logical host operation

```
jimasecret-rm-key MSSQL.hostname.instance-name.username -l shared-folder
```

For details about `jimasecret` command, see `jimasecret` in *Chapter 1. Commands* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

3. Deletes the monitored connectivity from SQL exporter configuration file.

Removes SQL exporter monitored connectivity from SQL exporter configuration file (`jpc_sql_exporter`).

For details about SQL exporter configuration file, see *SQL exporter configuration file (jpc_sql_exporter)* in *Chapter 2. Definition Files* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

4. Start SQL exporter.

- To delete all monitoring targets

1. Shut down SQL exporter.

2. Deregister a service.

Unregister the service by executing the following command.

- For physical host operation

```
sql_exporter_service.exe uninstall
```

- For logical host operation

```
sql_exporter_logical-hostname_service.exe uninstall
```

In the case of logical host operation, it must be executed on both nodes of the cluster.

3. Deletes the password for the user used to connect to Microsoft SQL Server.

- For physical host operation

```
jimasecret-rm-key MSSQL.hostname.instance-name.username
```

- For logical host operation

```
jimasecret-rm-key MSSQL.hostname.instance-name.username -l shared-folder
```

For details about `jimasecret` command, see `jimasecret` in *Chapter 1. Commands in the JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

If you have registered passwords for more than one Microsoft SQL Server user, perform the same procedure for all users.

(d) Configure SQL exporter alive monitoring (optional)

You can monitor SQL exporter service-alive monitoring with up metric on Prometheus server. The following is an example of how to monitor SQL exporter in the alert-definition.

```
groups:
- name: exporter_healthcheck
  rules:
  - alert: jpl_pc_exporter_healthcheck
    expr: up{jpl_pc_remote_monitor_instance=""} == 0 or label_replace(up{jpl_pc_exporter="JPC SQL exporter"}, "jpl_pc_nodelabel", "${1}", "jpl_pc_remote_monitor_instance", "^[^:]*:([^:]*)$") == 0 or label_replace(up{jpl_pc_remote_monitor_instance!="", jpl_pc_exporter!="JPC SQL exporter"}, "jpl_pc_nodelabel", "${1}", "jpl_pc_remote_monitor_instance", "^[^:]*:([^:]*)$") == 0
    for: 3m
    labels:
      jpl_pc_product_name: "/HITACHI/JP1/JPCCS2"
      jpl_pc_component: "/HITACHI/JP1/JPCCS/CONFINFO"
      jpl_pc_severity: "Error"
      jpl_pc_metricname: "up"
    annotations:
      jpl_pc_firing_description: "Communication to Exporter failed. instance={{ $labels.instance }}"
      jpl_pc_resolved_description: "Communication to Exporter successful. instance={{ $labels.instance }}"
```

(e) Modifying Users for Connections (Optional)

1. Add a new person to Microsoft SQL Server.

Perform this procedure only if a new monitoring user is required and not registered.

2. Shut down SQL exporter.

3. Delete the password of the user before the change.

Use `jimasecret` command to remove the password of the user who was connecting to Microsoft SQL Server.

- For physical host operation

```
jimasecret-rm-key MSSQL.hostname.instance-name.old-username
```

- For logical host operation

```
jimasecret-rm-key MSSQL.hostname.instance-name.old-username -l shared-folder
```

For details about `jimasecret` command, see `jimasecret` in *Chapter 1. Commands* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

4. Register the password of the user after change.

Use `jimasecret` command. Register the password of the user used to connect to Microsoft SQL Server.

- For physical host operation

```
jimasecret-add-key MSSQL.hostname.instance-name.new-username -s password
```

- For logical host operation

```
jimasecret-add-key MSSQL.hostname.instance-name.new-username -s password  
-l shared-folder
```

For details about `jimasecret` command, see `jimasecret` in *Chapter 1. Commands* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

5. Change the username of the connection-information described in SQL exporter configuration file.

Removes the username for SQL exporter connectivity from SQL exporter configuration file (`jpc_sql_exporter`).

For details about SQL exporter configuration file, see *SQL exporter configuration file (jpc_sql_exporter)* in *Chapter 2. Definition Files* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

6. Start SQL exporter.

7. Deletes the previous person from Microsoft SQL Server.

If the old user is not needed, remove the old user from Microsoft SQL Server.

(5) Troubleshooting SQL exporter Building

- Metrics are not available after SQL exporter has been configured.

After performing the procedure of *1.23.4(4)(a) Adding monitoring targets (required)*, the following shows what to check when the value of the metric cannot be obtained and how to target it.

Check details	Corrective action	See...
Are the monitored Microsoft SQL Server's services and instance running?	Start the monitored Microsoft SQL Server services and instance.	None

Check details	Corrective action	See...
Are the permissions of the user used to connect to the monitored Microsoft SQL Server set correctly?	Grant the correct permissions to the user you want to use to connect.	<i>Prerequisites for monitoring Microsoft SQL Server in 3.15.1(1)(q) SQL exporter (Microsoft SQL Server Monitoring Feature in the JP1/Integrated Management 3 - Manager Overview and System Design Guide</i>
Is the password for the user used to connect to the monitored Microsoft SQL Server registered?	Register the password of the user used for connection.	None
Is the error log displayed in <i>SQL-exporter-location\sql_exporter_windows\jp1ima\logs</i> folder? If an error log is output, is there a remedy described in the explanation of the reference destination?	Perform the action described in the reference.	<i>12.5.1 (14) sql_exporter Logging in the JP1/Integrated Management 3 - Manager Administration Guide</i>

(6) Cluster environment

SQL exporter must also be logical host operation if scrape of JP1/IM - Agent is logical host operation.

1.24 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.

Of the data in the folder containing the media that provides the manuals, copy all target data for each manual to the folders containing JP1/IM - Manager and JP1/IM - View.

If all manuals are stored in their correct locations, you can view the table of contents of each manual.

When you select **Help** and then **Help Contents** if the data is placed in an incorrect location or only part of the data is placed, an error dialog box (KAVB8550-E) appears.

- Stored target data (HTML manuals)
CSS file, all HTML files, and the GRAPHICS folder
- Locations of data in the manual distribution medium (inserted in the drive of the Windows machine)
In the manual distribution media, manuals are stored in folders with manual numbers under *applicable drive\MAN\3021*. If you want to know which manual corresponds to which product, check *INDEX.HTM* under each folder with a manual number.
- Locations to store the target data on the JP1/IM - Manager side:
Under *installation-folder\JP1Cons\www>manual\en*
Under *installation-folder\JP1IMM\public>manual\en*
Store all the target data stored under the manual number folder of the manual distribution media in the folder of each manual number.
- Locations to store the target data on the JP1/IM - View side:
JP1/Integrated Management 3: Getting Started (Integrated Console) (Locations of data in the manual distribution medium\en\03L0100L)
installation-folder\JP1CoView>manual\en\03L0100L
JP1/Integrated Management 3 - Manager Overview and System Design Guide (Locations of data in the manual distribution medium\en\03L0200L)
installation-folder\JP1CoView>manual\en\03L0200L
JP1/Integrated Management 3 - Manager Configuration Guide (Locations of data in the manual distribution medium\en\03L0300L)
installation-folder\JP1CoView>manual\en\03L0300L
JP1/Integrated Management 3 - Manager Administration Guide (Locations of data in the manual distribution medium\en\03L0400L)
installation-folder\JP1CoView>manual\en\03L0400L
JP1/Integrated Management 3 - Manager GUI Reference (Locations of data in the manual distribution medium\en\03L0500L)
installation-folder\JP1CoView>manual\en\03L0500L
JP1/Integrated Management 3 - Manager Command, Definition File and API Reference (Locations of data in the manual distribution medium\en\03L0600L)
installation-folder\JP1CoView>manual\en\03L0600L
JP1/Integrated Management 3 - Manager Messages (Locations of data in the manual distribution medium\en\03L0700L)

installation-folder\JP1CoView\manual\en\03L0700L

After copying the manual number folder from the manual distribution medium to a desired location, rename the folder so that its name is identical to the manual number folder to which the target data is saved.

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

1.25 Uninstallation (for Windows)

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

1.25.1 Uninstallation procedure (for Windows)

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

(1) The procedure for delete Intelligent Integrated Management Database

Back up Intelligent Integrated Management Database before you delete it to rebuild it. For details on how to back up the data, see *1.2 Managing the databases* in the *JP1/Integrated Management 3 - Manager Administration Guide*.

Perform the following steps to delete Intelligent Integrated Management Database:

1. Stop JP1/IM - Manager.

Stop JP1/IM - Manager.

2. Delete Intelligent Integrated Management Database.

Execute the following command.

- For physical host operation

```
jimgndbunsetup [-q]
```

- For active host in logical host operation

```
jimgndbunsetup -h logical-host-name -c online [-q]
```

- For standby host in logical host operation

```
jimgndbunsetup -h logical-host-name -c standby [-q]
```

3. Restart the machine.

(2) 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 3 - Manager Administration Guide*.

For details about the commands, see *Chapter 1. Commands* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API 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/IM3-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/IM3-Manager) is stopped.
- For logical hosts
The IM database (JP1/IM3-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/IM3-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.

(3) How to uninstall JP1/IM - Manager

To uninstall:

If you uninstall JP1/IM - Manager, JP1/IM agent management base for using JP1/IM - Agent is also uninstalled.

1. Terminate the programs.

Before you start the uninstallation procedure, terminate all programs.

Terminate JP1/IM3-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. To uninstall JP1/IM - Manager, use the Uninstall a program tool in Control Panel[#].

Follow the instructions of the installer to perform uninstallation.

No entries are required during uninstallation.

[#]: If you are using Classic View in Control Panel, use the Programs and Features tool in Control Panel.

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.

(4) 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. To uninstall JP1/IM - View, use the Uninstall a program tool in Control Panel[#].

Follow the instructions of the installer to perform uninstallation.

No entries are required during uninstallation.

[#]: If you are using Classic View in Control Panel, use the Programs and Features tool in Control Panel.

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.

(5) How to uninstall JP1/IM - Agent

Follow the procedure below to uninstall.

1. Stop JP1/IM - Agent service.

2. If you are using the data delivery function to multiple manager hosts, perform the following steps before deleting the service.

Execute *Uninstalling JP1/IM - Agent* described in *1.21.2(2)(j) Deactivating the data delivery function to multiple manager hosts (for Windows) (optional)*.

3. Execute the service delete of JP1/IM - Agent.

For details about how to delete the service, see [1.21.1\(1\)\(b\) Disable add-on program](#).

4. Open Windows control-panel [Programs and Features] window, delete JP1/IM - Agent.
5. After the deletion is complete, log in to the Integration Manager integrated operation viewer and manually remove integrated agent for the deleted hosts.

For how to delete integrated agent information, see [2.2.1 List of Integrated Agents window](#) in the *JP1/Integrated Management 3 - Manager GUI Reference*.

6. 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 - Agent had been installed.

Important

If logical host service is running, delete logical host service after stopping the service and then execute it. If you uninstall while logical host service is running, file used by logical host service may be deleted and the service may terminate abnormally. Logical host service must be deleted after uninstallation if logical host service was uninstalled without deletion services.

1.25.2 Notes on uninstallation (for Windows)

(1) 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.

(2) 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.

(3) About uninstalling JP1/IM - Manager, JP1/IM - View and JP1/IM - Agent

- After you have uninstalled JP1/IM - Manager and JP1/IM - View, the program folder may still remain in the start menu. If you don't need the program folder, refer to Windows help from **Start Menu** to determine how to delete it.
- Uninstalling the product deletes the monitoring object DB and the host information DB.
- If you want to uninstall JP1/IM - Manager and JP1/IM - View and then re-install it, make sure that you restart the OS after the uninstallation. After the OS restarts, delete the folder where this program was installed by using Windows Explorer, and then re-install JP1/IM - Manager and JP1/IM - View.
- If you attempt to uninstall JP1/IM - View while it is being used, a dialog box appears. In this case, click the **Cancel** button to abort the uninstallation, stop all running JP1/IM - View instances, and then retry the uninstallation of JP1/IM - View.

(4) About uninstalling JP1/Base

Uninstalling JP1/Base deletes the definition information for JP1/IM - Manager and JP1/IM - View. Even if you reinstall JP1/Base, JP1/IM - Manager and JP1/IM - View will not work. If this occurs, you need to uninstall JP1/IM - Manager and JP1/IM - View, and then reinstall it.

(5) About the procedure for manually uninstalling an IM database on a physical host

To manually uninstall an IM database on a physical host, use the following procedure:

1. Log on as a user with Administrator privileges.
2. If JP1/IM - Manager service (JP1/IM3-Manager) is operating, terminate the service.
3. If an IM database service (JP1/IM3-Manager DB Server) is operating, terminate the service.
4. Delete the following folders, if they exist:
value-of-setup-information-file-IMDBENVDIR\JM0
value-of-setup-information-file-IMDBDIR\imdb
5. Use the registry editor to select the following registry and check the value of InstallGuid:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Hitachi\HiRDBEmbeddedEdition_JM0\{  
alphanumeric-string}#1,#2
```

#1: Example of {*alphanumeric-string*}: 08042Y

#2: Example value of [InstallGuid]: BAB5F425-3C8F-4CD5-9117-DA371EAD50DF

6. Use the registry editor to delete the following registry items, if they exist:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Hitachi\HiRDBEmbeddedEdition_JM0#1  
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\U  
ninstall\{alphanumeric-strin}#1,#2  
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\HiRDBEmbeddedEdition_  
JM0  
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\HiRDBClusterService_J  
M0  
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\Application\  
JP1/IM-M_DB_Server
```

#1: For Windows 32-bit environment,
replace "HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\HITACHI\
with "HKEY_LOCAL_MACHINE\SOFTWARE\HITACHI\".

#2: Make sure that the value of {*alphanumeric-string*} is equal to the value of [InstallGuid] you checked at step 5, and then delete the registry.

7. Delete the following folder (hidden folder) if it exists:

```
OS-drive:\Program Files (x86)\  
InstallShield Installation Information\{alphanumeric-string}#
```

#: Make sure that the value of {*alphanumeric-string*} is equal to the value of InstallGuid you checked at step 5, and then delete the registry.

8. Update the configuration file for the IM database by performing the following procedure:

- Delete *Manager-path*\conf\imdb\system\dbconf\JM0.

- Open *Manager-path\conf\imdb\system\dbconf\jimdbsetuplist.conf* in a text editor and edit it as follows, delete JP1_DEFAULT, and then overwrite the file.

(Before editing) _JM0=JP1_DEFAULT

(After editing) _JM0=

9. Restart the OS. The OS must be restarted in order to synchronize the registry editor value with the value in memory.

(6) About the procedure for manually uninstalling an IM database on a cluster system

To manually uninstall an IM database on a cluster system, use the following procedure:

1. Log on to the active host as a user with Administrator privileges.
2. If a JP1/IM - Manager service (JP1/IM3-Manager_ *logical-host-name*) is operating on the active host, terminate the service.
3. If an IM database service is operating on the active host, terminate the service.
JP1/IM3-Manager DB Server_ *logical-host-name*
JP1/IM3-Manager DB Cluster Service_ *logical-host-name*
4. If the following folder exists in the active server, delete the folder.
value-of-IMDBENVDIR-for-cluster-setup-information-file\JMn[#]
value-of-IMBDDIR-for-cluster-setup-information-file\imdb
value-of-SHAREDBDIR-for-cluster-setup-information-file\imdb
#: *n* is the value of LOGICALHOSTNUMBER for the cluster setup information file.
5. Use the registry editor to select the following registry and check the value of [InstallGuid]^{#2}:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Hitachi\HiRDBEmbeddedEdition_JMn\{
alphanumeric-string} #1, #2
```

#1: Example of { *alphanumeric-string* }: 08042Y

#2: Example value of [InstallGuid]: BAB5F425-3C8F-4CD5-9117-DA371EAD50DF

6. On the active host, use the registry editor to delete the following registries, if they exist:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Hitachi\HiRDBEmbeddedEdition_JMn #1
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\U
ninstall\{alphanumeric-string} #1, #2
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\HiRDBEmbeddedEdition_
JMn
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\HiRDBClusterService_J
Mn
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\Application\
HiRDBEmbeddedEdition_JMn
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\Application\
JP1/IM-M_DB_Server_ logical-host-name
```

#1: For a 32-bit Windows environment,

replace HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\HITACHI\
with HKEY_LOCAL_MACHINE\SOFTWARE\HITACHI\.

#2: Make sure that the value of { *alphanumeric-string* } is equal to the value of [InstallGuid] you checked at step 5, and then delete the registry.

7. If the following folder (hidden folder) exists on the active host, delete it:

```
OS-drive:\Program Files (x86) \
InstallShield Installation Information\{alphanumeric-string}#
```

#: Make sure that the value of {*alphanumeric-string*} is equal to the value of [InstallGuid] you checked at step 5, and then delete the registry.

8. Update the configuration file for the IM database on the active host by performing the following procedure:

- Delete *Manager-path*\conf\imdb\system\dbconf\JMn#.
- Open *Manager-path*\conf\imdb\system\dbconf\jimdbsetuplist.conf in a text editor, edit the line equal to *n*+1 as follows, delete the logical host name, and then overwrite the file.

#: *n* is the value of LOGICALHOSTNUMBER for the cluster setup information file.

(Before editing) jimdbsetuplist.conf, line *n*+1

_JMn=*logical-host-name*

(After editing) jimdbsetuplist.conf, line *n*+1

_JMn=

9. Restart the OS on the active host.

The OS must be restarted in order to synchronize the registry editor value with the value in memory.

10. Log on to the standby host as a user with Administrator privileges.

11. If a JP1/IM - Manager service (JP1_IM3-Manager_*logical-host-name*) is operating on the standby host, terminate the service.

12. If an IM database service is operating on the standby host, terminate the service.

- JP1/IM3-Manager DB Server_*logical-host-name*
- JP1/IM3-Manager DB Cluster Service_*logical-host-name*

13. If the following folder exists in the standby host, delete the folder.

value-of-IMDBENVDIR-for-cluster-setup-information-file\JMn#

value-of-IMDBDIR-for-cluster-setup-information-file\imdb

value-of-SHAREDBDIR-for-cluster-setup-information-file\imdb

#: *n* is the value of LOGICALHOSTNUMBER for the cluster setup information file.

14. On the standby host, use the registry editor to delete the following registry, if it exists:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Hitachi\HiRDBEmbeddedEdition_JMn#1
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\U
ninstall\{alphanumeric-string}#1,#2
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\HiRDBEmbeddedEdition_
JMn
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\HiRDBClusterService_J
Mn
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\Application\
HiRDBEmbeddedEdition_JMn
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\Application\
JP1/IM-M_DB_Server_logical-host-name
```

#1: For a 32-bit Windows environment,

replace HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\HITACHI\

with HKEY_LOCAL_MACHINE\SOFTWARE\HITACHI\.

- #2: Make sure that the value of { *alphanumeric-string* } is equal to the value of [InstallGuid] you checked at step 5, and then delete the registry.
15. On the standby host, delete the following folder (hidden folder), if it exists:
OS-drive: \Program Files (x86) \InstallShield Installation Information \{ *alphanumeric-string* }#
#: Make sure that the value of { *alphanumeric-string* } is equal to the value of [InstallGuid] you checked at step 5, and then delete the registry.
16. Update the configuration file for the IM database on the standby host by performing the following procedure:
- Delete *Manager-path* \conf \imdb \system \dbconf \JMn#.
 - Open *Manager-path* \conf \imdb \system \dbconf \jimdbsetuplist.conf by text editor, edit the line equal to *n*+1 as follows, delete the logical host name, and then overwrite the file.
- #: *n* is the value of LOGICALHOSTNUMBER for the cluster setup information file.
- (Before editing) jimdbsetuplist.conf, line *n*+1
_JMn=*logical-host-name*
(After editing) jimdbsetuplist.conf, line *n*+1
_JMn=
17. Restart the OS on the standby host. The OS must be restarted in order to synchronize the registry editor value with the value in memory.

1.26 Notes about installation and setting up (for Windows)

Important

When creating a container environments on CentOS 8 (or later) or Linux 8 (or later), read Docker as Podman.

- JP1/IM can replicate integrated agent host by installing ServerConductor/DeploymentManager and JP1/ServerConductor/Deployment Manager disk-duplicate installations and using virtualization platform-provided image filling. JP1/IM - Manager and JP1/IM - View cannot be replicated. The following virtualization platforms support replication of the integrated agent host:

- VMware ESX
- Hyper-V
- SCVMM
- Amazon EC2

For unsupported virtual platforms other than the above, uninstall JP1/IM and then reinstall JP1/IM after the disk-duplicate installation or replication by the virtualization platform.

For details on how to perform disk-copy installations, see the manuals for ServerConductor/DeploymentManager and JP1/ServerConductor/Deployment Manager. For details on the copy functions of virtualization platforms, see the relevant manual for the applicable virtualization software.

- Notes on monitoring containers in Docker environments as agent hosts
 - JP1/Base must be installed in the container. For details about Docker environments supported by JP1/Base, see the Release Notes for JP1/Base.
 - Specify the settings of port numbers to be used by JP1/Base in the container, so that TCP/IP communication is available from the JP1/IM - Manager host.
 - Because network address translation (NAT) is used for communication from containers to external locations, "Source IP address" does not display the correct value (in the way it is usually displayed) for an event issued from JP1/Base in the container. Do not use the IP address displayed in "Source IP address" for conditions of JP1/IM - Manager functions.
- Notes on monitoring containers in Docker environments as remote monitoring hosts
 - The remote monitoring function supports the following Docker environments:
Docker host OSs
Among the OSs supported by the remote monitoring function, the following OSs are supported:
- Red Hat Enterprise Linux Server 7.1 or later
Docker version
- Versions that support the previously described Docker host OSs.
 - SSH must be installed in the container.
 - Specify the settings so that SSH connections can be made from the JP1/IM -Manager host to the container.

2

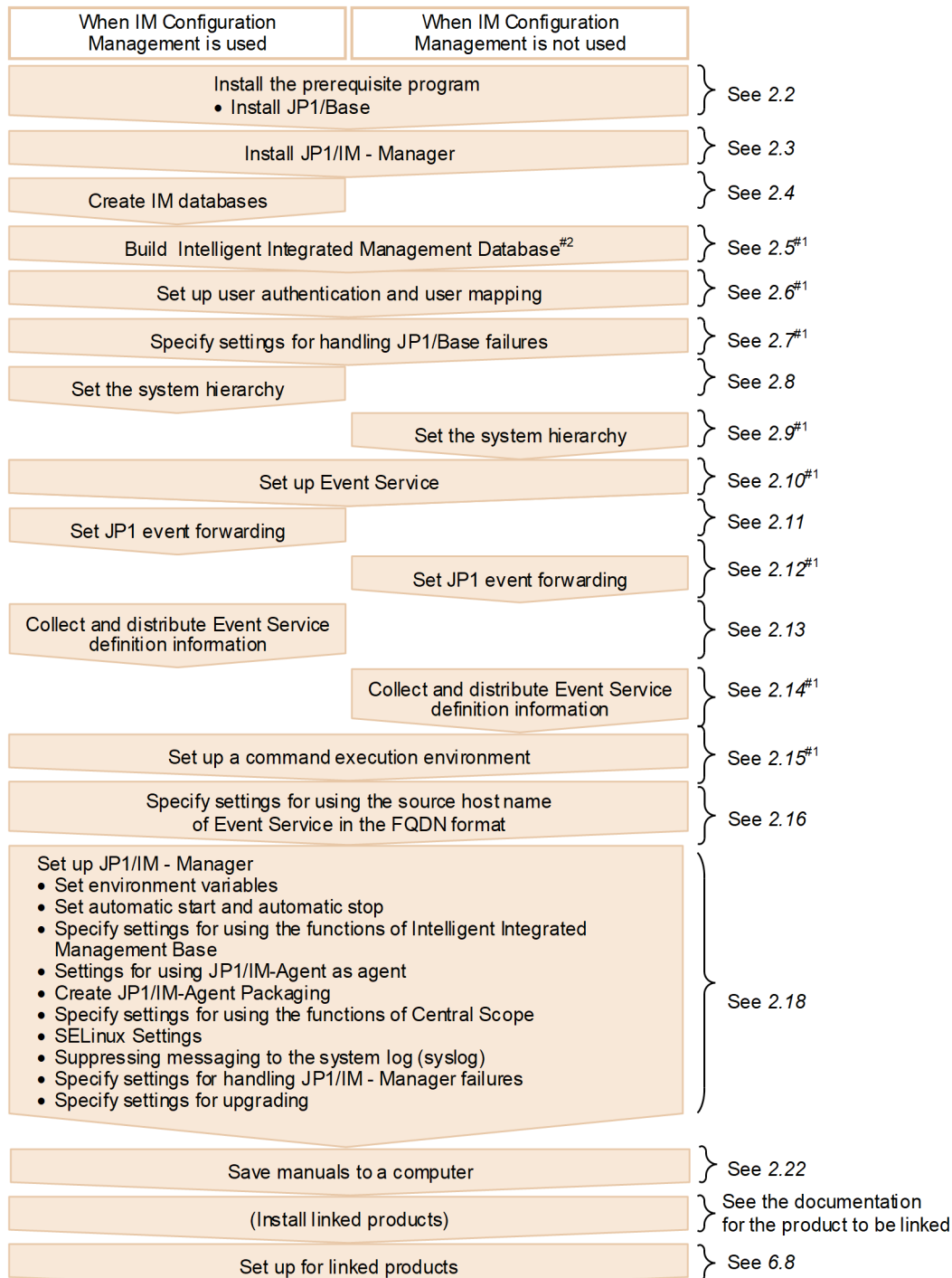
Installation and Setup (for UNIX)

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 [2.23.1 Uninstallation procedure \(for UNIX\)](#).

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



#1: For more information, see *JP1/Base Administration Guide* documentation.

#2: This is performed when Intelligent Integrated Management Database is used.

Figure 2–2: Installation and setup workflow (agent (JP1/IM - Agent))

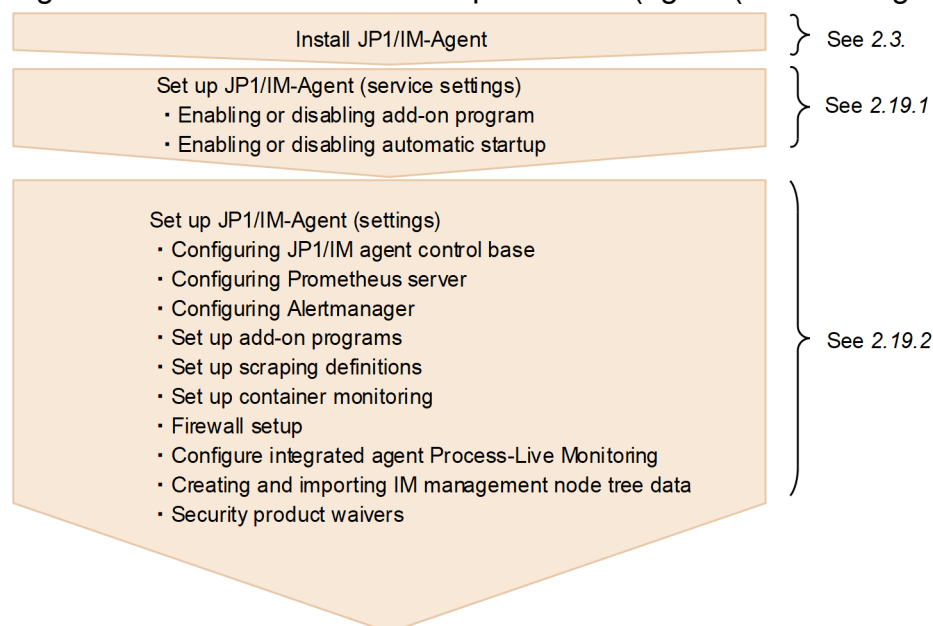
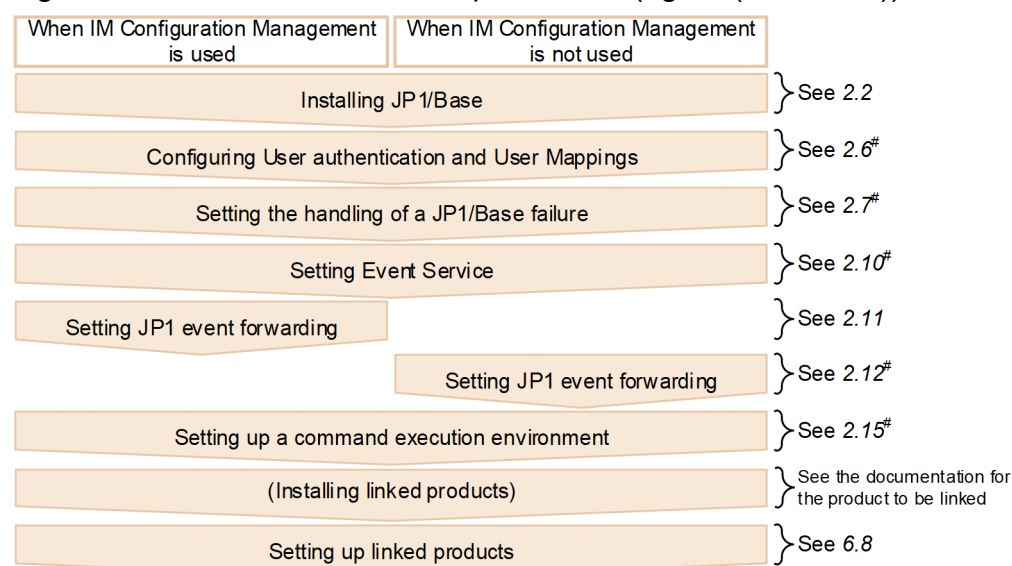


Figure 2–3: Installation and setup workflow (agent (JP1/Base))



[#]:For more information, see *JP1/Base Administration Guide* documentation.

For details about the settings for monitoring logs on hosts that will be monitored remotely, see [2.17 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 [9.4 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 3 - 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.
- When IM databases are used, a host name must be a character string of not more than 32 characters consisting of only one-byte alphanumeric characters, -, and . (period).

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.

When you apply an OS patch, stop the product first, and then apply the patch while the product is stopped.

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 3 - 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 and JP1/IM - Agent.

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 and JP1/IM - Agent.

(1) How to install JP1/IM - Manager

Install JP1/IM - Manager and JP1/IM - Agent as follows: You need `root` permissions to perform this procedure.

If you install JP1/IM - Manager, JP1/IM agent management base for using JP1/IM - Agent is also installed.

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/jplimm_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.

To perform encrypted communication with JP1/IM - Agent, perform the following steps related to JP1/IM agent management base.

1. Setup Server certificate and its key file.

When performing cryptographic communication with integrated agent host, specify the full path of Server certificate file to `tls_config.cert_file` of `imbase common` configuration file (`jpc_imbasecommon`), and the full path of the key file of server certificate in `"tls_config.key_file"`.

For details, see *imbase common configuration file (jpc_imbasecommon.json)* in *Chapter 2. Definition Files* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

(2) Procedure of JP1/IM - Agent installation

(a) Information required before installation

If you are installing JP1/IM - Agent newly, you need the following: Prepare before installation.

Table 2–1: Information required for a new installation

Item	Needing to specify	Description
Host name of the install destination JP1/IM - Manager	Required	Specifies Host name of the manager host that manages integrated agent to be installed. The name must be resolved to IP address.
Listen port for imbase processes	Optional	Specifies the listen port for imbase processes running on the manager host to connect, from 5001 to 65535. When this is omitted, imbase default port (20724) is used.
Listen port for imbaseproxy processes	Optional	Specifies the listen port for imbaseproxy processes running on the manager host to which the connection is made, from 5001 to 65535. By default, imbaseproxy defaultport (20725) is used.
Initial secret to connect to imbase for the first time	Required	Specifies initial secret to connect to imbase process running on the manager host to connect for the first time. Check from integrated operation viewer.
URL of proxy	Optional	If you are connecting to the manager host through a proxy server, specify the proxy URL in "http://host:port" format. The default for when this is omitted is an empty string.
User ID for proxy authentication	Optional	When connecting to the manager host, specify ID for authentication of the proxy server when passing through the proxy server. The characters that can be specified are the characters in ASCII encoding 0x20 to 0x7E. You can specify up to 1007-charaters-long string. The default for when this is omitted is an empty string.
Password for Proxy authentication	Optional	When connecting to the manager host, specify password for authentication of the proxy server when passing through the proxy server. The characters that can be specified are the characters in ASCII encoding 0x20 to 0x7E. You can specify up to 1007-charaters-long string. The default for when this is omitted is an empty string.
Functions to be used	Optional	Allows you to select the function that you use in JP1/IM - Agent. A new install setup the service for the feature you use to start automatically.

(b) Install Instructions

Follow the procedure below to install.

1. Login agent host with administrator privileges.

You must have root privilege to complete the install process.

2. Prepare a medium for installing JP1/IM - Agent.

There are two ways to install JP1/IM - Agent: Prepare the installation media according to the installation method to be used.

- To install by setting the offered media on the drive
Provide the offered media as an installation medium.
- To install by downloading JP1/IM - Agent packages registered to the manager host[#]
Download and extract JP1/IM - Agent packages to prepare them.

#

For the procedure for downloading JP1/IM - Agent package, see [2.18.6\(3\) How to Download JP1/IM - Agent Package](#).

3. Setup the environment variables for default settings for the host to be installed.

- For normal, silent, and Remote installations (required)

The parameters required for installation must be setup in the environment-variable # beforehand.

#

For details about environment variable, see [1.3.1\(3\)\(c\) Initialization environment variable used by the installer](#).

4. Terminate all programs.

Close all programs before installing.

Stop JP1/IM - Agent servicing before installing the version upgrade.

5. Install JP1/IM - Agent by executing the downloaded JP1/IM - Agent installer.

Follow the instructions on Hitachi PP Installer# to install.

#: For details about the operating procedure, see [2.3.2 How to use the Hitachi Program Product Installer \(for UNIX\)](#).

Select the software you want to install.

6. After the install, change the required settings.

Change required settings described in "[2.19.2 Settings of JP1/IM - Agent](#)". The mandatory settings should be executed for sure.

After JP1/IM - Agent is newly installed, check whether the/tmp/HITACHI_JP1_INST_LOG/jp1imagent_inst1 displays an error message indicating that jimasetup command or jimasecret command failed to execute. If an error message has been output, check the log file of jimasetup command or jimasecret command and take appropriate action according to the displayed error message.

Important

If you have changed initial secret after you installed JP1/IM - Agent and before the first boot of JP1/IM - Agent on integrated agent host, you must either update initial secret registered with integrated agent or uninstall and reinstall JP1/IM - Agent. For details about updating initial secret registered in integrated agent, see step 4 in [1.21.2\(2\)\(a\) Change Integrated manager to connect to \(for Windows\) \(optional\)](#).

(3) Various Installations

Upgrade installation

Perform the following contents before installing the version upgrade.

- For JP1/IM - Agent

If the logical host service is running, stop the service and then perform the upgrade installation. If you perform an upgrade installation while the logical host service is running, the files used by the logical host service may be deleted, resulting in abnormal termination of the service.

If you are upgrading from a previous version of JP1/IM - Manager, first read the notes about upgrading that you will find in [14.2 Upgrading from a previous version of JP1/IM](#) in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

Also, for precautions when upgrading JP1/IM - Agent from version 13-00 or 13-01, see [2.3.4\(9\) Notes on upgrading JP1/IM - Agent from version 13-00 or 13-01](#) and [2.3.4\(10\) Notes on upgrading JP1/IM - Agent from version 13-00 or 13-10](#).

Important

When performing an upgrade installation on a computer where logical host settings are set, terminate the daemon for JP1/IM - Manager of the logical host before performing the upgrade installation.

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.

The following remote installation methods are available:

- Update installation

- For JP1/IM - Manager

Settings of the installed JP1/IM - Manager is inherited. If JP1/IM - Manager is not installed, updating cannot be installed.

- For JP1/IM - Agent

Settings of the installed JP1/IM - Agent is inherited. If JP1/IM - Agent is not installed, updating cannot be installed.

- New installation

The product is newly installed.

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 or JP1/IM - Agent
- How to use the Hitachi Program Product Installer to remove JP1/IM - Manager or JP1/IM - Agent
- 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 or JP1/IM - Agent 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 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 Linux

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

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

Note:

During installation, do not start Hitachi Program Product Installer by executing `/etc/hitachi_x64setup`.

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 Linux

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

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

(2) Installing JP1/IM - Manager and JP1/IM - Agent

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

Figure 2–4: 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 or JP1/IM - Agen. After installation is completed, enter **Q** to return to the initial window.

(3) Removing JP1/IM - Manager and JP1/IM - Agent

Enter the following command to start the Hitachi Program Product Installer:

```
/etc/hitachi_ x64setup
```


The Hitachi Program Product Installer's initial window is displayed. For details about the initial window, see [Figure 2-4 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_ x64setup
```

The Hitachi Program Product Installer's initial window is displayed. For details about the initial window, see [Figure 2-4 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 2–2: Values that can be specified for `LANG` in the `jp1co_env.conf` file

OS	Language type	Encoding	Value of <code>LANG</code> environment variable ^{#3}
Linux	Japanese	SJIS ^{#1}	<code>ja_JP.SJIS</code> or <code>ja_JP.sjis</code>
		UTF-8 ^{#2}	<code>ja_JP.UTF-8</code> or <code>ja_JP.utf8</code>
	English	C	C
		UTF-8 ^{#2}	<code>en_US.UTF-8</code> or <code>en_US.utf8</code>
	Chinese	GB18030	<code>zh_CN.gb18030</code>

^{#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`.

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 2–3: 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
		UTF-8
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)

(1) 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.

(2) About Hitachi Network Objectplaza Trace Library (HNTRLib2)

When you install JP1/Base, Hitachi Network Objectplaza Trace Library (HNTRLib2) is installed.

(3) 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 3 - 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 3 - Manager Overview and System Design Guide* are deleted.

(4) About downgrade installation

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

(5) About information that JP1/IM - Manager manages

Do not perform the following operations, because JP1/IM - Manager manages such information as program information, configuration information, and maintenance information in files and in the registry. If you perform the following operations, JP1/IM - Manager may not work properly.

- Use an application such as Explorer to delete or change files and folders for JP1/IM - Manager. Or, change the access permissions.
- Use Registry Editor to delete or change the information on JP1/IM - Manager, or change the access permissions.

(6) About installation

Before installing JP1/IM - Manager, confirm that the temporary directory (`/tmp`) has 5 MB of free space.

(7) About anti-virus software

When you install JP1/IM - Manager, if anti-virus software performs a virus scan on the installation destination of JP1/IM - Manager, an application error might occur due to conflict between the installer and the anti-virus software and installation might fail. To avoid this, stop the anti-virus software before performing an installation.

(8) About silent installation

(a) For JP1/IM - Manager

JP1/IM - Manager can be installed by using the silent installation functionality. Execute the following command:

For Linux: `<DVD-R-media>/X64LIN/setup -f -k P-CC842C-9MDL <path-of-DVD-R-media>`

For SUSE Linux: `<DVD-R-media>/SLES/setup -f -k P-CC9W2C-9MDL <path-of-DVD-R-media>`

- To execute the contents of DVD-R media directly from a hard drive, copy the contents of the DVD-R media to a directory on the hard drive whose path does not include any spaces. Then, compare the copied files to the original files (at the binary level, for example) to ensure that they are the same.
- Check the return value of the execution result to verify that the installation ended successfully. For details about the return values, see the JP1 website.
- When installing this software product by using the silent installation functionality, you can not specify user information. To specify user information, install software product in the installation procedure described in the [2.3.1 Installation procedure \(for UNIX\)](#).

(b) For JP1/IM - Agent

The silent installation feature provides an installation method for JP1/IM - Agent.

Command

For Linux: `DVD-R media/X64LIN/setupΔ-fΔ--kΔP-CC842C-9GDLΔDVD-R media pass`

Δ: One or more half-width spaces

(9) Notes on upgrading JP1/IM - Agent from version 13-00 or 13-01

See [1.3.3\(14\) Notes on upgrading JP1/IM - Agent from version 13-00 or 13-01](#).

(10) Notes on upgrading JP1/IM - Agent from version 13-00 or 13-10

When JP1/IM - Agent is upgraded, ExecStart rows are updated for unit definition file listed in the following tables in order to apply OSS wrapper to OSS that supports the add-on management functionality. In JP1/IM - Agent installer log, verify that KAVB9447-I messaging is displayed for the respective unit definition file. For details about JP1/IM - Agent installer log, see [12.2.2\(8\) Installer Log](#) in the *JP1/Integrated Management 3 - Manager Administration Guide*.

Add-on program	Unit definition file Name	Backup file name
Prometheus server	jpc_prometheus_server.service	jpc_prometheus_server.service.bk
Alertmanager	jpc_alertmanager.service	jpc_alertmanager.service.bk
Blackbox exporter	jpc_blackbox_exporter.service	jpc_blackbox_exporter.service.bk
Yet another cloudwatch exporter	jpc_ya_cloudwatch_exporter.service	jpc_ya_cloudwatch_exporter.service.bk
process_exporter	jpc_process_exporter.service	jpc_process_exporter.service.bk
Promitor	jpc_promitor_resource_discovery.service	jpc_promitor_resource_discovery.service.bk
	jpc_promitor_scraper.service	jpc_promitor_scraper.service.bk
Script exporter	jpc_script_exporter.service	jpc_script_exporter.service.bk
Fluentd	jpc_fluentd.service	jpc_fluentd.service.bk
VMware exporter	jpc_vmware_exporter.service	jpc_vmware_exporter.service.bk
node exporter	jpc_node_exporter.service	jpc_node_exporter.service.bk

If KAVB9448-W and KAVB9450-W messages are displayed, update ExecStart row by manually editing the appropriate unit definition file. For details about the descriptions in ExecStart line, see *Unit definition file (jpc_program-name.service)* in [Chapter 2. Definition Files](#) of the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

(11) Notes on upgrading JP1/IM - Manager from version 13-00 to 13-11 to 13-50 or later

When JP1/IM - Manager is upgraded, the recommended settings for log output of the Intelligent Integrated Management Database are not reflected. Check the setting values of the following parameters of Intelligent Integrated Management Database configuration file (postgresql.conf). If there are no parameters or the settings are different from those listed below, set them as shown below.

Parameters	Set value
log_min_messages	fatal
log_error_verbosity	terse
log2	on
log2_rotation_count	5
log2_rotation_max_size	70M

For details about the parameters of Intelligent Integrated Management Database configuration file and for information about reflecting changed settings, see *Intelligent Integrated Management Database configuration file (postgresql.conf)* in *Chapter 2. Definition Files* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

2.3.5 How to collect data in installing (for UNIX)

(1) How to collect documentation when installing JP1/IM - Manager

The following describes how to collect data if an error occurs during installation.

1. Login to the manager host.
2. Collect the following File manually:
 - `/etc/.hitachi/.hitachi.log`
 - `/etc/.hitachi/.install.log`
 - `/etc/.hitachi/.uninstall.log`
 - Files under the `/tmp/HITACHI_JP1_INST_LOG/`

(2) How to collect documentation when installing JP1/IM - Agent

The following describes how to collect data if an error occurs during installation.

1. Login to integrated agent host.
2. Collect the following File manually.
 - `/etc/.hitachi/pplisted/pplisted`
 - `/etc/.hitachi/.install.log*`
 - `/etc/.hitachi/.uninstall.log*`
 - Files under the `/tmp/HITACHI_JP1_INST_LOG/`

2.3.6 How to link with the auto scale function (for UNIX)

(1) How to link with the auto-scale function in JP1/IM - Agent

(a) Prerequisite Services and conditions

The prerequisite services and conditions for operation corporate with the auto-scale function are as follows:

Prerequisite service

- Amazon EC2
- Amazon EC2 Auto Scaling

Prerequisite conditions

The following describes the prerequisites for operation corporate with the auto-scale function.

- It is not possible to target Logical host in a clustered environment.
- The system should not exceed 2500 units including the manager host.
- After scale-out or scale-in, you must create and reflect system configuration information. For details, see [2.19.2\(18\) Creating and importing IM management node tree data \(for Linux\) \(required\)](#).

(b) Create a Virtual Machine Image (AMI)

Following are the steps to create a virtual machine image (AMI).

1. Install JP1/IM - Agent.

In this case, select the installation mode **Image creation mode**. For details, see [1.3.1\(3\)\(c\) Initialization environment variable used by the installer](#).

2. Create a virtual machine image (AMI).

For details about creating a virtual machine image (AMI), see the official Amazon Web Services website.

(c) Creating an Auto Scaling Boot Setup

Following are the steps to create an Auto Scaling boot setup.

1. Open the [Amazon EC2] console from [AWS Management Console].
2. Click [Boot settings].of [Auto Scaling]in the left navigation pane.
3. Click [Create a boot settings].
4. Select the virtual machine image (AMI) created in step 1 from the [Select AMI] window.
5. In the [Detailed settings] window, select [by Text] from [Advanced details] - [User data] and write the following in the text box.

```
#!/bin/sh
/opt/jplima/tools/jimasetup phost
/opt/jplima/tools/jpc_ service_start -s all
```

2.3.7 Cloning a Virtual Machine (for UNIX)

On the following virtualization platforms, you can clone a virtual machine from a virtual machine template in an integrated agent host deployment where JP1/IM - Agent is installed in image creation mode.

- VMware ESX
- Hyper-V
- SCVMM

(1) Prerequisites

The following are the prerequisites for replicating agent:

- You can clone virtual machines on agent host only. Also, it cannot target logical hosts in a cluster environment.
- Agent configuration can have up to 2,500 hosts, including manager hosts.
- When creating a virtual machine template, select **Image creation mode** for JP1/IM - Agent install mode.

(2) How to Create a Virtual Machine Template

The following describes how to create a VM template.

1. Install JP1/IM - Agent on the virtual machine.

Select **Image creation mode** as the installation mode during installation.

For details about how to install the software, see [2.3.1\(2\) Procedure of JP1/IM - Agent installation](#).



Important

JP1/IM - Agent is not initialized.

(3) How to Clone a Virtual Machine

The following shows how to clone a virtual machine.

1. Clone a new virtual machine from a virtual machine template.

See virtualization software documentation for details about the replication features provided by virtualization platforms.

Check OS specifications for the tasks required by OS for duplication.

2. Start a new virtual machine.

3. Change the host name of the new virtual machine.

If necessary, change the host name of the virtual machine.

4. Change IP of the new virtual machine.

Change IP addressing of the virtual machine as needed.

For the procedure to be performed when IP address is changed, see [2.3.1\(3\) Tasks to be performed when IP address for agent is changed](#) in the *JP1/Integrated Management 3 - Manager Administration Guide*.

5. Perform JP1/IM - Agent initialization.

Run initial setting command of JP1/IM - Agent.

```
JP1/IM-Agent-installation-destination/jplima/tools/jimasetup phost
```

6. Refresh the tree of IM managed nodes on JP1/IM - Manager to which JP1/IM - Agent is connected.

For details, see [2.19.2\(18\) Creating and importing IM management node tree data \(for Linux\) \(required\)](#).

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 or the Intelligent Integrated Management Base are 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 *2.6 Functions provided by the IM database* in the *JP1/Integrated Management 3 - 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/IM3-Manager service has started are stored in the integrated monitoring database. For details, see *4.1.3(2) JP1 event control when using the integrated monitoring database* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

This section explains how to create an IM database.

Important

When operating in an Amazon EC2 instance environment, the host name can exceed 32 characters (for example, `ip-xx-xx-xx-xx.ap-northeast-1.compute.internal` (where `xx-xx-xx-xx` is the IP address)). When setting up an IM database, if the host name of the IM database exceeds the upper limit (32 characters), the setup fails with an KNAN11141-E error message. Therefore, follow the method of permanently assigning a static host name to an Amazon EC2 instance published by AWS and change it to a host name that does not exceed the upper limit (32 characters).

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 *JP1/Integrated Management 3 - Manager Command, Definition File and API 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 `IMDBDIR`, and paths containing symbolic links are not specified for `IMDBENVDIR` and `IMDBDIR`.

Important

Make sure that there are sufficient disk space allocated under `/etc/opt/jplimm/` while executing the `jcodbsetup` or `jcfdbsetup` command. If disk space is not enough, the `jcodbsetup` or `jcfdbsetup` command outputting the following message and terminating abnormally:

KNAN11053-E An attempt to read a file failed. (file name = instdb.log)

2.4.2 Setting up the integrated monitoring database (for UNIX)

Create an integrated monitoring database and use the Intelligent Integrated Management Base or 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/IM3-Manager Service. The following are the setup procedures for the two cases.

- To stop JP1/IM3-Manager Service and set up the integrated monitoring database:

1. Check if the IM database service (JP1/IM3-Manager DB Server) is running.
2. Stop the following services:
 - JP1/IM3-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/IM3-Manager Service.

- To set up the integrated monitoring database without stopping JP1/IM3-Manager Service:

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

2. Restart JP1/IM3-Manager Service.
3. Check if the IM database service (JP1/IM3-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/IM3-Manager Service.

For details about the `jcodbsetup` command, see *jcodbsetup* in *Chapter 1. Commands in the JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

For details about the `jcoimdef` command, see *jcoimdef* in *Chapter 1. Commands in the JP1/Integrated Management 3 - Manager Command, Definition File and API 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/IM3-Manager Service.

For details about the `jcodbsetup` command, see *jcodbsetup* in *Chapter 1. Commands in the JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

For details about the `jcoimdef` command, see *jcoimdef* in *Chapter 1. Commands in the JP1/Integrated Management 3 - Manager Command, Definition File and API 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/IM3-Manager Service. The following are the setup procedures for the two cases.

- To stop JP1/IM3-Manager Service and set up the IM Configuration Management database:
 1. Check if the IM database service (JP1/IM3-Manager DB Server) is running.
 2. Stop the following services:
 - JP1/IM3-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/IM3-Manager Service:
 1. Execute the `jcoimdef` command to disable the integrated monitoring database.
`jcoimdef -db OFF`
 2. Restart JP1/IM3-Manager Service.
 3. Check if the IM database service (JP1/IM3-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 JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

For details about the `jcoimdef` command, see *jcoimdef* in *Chapter 1. Commands in the JP1/Integrated Management 3 - Manager Command, Definition File and API 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 JP1/Integrated Management 3 - Manager Command, Definition File and API 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 (`jcfmain`).
`jcoimdef -cf ON`
2. Restart JP1/IM - Manager.
3. Execute the `jco_spmd_status` command to ensure that the IM Configuration Management service (`jcfmain`) is displayed in the active processes.

For details about the `jcoimdef` command, see `jcoimdef` in *Chapter 1. Commands in the JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

For details about the `jco_spmd_status` command, see `jco_spmd_status` in *Chapter 1. Commands in the JP1/Integrated Management 3 - Manager Command, Definition File and API 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:

If the status are different from the following status, stop the services to create the following status.

- If JP1/IM - MO is being used, the JP1/IM - Message Optimizer service of JP1/IM - MO is stopped at the connection source.
- If JP1/OA is receiving JP1 event from JP1/IM2 - Manager, JP1/OA is stopped at the connection source.
- JP1/IM2 - Manager is stopped.

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

- If the following message is output, perform step 6:
`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.`
`KNAN11211-I An update of the configuration files 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. Execute the `jimdbstop` command (without option) to stop the IM databases.

```
jimdbstop
```

Check that one of the following messages has been output.

```
KNAN11186-I Processing to stop the IM database service ended normally.
```

```
KNAN11183-I The IM database service is stopped.
```

6. Start JP1/IM2 - Manager.

7. If the following services were stopped in step 1, start the services.

- JP1/IM - Message Optimizer service of JP1/IM - MO on the connection source
(If using JP1/IM - MO)
- JP1/OA on the connection source
(If JP1/OA is receiving JP1 event from JP1/IM2 - 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 Construction of Intelligent Integrated Management Database (for UNIX)

If you are using Intelligent Integrated Management Database, execute the setup command (`jimgndbsetup` command) manually after installing JP1/IM - Manager.

By constructing Intelligent Integrated Management Database, you can create a DB for managing the various types of information shown in 2.7.1(1)(a) *Database configuration* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*. This enables you to manage the data used by the various functions.

The procedure for building the Intelligent Integrated Management Database is described below.

2.5.1 Preparations for Building Intelligent Integrated Management Database (in UNIX)

Prepare an *Intelligent Integrated Management Database setup information file* that contains the definitions required to build the Intelligent Integrated Management Database.

See *Intelligent Integrated Management Database setup information file (jimgndbsetupinfo.conf)* in *Chapter 2. Definition Files* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*, for editing Intelligent Integrated Management Database setup information file.

2.5.2 Settings of Intelligent Integrated Management Database (for UNIX)

Create an Intelligent Integrated Management Database and configure the Intelligent Integrated Management Base to use the Intelligent Integrated Management Database. If you are not using the Intelligent Integrated Management Database, this step is not required.

Here are the steps to set it up:

1. Create a non-root OS user.

A non-root OS user (a user who can log in) is required to start the Intelligent Integrated Management Database.

If necessary, use the `useradd` command of the OS to create a user to start the Intelligent Integrated Management Database. If you have already created one, proceed to the next step.

The following example shows how to run the `useradd` command when creating the user "imdbuser".

```
useradd imdbuser
```

2. Run the `jimgndbsetup` command to create the Intelligent Integrated Management Database.

```
jimgndbsetup -f Intelligent-Integrated-Management-Database-setup-information-file
```

For details of `jimgndbsetup` command, see *jimgndbsetup* in *Chapter 1. Commands* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

2.5.3 Excluding settings in security product(for UNIX)

JP1/IM - If you want to perform a virus check while Manager is running, exclude the following files and directories from scanning. Also, if you restart JP1/IM - Manager by performing a virus check while JP1/IM - Manager is stopped, make sure that the virus check has been completed for the following files and directories.

JP1/IM - Manager files and directories (UNIX)

- Where the executable files of the Intelligent Integrated Management Database are stored/all of the following:
- Intelligent Integrated Management Database data file location / All of the following[#]
- Storage location of related libraries of the Intelligent Integrated Management Database / All of the following[#]
- Intelligent Integrated Management Database configuration file location / All of the following[#]
- Storage location of operation commands of the Intelligent Integrated Management Database / All of the following[#]
- Storage location of individual logs of operational commands of the Intelligent Integrated Management Database / All of the following[#]
- Location of Trend Data Management Service logs / All of the following[#]

For details of the above storage destinations, see 2.7.1 (1)(d) *Where related files are stored in Intelligent Integrated Management Database* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

In a logical hosting environment, exclude shared directories from the scan.

- Shared directory/jplimm/all of the following
- Logical host Intelligent Integrated Management Database data files are stored in all of the following

[#]

Exclude if you are setting up the Intelligent Integrated Management database.

2.6 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 2–4: 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 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 2–5: 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).

2.6.1 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/jplbase/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*.

2.6.2 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/jplbase/bin/jbsadduser JP1-user-name
```

2.6.3 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 *9.4.1 Managing JP1 users* and *Appendix E. Operating Permissions* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

2.6.4 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.

2.6.5 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*.

2.7 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*.

2.8 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 [2.9 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.

2.8.1 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 [8.2.1 Hierarchical configurations managed by IM Configuration Management](#) in the *JP1/Integrated Management 3 - 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](#).

2.8.2 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](#).

2.8.3 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](#).

2.9 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 [2.8 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 [9.4.3 Managing the system hierarchy in the JP1/Integrated Management 3 - Manager Overview and System Design Guide](#).

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

2.9.1 Setting the configuration definition information (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, `jbsrt_distrib` command and the `jbsrt_sync` command, see the *JP1/Base User's Guide*.

2.9.2 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*.

2.9.3 Changing the configuration definition information (for UNIX)

If you change the configuration definition information, follow the same procedure as in [2.9.1 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 [2.9.2 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 [2.9.1 Setting the configuration definition information \(for UNIX\)](#).

2.9.4 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*.

2.10 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.

Important

JP1/IM - Manager obtains an event with user name "root" from JP1/Base (Event Service). If the `users` parameter is specified in the event server configuration file of the JP1/Base (Event Service) running on the same host, specify to include `root`. If `root` is not included, JP1/IM - Manager is unable to start normally.

2.11 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 [2.8 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](#).

2.12 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 [2.9 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*.

2.13 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](#).

2.14 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*.

2.15 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.

2.15.1 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 the chapter that environment variable file in the *JPI/Base User's Guide*.
- Host group definition
See the chapter that host group definition in the *JPI/Base User's Guide*.
- Creation of a command button definition file

See *Command button definition file (cmdbtn.conf)* in *Chapter 2. Definition Files* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API 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 *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

2.15.2 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 *JP1/Integrated Management 3 - Manager Command, Definition File and API 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 *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

2.16 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.

2.16.1 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.

2.16.2 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/jplcons  
cp -p jco_start.model any-name
```
2. Use a text editor to open the script copied in step 1 and then edit it as follows:
Before change: `EVS_HOST='hostname'`
After change: `EVS_HOST=FQDN-format-host-name`

For details about how to set the event server in the FQDN format, see the following descriptions in the *JP1/Base User's Guide*:

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

2.16.3 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 3 - Manager Administration Guide*.

2.17 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 *13.5.2 Managing the remote monitoring configuration* in the *JP1/Integrated Management 3 - 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 *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

2.17.1 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 or AIX: `/etc/ssh/sshd_config`

3. Set `yes` for `PubkeyAuthentication`^{#1}.

4. Set `no` for `UseDNS`^{#1, #2}.

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 9 example)
`systemctl restart sshd.service`
- For AIX (AIX 7.3 example)
`stopsrc -s sshd`
`startsrc -s sshd`

#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`.

(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. In addition, grant appropriate access privileges so that the private key file is not accessed by OS users without administrator privileges.
- 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 [2.17.1\(2\) 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 [2.17.1\(2\) 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 [2.17.1\(2\) 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: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 Linux) `wc -l monitored-log-file-path`

Example of executing the command:

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

Example of execution result:

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

- `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 AIX) `/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
```

2.17.2 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 (`jplcf_remote_logtrap.conf`).

```
/etc/opt/jplimm/conf/imcf/jplcf_remote_logtrap.conf
```

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

```
/opt/jplbase/bin/jbssetcnf /etc/opt/jplimm/conf/  
imcf/jplcf_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 (`jplcf_remote_logtrap.conf`)

For details, see *Remote log trap environment definition file (`jplcf_remote_logtrap.conf`)* in *Chapter 2. Definition Files in the JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

2.18 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.

2.18.1 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.

2.18.2 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 jpl_cons.service
```

Logical hosts:

```
systemctl start jpl_cons_logical-host-name.service
```

- Stopping JP1/IM - Manager

Physical hosts:

```
systemctl stop jpl_cons.service
```

Logical hosts:

```
systemctl stop jpl_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 jpl_cons.service
```

Logical hosts:

```
systemctl is-active jpl_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/jplcons/jco_start
```

```
/etc/opt/jplcons/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.`

(c) Notes about automatic stop of services

If you setup JP1/IM - Manager to terminate automatically, note the following:

- JP1/IM - Manager automatically stops only when the run level is set to 0. Thus, it does not automatically stop even if the run level is changed to single-user mode.
- To change the run level of JP1/IM - Manager, you must first stop JP1/IM - Manager, if it is running. To stop JP1/IM - Manager, you can also execute the following command to set the JP1/IM - Manager automatic stop script:

```
ln -s /etc/rc.d/init.d/jp1_cons /etc/rc.d/rc<run-level>.d/K01_JP1_80_CONS
```

2.18.3 Editing Configuration file of JP1/IM - Manager (for UNIX)

Same as for Windows. See [1.19.1 Editing Configuration file of JP1/IM - Manager \(for Windows\)](#).

2.18.4 Specifying settings for using the functions of the Intelligent Integrated Management Base (for UNIX)

When you install JP1/IM - Manager for the first time, the functions of the Intelligent Integrated Management Base are disabled by default.

To use the functions of the Intelligent Integrated Management Base, perform the following steps:

1. Set the integrated monitoring database.
2. Setup Intelligent Integrated Management Database.
3. Enable event source host mapping.
Execute `jcoimdef -hostmap ON`.
4. Enable the Intelligent Integrated Management Base service (`jddmain`).
Execute `jcoimdef -dd ON`.
5. Start JP1/IM - Manager.
6. Confirm that the Intelligent Integrated Management Base service is up and running.
Execute the `jco_spmc_status` command. Confirm that `jddmain` is displayed as an active process.

For details about the integrated monitoring database, see [2.4.2 Setting up the integrated monitoring database \(for UNIX\)](#).

For details about Intelligent Integrated Management Database, see [2.5.2 Settings of Intelligent Integrated Management Database \(for UNIX\)](#).

For details about the `jcoimdef` command, see `jcoimdef` in *Chapter 1. Commands in the JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

Important

Once you configure the Intelligent Integrated Management Base, it will take longer for the JP1/IM3-Manager service to start. If your clustering software monitors the start-up time of the JP1/IM3-Manager service or the startup control of JP1/Base is used to start the JP1/IM3-Manager service, you need to check and, if necessary, revise the timeout value of the software. After configuring the Intelligent Integrated Management Base, check the start-up time of the service and adjust the timeout value.

2.18.5 Setup When Using JP1/IM - Agent as an agent

(1) Setup for Services in JP1/IM agent management base

(a) Auto-start Setup

Follow JP1/IM - Manager auto-start settings. For details about JP1/IM - Manager auto-start settings, see [2.18.2 Setting automatic startup and automatic stop \(for UNIX\)](#).

(2) Setup Changes for JP1/IM agent management base

(a) Common way for setting

■ Edit the configuration files

See *To edit the configuration files (for Windows)* in [1.19.3\(1\)\(a\) Common way to setup](#).

(b) Change settings for JP1/IM agent management base

See [1.19.3\(1\)\(b\) Change settings of JP1/IM agent management base \(for Windows\)](#).

(c) Creating and importing IM management node tree data (required)

See [1.19.3\(1\)\(c\) Creation and import of IM management node tree data \(for Windows\) \(required\)](#).

(d) Setup for product plugin

See [1.19.3\(1\)\(d\) Settings of product plugin \(for Windows\)](#).

2.18.6 Register JP1/IM - Agent package (for Windows) (for UNIX)

You can add JP1/IM - Agent package (hereinafter it is called as JP1/IM - Agent package) to JP1/IM - Manager host. You can also add JP1/IM - Agent packages of more than one Version.

You can install JP1/IM - Agent on agent host by downloading JP1/IM - Agent packages registered on JP1/IM - Manager host without using JP1/IM - Agent offered media.

To add JP1/IM - Agent packages is optional.

(1) How to register JP1/IM - Agent Package

When you install JP1/IM - Manager on JP1/IM - Manager host, the included JP1/IM - Agent packages are registered automatically.

Important

To be able to download JP1/IM - Agent package registered to the manager host, you need to setup Intelligent Integrated Management Base.

If you upgrade and install JP1/IM - Manager on the manager host, any previous versions of JP1/IM - Agent packages that are already installed will be removed.

(2) How to delete JP1/IM - Agent Packages

If you want to delete JP1/IM - Agent package registered on the manager host, delete files of register place for JP1/IM - Agent packages as follows:

Table 2–6: Register place for JP1/IM - Agent Packages (Integrated manager Hosts (for Windows))

OS	JP1/IM - Agent packaging		
	Register place	File Name	Product name
Linux	/opt/jplimm/public/ download/imagent/	jpl_pc_agent_windows_Version number of JP1/IM - Agent (in VRRSS format). zip	JP1/IM - Agent(Windows version)
		jpl_pc_agent_linux_Version number of JP1/IM - Agent (in VRRSS format). tar.gz	JP1/IM - Agent(Linux version)

(3) How to Download JP1/IM - Agent Package

To download JP1/IM - Agent package, follow these steps:

- Prerequisites

- JP1/IM - Agent packaging is registered on the manager host.
- Setup of Intelligent Integrated Management Base is Completed.
- The JP1 user used to log in has been assigned the necessary permissions.

- Steps

1. Execute REST API of File downloads to download JP1/IM - Agent package.

To obtain a distribution (File downloading) from a JP1/IM - Manager, you need JP1 user's authentication. For details, see *5.2.8 Authentication methods for REST API* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

The following is an example of how to use OSS's curl command to obtain File in REST API of downloading File.

```
curl -OL -H "Authorization: Bearer token" -H "Cookie: JSESSIONID = Session ID" -v http://JP1/IM - Manager Host name : 20703/download/imagent/ File name
```

The token and session ID are obtained by issuing a REST API for Login.

```
curl -X POST -H "Content-Type: application/json" -d '{"user": " User name", "password": " Password"}' -v http://JP1/IM - Manager Host name :20703/im/api/v1/login
```

It is recommended to issue a REST API of Log Out immediately after completion of File acquisition.

```
curl -X POST -H "Content-Type: application/json" -H "Cookie: JSESSIONID = Session ID " -v http://JP1/IM - Manager Host name : 20703/im/api/v1/logout
```

2. Unzip the downloaded JP1/IM - Agent packages.

- For Windows

Use PowerShell to execute the following command:

```
Expand-Archive -Path jpl_pc_agent_windows_JP1/IM - Agent-version-number (V VRRSS format).zip
```

- For Linux

Use a shell to execute the following command:

```
tar -zxvf jpl_pc_agent_linux_ JP1/IM - Agent-version-number (V VRRSS format).tar.gz
```

2.18.7 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_spmd_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 JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

For details about the `jcoimdef` command, see *jcoimdef* in *Chapter 1. Commands in the JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

2.18.8 Settings for SELinux (for UNIX)

This section describes the steps required to operate JP1/IM - Manager when SELinux of Linux 8 or later is enabled.

In enabling or disabling SELinux security-context, you use semanage fcontext command and restorecon command.

(1) Setup for Auto-Start and Auto-Stop

If SELinux is enabled, the context type of jco_start and jco_stop SELinux security contexts must be set to bin_t.

Setup process is as follows:

```
# semanage fcontext -a -t bin_t '/etc/opt/jplcons/jco_start'
# semanage fcontext -a -t bin_t '/etc/opt/jplcons/jco_stop'
# restorecon -F /etc/opt/jplcons/jco_start
# restorecon -F /etc/opt/jplcons/jco_stop
```

(2) Setup for IM database

If SELinux is set to be enabled, SELinux security-context must be setup for file under the directory where IM database is installed, but IM database configuration, updating, and deletion are executed in internal operation in each command. You do not need to manually setup Individually.

In addition, enabling and disabling of SELinux security contexts are performed regardless of SELinux's enable disable Status, but you do not need to operate enabled or disabled in the same way if you change enable or disable IM database during operation after building IM database.

If setup of SELinux security-context fails, SELinux continues without stopped in error because the subsequent operation is OK even if it is in disabled status. After that, if you change SELinux to enabled Status, it becomes Error when IM database is started (including when it is started internally by commands related to IM database). If this occurs, re-execute setup of SELinux security context (Execution of jimdbupdate command) according to the handling of the error message.

- Trigger of enabling and disabling in SELinux security-context

The triggers of enabling and disabling in SELinux security-context of IM database are as follows:

Table 2–7: Enabling and Disabling triggers for IM database

Trigger	Supported Commands	Classification	Description
Newly constructed	• jcodbsetup • jcfdbsetup	Setup	Enables SELinux security-context when the command is executed regardless of status of enabling or disabling. Setup if the embedded HiRDB is not installed when the command is executed (skip if either the Integrated Monitoring DB or IM Configuration Management database is set up). When SELinux is in disabled, even if setup in SELinux security-context fails, continues without error because there is no issue with the subsequent operation. After that, if you change SELinux to enabled, it will become Error when IM database is started (including internally started commands). If this occurs, re-setup of SELinux security context (Execution of jimdbupdate command) according to the handling of the error message.
Update	jimdbupdate	Setup or re-setup	Setup or re-setup SELinux security-context automatically when the command is executed regardless of whether SELinux is disabled. If there are no HiRDB upgrades or schema changes, you can also setup SELinux security context.

Trigger	Supported Commands	Classification	Description
Delete	• jcodbunsetup • jcfdbunsetup	Delete	Delete SELinux security-context when the command is executed regardless of whether SELinux is disabled.. Delete embedded HiRDB is installed and IM Configuration Management database is not set up when the command is executed. (skip if either the integrated monitoring DB or IM Configuration Management database is not set up).

- Notes on upgrading JP1/IM - Manager from Version prior to 13-00 to 13-00 or later

If you are upgrading JP1/IM - Manager from a Version earlier than 13-00 to 13-00 or later when IM database is setup, be sure to execute jimdbupdate command and update IM database before making SELinux enabled.

Because JP1/IM - Manager pre-13-00 Version does not setup SELinux security context to IM database, SELinux security context remains unset until you execute the jimdbupdate command. Therefore, if you turn enable SELinux in this status, IM database fails to start and displays an error message prompting you to execute jimdbupdate command.

- Setup Target Directories for SELinux Security Contexts

The following are the target directory which SELinux security contexts is set when /var/opt/jplimm/dbms/JM0 (the default path of IM database for Physical host[#]) is assumed for install destination directory of IM database and SELinux security context type which is set in files under the directory:

[#]: Replace the path as necessary.

Target directory	Types of SELinux security contexts to Setup to the underlying File
Under /var/opt/jplimm/dbms/JM0	user_t
Under /var/opt/jplimm/dbms/JM0/bin	bin_t
Under /var/opt/jplimm/dbms/JM0/lib	lib_t
Under /var/opt/jplimm/dbms/JM0/bin/servers	bin_t

The path to the directory where IM database is installed is different for Physical host and Logical host as follows.

- For Physical host
Follow the definition of setup information file (jimdbsetupinfo.conf) for the IM database setup for Physical host. The path is " Value of IMDBENVDIR /JM0".
- For Logical host
Follow the definition of cluster IM database setup information file (jimdbclustersetupinfo.conf) for the IM database setup for logical host. The path is " the value of **IMDBENVDIR**/the value of **JMLOGICALHOSTNUMBER**".

(3) Setup for Intelligent Integrated Management Database

If SELinux is set to be enabled, SELinux security-context must be setup for file under the directory where Intelligent Integrated Management Database is installed, but Intelligent Integrated Management Database configuration, updating, and deletion are executed in internal operation in each command. You do not need to manually setup Individually.

In addition, enabling and disabling of SELinux security contexts are performed regardless of SELinux's enable disable status, but you do not need to operate enabled or disabled in the same way if you change enable or disable IM database during operation after building Intelligent Integrated Management Database.

If setup of SELinux security-context fails, SELinux continues without stopped in error because the subsequent operation is OK even if it is in disabled status. If you change SELinux to enabled status, it will not become error after that.

- Trigger of enabling and disabling in SELinux security-context

The triggers of enabling and disabling in SELinux security-context of Intelligent Integrated Management Database are as follows:

Table 2–8: Setup and Delete triggers for Intelligent Integrated Management Database

Trigger	Supported Commands	Classification	Description
Newly constructed	jimgndbsetup	Setup	SELinux security-context is setup automatically when the command is executed regardless of SELinux is enabled or disabled.
Delete	jimgndbunsetup	Delete	SELinux security-context is deleted automatically when the command is executed regardless of SELinux is enabled or disabled.

- Setup Target Directories for SELinux Security Contexts

The following are the target directory which SELinux security contexts is set when `"/var/opt/jplimm/dbms/imgndbbin/pgsql"` (the default path of Intelligent Integrated Management Database for Physical host[#]) is assumed for install destination directory of Intelligent Integrated Management Database and SELinux security context type which is set in files under the directory:

[#]: Replace the path as necessary.

Target directory	Types of SELinux security contexts to Setup to the underlying File
Under <code>/var/opt/jplimm/dbms/imgndbbin/pgsql</code>	<code>postgresql_db_t</code>

The path to the directory where Intelligent Integrated Management Database is installed is different for Physical host and Logical host as follows.

- For Physical host

Follow the definition of setup information file (`jimdbsetupinfo.conf`) for the Intelligent Integrated Management Database setup for Physical host. The path is " Value of `IMDBENVDIR/imgndbbin/pgsql` ".

- For Logical host

Follow the definition of cluster Intelligent Integrated Management Database setup information file (`jimdbclustersetupinfo.conf`) for the Intelligent Integrated Management Database setup for logical host. The path is " the value of `IMDBENVDIR` / the value of `/imgndbbinLOGICALHOSTNUMBER/pgsql`".

2.18.9 Suppressing Message to be output to the system log (syslog)

When the Linux version of JP1/IM - Manager is running, messages are repeatedly output to the system log (syslog) of the OS (Linux). For this reason, pay close attention to the capacity of the system log and the interval between log rotation (switching), and take measures such as increasing the disk space or shortening the log rotation interval as necessary.

For example, on Linux 8, the following message is output to the system log:

- The `/var/log/messages` file

```
Feb  8 13:11:17 RHEL-8 su[17358]: (to imdbuser) root on pts/4
```

- The `/var/log/secure` file

```
Feb  8 13:12:38 RHEL-8 su[17462]: pam_systemd(su-l:session): Cannot create session: Already running in a session or user slice
Feb  8 13:12:38 RHEL-8 su[17462]: pam_unix(su-l:session): session opened for user imdbuser by root(uid=0)
Feb  8 13:12:38 RHEL-8 su[17462]: pam_unix(su-l:session): session closed for user imdbuser
```

If you do not need to monitor these messages, you can suppress them from being output to the system log. Please note that changing the settings of the system log affects the entire system (Linux environment). For details on suppressing output to the system log, refer to the documentation related to the OS.

2.18.10 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 *12.3 Data that needs to be collected when a problem occurs* in the *JP1/Integrated Management 3 - Manager Administration Guide*.

About the data collection tool

- About `jim_log.sh`

See `jim_log.sh` (UNIX only) in *Chapter 1. Commands* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API 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)

In kernel parameter of Linux (`kernel.core_pattern`), when the output destination of core dump file is set to directory other than collection-target log file directory, or when the name of the core dump file is changed from the default setting, the data collection tool would not be able to acquire the core dump file when the tool is executed.

The data collection tool collects files whose file names start with `core` in the following default collection-target log file directories.

For physical hosts:

- `/var/opt/jplcons/log/`
- `/var/opt/jplscope/log/`
- `/var/opt/jplimm/log/imcf/`
- `/var/opt/jplimm/log/imdb/`
- `/var/opt/jplimm/log/imdd/`

For logical hosts:

- `shared-directory/jplcons/log/`
- `shared-directory/jplsocpe/log/`
- `shared-directory/jplimm/log/imcf/`
- `shared-directory/jplimm/log/imdb/`
- `shared-directory/jplimm/log/imdd/`

Depending on the setting of `kernel.core_pattern`, it might be necessary to check and address the following points before executing the data collection tool. The default setting values vary depending on the OS version, so be sure to check the setting values.

- When the output directory for a core dump file is not the collection-target log file directory
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`.
- When core dump files are compressed
Uncompress the core dump files.

(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.

(d) The systemd settings related to core dump files (Linux only)

These settings apply to Linux environments where the settings file for core dump file names (`/proc/sys/kernel/core_pattern`) begins with the character string "`|/usr/lib/systemd/systemd-coredump`".

If the operation settings file for core dump files (`/etc/systemd/coredump.conf`) includes a setting that specifies that no core dump files are to be created, no core dump file will be output and users will not be able to investigate the failure in situations such as when a segmentation fault or a bus failure occurs in a JP1/IM - Manager process, or when the `jcogencore` command is executed.

Based on operations to be performed, revise the settings in the operation settings file for core dump files (`/etc/systemd/coredump.conf`) so that core dump files are created. For details, see the documentation for your Linux.

(e) Notes for SUSE Linux

In SUSE Linux Enterprise Server 12 SP2, when the `jcogencore` command is used to output a core dump file, the core dump file is not output to the directory storing the command, and either

of the following messages is output:

- KAVB8428-W The core dump file was not found.
- KAVB8408-E The specified process is not running.

The following procedure assumes that core dump files are set to be output to `/var/lib/systemd/coredump/`.

1. From `/var/lib/systemd/coredump/`, copy the files that contain the JP1/IM - Manager execution file name with the timestamp corresponding to the time when the `jcogencore` command was executed. Copy these files to the applicable copy-direction directory as follows.

No	JP1/IM - Manager execution file name	Copy-destination directory for each execution file	
		Physical host	Logical host
1	evflow	/var/opt/jp1cons/log/	<shared-directory>/jp1cons/log/
2	jcain		
3	evtcon		
4	evgen		
5	jcdmain		
6	jcfmain	/var/opt/jp1imm/log/imcf/	<shared-directory>/jp1cons/log/
7	jcfalllogtrap		

2. If the file is a compressed file, decompress the file. (If the file is not a compressed file, go to step 3.) If the extension of the copied file is `.xz`, use the following command to decompress the file:
`unxz <file-path-copied-in-step-1>`
3. Rename the files as follows.

No	Original file name (by default)	New file name
1	File name that begins with "core.evflow."	core.evflow
2	File name that begins with "core.jcamain."	core.jcamain
3	File name that begins with "core.evtcon"	core.java
4	File name that begins with "core.evgen"	core.evgen
5	File name that begins with "core.jcdmain "	core.jcdmain
6	File name that begins with "core.jcfmain"	core.jcfmain
7	File name that begins with "core.jcfallogtrap"	core.<PID>.jcfallogtrap [#]

#: For <PID>, specify the PID of the original file. The original file names conform to the following naming convention. (Exclude the extension ".xz" if the file is not a compressed file.) core.<execution-file-name>.<real-UID>.<boot-ID>.<PID>.<total-seconds>.xz

In the following file name, the PID is 1378.

core.jcfallogtrap.0.71abdba3becd450a8ac5c4469dfcd648.1378.1493089252000000.xz

(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_spmc_reload
```

About process restart definition

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

See *Extended startup process definition file (jplco_service.conf)* in Chapter 2. Definition Files in the JP1/Integrated Management 3 - Manager Command, Definition File and API 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 JP1/Integrated Management 3 - Manager Command, Definition File and API 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 JP1/Integrated Management 3 - Manager Command, Definition File and API Reference.

- About the `jcohctest` command

See *jcohctest* in Chapter 1. Commands in the JP1/Integrated Management 3 - Manager Command, Definition File and API 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 *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

3. Start JP1/IM - Manager.

2.18.11 Specifying settings for upgrading (for UNIX)

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

If you are using IM database, you must update IM database by referring to "[2.4.5 Updating IM databases \(for UNIX\)](#)".

(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 4.2.2 *Event acquisition filter* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.
- About the `jcochafmode` command
See *jcochafmode (UNIX only)* in *Chapter 1. Commands* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

(2) Executing the Central Scope upgrade command

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

To execute the Central Scope upgrade command:

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

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

`/var/opt/jplscope/database/jcsdb/`

3. Execute the `jplcsverup` command.
4. Execute the `jbssetcnf` command.

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

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

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

Table 2–9: 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 `jplcsverup` command
See *jplcsverup (UNIX only)* in *Chapter 1. Commands* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API 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/jplcons/conf/action/actdef.conf`
For a logical host: `shared-directory/jplcons/conf/action/actdef.conf`
4. Start JP1/IM - Manager.
 - About the automated action function
See *Chapter 6. Command Execution by Automated Action (JP1/Base linkage)* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.
 - About the `jcadefconv` command
See `jcadefconv` in *Chapter 1. Commands* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API 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 *3.33.1 Action Parameter Detailed Definitions window* in the *JP1/Integrated Management 3 - 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 *JP1/Integrated Management 3 - Manager Command, Definition File and API 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 *JP1/Integrated Management 3 - Manager Command, Definition File and API 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 *JP1/Integrated Management 3 - Manager Command, Definition File and API 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 *JP1/Integrated Management 3 - Manager Command, Definition File and API 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 *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

(9) Upgrading the Intelligent Integrated Management Base (forUNIX)

If you are using the Intelligent Integrated Management Base, you can upgrade it as follows:

Note that if you want to perform the version upgrade install of the linked products at the same time, execute the version upgrade install of the linked products before performing step 5.

1. Terminate JP1/IM - Manager.
2. When upgrading JP1/IM - Manager from version 12-50 or earlier, construct the Intelligent Integrated Management Database.
For details, see [2.5 Construction of Intelligent Integrated Management Database \(for UNIX\)](#).
3. Add new settings.
Add new settings corresponding to the new functions you are going to use.[#]

#

If you upgrade JP1/IM -Manager from 13-00 or 13-01 to 13-10 or later, add the line "web-enable-admin-api: true" to the end of the following file in a text editor, etc.

When upgrading JP1/IM - Manager from 13-00 or 13-01 to 13-10 or later, add three lines ("web-enable-admin-api: true", "db-connections-max: 50", "db-writer-connection-concurrency: 1" (underlined part of "after change" below) to the end of the following file in a text editor. When the Intelligent Integrated Management database is rebuilt, this procedure is not required because it is added automatically.

- For physical hosts: /etc/opt/jplimm/conf/imgndb/config.yml

- For logical hosts: *shared-directory*/jplimm/conf/imgndb/config.yml

<Example of change>

- Before change

```
db-host: localhost
db-name: imgndb
db-user: imuser
db-password: rCKsdJ8vSQn2
db-port: 20705
web-listen-address: localhost:20706
log-level: info
db-ssl-mode: allow
promql-max-points-per-ts: 30001
```

- After change

```
db-host: localhost
db-name: imgndb
db-user: imuser
db-password: rCKsdJ8vSQn2
db-port: 20705
web-listen-address: localhost:20706
log-level: info
db-ssl-mode: allow
promql-max-points-per-ts: 30001
web-enable-admin-api: true
db-connections-max: 50
db-writer-connection-concurrency: 1
```

If you do not add a "web-enable-admin-api: true" line, deleting the trend data and deleting integrated agent info will fail.

For details about deleting trend data and integrated agent information, see *2.2.1 List of Integrated Agents window* in the *JP1/Integrated Management 3 - Manager GUI Reference* and see *5.11.4 Delete Trend Data* and *5.18.2 Delete integrated agent info* in the *JP1/Integrated Management 3 -Manager Command, Definition File and API Reference*.

If you do not add the "db-connections-max: 50" and "db-writer-connection-concurrency: 1" rows, the following events may occur when collecting a large amount of performance data (when the sum of sample collected by integrated agent in the system (in the system of lower manager in a multi-stage configuration) exceeds 10,000 seconds):

- Performance data is not saved in Intelligent Integrated Management Database and cannot be displayed and retrieved

- Trend data management service memory usage increases

4. Start JP1/IM - Manager.

5. Execute the `jddcreatetree` command.

6. Execute the `jddupdatetree` command in new and rebuilding mode.

- `jddcreatetree` command

For details, see `jddcreatetree` in *Chapter 1. Commands* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

- `jddupdatetree` command

For details, see `jddupdatetree` in *Chapter 1. Commands* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

Unless you upgrade the Intelligent Integrated Management Base, you cannot use the functionality provided by Intelligent Integrated Management Base 13-00.

(10) Upgrading Intelligent Integrated Management Database version (for UNIX)

This section describes the settings required during a version upgrade when using Intelligent Integrated Management Database.

If you have upgraded JP1/IM - Manager from version 13-10 or earlier and you are using Intelligent Integrated Management Database, you must execute `jimgndbupdate` command.

If you want to see the current version of the Intelligent Integrated Management Database, you must execute `jimgndbsetup` command with the `"-display"` parameter. Also, when the Intelligent Integrated Management Database is versioned as "No Data" or "131100", `jimgndbupdate` command must be executed.

For details about `jimgndbsetup` command and `jimgndbupdate` command, see `jimgndbsetup` in *Chapter 1. Commands* and `jimgndbupdate` in *Chapter 1. Commands* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

(11) Updating extended startup process definition file

If you upgraded from JP1/IM - Manager version 11 or earlier, add `jddmain`, `imbase`, `imbaseproxy` process-definition to extended startup process definition file (`jp1co_service.conf`).

When upgrading from version 12, add `imbase`, `imbaseproxy` process-definition.

For details about extended startup process definition file, see *Extended startup process definition file (jp1co_service.conf)* in *Chapter 2. Definition Files* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

2.19 Setup for JP1/IM - Agent (for UNIX)

2.19.1 Setup for JP1/IM - Agent servicing

(1) Enable or disable add-on program

This section explains how to enable or disable add-on program. JP1/IM - Agent contains more than one add-on programs and can only start services that are enabled.

(a) Enable add-on programs

- To setup when installing

In initial setting command to use when installing, select add-on program that you want to enable.

For details, see 3.15.9 *Initial setting command* in the *JP1/Integrated Management 3 - Manager Deployment and Design Guide*.

During the version upgrade installation, the existing settings are inherited. However, add-on programs that is newly added in new Version are in the disabled Status.

- To setup after installing

The following are the steps to enable add-on program services for a JP1/IM - Agent:

1. If the service is running, execute the following command to terminate.

```
/opt/jplima/tools/jpc_service_stop -s all
```

2. Execute the following command to enable the service.

```
/opt/jplima/tools/jpc_service -on [Service-key-of-JP1/IM-Agent]
```

3. Move the discovery configuration file corresponding to the service.

Move the discovery configuration file corresponding to the following services from the `/opt/jplima/conf/jpc_file_sd_config_off` directory to `/opt/jplima/conf` directory:

Service	Discovery configuration file
prometheus_server	None
alertmanager	None
node_exporter	jpc_file_sd_config_node.yml
blackbox_exporter	• jpc_file_sd_config_blackbox_http.yml • jpc_file_sd_config_blackbox_icmp.yml
ya_cloudwatch_exporter	jpc_file_sd_config_cloudwatch.yml
fluentd	None
process_exporter	jpc_file_sd_config_process.yml
promitor	jpc_file_sd_config_promitor.yml
script_exporter	None

4. Verify that the service is enabled.

Execute `systemctl list-unit-files` command. It is enabled if value of STATE of the corresponding service is not "masked".

5. Perform [2.19.2\(18\) Creating and importing IM management node tree data \(for Linux\) \(required\)](#).

(b) Disabling add-on program

The following are the steps to disable service of add-on program for a JP1/IM - Agent:

1. If the service is running, execute the following command to terminate.

```
/opt/jplima/tools/jpc_service_stop -s all
```

2. Disable the service by execute the following command:

```
/opt/jplima/tools/jpc_service -off [Service-key-of-JP1/IM-Agent]
```

3. Move the discovery configuration file corresponding to the service.

Move the discovery configuration file corresponding to the following services from the `/opt/jplima/conf/jpc_file_sd_config_off` directory to `/opt/jplima/conf` directory:

Service	Discovery configuration file
prometheus_server	None
alertmanager	None
node_exporter	jpc_file_sd_config_node.yml
blackbox_exporter	- jpc_file_sd_config_blackbox_http.yml - jpc_file_sd_config_blackbox_icmp.yml
ya_cloudwatch_exporter	jpc_file_sd_config_cloudwatch.yml
fluentd	None
process_exporter	jpc_file_sd_config_process.yml
promitor	jpc_file_sd_config_promitor.yml
script_exporter	None

4. Verify that the service is disabled.

Execute `systemctl list-unit-files` command. It is disabled if value of STATE of the corresponding service is "masked".

(2) Enable and Disable of Auto-start

(a) Enable for Auto-start

To enable the service-auto-start when OS starts, follow these steps:

1. Execute the following command to enable all the auto-start of services on JP1/IM - Agent.

```
jpc_service_autostart -on
```

(b) Disable for Auto-start

To disable the service-auto-start when OS starts, follow these steps:

1. Execute the following command to disable all the auto-start of services on JP1/IM - Agent.

```
jpc_service_autostart -off
```

(c) How to Check Automatic Start and Stop

Check with the following command.

```
systemctl list-unit-files
```

If value of the corresponding service's STATE is "enabled," it is enable. It is disabled if it is "disabled". For details about the service name, see *2.9 Service of JP1/IM - Agent* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*

(d) Notes on Automatically Stopping During OS Shutdown

Although integrated agent service is stopped when shuts down Linux while integrated agent service is running, /var/log/messages file may not receive an message indicating that integrated agent service is stopped.

(3) How to start and stop manually

To start or stop JP1/IM - Agent manually, use the following command:

Table 2–10: Start/stop command

Command	Description
jpc_service_start	Start the Agent service.
jpc_service_stop	Stop the Agent service.

For details of the command, see *Chapter 1. Commands* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

(4) How to check Startup status of a service

Check with the following command.

```
systemctl list-units --all --type=service
```

Starting if ACTIVE column is "active", otherwise it is Stopped.

(5) Location of configuration file

Place systemd's unit definition file in the following location:

For details about the unit definition file, see *Unit definition file (jpc_program-name.service)* in *Chapter 2. Definition Files* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

Table 2–11: Location of unit definition file for systemd

Location (path)	Typical Uses	Layout method
/opt/jplima/conf/ (For Physical host)	Model file (unit definition file template) Do not edit the model file.	Place in the installer.
Shared-disk/jplima/conf/ (For Logical host)	Model file (unit definition file template) Do not edit the model file.	Place manually.
/usr/lib/systemd/system/	Unit definition file main unit. Edit this file. Systemd uses this file.	It is initial setting command for the physical host and manually for the logical host.

(6) Configuration file editing

If you want to change setup of a service, you can do so by editing unit definition file. If you have edited unit definition file, to reflect definition, you need to execute the following command with a user who has root permission:

```
systemctl daemon-reload
```

2.19.2 Settings of JP1/IM - Agent

(1) Common way for setting

(a) Edit the configuration files (for Linux)

See [1.21.2\(1\)\(a\) Edit the configuration files \(for Windows\)](#).

(b) Changing unit definition file (for Linux only)

The following lists unit definition file storage locations and filenames:

- Storage destination: /usr/lib/systemd/system/
- File name: jpc_ Service name.service

To change unit definition file, follow these steps:

1. Login to integrated agent host.
2. Stop JP1/IM - Agent service.
3. Edit unit definition file.
4. Execute the following command to reflect the unit definition.

```
# systemctl daemon-reload
```

5. Start JP1/IM - Agent service.

(c) Change command-line options (for Linux)

On ExecStart line of unit definition file, change the command-line options.

For editing methods, see *2.19.2(1)(b) Changing unit definition file (for Linux only)*.

(2) Setup for JP1/IM agent control base

(a) Change Integrated manager to connect to (for Linux) (optional)

See *1.21.2(2)(a) Change Integrated manager to connect to (for Windows) (optional)*.

(b) Changing Ports (for Linux) (optional)

See *1.21.2(2)(b) Change the port (for Windows) (optional)*.

(c) Deploy a CA certificate (for Linux) (optional)

See *1.21.2(2)(c) Place CA certificate (for Windows) (optional)*.

(d) Modify settings related to Action Execution (on Linux) (optional)

See *1.21.2(2)(d) Modify settings related to Action Execution (for Windows) (optional)*.

(e) Setup the proxy authentication's authentication ID and Password (optional)

See *1.21.2(2)(e) Setup the proxy authentication's authentication ID and Password (for Windows) (optional)*.

(f) Change the user of Action Execution (for Linux) (required)

Change action.username in imagent configuration file (jpc_imagent.json).

For setup procedure, see *2.19.2(1)(a) Edit the configuration files (for Linux)*.

(g) Configuring the event-forwarding relay function (for Linux) (optional)

See *1.21.2(2)(g) Configuring the event-forwarding relay function (for Windows) (optional)*.

(h) Setting the data delivery function to multiple manager hosts (for Linux) (optional)

■ New setting

1. Shut down JP1/IM - Agent servicing.

The service key of the service to be stopped is shown below.

- jpc_imagent
- jpc_imagentaction
- jpc_imagentproxy
- jpc_alertmanager
- jpc_prometheus_server
- jpc_fluentd

2. Create a directory for the secondary of JP1/IM agent management base.

Create the following directory as the directory for the secondary of JP1/IM agent management base:

- /opt/jplima/tmp/download-imagent-group-identifier
- /opt/jplima/tmp/upload-imagent-group-identifier

- /opt/jplima/tmp/jbsfwd-*imagent-group-identifier*
- /opt/jplima/logs/imagent-*imagent-group-identifier*
- /opt/jplima/logs/imagentproxy-*imagent-group-identifier*
- /opt/jplima/logs/imagentaction-*imagent-group-identifier*

To create the above directory, use the following command:

```
mkdir-m 700 directory
chown-R root:root directory
```

3. Create a unit definition file for JP1/IM agent management base secondary.

Copy the source unit definition file at the bottom of /usr/lib/systemd/system and rename it to the destination filename.

The owner and owner group of the created unit definition file must have root, accessibility of 644.

Source file name	Destination file name
jpc_imagent.service	jpc_imagent- <i>imagent-group-identifier</i> .service
jpc_imagentproxy.service	jpc_imagentproxy- <i>imagent-group-identifier</i> .service
jpc_imagentaction.service	jpc_imagentaction- <i>imagent-group-identifier</i> .service

4. Configure settings for JP1/IM agent control base secondary.

See 3.15.7(5)(d) *configuration file of JP1/IM agent control base* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

5. Register a secret for the secondary of JP1/IM agent control base.

Obtain and register initial secret of JP1/IM - Manager to which the secondary JP1/IM agent control base connects. If you connect to JP1/IM - Manager through a HTTP proxy server that requires password-based HTTP authentication (Basic authentication), register HTTP proxy password as secret.

For the key of initial secret to register and the key of HTTP proxy password, see 3.15.7(5)(e) *Keys for initial secret, client secret, and HTTP proxy password* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

6. Perform settings other than JP1/IM agent control base.

See 3.15.7(5)(f) *Send settings for programs other than JP1/IM agent control base* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

7. Configure the service startup settings.

See 3.15.7(5)(c) *Configuring secondary service startup* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

8. Refresh systemd.

Run the following command:

```
systemctl daemon-reload
```

9. Run systemctl list-unit-files and activate the service by running the following command for a secondary service whose service status is masked:

```
/opt/jplima/tools/jpc_service -on service-key
```

For the service key, use the service key of JP1/IM - Agent in Linux described in *10.1 JP1/IM - Agent Service* in the *JP1/Integrated Management 3 - Manager Administration Guide* with the `-imagent-group-identifier`.

10. Start JP1/IM - Agent servicing.

The service key of the service to be stopped is shown below.

- `jpc_imagent`
- `jpc_imagentaction`
- `jpc_imagentproxy`
- `jpc_imagent-imagent-group-identifier`
- `jpc_imagentaction-imagent-group-identifier`
- `jpc_imagentproxy-imagent-group-identifier`
- `jpc_alertmanager`
- `jpc_prometheus_server`
- `jpc_fluentd`

11. Set auto start at OS startup.

For details about enabling auto start, see *2.19.1(2)(a) Enable for Auto-start*.

(i) Deactivating the data delivery function to multiple manager hosts (for Linux) (optional)

The following describes the procedure for configuring the data delivery function to multiple manager hosts when the data delivery function is no longer used.

Perform one of the following depending on your operating environment.

- Remove only the data delivery function to multiple manager hosts without uninstalling JP1/IM - Agent
- Uninstall JP1/IM - Agent itself.

■ To remove only the data delivery function to multiple manager hosts without uninstalling JP1/IM - Agent

1. Stop all JP1/IM - Agent servicing.

If the service is running, execute the following command to stop it.

```
/opt/jplima/tools/jpc_service_stop -s all
```

2. Enable the secondary service.

Enable the secondary services for JP1/IM agent control base by running the following command:

```
/opt/jplima/tools/jpc_service -off service-key
```

For how to enable the service, see step 2 and step 4 in *2.19.1(1)(a) Enable add-on programs*.

For the service key, use the service key of JP1/IM - Agent in Linux described in *10.1 Service of JP1/IM - Agent* in the *JP1/Integrated Management 3 - Manager Administration Guide* with the `-imagent-group-identifier`.

3. Delete the secret that you created to use the data delivery function to multiple manager hosts.

Remove the secret for JP1/IM agent control base secondary you registered in step 5 of *2.19.2(2)(h) Setting the data delivery function to multiple manager hosts (for Linux) (optional)*.

For the key of the secret to be deleted, see *3.15.7(5)(e) initial secret, client secret, and HTTP Proxy Password Keys* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

This step is not necessary for secrets that have already been deleted.

4. Restores the settings for using the data delivery function to multiple manager hosts.

2.19.2(2)(h) Setting the data delivery function to multiple manager hosts (for Linux) (optional). Restores the settings for the secondary JP1/IM agent control base that were set in step 4.

5. Delete the files copied to use the data delivery function to multiple manager hosts.

Remove unit definition file for the secondary JP1/IM agent management base that you copied in step 3 of *2.19.2(2)(h) Setting the data delivery function to multiple manager hosts (for Linux) (optional)*.

6. Delete the directory created to use the data delivery function to multiple manager hosts.

After saving the log and other required files, delete the directory for the secondary JP1/IM agent management base created in step 2 of *2.19.2(2)(h) Setting the data delivery function to multiple manager hosts (for Linux) (optional)*.

7. Refresh systemd.

Run the following command:

```
systemctl daemon-reload
```

8. Deletes integrated agent registered on JP1/IM - Manager to which the disabled secondary service is connected.

For details on deleting integrated agent data, see *2.2.1 List of Integrated Agents window* in the *JP1/Integrated Management 3 - Manager GUI Reference*.

■ When uninstalling JP1/IM - Agent

Follow the procedure from step 3 to step 6 in *To remove only the data delivery function to multiple manager hosts without uninstalling JP1/IM - Agent* above between steps 1 and 2 in *2.23.1(4) Steps for uninstalling JP1/IM - Agent*.

Follow step 8 in *To remove only data delivery function to multiple manager hosts without uninstalling JP1/IM - Agent* above.

(3) Setup of Prometheus server

(a) Changing Ports (for Linux) (optional)

The listen port used by Prometheus server is specified in `--web.listen-address` option of `prometheus` command.

For details about how to change `prometheus` command options, see *2.19.2(1)(c) Change command-line options (for Linux)*. For details of `--web.listen-address` option, see *If you want to change command line options in Unit definition file (jpc_program-name.service)* in Chapter 2. *Definition Files* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

The default port is "20713". If port number is changed, review setup of the firewall and prohibit accessing from outside. However, if you want to monitor Prometheus server with external shape monitoring by Blackbox exporter in other host, allow it to be accessed. In such cases, consider security measures such as limiting the source IP address as required.

(b) Add the alert definition (for Linux) (optional)

See *1.21.2(3)(b) To Add the alert definition (for Windows) (optional)*.

(c) Add a Blackbox exporter scrape job (for Linux) (optional)

See [1.21.2\(3\)\(c\) Add Blackbox exporter scrape job \(for Windows\) \(optional\)](#).

(d) Add a user-defined Exporter scrape job (for Linux) (optional)

See [1.21.2\(3\)\(d\) Add user-defined Exporter scrape job \(for Windows\) \(optional\)](#).

(e) Change RemoteWrite destination (for Linux) (optional)

See [1.21.2\(3\)\(e\) Changing Remote Write destination \(for Windows\) \(optional\)](#).

(f) Configuring service monitor settings (for Linux) (optional)

To use the service monitoring function in an environment where the version is upgraded and installed from JP1/IM - Agent 13-00 to 13-01 or later, configure the following settings. This setting is not required if JP1/IM - Agent 13-01 or later is newly installed.

■ Editing Prometheus configuration file (jpc_prometheus_server.yml)

If "node_systemd_unit_state" is not set to Keep metric in the metric_relabel_configs settings of the jpc_node scrape job, add the settings. Also, if the same metric_relabel_configs configuration does not have a relabel config for the "node_systemd_unit_state" metric, add the configuration. Add the underlined settings as follows.

```
(Omitted)
scrape_configs:
(Omitted)
  - job_name: 'jpc_node'
(Omitted)
    metric_relabel_configs:
      - source_labels: ['__name__']
        regex: 'node_network_receive_bytes_total|node_network_transmit_bytes_total|-- Omitted --|node_vmstat_pswpin|node_vmstat_pswpout|node_systemd_unit_state'
        action: 'keep'
      - source_labels: ['__name__']
        regex: 'node_systemd_unit.*'
        target_label: 'jpl_pc_trendname'
        replacement: 'node_exporter_service'
      - source_labels: ['__name__']
        regex: 'node_systemd_unit.*'
        target_label: 'jpl_pc_category'
        replacement: 'service'
      - source_labels: ['__name__', 'name']
        regex: 'node_systemd_unit.*;(.*)'
        target_label: 'jpl_pc_nodelabel'
        replacement: ${1}
      - regex: jpl_pc_multiple_node
        action: labeldrop
```

■ Editing Node exporter discovery configuration file (jpc_file_sd_config_node.yml)

If the jpl_pc_multiple_node is not set, add the underlined settings as follows.

```
- targets:
  - hostname:20716
  labels:
```

```
jp1_pc_exporter: JPC Node exporter
jp1_pc_category: platform
jp1_pc_trendname: node_exporter
jp1_pc_multiple_node: "{__name__=~'node_systemd_unit_.*'}"
```

(g) Set when the IM management node label name (jp1_pc_nodelabel value) exceeds the upper limit (for Linux) (optional)

See [1.21.2\(3\)\(g\) Configure the settings when the label name \(jp1_pc_nodelabel value\) of the IM management node exceeds the upper limit \(for Windows\) \(optional\)](#).

(h) Setting for executing the SAP system log extract command using Script exporter (for Linux) (optional)

See [1.21.2\(3\)\(h\) Setting for executing the SAP system log extract command using Script exporter \(for Windows\) \(optional\)](#).

(i) Add a VMware exporter scrape job (for Linux) (optional)

See [1.21.2\(3\)\(j\) Add a VMware exporter scrape job \(for Windows only\) \(optional\)](#).

(4) Setup of Alertmanager

(a) Changing Ports (For Linux) (optional)

The listen port used by Alertmanager is specified in `--web.listen-address` option of `alertmanager` command.

For details about how to change alertmanager command options, see [2.19.2\(1\)\(c\) Change command-line options \(for Linux\)](#). For details of `--web.listen-address` option, see *If you want to change command line options in Unit definition file (jpc_program-name.service) in Chapter 2. Definition Files in the JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

The default port is "20714". If port number is changed, review setup of the firewall and prohibit accessing from outside. However, if you want to monitor Alertmanager with external shape monitoring by Blackbox exporter in other host, allow it to be accessed. In such cases, consider security measures such as limiting the source IP address as required.

(b) Changing the alert notification destination (for Linux) (optional)

See [1.21.2\(4\)\(b\) Changing the alert notification destination \(for Windows\) \(optional\)](#).

(c) Setup silence (on Linux) (optional)

See [1.21.2\(4\)\(c\) Setup silence \(for Windows\) \(optional\)](#).

(5) Setup of Node exporter

(a) Changing Ports (optional)

The listen port used by Node exporter is specified in `--web.listen-address` option of `node_exporter` command.

For details about how to change the options of the `node_exporter` command, see [2.19.2\(1\)\(c\) Change command-line options \(for Linux\)](#). For details of `--web.listen-address` option, see *If you want to change command line options*

in *Unit definition file (jpc_program-name.service)* in *Chapter 2. Definition Files in the JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

The default port is "20716". If port number is changed, review setup of the firewall and prohibit accessing from outside.

(b) Change metric to collect (optional)

1. In the `metric_relabel_configs` of Prometheus configuration file (`jpc_prometheus_server.yml`), metric to be collected are defined separated by "|". Delete metric that you do not need to collect and add metric that you want to collect.

For instructions on updating configuration file, see [1.21.2\(1\)\(a\) Edit the configuration files \(for Windows\)](#).

<Sample Setup>

```
- job_name: 'jpc_node'
  :
  metric_relabel_configs:
    - source_labels: ['__name__']
      regex: 'node_boot_time_seconds|node_context_switches_total|node_cp
u_seconds_total|node_disk_io_now|node_disk_io_time_seconds_total|node_disk
_read_bytes_total|node_disk_reads_completed_total|.....|node_time_second
s|node_uname_info|node_vmstat_pswpin|node_vmstat_pswpout [Add metric here
]'
    action: 'keep'
```

2. If required, define a trend view in metric definition file.

In Node exporter metric definition file, you define a trend view.

For descriptions, see *Node exporter metric definition file (metrics_node_exporter.conf)* in *Chapter 2. Definition Files in the JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

3. Configure the service monitor settings.

- Editing Node exporter's unit definition file (`jpc_node_exporter.service`).

When monitoring services, edit the unit definition file (`jpc_node_exporter.service`) of Node exporter as shown in the underlined part below.

```
[Unit]
Description = JP1/IM3-Agent Linux metric collector
After=local-fs.target remote-fs.target rsyslog.service network.target
[Service]
WorkingDirectory = @@installdir2@@/jplima/bin
ExecStart = /bin/sh -c '"@@installdir1@@/jplima/bin/node_exporter" \
  --collector.cpu.info \
(Omitted)
  --no-collector.supervisord \
  --collector.systemd \
  --collector.systemd.unit-include="Regular expressions to match unit fil
e names" \
  --no-collector.tcpstat \
  --no-collector.textfile \
  --no-collector.thermal_zone \
(Omitted)
```

If "--no-collector.systemd" is set as the value of the argument to be set on the ExecStart line, change it to "--collector.systemd". If "--collector.systemd.unit-include" is not set, add a line and set the value to a regular expression that matches the unit file name of the unit you want to monitor.

Depending on how regular expressions are specified, it may take some time to collect performance information. For details, see *G.4 Tips on using regular expressions* section in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

- Node exporter unit definition file (jpc_node_exporter.service) definition example

The following shows a sample configuration for monitoring jpc_imagent.service and jpc_imagentproxy.service units.

```
[Unit]
Description = JP1/IM3-Agent Linux metric collector
After=local-fs.target remote-fs.target rsyslog.service network.target
[Service]
WorkingDirectory = @@installdir2@@/jplima/bin
ExecStart = /bin/sh -c '"@@installdir1@@/jplima/bin/node_exporter" \
  --collector.cpu.info \
(Omitted)
  --no-collector.supervisord \
  --collector.systemd \
  --collector.systemd.unit-include="^(jpc_imagent|jpc_imagentproxy)\.service$" \
  --no-collector.tcpstat \
  --no-collector.textfile \
  --no-collector.thermal_zone \
(Omitted)
```

Among the units that correspond to the above specification, the units for which automatic startup is enabled or the status is being executed are monitored. For details, see the *Specifying monitored services* in 3.15.1(1)(d) *Node exporter (Linux performance data collection capability)* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

(6) Setting up Process exporter

(a) Specifying monitored processes (required)

- Edit the Process exporter configuration file (jpc_process_exporter.yml)

Edit the Process exporter configuration file (jpc_process_exporter.yml) to define which processes are to be monitored.

By default, no process is to be monitored, and therefore you will uncomment the initial settings and then specify the processes you want to monitor in the Process exporter configuration file.

For details on the Process exporter configuration file, see *Process exporter configuration file (jpc_process_exporter.yml)* in *Chapter 2. Definition Files* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

(b) Modifying monitoring metrics (optional)

- Edit the Prometheus configuration file (jpc_prometheus_server.yml)

If you want to change metrics to be collected, modify the `metric_relabel_configs` setting in the Prometheus configuration file (jpc_prometheus_server.yml).

For details on the Prometheus configuration file, see *Prometheus configuration file (jpc_prometheus_server.yml)* in *Chapter 2. Definition Files* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

- Edit the Process exporter metric definition file (metrics_process_exporter.conf)

If you want to change metrics displayed in the **Trends** tab of the integrated operation viewer, edit the settings in the Process exporter metric definition file (metrics_process_exporter.conf).

For details on the Process exporter metric definition file, see *Process exporter metric definition file (metrics_process_exporter.conf)* in *Chapter 2. Definition Files in the JPI/Integrated Management 3 - Manager Command, Definition File and API Reference*.

(c) Changing Ports (optional)

The listen port used by Process exporter is specified in `--web.listen-address` option of the `process_exporter` command.

For details about how to change the options of `process_exporter` command, see [2.19.2\(1\)\(c\) Change command-line options \(for Linux\)](#). For details about `--web.listen-address` option, see *If you want to change command line options in Unit definition file (jpc_program-name.service)* in *Chapter 2. Definition Files in the JPI/Integrated Management 3 - Manager Command, Definition File and API Reference*.

The default port is "20721". If port number is changed, review setup of the firewall and prohibit accessing from outside.

Notes:

- When specifying the host name for this option, the same host name must be set for `targets` in the Process exporter discovery configuration file (`jpc_file_sd_config_process.yml`) on the same host.
- When specifying an IP address for this option, the host name that is resolved to the IP address specified for this option must be set for `targets` in the Process exporter discovery configuration file (`jpc_file_sd_config_process.yml`) on the same host.

(d) Optional setting to remove child processes from monitoring

By default, when monitoring a monitored process, Process exporter monitors the child process and retrieves the operational data including the child process.

If you want Process exporter to acquire the activity without including the child process, modify unit definition file of Process exporter as follows:

File to be edited

- For physical hosts
`/usr/lib/systemd/system/jpc_process_exporter.service`
- For logical hosts
`/usr/lib/systemd/system/jpc_process_exporter_logical_hostname.service`

Editing data

Configure `-children=false` with the `process_exporter` boot options listed in `ExecStart`.

Setting example

```
ExecStart = /bin/sh -c "/opt/jplima/bin/process_exporter" \  
-Children=false \  
-Debug=true \  
--Config.path="/opt/jplima/conf/jpc_process_exporter.yml" \  

```

(7) Setup of Blackbox exporter

(a) Changing Ports (For Linux) (optional)

The listen port used by Blackbox exporter is specified in `--web.listen-address` option of the `blackbox_exporter` command.

For details about how to change the options of `blackbox_exporter` command, see [2.19.2\(1\)\(c\) Change command-line options \(for Linux\)](#). For details about `--web.listen-address` option, see [If you want to change command line options in Unit definition file \(jpc_program-name.service\) in Chapter 2. Definition Files in the JPI/Integrated Management 3 - Manager Command, Definition File and API Reference](#).

The default port is "20715". If port number is changed, review setup of the firewall and prohibit accessing from outside.

(b) Add, Modify, or Delete a Module. (optional)

See [1.21.2\(6\)\(b\) Add, change, and delete modules \(for Windows\) \(optional\)](#).

(c) Add, Modify, or Delete a monitoring target (for Linux) (required)

See [1.21.2\(6\)\(c\) Add, change, or Delete the monitoring target \(for Windows\) \(required\)](#).

(d) Monitor HTTP through proxy (on Linux) (optional)

See [1.21.2\(6\)\(d\) Monitoring HTTP through proxy \(for Windows\) \(optional\)](#).

(e) Setup the proxy authentication ID and Password (optional)

See [1.21.2\(6\)\(e\) Setup the proxy authentication ID and Password \(for Windows\) \(optional\)](#).

(f) Setup authentication ID, Password, and Bearer tokens for accessing the monitored Web Server (optional)

See [1.21.2\(6\)\(f\) Setup authentication ID, Password, and Bearer tokens for accessing the monitored Web Server \(for Windows\) \(optional\)](#).

(8) Setup in Yet another cloudwatch exporter

(a) Changing Ports (For Linux) (optional)

See [1.21.2\(7\)\(a\) Changing Ports \(For Windows\) \(optional\)](#).

(b) Modify Setup to connect to CloudWatch (for Linux) (required)

See [1.21.2\(7\)\(b\) Modify Setup to connect to CloudWatch \(for Windows\) \(required\)](#).

(c) Connect to CloudWatch through a proxy (for Linux) (optional)

See [1.21.2\(7\)\(c\) Connect to CloudWatch through a proxy \(for Windows\) \(optional\)](#).

(d) Add AWS Services to be Monitored (optional)

See [1.21.2\(7\)\(d\) Add AWS Services to be Monitored \(optional\)](#).

(e) Monitoring AWS Resources (required)

See *1.21.2(7)(e) Monitoring AWS Resources (required)*.

(f) Modify metric to Collect (optional)

See *1.21.2(7)(f) Modify metric to Collect (optional)*.

(9) Setup of Promitor

See *1.21.2(8) Set up of Promitor*.

(10) Setup of Fluentd

(a) Changing Setup of Common Definition file for Log Monitor (optional)

See *1.21.2(9)(a) Changing Setup of Common Definition file for Log Monitor (for Windows) (optional)*.

(b) Monitoring the text-formatted log file (required)

1.21.2(9)(b) Monitoring the text-formatted log file (for Windows) (required)".

(c) Modifying the monitoring settings of the text-formatted log file (optional)

See *1.21.2(9)(c) Modifying the monitoring settings of the text-formatted log file (for Windows) (optional)*.

(d) Deleting the monitoring settings of the text-formatted log file (optional)

See *1.21.2(9)(d) Deleting the monitoring settings of the text-formatted log file (for Windows) (optional)*.

(e) Setup of the log metrics definition (required)

See *1.21.2(9)(h) Setup of the log metrics definition (optional)*.

(f) Changing Ports (optional)

See *1.21.2(9)(i) Changing Ports (optional)*.

(g) Monitoring SAP system log information (optional)

See *1.21.2(9)(j) Monitoring SAP system logging (optional)*.

(h) Change monitoring settings for SAP system log information (optional)

See *1.21.2(9)(k) Modify SAP system logging monitoring configuration (optional)*

(i) Delete the monitoring settings for log information in SAP systems (optional)

See *1.21.2(9)(l) Remove SAP system logging monitoring configuration (optional)*.

(j) Monitoring CCMS alert information for SAP systems (optional)

See *1.21.2(9)(m) Monitoring CCMS alerting for SAP system (optional)*.

(k) Change monitoring settings for CCMS alert information in SAP systems (optional)

See *1.21.2(9)(n) Modify SAP system CCMS alert information monitoring settings (optional)*.

(I) Delete the monitoring settings for CCMS alert information in SAP systems (optional)

See [1.21.2\(9\)\(o\) Remove SAP system CCMS alert information monitoring settings \(optional\)](#).

(11) Setting up scraping definitions

See [1.21.2\(10\) Setting up scraping definitions](#).

(12) Setting up container monitoring

See [1.21.2\(11\) Setting up container monitoring](#).

(13) Editing the Script exporter definition file

See [1.21.2\(12\) Editing the Script exporter definition file](#).

(14) Setting up VMware exporter

See [1.21.2\(14\) Setting up VMware exporter](#).

(15) Specifying a listening port number and listening address (optional)

See [1.21.2\(16\) Specifying a listening port number and listening address \(optional\)](#).

(16) Firewall Setup (for Linux) (required)

See [1.21.2\(17\) Firewall's Setup \(for Windows\) \(required\)](#).

(17) Setup of integrated agent process alive monitoring (for Linux) (optional)

You monitor integrated agent processes in the following ways:

- External shape monitoring by other-host Blackbox exporter
- Monitoring Processes by Process exporter
- Monitoring Prometheus server with up metric

(a) External shape monitoring by other-host Blackbox exporter

Prometheus server and Alertmanager services monitors from Blackbox exporter of integrated agent running on other hosts. The following tables show URL to be monitored.

For details about how to Add HTTP monitor of Blackbox exporter, see [1.21.2\(6\)\(c\) Add, change, or Delete the monitoring target \(for Windows\) \(required\)](#). For details about how to set the alert definition, see [1.21.2\(3\)\(b\) To Add the alert definition \(for Windows\) \(optional\)](#)".

For an example of the alert definitions to be monitored by HTTP Monitor of Blackbox exporter, see [1.21.2\(18\) Setup of integrated agent process alive monitoring \(for Windows\) \(optional\)](#).

Table 2–12: URL monitored by HTTP monitoring of Blackbox exporter

Service	URL to monitor
Prometheus server	<code>http://host-name-of-integrated-agent:port-number-of-Prometheus-server/-/healthy</code>
Alertmanager	<code>http://host-name-of-integrated-agent:port-number-of-Alertmanager/-/healthy</code>

(b) Alive Monitoring Processes by Process exporter

Imagentproxy service, imagentaction service, and Fluentd service are monitored by the operation status of the process monitor of Process exporter. The processes to be monitored are described in the following table.

For details about how to set up, see *Process exporter configuration file (jpc_process_exporter.yml)* in *Chapter 2. Definition Files* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

For details about setting method of the alert definition, see [1.21.2\(3\)\(b\) To Add the alert definition \(for Windows\) \(optional\)](#).

Table 2–13: Processes monitored by the Process exporter

Service	Processes to monitor	Remarks
imagent	<i>Agent-path/bin/imagent</i>	Set this when you want to detect a case that starts up quickly after imagent described in 3.15.8(2) <i>Polling monitoring for JP1/IM agent control base</i> in the <i>JP1/Integrated Management 3 - Manager Overview and System Design Guide</i> has stopped abnormally.
imagentproxy	<i>Agent-path/bin/imagentproxy</i>	Not applicable.
imagentaction	<i>Agent-path/bin/imagentaction</i>	Not applicable.
Fluentd	<i>Agent-path/lib/ruby/bin/ruby</i>	The "jpc_fluentd_common.conf" text on the command-line distinguishes it from ruby other than Fluentd.
Rotatelog (only for Fluentd)	<i>Agent-path/bin/rotatelog</i>	The "Agent-path/logs/fluentd" text on the command line distinguishes it from rotatelog other than Fluentd.

The following is a sample Process exporter configuration file that is monitored by Process exporter.

```
process_names:
- name: "{{.ExeBase}};{{.Username}};{{.Matches.cmdline}}"
  exe:
    - /opt/jplima/bin/imagent
    - /opt/jplima/bin/imagentproxy
    - /opt/jplima/bin/imagentaction

- name: "{{.ExeBase}};{{.Username}};{{.Matches.cmdline}}"
  exe:
    - /opt/jplima/bin/rotatelog
  cmdline:
    - (?P<cmdline>.*\/opt\/jplima\/logs\/fluentd\.*)

- name: "{{.ExeBase}};{{.Username}};{{.Matches.cmdline}}"
  exe:
```

```
- /opt/jplima/lib/ruby/bin/ruby
cmdline:
- (?P<cmdline>.*jpc_fluentd_common\.conf.*)
```

Here is a sample alertdefinition that Process exporter monitors:

```
groups:
- name: process_exporter
  rules:
- alert: jpl_pc_procmon_imagent
  expr: 1 > sum by (program, instance, job, jpl_pc_nodelabel, jpl_pc_ex
porter) (namedprocess_namegroup_num_procs{program="imagent"})
  for: 3m
  labels:
    jpl_pc_product_name: "/HITACHI/JP1/JPCCS2"
    jpl_pc_component: "/HITACHI/JP1/JPCCS/CONFINFO"
    jpl_pc_severity: "Error"
    jpl_pc_eventid: "1303"
    jpl_pc_metricname: "namedprocess_namegroup_num_procs"
  annotations:
    jpl_pc_firing_description: "The number of processes was less than th
e threshold Value (1). value={{ $value }}"
    jpl_pc_resolved_description: "The number of processes exceeded the t
hreshold Value (1)."
```

```
- alert: jpl_pc_procmon_imagentproxy
  expr: 1 > sum by (program, instance, job, jpl_pc_nodelabel, jpl_pc_ex
porter) (namedprocess_namegroup_num_procs{program="imagentproxy"})
  for: 3m
  labels:
    jpl_pc_product_name: "/HITACHI/JP1/JPCCS2"
    jpl_pc_component: "/HITACHI/JP1/JPCCS/CONFINFO"
    jpl_pc_severity: "Error"
    jpl_pc_eventid: "1303"
    jpl_pc_metricname: "namedprocess_namegroup_num_procs"
  annotations:
    jpl_pc_firing_description: "The number of processes was less than th
e threshold Value (1). value={{ $value }}"
    jpl_pc_resolved_description: "The number of processes exceeded the t
hreshold Value (1)."
```

```
- alert: jpl_pc_procmon_imagentactoin
  expr: 1 > sum by (program, instance, job, jpl_pc_nodelabel, jpl_pc_ex
porter) (namedprocess_namegroup_num_procs{program="imagentaction"})
  for: 3m
  labels:
    jpl_pc_product_name: "/HITACHI/JP1/JPCCS2"
    jpl_pc_component: "/HITACHI/JP1/JPCCS/CONFINFO"
    jpl_pc_severity: "Error"
    jpl_pc_eventid: "1303"
    jpl_pc_metricname: "namedprocess_namegroup_num_procs"
  annotations:
    jpl_pc_firing_description: "The number of processes was less than th
e threshold Value (1). value={{ $value }}"
    jpl_pc_resolved_description: "The number of processes exceeded the t
hreshold Value (1)."
```



```

- alert: jpl_pc_procmon_fluentd_rotatelog Log trapper(Fluentd) #1
  expr: 1 > sum by (program, instance, job, jpl_pc_nodelabel, jpl_pc_exporter) (namedprocess_namegroup_num_procs{program="rotatelog"})
  for: 3m
  labels:
    jpl_pc_product_name: "/HITACHI/JP1/JPCCS2"
    jpl_pc_component: "/HITACHI/JP1/JPCCS/CONFINFO"
    jpl_pc_severity: "Error"
    jpl_pc_eventid: "1303"
    jpl_pc_metricname: "namedprocess_namegroup_num_procs"
  annotations:
    jpl_pc_firing_description: "The number of processes was less than the threshold Value (1). value={{ $value }}"
    jpl_pc_resolved_description: "The number of processes exceeded the threshold Value (1). "

- alert: jpl_pc_procmon_fluentd_ruby Log trapper(Fluentd) #2
  expr: 2 > sum by (program, instance, job, jpl_pc_nodelabel, jpl_pc_exporter) (namedprocess_namegroup_num_procs{program="ruby"}) #3
  for: 3m
  labels:
    jpl_pc_product_name: "/HITACHI/JP1/JPCCS2"
    jpl_pc_component: "/HITACHI/JP1/JPCCS/CONFINFO"
    jpl_pc_severity: "Error"
    jpl_pc_eventid: "1303"
    jpl_pc_metricname: "namedprocess_namegroup_num_procs"
  annotations:
    jpl_pc_firing_description: "The number of processes was less than the threshold Value (2). value={{ $value }}"
    jpl_pc_resolved_description: "The number of processes exceeded the threshold Value (2). "

```

#1

If only log metrics feature is used, specify "jpl_pc_procmon_fluentd_prome_rotatelog Log trapper(Fluentd)".

#2

If only log metrics feature is used, specify "jpl_pc_procmon_fluentd_prome_ruby Log trapper(Fluentd)".

#3

The Ruby process starts the number of workers + 1. For the threshold, specify the number of workers + 1. For details on the number of workers, see *Log monitoring common definition file (jpc_fluentd_common.conf)* in Chapter 2. *Definition Files* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

(c) Monitoring by Prometheus server up metric

Node exporter service, Process exporter service, Blackbox exporter service, and Yet another cloudwatch exporter service are monitored through Prometheus server alert-monitoring. For setting method of the alert definition, see [1.21.2\(3\)\(b\) To Add the alert definition \(for Windows\) \(optional\)](#).

For an example of an alert definition that monitors up metric, see [1.21.2\(18\) Setup of integrated agent process alive monitoring \(for Windows\) \(optional\)](#).

(18) Creating and importing IM management node tree data (for Linux) (required)

See [1.21.2\(19\) Creation and import of IM management node tree data \(for Windows\) \(required\)](#).

(19) Security product exclusion Setup (for Linux) (optional)

See *1.21.2(20) Security-product exclusion Setup (for Windows) (optional)*.

(20) Notes on updating definition file (for Linux)

See *1.21.2(21) Notes on updating the definition file (for Windows)*.

2.20 Building Container Environments in JP1/IM - Agent (for UNIX)

For details on how to build a container environments in JP1/IM - Agent, see [1.22 Building Container Environments in JP1/IM - Agent \(for Windows\)](#).

2.21 Building optional features for JP1/IM - Agent (for UNIX)

2.21.1 Configuring OracleDB exporter

This section describes how to configure OracleDB exporter, an optional feature of integrated agent host.

(1) Preparing for setting up OracleDB exporter

This is the same as for Windows. See [1.23.1\(1\) Preparing for OracleDB exporter configuration](#).

(2) Installing OracleDB exporter

This is the same as for Windows. See [1.23.1\(2\) Installing OracleDB exporter](#).

(3) Uninstalling OracleDB exporter

This is the same as for Windows. See [1.23.1\(3\) Uninstalling OracleDB exporter](#).

(4) Configuring OracleDB exporter

This section explains how to configure OracleDB exporter.

(a) Adding monitoring targets (required)

■ Preparing to add monitoring targets

This is the same as for Windows. See [Preparing to add a monitoring target](#) in [1.23.1\(4\)\(a\) Adding a monitoring target \(required\)](#).

■ Configuring OracleDB exporter

1. Create a unit definition file.

Copy the source unit definition file and rename it to the destination filename.

The owner and owner group of the created unit definition file should be root, and the access rights should be 644.

Source filename: *OracleDB-exporter-location/oracledb_exporter_linux/jplima/conf/oracledb_exporter_@@instance@@.service.model*

Destination file name:

- For physical host operation
OracleDB-exporter-location/oracledb_exporter_linux/jplima/conf/oracledb_exporter_instance#.service
- For logical host operation
OracleDB-exporter-location/oracledb_exporter_linux/jplima/conf/oracledb_exporter_instance#_logical-host-name.service

#

For instance name, specify the name determined in [Preparing to add a monitoring target](#) in [1.23.1\(4\)\(a\) Adding a monitoring target \(required\)](#).

2. Updating unit definition file.

Modify the following values of unit definition file created in step 1 as shown in the tables.

Value to be changed	Value to specify
@@instance@@	- For physical host operation Replace with the name determined in step 1 of <i>Preparing to add a monitoring target</i> in <i>1.23.1(4)(a) Adding a monitoring target (required)</i> . - For logical host operation Replace with the name determined in step 1 of <i>Preparing to add a monitoring target</i> in <i>1.23.1(4)(a) Adding a monitoring target (required)</i> with the name "_logical host name".
@@oracledb_exporter_installdir@@	Replace with OracleDB exporter location.
@@port@@	Replace with the port number determined in step 2 of <i>Preparing to add a monitoring target</i> in <i>1.23.1(4)(a) Adding a monitoring target (required)</i> . For a logical host, specify the logical host name, and replace it so that <code>--web.listen-address="logical host name: port number"</code> .
@@installdir2@@	Replace with the directory confirmed in step 3 of <i>Preparing to add a monitoring target</i> in <i>1.23.1(4)(a) Adding a monitoring target (required)</i> .
@@data_source_name@@	Replace with the content confirmed in step 4 of <i>Preparing to add a monitoring target</i> in <i>1.23.1(4)(a) Adding a monitoring target (required)</i> .

3. Register the unit definition file in systemd.

Copy[#] the unit definition file updated in step 2 to the following directory. For logical host operation, copy on both nodes of the cluster.

Destination directory: `/usr/lib/systemd/system`

Please copy, not move. If you move, SELinux permissions may not be set correctly and the services may not start correctly.

After copying the unit definition file to the destination directory, run the following command to reload systemd. For logical host operation, execute the command on both nodes of the cluster.

```
systemctl daemon-reload
```

If you want the system to start automatically when OS is started in physical-host operation, execute the following command. In the case of logical host operation, automatic startup is not performed.

```
systemctl enable service-name
```

4. Create a log directory.

Create a log directory in the location of the OracleDB exporter.

The owner and owner group of the created directory should be root, and the access rights should be 700.

- For physical host operation
`OracleDB-exporter-location/oracledb_exporter_linux/jplima/logs/oracledb_exporter/instance-name#`
- For logical host operation
`OracleDB-exporter-location/oracledb_exporter_linux/jplima/logs/oracledb_exporter/instance-name#_logical-host-name`

#

For instance name, specify the name determined in *Preparing to add a monitoring target* in [1.23.1\(4\)\(a\) Adding a monitoring target \(required\)](#).

5. Register the password of the user used to connect to Oracle Database.

Register the password of the user used to connect to Oracle Database with the `jimasecret` command.

- For physical host operation

```
jimasecret -add -key OracleDB.user.user-name -s password
```

- For logical host operation

```
jimasecret -add -key OracleDB.user.user-name -s password -l shared-directory
```

If you want to register users with the same username but different passwords, you can use a key that includes the host name and the service name.

For details about the `jimasecret` command, see `jimasecret` in *Chapter 1. Commands* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

6. Register the service in the cluster software.

In the case of a cluster configuration, the service is registered in the cluster software.

7. Start the OracleDB exporter service.

Start the OracleDB exporter service with the `systemctl start` command.

For a cluster configuration, start the service from the cluster software.

8. Confirm that OracleDB exporter can acquire the performance data.

Access the following URL with the `curl` command or browser and check whether the performance information has been obtained.

```
http://hostname:port/metrics
```

The *host-name* is the host on which OracleDB exporter is booting, and the *port* is the listen port of OracleDB exporter.

■ Configuring Prometheus

This is the same as for Windows. See *Configuring Prometheus* in [1.23.1\(4\)\(a\) Adding a monitoring target \(required\)](#).

■ Configuring Intelligent Integrated Management Base

This is the same as for Windows. See *Configuring Intelligent Integrated Management Base* in [1.23.1\(4\)\(a\) Adding a monitoring target \(required\)](#).

(b) Change the port for OracleDB exporter (optional)

This is the same as for Windows. See [1.23.1\(4\)\(b\) Changing OracleDB exporter port \(optional\)](#).

(c) Change the password for the connection (optional)

This is the same as for Windows. See [1.23.1\(4\)\(c\) Change the password for connecting \(optional\)](#).

(d) Delete a monitoring target (optional)

■ Configuring Prometheus

This is the same as for Windows. See *Configuring Prometheus* in [1.23.1\(4\)\(d\) Deleting a monitoring target \(optional\)](#).

■ Configuring Prometheus

This is the same as for Windows. See *Removing OracleDB exporter from Cluster Software* in [1.23.1\(4\)\(d\) Deleting a monitoring target \(optional\)](#).

■ Configuring OracleDB exporter

1. Stop the monitoring target OracleDB exporter service that you want to delete.

Stop the OracleDB exporter service with the `systemctl start` command.

2. Delete the unit definition file.

Delete the unit definition file shown below.

- For physical host operation
`oracledb_exporter_instance name_service`
- For logical host operation
`oracledb_exporter_instance name_logical host name_service`

For logical host operation, delete on both nodes of the cluster.

3. Refresh systemctl.

Execute the following command to refresh systemctl.

```
systemctl daemon-reload
```

For logical host operation, delete on both nodes of the cluster.

4. Deletes the password for the user used to connect to Oracle Database.

If you are not using the same user in another OracleDB exporter, use `jimasecret` command to delete the registered password.

- For physical host operation
`jimasecret -rm -key OracleDB.user.username`
- For logical host operation
`jimasecret -rm -key OracleDB.user.username -s password -l shared directory`

If you register by specifying a key that includes a host name or listener name, specify that key.

(e) Configuring OracleDB exporter life-and-death monitoring (optional)

This is the same as for Windows. See [1.23.1\(4\)\(e\) Setting up OracleDB exporter life-and-death monitoring \(optional\)](#).

(f) Modifying users for connections (optional)

1. Add a new person to Oracle Database.

2. Stop OracleDB exporter.

3. Delete the password of the user before the change.

Use `jimasecret` command to delete the password of the user used to connect to Oracle Database.

- For physical host operation
`jimasecret -rm -key OracleDB.user.old username`
- For logical host operation
`jimasecret -rm -key OracleDB.user.old username -l shared directory`

If you want to register users with the same user name but different passwords, use a key that includes the host name and the service name.

4. Register the password of the user after change.

Register the password of the user used to connect to Oracle Database with the `jimasecret` command.

- For physical host operation

```
jimasecret -add -key OracleDB.user.new username -s password
```

- For logical host operation

```
jimasecret -add -key OracleDB.user.new username -s password -l shared directory
```

If you want to register users with the same user name but different passwords, you can use a key that includes the host name and the service name.

5. Modify the environment variable `DATA_SOURCE_NAME`.

Open unit definition file in a text editor, change the username in the environment variable `DATA_SOURCE_NAME` to the new username, and save it.

6. Start OracleDB exporter.

7. Deletes the previous person from Oracle Database.

If the old user is not needed, remove the old user from Oracle Database.

(5) Cluster environment

This is the same as for Windows. See [1.23.1\(5\) Cluster environment](#).

2.21.2 Configuring the Node exporter for AIX

This is the same as for Windows. See [1.23.2 Setting up Node exporter for AIX](#).

2.21.3 Configuring SAP system monitoring

This is the same as for Windows. See [1.23.3 Configuring SAP system monitoring](#).

2.22 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.

Of the data in the directory containing the media that provides the manuals, copy all target data for each manual to the directory containing JP1/IM - Manager.

If all manuals are stored in their correct locations, you can view the table of contents of each manual.

When you select **Help** and then **Help Contents** if the data is placed in an incorrect location or only part of the data is placed, an error dialog box (KAVB8550-E) appears.

- Stored target data (HTML manuals)
CSS file, all HTML files, and the GRAPHICS directory
- Locations of the target data in the manual distribution medium (when the medium is inserted in the drive of the UNIX machine)
In the manual distribution media, manuals are stored in folders with manual numbers under *applicable drive* \MAN\3021. If you want to know which manual corresponds to which product, check INDEX . HTM under each folder with a manual number.
- Locations to store the target data on the JP1/IM - Manager side:
Under /opt/jplcons/www/manual/ja/
Under /opt/jplimm/public/manual/ja
Store all the target data stored under the manual number folder of the manual distribution media in the folder of each manual number.

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.

2.23 Uninstallation (for UNIX)

This section describes how to uninstall JP1/IM - Manager and JP1/IM - Agent. Note that the uninstallation procedure must be performed by a user with root privileges.

2.23.1 Uninstallation procedure (for UNIX)

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

Also, if Intelligent Integrated Management Database service is set up, "Deletion failed." is displayed on Hitachi PP Installer terminal and uninstallation fails. Make sure that JP1/IM - Manager installer log (/tmp/HITACHI_JP1_INST_LOG/jplimm_inst{1|2|3|4|5}.log) for Latest refresh Date/time is either KAVB9944-E Message (for Physical host) or KAVB9945-E Message (for Logical host).

If the KAVB9944-E message or the KAVB9945-E message is output, use the unsetup command (jimgnadbunsetup command) to unset the Intelligent Integrated Management database service, and then uninstall JP1/IM - Manager again. If the KAVB9946-E message is output, follow the actions for the KAVB9946-E message.

(1) The procedure for delete Intelligent Integrated Management Database

Back up Intelligent Integrated Management Database before you delete it to rebuild it. For details on how to back up the data, see *1.2 Managing the databases* in the *JP1/Integrated Management 3 - Manager Administration Guide*.

Perform the following steps to delete Intelligent Integrated Management Database:

1. Stop JP1/IM - Manager.

Stop JP1/IM - Manager.

2. Delete Intelligent Integrated Management Database.

Execute the following command.

- For physical host operation

```
jimgnadbunsetup [-q]
```

- For active host in logical host operation

```
jimgnadbunsetup -h logical-host-name -c online [-q]
```

- For standby host in logical host operation

```
jimgnadbunsetup -h logical-host-name -c standby [-q]
```

3. Restart the machine.

(2) 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 3 - Manager Administration Guide*.

For details about the commands, see *Chapter 1. Commands* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API 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/IM3-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/IM3-Manager) is stopped.

- For logical hosts

The IM database (JP1 / IM3-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 / IM3-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 (`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 `/var/opt/jplimm/data/imcf/imconfig`

Files and folders under `/var/opt/jplimm/data/imcf/profiles`

8. Restart the machine.

(3) How to uninstall JP1/IM - Manager

You need `root` permissions to perform this procedure.

If you uninstall JP1/IM - Manager, JP1/IM agent management base for using JP1/IM - Agent is also uninstalled.

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`

(4) Steps for uninstalling JP1/IM - Agent

Follow the procedure below to uninstall. You must have root privilege to do this. When you uninstall JP1/IM - Agent, folders containing files, such as definition files and log files, are also deleted. If necessary, back them up.

1. Stop JP1/IM - Agent service.

2. If you are using the data delivery function to multiple manager hosts, perform the following steps before deleting the service.

Follow the procedure described in [2.19.2\(2\)\(i\) Deactivating the data delivery function to multiple manager hosts \(for Linux\) \(optional\)](#) to uninstall JP1/IM - Agent.

3. Execute the service delete of JP1/IM - Agent.

For details about how to delete the service, see [2.19.1\(1\)\(b\) Disabling add-on program](#).

4. Start Hitachi PP Installer and delete JP1/IM - Agent.

5. After the deletion is completed, login to Integrated manager's integrated operation viewer and make sure that integrated agent information of the host you just deleted is deleted. If the information is remained, manually delete it. For details on how to remove integrated agent data, see *2.2.1 List of Integrated Agents window* in the *JP1/Integrated Management 3 - Manager GUI Reference*.

Important

If logical host service is running, delete logical host service after stopping the service and then execute it. If you uninstall while logical host service is running, file used by logical host service may be deleted and the service may terminate abnormally. Logical host service must be deleted after uninstallation if logical host service was uninstalled without deletion services.

2.23.2 Notes on uninstallation (for UNIX)

(1) 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 3 - Manager Overview and System Design Guide*.

(2) About uninstalling JP1/Base

When you uninstall JP1/Base, the definition information of JP1/IM - Manager is also deleted. Even if you reinstall JP1/Base, JP1/IM - Manager will not work. In such a case, you need to execute the `jplcc_setup`, `jplcs_setup`, and `jplcf_setup` commands to configure the environment settings.

(3) About check after uninstallation

After uninstalling JP1/IM - Manager, check if the following directories remain. If any remain, delete them.

- `/etc/opt/jplcons`
- `/opt/jplcons`
- `/var/opt/jplcons`
- `/etc/opt/jplscope`
- `/opt/jplscope`
- `/var/opt/jplscope`

Uninstalling the product deletes the monitoring object DB and the host information DB.

(4) About the procedure for manually uninstalling an IM database on a physical host

Steps for Manually Uninstalling IM database on Physical Hosts (on Linux).

1. Log in as a superuser.
2. If JP1/IM - Manager is running, stop the program.

3. Delete the following files:

- /usr/lib/systemd/system/2248-PDxx-start.service
- /usr/lib/systemd/system/2248-PDxx-stop.service
- /usr/lib/systemd/system/2248-PDxx.service
- /usr/lib/systemd/system/2248-pexx.service

Note that the *xx* in the file name stands for a number in a series, starting with 01. Before deleting the files, verify that they contain the following information.

Caution: Deleting files may adversely affect the system. For example, the IM database for the physical host may cease to operate correctly.

Verify that the files contain the following

```
<IMDBENVDIR>/JM0
```

```
<IMDBENVDIR>: The path specified for the IMDBENVDIR parameter in the setup information file
(jimdbsetupinfo.conf) that was specified when the IM Configuration Management database and the
integrated monitoring database for the physical host that is to be deleted were compiled.
```

4. Delete the following symbolic link files:

- /etc/systemd/system/multi-user.target.wants/2248-PDxx-start.service
- /etc/systemd/system/multi-user.target.wants/2248-PDxx-stop.service
- /etc/systemd/system/multi-user.target.wants/2248-PDxx.service
- /etc/systemd/system/multi-user.target.wants/2248-pexx.service

Note that the *xx* in the file name stands for a number in a series, starting with 01. Before deleting the files, verify that they contain the following information.

Caution: Deleting files may adversely affect the system. For example, the IM database for the physical host may cease to operate correctly.

Verify that the files contain the following

```
<IMDBENVDIR>/JM0
```

```
<IMDBENVDIR>: : The path specified for the IMDBENVDIR parameter in the setup information file
(jimdbsetupinfo.conf) that was specified when the IM Configuration Management database and the
integrated monitoring database for the physical host that is to be deleted were compiled.
```

5. Update the configuration file for the IM database by performing the following procedure:

- Delete /etc/opt/jplimm/conf/imdb/system/dbconf/JM0.
- Open /etc/opt/jplimm/conf/imdb/system/dbconf/jimdbsetuplist.conf in a text editor and edit it as follows, delete JP1_DEFAULT, and then overwrite the file.

(Before editing)

```
_JM0=JP1_DEFAULT
```

(After editing)

```
_JM0=
```

6. Restart the operating system.

7. Delete the following folder if it exists:

- <IMDBDIR>/imdb
- <IMDBENVDIR>/JM0

<IMDBDIR>: The path specified for the IMDBDIR parameter in the setup information file (jimdbsetupinfo.conf) that was specified when the IM Configuration Management database and the integrated monitoring database for the physical host that is to be deleted were compiled.

<IMDBENVDIR>: The path specified for the IMDBENVDIR parameter in the setup information file (jimdbsetupinfo.conf) that was specified when the IM Configuration Management database and the integrated monitoring database for the physical host that is to be deleted were compiled.

(5) About the procedure for manually uninstalling an IM database on a cluster system

1. Log in to the active host as a superuser.
2. On the active host, if JP1/IM - Manager is running, stop the program.
3. On the active host, delete the following files:

- /usr/lib/systemd/system/2248-PDxx-start.service
- /usr/lib/systemd/system/2248-PDxx-stop.service
- /usr/lib/systemd/system/2248-PDxx.service
- /usr/lib/systemd/system/2248-pexx.service

Note that the *xx* in the file name stands for a number in a series, starting with 01. Before deleting the files, verify that they contain the following information.

Caution: Deleting files may adversely affect the system. For example, the IM database for the physical host may cease to operate correctly.

Verify that the files contain the following

<IMDBENVDIR>/JM<n>

<IMDBENVDIR>: The path specified for the IMDBENVDIR parameter in the cluster setup information file (jimdbclustersetupinfo.conf) that was specified when the IM Configuration Management database and the integrated monitoring database for the logical host that is to be deleted were compiled, with the forward slashes replaced with periods.

<n>: The value specified for the LOGICALHOSTNUMBER parameter in the cluster setup information file (jimdbclustersetupinfo.conf) that was specified when the IM Configuration Management database and the integrated monitoring database for the logical host that is to be deleted were compiled.

4. On the active host, delete the following symbolic link files:

- /etc/systemd/system/multi-user.target.wants/2248-PDxx-start.service
- /etc/systemd/system/multi-user.target.wants/2248-PDxx-stop.service
- /etc/systemd/system/multi-user.target.wants/2248-PDxx.service
- /etc/systemd/system/multi-user.target.wants/2248-pexx.service

Note that the *xx* in the file name stands for a number in a series, starting with 01. Before deleting the files, verify that they contain the following information.

Caution: Deleting files may adversely affect the system. For example, the IM database for the physical host may cease to operate correctly.

Verify that the files contain the following

<IMDBENVDIR>/JM<n>

<IMDBENVDIR>: The path specified for the IMDBENVDIR parameter in the cluster setup information file (imdbsetupinfo.conf) that was specified when the IM Configuration Management database and the integrated monitoring database for the logical host that is to be deleted were compiled.

<n>: The value specified for the LOGICALHOSTNUMBER parameter in the cluster setup information file (jimdbclustersetupinfo.conf) that was specified when the IM Configuration Management database and the integrated monitoring database for the logical host that is to be deleted were compiled.

5. Update the configuration file for the IM database on the active host by performing the following procedure:

- Delete /etc/opt/jplimm/conf/imdb/system/dbconf/JM<n>.
- Open /etc/opt/jplimm/conf/imdb/system/dbconf/jimdbsetuplist.conf in a text editor, edit the line equal to n+1 as follows, delete the logical host name, and then overwrite the file.

(Before editing) jimdbsetuplist.conf <line-number-n+1>

_JM<n>=<logical-host-name>

(After editing) jimdbsetuplist.conf <line-number-n+1>

_JM<n>=

<n>: The value specified for the LOGICALHOSTNUMBER parameter in the cluster setup information file (jimdbclustersetupinfo.conf) that was specified when the IM Configuration Management database and the integrated monitoring database for the logical host that is to be deleted were compiled.

6. Restart the operating system on the active host.

7. Delete the following folder if it exists on the active host:

- <IMDBDIR>/imdb
- <SHAREDDBDIR>/imdb
- <IMDBENVDIR>/JM<n>

<IMDBDIR>: The path specified for the IMDBDIR parameter in the cluster setup information file (jimdbclustersetupinfo.conf) that was specified when the IM Configuration Management database and the integrated monitoring database for the logical host that is to be deleted were compiled.

<SHAREDDBDIR>: The path specified for the SHAREDDBDIR parameter in the cluster setup information file (jimdbclustersetupinfo.conf) that was specified when the IM Configuration Management database and the integrated monitoring database for the logical host that is to be deleted were compiled.

<IMDBENVDIR>: The path specified for the IMDBENVDIR parameter in the cluster setup information file (jimdbclustersetupinfo.conf) that was specified when the IM Configuration Management database and the integrated monitoring database for the logical host that is to be deleted were compiled.

<n>: The value specified for the LOGICALHOSTNUMBER parameter in the cluster setup information file (jimdbclustersetupinfo.conf) that was specified when the IM Configuration Management database and the integrated monitoring database for the logical host that is to be deleted were compiled.

8. Log in to the standby host as a superuser.

9. On the standby host, if JP1/IM - Manager is running, stop the program.

10. On the standby host, delete the following files:

- /usr/lib/systemd/system/2248-PDxx-start.service
- /usr/lib/systemd/system/2248-PDxx-stop.service
- /usr/lib/systemd/system/2248-PDxx.service

- /usr/lib/systemd/system/2248-pexx.service

Note that the *xx* in the file name stands for a number in a series, starting with 01. Before deleting the files, verify that they contain the following information.

Caution: Deleting files may adversely affect the system. For example, the IM database for the physical host may cease to operate correctly.

Verify that the files contain the following

<IMDBENVDIR>/JM<n>

<IMDBENVDIR>: The path specified for the IMDBENVDIR parameter in the cluster setup information file (jimdbclustersetupinfo.conf) that was specified when the IM Configuration Management database and the integrated monitoring database for the logical host that is to be deleted were compiled.

<n>: The value specified for the LOGICALHOSTNUMBER parameter in the cluster setup information file (jimdbclustersetupinfo.conf) that was specified when the IM Configuration Management database and the integrated monitoring database for the logical host that is to be deleted were compiled.

11. On the standby host, delete the following symbolic link files:

- /etc/systemd/system/multi-user.target.wants/2248-PDxx-start.service
- /etc/systemd/system/multi-user.target.wants/2248-PDxx-stop.service
- /etc/systemd/system/multi-user.target.wants/2248-PDxx.service
- /etc/systemd/system/multi-user.target.wants/2248-pexx.service

Note that the *xx* in the file name stands for a number in a series, starting with 01. Before deleting the files, verify that they contain the following information.

Caution: Deleting files may adversely affect the system. For example, the IM database for the physical host may cease to operate correctly.

Verify that the files contain the following

<IMDBENVDIR>/JM<n>

<IMDBENVDIR>: The path specified for the IMDBENVDIR parameter in the cluster setup information file (jimdbsetupinfo.conf) that was specified when the IM Configuration Management database and the integrated monitoring database for the logical host that is to be deleted were compiled.

<n>: The value specified for the LOGICALHOSTNUMBER parameter in the cluster setup information file (jimdbclustersetupinfo.conf) that was specified when the IM Configuration Management database and the integrated monitoring database for the logical host that is to be deleted were compiled.

12. Update the configuration file for the IM database on the standby host by performing the following procedure:

- Delete /etc/opt/jplimm/conf/imdb/system/dbconf/JM<n>.
- Open /etc/opt/jplimm/conf/imdb/system/dbconf/jimdbsetuplist.conf in a text editor, edit the line equal to n+1 as follows, delete the logical host name, and then overwrite the file.

(Before editing) jimdbsetuplist.conf <line-number-n+1>

_JM<n>=<logical-host-name>

(After editing) jimdbsetuplist.conf <line-number-n+1>

_JM<n>=

<n>: The value specified for the LOGICALHOSTNUMBER parameter in the cluster setup information file (jimdbclustersetupinfo.conf) that was specified when the IM Configuration Management database and the integrated monitoring database for the logical host that is to be deleted were compiled.

13. Restart the operating system on the standby host.

14. Delete the following folder if it exists on the standby host:

- <IMDBDIR>/imdb
- <SHAREDDBDIR>/imdb
- <IMDBENVDIR>/JM<n>

<IMDBDIR>: The path specified for the IMDBDIR parameter in the cluster setup information file (jimdbclustersetupinfo.conf) that was specified when the IM Configuration Management database and the integrated monitoring database

for the logical host that is to be deleted were compiled.

<SHAREDDBDIR>: The path specified for the SHAREDDBDIR parameter in the cluster setup information file (jimdbclustersetupinfo.conf) that was specified when the IM Configuration Management database and the integrated monitoring database for the logical host that is to be deleted were compiled.

<IMDBENVDIR>: The path specified for the IMDBENVDIR parameter in the cluster setup information file (jimdbclustersetupinfo.conf) that was specified when the IM Configuration Management database and the integrated monitoring database for the logical host that is to be deleted were compiled.

<n>: The value specified for the LOGICALHOSTNUMBER parameter in the cluster setup information file (jimdbclustersetupinfo.conf) that was specified when the IM Configuration Management database and the integrated monitoring database for the logical host that is to be deleted were compiled.

2.24 Notes about installation and setting up (for UNIX)

Important

When creating a container environments on CentOS 8 (or later) or Linux 8 (or later), read Docker as Podman.

- JP1/IM can replicate integrated agent host by installing ServerConductor/DeploymentManager and JP1/ServerConductor/Deployment Manager disk-duplicate installations and using virtualization platform-provided image filling. The following virtualization platforms are supported:

- VMware ESX
- Hyper-V
- SCVMM
- Amazon EC2

For unsupported virtual platforms other than the above, uninstall JP1/IM and then reinstall JP1/IM after the disk-duplicate installation or replication by the virtualization platform.

For details on how to perform disk-copy installations, see the manuals for ServerConductor/DeploymentManager and JP1/ServerConductor/Deployment Manager. For details on the copy functions of virtualization platforms, see the relevant manual for the applicable virtualization software.

- Notes on monitoring containers in Docker environments as agent hosts
 - JP1/Base must be installed in the container. For details about Docker environments supported by JP1/Base, see the Release Notes for JP1/Base.
 - Specify the settings of port numbers to be used by JP1/Base in the container, so that TCP/IP communication is available from the JP1/IM - Manager host.
 - Because network address translation (NAT) is used for communication from containers to external locations, "Source IP address" does not display the correct value (in the way it is usually displayed) for an event issued from JP1/Base in the container. Do not use the IP address displayed in "Source IP address" for conditions of JP1/IM - Manager functions.

- Notes on monitoring containers in Docker environments as remote monitoring hosts

SSH must be installed in the container.

Specify the settings so that SSH connections can be made from the JP1/IM -Manager host to the container.

The remote monitoring function supports the following Docker environments:

Docker host OSs

Among the OSs supported by the remote monitoring function, the following OSs are supported:

- Red Hat Enterprise Linux Server 7.1 or later
- Cent OS 7.1 or later

Docker version

- Versions that support the previously described Docker host OSs.

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 `jplhosts` or `jplhosts2`. 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 `jplhosts` or `jplhosts2` are not referenced.
- Set a host name to be registered in IM Configuration Management so that the total number of characters in the host name and the installation path of JP1/IM -Manager does not exceed 235. If the total number exceeds 235, profiles cannot be collected from the monitored host.
- 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 *14.3.10 System configuration for managing monitored hosts with host names in FQDN format* in the *JP1/Integrated Management 3 - 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 *5.2 Register Host window* in the *JP1/Integrated Management 3 - 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 5.2 *Register Host window* in the *JP1/Integrated Management 3 - 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 5.20 *System Common Settings window* in the *JP1/Integrated Management 3 - 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 5.20 *System Common Settings window* in the *JP1/Integrated Management 3 - 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 5.7 *Remote Monitoring Settings window* in the *JP1/Integrated Management 3 - 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 *5.20 System Common Settings window* in the *JP1/Integrated Management 3 - 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 *5.7 Remote Monitoring Settings window* in the *JP1/Integrated Management 3 - 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 *5.1.1 Host List page* in the *JP1/Integrated Management 3 - 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 *5.4 Edit Host Properties window* in the *JP1/Integrated Management 3 - 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 *5.7 Remote Monitoring Settings window* in the *JP1/Integrated Management 3 - 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 *5.20 System Common Settings window* in the *JP1/Integrated Management 3 - 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 *5.1.2 IM Configuration page in the JP1/Integrated Management 3 - 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 *5.6 Edit Agent Configuration window* in the *JP1/Integrated Management 3 - 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 *5.8 Edit Remote Monitoring Configuration window* in the *JP1/Integrated Management 3 - 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 *5.5 Select Hosts window* in the *JPI/Integrated Management 3 - 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 *8.2.5 Editing the system hierarchy* in the *JPI/Integrated Management 3 - 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 *8.2.6 Applying the system hierarchy* in the *JP1/Integrated Management 3 - 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 *12.5.3(36) Actions to take when IM Configuration Management fails to apply the system hierarchy* in the *JP1/Integrated Management 3 - 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 *8.2.6 Applying the system hierarchy* in the *JP1/Integrated Management 3 - 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	• The domain name of the SCVMM host to which the manager connects, the names of users with administrator	• The OS on the host on which SCVMM is running is Windows Server 2012. • The SCVMM management console	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
	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.	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	- 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.	- 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
- 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.	- 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 `Id Name` when the `virsh list` command is executed, defined by KVM as the host name of a virtual host.

For details, see *8.3 Virtualization configuration management* in the *JP1/Integrated Management 3 - 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).

Important

Due to vCenter and VMware ESX specifications, vCenter and VMware ESX version 5.5 and version 6 only support HTTPS as the communication type used for acquiring the virtualization configuration information.

In addition, for other versions, HTTP connections might not be supported due to vCenter and VMware ESX specifications. When HTTP connections cannot be used, use HTTPS as the connection protocol between JP1/IM - Manager and vCenter and VMware ESX. For details about the support status of the vCenter and VMware ESX connection protocol, contact the original distributor of vCenter and VMware ESX.

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 Microsoft Edge and by obtaining the certificate files directly. To obtain an SSL certificate from vCenter, use Microsoft Edge. This subsection describes both methods.



Important

Grant appropriate access permissions so that the obtained certificate file is not accessed by OS users without administrator privileges.

■ Using Microsoft Edge

If you are using Microsoft Edge to obtain SSL certificates from VMware ESX or vCenter, see Microsoft Edge'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\jdk\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/jdk/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\jdk\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 italic 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 italic 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. Grant appropriate access permissions so that the obtained certificate file is not accessed by OS users without administrator privileges. 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. Grant appropriate access permissions so that the obtained certificate file is not accessed by OS users without administrator privileges.
- 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.
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.
2. 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.

1. Execute the `jcsdbexport` command to export monitoring tree information from Central Scope.
The exported information is output to the configuration file for monitoring tree.
2. 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.

Option	Value
-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.

3. 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 8.8.1 *Types of information that can be imported or exported* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

4. 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 *JPI/Integrated Management 3 - Manager Command, Definition File and API 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 *8.8.1 Types of information that can be imported or exported* in the *JPI/Integrated Management 3 - 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.

3.3.4 Notes when collecting the virtualization configuration

- When collecting the virtualization configuration, the IP address of the collected host will not be set.
- If virtualization configuration information is to be collected from versions of virtualization environment management software that are not supported by JP1/IM - Manager, the following message might be issued and the collection might fail:
KNAN22066-E Collection of the virtualization configuration failed because communication with host "host-name" was not possible.
For information about the virtualization environment management software that is supported, see the release note for JP1/IM - Manager.
- When collecting virtualization configurations from JP1/SC/CM When you collect virtualization configurations from JP1/SC/CM, an HVM IP address is set as the VMM host name.
- When collecting the virtualization information from the SCVMM and vCenter, do not specify ports other than the default port (SCVMM VMM Server:8100, vCenter Server HTTP:80, vCenter Server HTTPS:433) as the port used by SCVMM's VMM server to communicate with the management console, or the port used by vCenter Server.
 - SCVMM:
You cannot collect the virtualization configuration when you specify ports other than the default.
 - vCenter:
When you have changed either of the HTTP or HTTPS ports, and when the other port remains as default, specify the default port (communication type) for communication. If you change both ports to ports other than the default, you cannot collect the virtualization configuration.
- When you run several types of virtualization environment management software (SCVMM or vCenter) on the same host, and when you collect the virtualization configuration from JP1/IM - Manager, use the following settings:
 - (1) Set the aliases of the hosts on which several types of virtualization environment management software are running to the host on which JP1/IM - Manager is running. Set the same number of aliases as the number of types of virtualization environment management software that are used.
 - (2) Register all the aliases of the hosts set on JP1/IM - Manager in the above process (1), and set the information of each type of virtualization environment management software to each host. When collecting the virtualization configuration, execute the collection by host, or execute batch collection, as normal.

Note: For IM configurations, do not use the aliases defined in (1).
- Configurations in which Hyper-V and the virtualization environment management software (either SCVMM, vCenter, or JP1/SC/CM) are on the same host are not supported by JP1/IM - Manager. When you collect the virtualization configuration from JP1/IM - Manager, run Hyper-V and the virtualization environment management software on separate hosts.
- When you use a guest OS not supported by SCVMM (Hyper-V) and vCenter (VMWare ESX), you cannot collect the information of the guest OS by using JP1/IM - Manager.

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 [13.5.4 Considerations for business groups](#) in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

Important

When you use the business group functionality, set either of the following settings after installation:

For Windows

- If you do not use the host mapping functionality
Execute the following command from the command prompt, and overwrite the file:
`jp1cf_treedefaultpolicy_default.csv` to `jp1cf_treedefaultpolicy.csv`.
`copy Manager-path\conf\imcf\jp1cf_treedefaultpolicy_default.csv Manager-path\conf\imcf\jp1cf_treedefaultpolicy.csv`
- If you use the host mapping functionality
Execute the following command from the command prompt, and overwrite the file:
`jp1cf_treedefaultpolicy_hostmapping.csv` to `jp1cf_treedefaultpolicy.csv`.
`copy Manager-path\conf\imcf\jp1cf_treedefaultpolicy_hostmapping.csv Manager-path\conf\imcf\jp1cf_treedefaultpolicy.csv`

For Unix

- If you do not use the host mapping functionality
Execute the following command from the shell prompt, and overwrite the file:
`jp1cf_treedefaultpolicy_default.csv` to `jp1cf_treedefaultpolicy.csv`.

```
# cp /etc/opt/jplimm/  
conf/imcf/jp1cf_treedefaultpolicy_default.csv /etc/opt/jplimm/conf/  
imcf/jp1cf_treedefaultpolicy.csv
```
- If you use the host mapping functionality
Execute the following command from the shell prompt, and overwrite the file:
`jp1cf_treedefaultpolicy_hostmapping.csv` to `jp1cf_treedefaultpolicy.csv`.

```
# cp /etc/opt/jplimm/conf/  
imcf/jp1cf_treedefaultpolicy_hostmapping.csv /etc/opt/jplimm/conf/  
imcf/jp1cf_treedefaultpolicy.csv
```

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 *5.14 Create Business Group window* in the *JP1/Integrated Management 3 - 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 JP1 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 *5.15 Edit Business Group Basic Information window* in the *JP1/Integrated Management 3 - 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 *5.1 IM Configuration Management window* in the *JP1/Integrated Management 3 - 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 *5.18 Add or Delete Affiliated Hosts window* in the *JP1/Integrated Management 3 - 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 *5.1 IM Configuration Management window* in the *JP1/Integrated Management 3 - 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 *5.16 Create Monitoring Group window* in the *JP1/Integrated Management 3 - 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 *5.17 Edit Monitoring Group window* in the *JPI/Integrated Management 3 - 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 *5.18 Add or Delete Affiliated Hosts window* in the *JP1/Integrated Management 3 - 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 [5.19 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.

Important

If you apply a business group definition to the central scope (view and jcfmkcsdata command), then toggle the host mapping functionality and change the default monitoring definition, and then apply the changes to the central scope - the monitoring definition created the first time you applied the definition will continue to be used. If you want to use a new default monitoring definition, apply the changes after deleting the business tree of the central scope.

(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 *8.8.1 Types of information that can be imported or exported in the JP1/Integrated Management 3 - 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, run the `jcfmkcsdata` command with the `-g` option specified to merge the exported business group information, monitoring group information, and Central Scope monitoring tree information.

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	• 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	• Event transfer information • Log file trap information • Event log trap information • Local action information	• 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 5.9.1 *Valid Configuration Information page* in the *JP1/Integrated Management 3 - 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 5.9.2 *Configuration File page* in the *JP1/Integrated Management 3 - 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 *5.10 Add Profile window* in the *JP1/Integrated Management 3 - 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 *5.9.2 Configuration File page* in the *JP1/Integrated Management 3 - 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-I 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\conf</i>
		<i>Base-path\conf\any-folder</i>
		<i>Base-path\conf\cf_log_file_trap</i>
	UNIX	<i>/etc/opt/jplbase/conf</i>
		<i>/etc/opt/jplbase/conf/any-directory</i>
		<i>/etc/opt/jplbase/conf/cf_log_file_trap</i>
Log-file trap startup definition file	Windows	<i>Base-path\conf\event\</i>
	UNIX	<i>/etc/opt/jplbase/conf/event/</i>

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\conf\cf_log_file_trap\</i>
	UNIX	<i>/etc/opt/jplbase/conf/cf_log_file_trap/</i>

Configuration file	Type of OS on agent	Send destination
Log-file trap startup definition file	Windows	<i>Base-path\conf\event\</i>
	UNIX	<i>/etc/opt/jplbase/conf/event/</i>

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 `jbs_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
• Edit, save • Apply in batch mode • Apply by reloading configuration files	• Remote-monitoring log file trap information • Remote-monitoring event log trap information	• Remote-monitoring log file trap action-definition file • Remote-monitoring event log trap action-definition file

Operation	Type of profile you can manipulate	Corresponding configuration file
Apply by restarting remote monitoring log file traps		

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:

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 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 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 **Log File Trapping**.
6. 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**.
7. 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 *5.10 Add Profile window* in the *JP1/Integrated Management 3 - 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 *5.9.1 Valid Configuration Information page in the JP1/Integrated Management 3 - 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 *5.9.2 Configuration File page in the JP1/Integrated Management 3 - 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 5.9.2 *Configuration File page* in the *JP1/Integrated Management 3 - 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 *JP1/Integrated Management 3 - Manager Command, Definition File and API 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 `jcfaleltdef` 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 `jcfaleltreload` 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 *8.8 Exporting and importing IM Configuration Management information* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

For details about the export procedure, see *9.7.1 Exporting management information of IM Configuration Management* in the *JP1/Integrated Management 3 - 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 *8.8 Exporting and importing IM Configuration Management information* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

For details about the import procedure, see *9.7.2 Importing management information of IM Configuration Management* in the *JP1/Integrated Management 3 - 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 the Intelligent Integrated Management Base

This chapter explains the configuration of the Intelligent Integrated Management Base and how to create an environment for the base.

4.1 Overview of configuring an environment for the Intelligent Integrated Management Base

To configure an environment for the Intelligent Integrated Management Base, you have to create definitions of management groups (which are used for centralized monitoring of system configuration information acquired from linked products) and hosts.

The information provided in this chapter assumes that the Intelligent Integrated Management Base has been set up and is already up and running.

About the setup of the Intelligent Integrated Management Base

See [1.19.2 Settings for using the functions of the Intelligent Integrated Management Base \(for Windows\)](#) or [2.18.4 Specifying settings for using the functions of the Intelligent Integrated Management Base \(for UNIX\)](#).

4.1.1 Before configuring an environment for the Intelligent Integrated Management Base

Before configuring an environment for the Intelligent Integrated Management Base, make the following preparations:

Familiarize yourself with the general aspects of JPI/IM as well as with the Intelligent Integrated Management Base

- Overview of how to use the Intelligent Integrated Management Base

See *Chapter 1. Overview of JPI/Integrated Management* in the *JPI/Integrated Management 3 - Manager Overview and System Design Guide*.

See *Chapter 2. Overview of Functions* in the *JPI/Integrated Management 3 - Manager Overview and System Design Guide*.

- About the functions of the Intelligent Integrated Management Base

See *Chapter 3. IT Operations Optimization Using the Intelligent Integrated Management Base* in the *JPI/Integrated Management 3 - Manager Overview and System Design Guide*.

Create a JPI/IM operating environment

See [Chapter 1. Installation and Setup \(for Windows\)](#).

See [Chapter 2. Installation and Setup \(for UNIX\)](#).

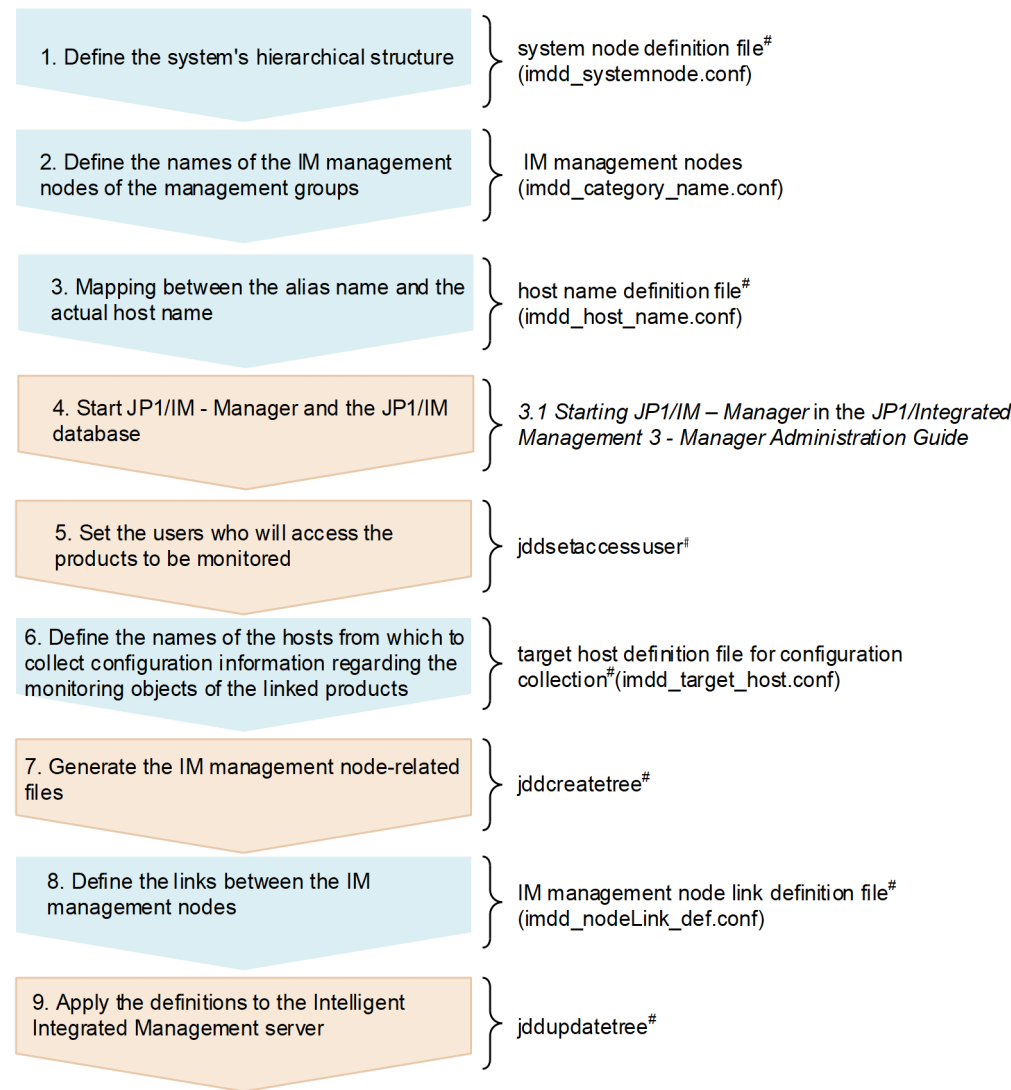
Set up the products to be monitored

Set up the products to be monitored and linked with the Intelligent Integrated Management Base in advance. For details about the setup procedures, see the manuals of the respective products.

4.2 Setting system configuration information

The following figure shows an overview of how system configuration information is acquired from linked products and set in the Intelligent Integrated Management Base.

Figure 4–1: Overview of acquiring system configuration information



For details see the manual *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

Legend:  : Required
 : Optional

The following steps correspond to the numbers shown in the figure:

1. Define the system's hierarchical structure by using the system node definition file (imdd_systemnode.conf). (optional)
For details about the system node definition file, see *System node definition file (imdd_systemnode.conf)* in Chapter 2. *Definition Files* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

2. By using the category name definition file for IM management nodes (`imdd_category_name.conf`), define the names of the IM management nodes of the management groups so that collected data can be displayed in a sunburst or tree chart format. (optional)
For details about the category name definition file for IM management nodes, see *Category name definition file for IM management nodes (imdd_category_name.conf)* in *Chapter 2. Definition Files* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.
3. By using the host name definition file (`imdd_host_name.conf`), define a mapping between the alias name and the actual host name. (optional)
This definition is necessary if you are to add a product in which an alias name can be specified as a host name to the IM management node configuration.
For details about the host name definition file, see *Host name definition file (imdd_host_name.conf)* in *Chapter 2. Definition Files* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.
4. Start JP1/IM - Manager and the JP1/IM database.
Start JP1/IM - Manager and the JP1/IM database, and then acquire system configuration management information.
For details about how to start the IM database, see *3.1 Starting JP1/IM - Manager* in the *JP1/Integrated Management 3 - Manager Administration Guide*.
5. Execute the `jddsetaccessuser` command to set the users who will access the products to be monitored while collecting system configuration information.
For details about the `jddsetaccessuser` command, see *jddsetaccessuser* in *Chapter 1. Commands* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.
6. By using the target host definition file for configuration collection (`imdd_target_host.conf`), define both the linked products and the names of the hosts from which to collect configuration information regarding the monitoring objects of the linked products. (optional)
For details about the target host definition file for configuration collection (`imdd_target_host.conf`), see *Target host definition file for configuration collection (imdd_target_host.conf)* in *Chapter 2. Definition Files* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.
7. By executing the `jddcreatetree` command, generate the IM management node-related files.
For details about the `jddcreatetree` command, see *jddcreatetree* in *Chapter 1. Commands* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.
Open the created IM management node-related files and check their content. For details about the IM management node-related files, see the section explaining the IM management node-related files in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.
8. By using the IM management node link definition file (`imdd_nodeLink_def.conf`), define the links between the IM management nodes. (optional)
For details about the IM management node link definition file (`imdd_nodeLink_def.conf`), see *IM management node link definition file (imdd_nodeLink_def.conf)* in *Chapter 2. Definition Files* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.
9. By executing the `jddupdatetree` command, apply the definitions to the Intelligent Integrated Management server.
For details about the `jddupdatetree` command, see *jddupdatetree* in *Chapter 1. Commands* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

**Note**

If you change the configuration of the IM management nodes, repeat this procedure starting from step 5.

4.3 Settings for using the encryption function with the Intelligent Integrated Management Base

The encrypted communication function for the Intelligent Integrated Management Base encrypts communication between the viewer (integrated operation viewer) of the Intelligent Integrated Management Base and JP1/IM - Manager.

Encrypted communication uses the port specified with `server.port` property in the Intelligent Integrated Management Base definition file (`imdd.properties`). For details, see *Intelligent Integrated Management Base definition file (imdd.properties)* in *Chapter 2. Definition Files* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

For details about encrypted communication, see the section explaining encrypted communication in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

4.4 Creating a cluster environment for the Intelligent Integrated Management Base

For details about creating a cluster environment for JP1/IM - Manager hosts running on a cluster system using Intelligent Integrated Management Base, see [7.4 Creating a cluster environment for the Intelligent Integrated Management Base \(for Windows\)](#) and [8.4 Setup for Intelligent Integrated Management Base's cluster environment \(for UNIX\)](#).

4.5 Settings necessary to use the custom UI display function

The custom UI display function displays in the **Details** area the window corresponding to the IM management node selected by a user. A window corresponding to each IM management node must be defined in advance.

You have to specify the following settings to use the custom UI display function:

1. Place the HTML files defining the windows to be displayed in the integrated operation viewer inside a subfolder or a subdirectory.

The location to place the definition files is the same between the physical host and the logical host. In the case of a cluster configuration, the same files must be placed on both the physical host and the logical host.

Create either a subfolder or a subdirectory in one of the following locations. Note that you cannot use a subfolder or subdirectory with a name that begins with `hitachi`.

For Windows

`Manager-path\public\customUI\`

For UNIX

`/opt/jp1imm/public/customUI/`

For details about how to create files defining the windows and definition examples, see *Chapter 6. Customization of Integrated Operation Viewer Window* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

2. Edit the Intelligent Integrated Management Base definition file (`imdd.properties`).

Specify the following properties. You cannot omit any of these properties.

`jp1.imdd.gui.settings.contentView.<custom UI Id>.title`

`jp1.imdd.gui.settings.contentView.<custom UI Id>.url`

`jp1.imdd.gui.settings.contentView.<custom UI Id>.sid`

`jp1.imdd.gui.settings.contentView.<custom UI Id>.target`

For details about a properties, see *Intelligent integrated management infrastructure definition file (imdd.properties)* in *Chapter 2. Definition Files* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

3. In the integrated operation viewer, select the IM management node that you have defined in the Intelligent Integrated Management Base definition file (`imdd.properties`), and confirm that a window shows up.

If the definition information is invalid, a message shows up in a dialog box. In that case, follow the instructions provided in the message.

If you are checking definition information by using Internet Explorer as the Web browser, do not enable Compatibility View of Internet Explorer. If you attempt to display a window with Compatibility View enabled, the window might become stuck at the loading state. Once you are done checking definition information, you can enable Compatibility View of Internet Explorer.

Although the location of HTML files is the same between the physical host and the logical host, you can define which HTML file to display by using the Intelligent Integrated Management Base definition file (`imdd.properties`) on the individual hosts. For example, if you simultaneously start JP1/IM - Manager belonging to the physical host and the one belonging to the logical host on the same host, you can view custom UI displays corresponding to the different HTML files on the integrated operation viewer. For details about the methods and objects available in HTML files you created, see *6.3 Methods and objects that can be used in the user definition window* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

For details about the *Intelligent integrated management infrastructure definition file (imdd.properties)*, see *Intelligent integrated management infrastructure definition file (imdd.properties)* in Chapter 2. *Definition Files* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

4.6 Compatible setting of the repeated event viewing suppression function

With JP1/IM - Manager (Intelligent Integrated Management Base) version 12-00, even when the `jcoimdef` command is executed with the repeated event monitoring suppression (`-storm` option) set to ON, repeated events are still displayed. Therefore, if you upgraded from version 12-00, to use the repeated event viewing suppression function, the compatible setting of the repeated event viewing suppression function must be disabled (false).

If you new install a version 12-10 or later, the compatible setting of the repeated event viewing suppression Function is setting to Disabled (false) beforehand.

You can edit the compatibility view setting for repeated events by using the `jpl.imdd.event.stormCompatible` property in the Intelligent Integrated Management Base definition file (`imdd.properties`).

The following table describes the conditions under which the repeated event display suppression function in the Intelligent Integrated Management Base becomes enabled.

Table 4–1: Conditions under which the repeated event display suppression function becomes enabled

Value set for <code>-storm</code>	Setting specified for <code>jpl.imdd.event.stormCompatible</code>	Repeated event display suppression function
on (enabled)	true (compatible with version 12-00)	Disabled
	false (disabled)	Enabled
off (disabled)	true (compatible with version 12-00)	Disabled
	false (disabled)	Disabled

For details about the `jcoimdef` command, see `jcoimdef` in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

For details about the Intelligent Integrated Management Base definition file, see *Intelligent Integrated Management Base definition file (imdd.properties)* in *Chapter 2. Definition Files* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

4.7 Defining links

If you want to define new links in addition to the links available as standard to users of JP1/IM products, you have to define links between IM management nodes in the IM management node link definition file (`imdd_nodeLink_def.conf`).

For details about the IM management node link definition file (`imdd_nodeLink_def.conf`), see *IM management node link definition file (imdd_nodeLink_def.conf)* in *Chapter 2. Definition Files* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

4.8 Setting work impact icons

By checking links between root jobnets on the **Job flow** tab of the integrated operation viewer, you can identify the scope of the impact a problem that has occurred in a preceding root jobnet has on the following root jobnet. However, depending on the type of job the preceding root jobnet failed to execute, the following root jobnet might not be impacted at all by the failure. Links between root jobnets are therefore accompanied by icons (*work impact icons*) indicating whether a failure that occurred in a preceding root jobnet has an impact on the following root jobnet.

The possible impact on the following root jobnet is determined by acquiring the status of the linked units of the preceding root jobnet. A work impact icon is displayed for information related to the IM management node selected in the tree that corresponds to either the preceding root jobnet or the following root jobnet. When there is no impact on the following root jobnet, no icon is displayed.

The following table describes the types and display criteria of work impact icons to be displayed.

Table 4–2: Types and display criteria of work impact icons

work impact icons	Display criteria
 (Impact found)	The icon is displayed if a linked unit of the preceding root jobnet has ended with an error or it has the <code>Not executed + Ended</code> status.
 (Error during an impact check)	The icon is displayed if one of the following criteria is met: - An attempt to get information from JP1/AJS - Manager failed. - The unit specified as the preceding unit is not found in JP1/AJS - Manager, or the execution registration of the unit is not performed. - The number of relations between root jobnets from which impact information is obtained exceeded its maximum number. For details about the maximum number setting, see the JP1/AJS documentation.
 (Impact unknown)	The icon is displayed if one of the following criteria is met: - The preceding or following root jobnet is one managed by JP1/AJS - Manager earlier than version 12-10. - Any relations defined in the IM management node link definition file (<code>imdd_nodeLink_def.conf</code>) do not specify linked unit information. - The preceding root jobnet is an UNKNOWN node.

When multiple unit information exists for one link connecting root jobnets, if the impact varies across units, the icons are displayed in the following order: di019170.tif (impact found), di019160.tif (error during an impact check), di019150.tif (impact unknown), and no icon.

You can specify whether to display the  icon by setting the `jp1.imdd.gui.linkedUnit.impact.unknownDisplay` property in the Intelligent Integrated Management Base definition file (`imdd.properties`). By default, display of work impact icons is enabled. If you disable the display of icons, a blank is displayed.

You can specify information regarding linked units by setting `unit` of the `value` parameter in the IM management node link definition file (`imdd_nodeLink_def.conf`). If you upgrade JP1/IM - Manager (Intelligent Integrated Management Base) from version 12-00, you have to add the `unit` definition of the `value` parameter to the link definition for which `rootJobnetExecutionOrder` (root jobnet execution order) is specified as the type in the `type` parameter. Without this definition added to the link definition, either the di019150.tif icon or a blank is displayed.

For details, see *IM management node link definition file (`imdd_nodeLink_def.conf`)* and *Intelligent Integrated Management Base definition file (`imdd.properties`)* in Chapter 2. *Definition Files* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

4.9 Monitor startup setting for linked products

For details about how to set up monitor startup in the Intelligent Integrated Management Base, see [5.17 Setting monitor startup for linked products](#).

4.10 Setting up the suggestion function for response actions depending on the system status

The system administrator sets up the suggestion function for response actions depending on the system status, based on the operating procedures.

To set up the suggestion function:

1. Create a suggestion definition file.

When creating it, define the following:

- Criteria for displaying response actions
Define which IM management nodes the response actions are displayed in.
- Criteria of the users which the response actions are displayed for
Associate the response actions with the users which they are displayed for.
- Criteria for suggesting the response actions
Define when the response action is suggested, such as criteria for JP1 events, the number of time-series data sets, and command execution results.
- What the response action does
Define what the action does, such as execution of the REST API or product plug-in functions, and change in the event status.

2. Use the `jddupdatesuggestion` command to apply the suggestion definition file you created to JP1/IM - Manager (Intelligent Integrated Management Base).

A suggestion icon now appears in the tree of the Integrated Operation Viewer, indicating that the defined IM management node has a suggestion. If the defined criteria for displaying the response action are satisfied, what the response action does and the information on the previous execution are displayed in the **Suggestion** tab of the Integrated Operation Viewer window.

For details about the suggestion definition file, see *Suggestion definition file* in *Chapter 2. Definition Files* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

4.11 Settings for linkage with an OpenID provider through single sign-on (linkage with external products)

This section describes the settings for linkage with external products other than JP1 products authenticated by an OpenID provider through single sign-on.

4.11.1 Providing linkage with an OpenID provider through single sign-on

This subsection describes how to provide linkage with an OpenID provider through single sign-on.

Note that the settings for OpenID authentication will take effect after JP1/IM - Manager is restarted. If you set up the linkage when JP1/IM - Manager is up and running, the settings are not applied yet when you go through the steps to step 6.

In addition, OpenID authentication may fail if there is a time difference between the OpenID provider and the JP1/IM - Manager host.

In such cases, align the time of the OpenID provider with the JP1/IM - Manager host with precision in seconds. The allowable time variance depends on the OpenID provider's specifications and settings.

1. Register the Intelligent Integrated Management Base in the linked OpenID provider and get the client ID and client secret in the Intelligent Integrated Management Base client information.

For details about how to register the client, see the specifications of the OpenID provider to be linked.

- If you use OpenID authentication as a method to authenticate the REST API of the Intelligent Integrated Management Base, you need the login user name in the access token when mapping the JP1 user name to the user name registered in the OpenID provider. Therefore, if you use OpenID authentication, configure the linked OpenID provider so that the login user name for the OpenID provider is contained in the `preferred_username` claim of the access token. For details about OpenID authentication, see 5.2.8 *Authentication methods for REST API* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.
- After the login or logout process via the OpenID provider is successful, the Web browser is redirected to the Intelligent Integrated Management Base. Therefore, allow the URI of the redirection URL specified for `jp1.imdd.oidc.<key-name-of-the-OpenID-provider>.redirect-uri` in the Intelligent Integrated Management Base and redirection of the login URI for the Intelligent Integrated Management Base.

2. Define the information on the linked OpenID provider in the Intelligent Integrated Management Base definition file (`imdd.properties`).

For details about the properties you define, see *Intelligent Integrated Management Base definition file (imdd.properties)* in *Chapter 2. Definition Files* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

Obtain the configuration information from the OpenID provider and configure the setting values of the properties with the information. The OpenID provider provides its configuration information using the following URI path, based on the OpenID Connect specifications:

```
/.well-known/openid-configuration
```

For details, see the specifications of the OpenID provider to be linked.

3. Use the `jddsetaccessuser` command to set up the JP1 user used in the Intelligent Integrated Management Base. If the user has already been set up, you can skip this step.

For details about the `jddsetaccessuser` command, see *jddsetaccessuser* in *Chapter 1. Commands* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

4. Use the `jddsetopinfo` command to set up the client ID and client secret registered in the OpenID provider obtained in step 1.
For details about the `jddsetopinfo` command, see *jddsetopinfo* in *Chapter 1. Commands* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.
5. If you connect the Intelligent Integrated Management Base with the OpenID provider via a proxy server, define proxy information in the Intelligent Integrated Management Base definition file (`imdd.properties`).
If you do not have any proxy server, you can skip this step. If user authentication for the proxy server is required, proceed to step 6.
6. If user authentication for the proxy server is required, define user information in the Intelligent Integrated Management Base definition file (`imdd.properties`) and use the `jddsetproxyuser` command to set up authentication information.
If no user authentication for the proxy server is required, you can skip this step.
For details about the `jddsetproxyuser` command, see *jddsetproxyuser* in *Chapter 1. Commands* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.
7. Start the JP1/IM - Manager service.
If the service is already running, restart it.
8. Define the mapping between the user name registered in the OpenID provider and the JP1 user name registered in JP1/Base, in the single sign-on mapping definition file.
For details about the single sign-on mapping definition file, see *Single sign-on mapping definition file (imdd_sso_mapping.properties)* in *Chapter 2. Definition Files* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.
9. Use the `jddupdatessomap` command or the single sign-on mapping definition application API (`im_api_v1_updateSsoMap`) for the definition to take effect.
For details about the `jddupdatessomap` command, see *jddupdatessomap* in *Chapter 1. Commands* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.
For details about the single sign-on mapping definition application API (`im_api_v1_updateSsoMap`), see *5.14.1 Single sign-on mapping definition application* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

4.11.2 How to reload the single sign-on mapping definition file (`imdd_sso_mapping.properties`)

This subsection describes how to reload the single sign-on mapping definition file (`imdd_sso_mapping.properties`).

For details about the single sign-on mapping definition file (`imdd_sso_mapping.properties`), see *Single sign-on mapping definition file (imdd_sso_mapping.properties)* in *Chapter 2. Definition Files* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

1. Edit the mapping between the user name registered in the OpenID provider and the JP1 user name registered in JP1/Base, in the single sign-on mapping definition file (`imdd_sso_mapping.properties`).

2. Use the `jddupdatessomap` command or the single sign-on mapping definition application API (`im_api_v1_updateSsoMap`) for the definition to take effect.
For details about the `jddupdatessomap` command, see *jddupdatessomap* in *Chapter 1. Commands* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.
For details about the single sign-on mapping definition application API (`im_api_v1_updateSsoMap`), see *5.14.1 Single sign-on mapping definition application* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

4.11.3 How to stop linkage with the OpenID provider

This subsection describes how to stop linkage with the OpenID provider.

1. Stop the JP1/IM - Manager service.
2. Remove the Intelligent Integrated Management Base information registered in the linked OpenID provider.
3. Use the `jddsetopinfo` command to remove the client ID and client secret registered in the OpenID provider.
For details about the `jddsetopinfo` command, see *jddsetopinfo* in *Chapter 1. Commands* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.
4. Use the `jddsetproxyuser` command to remove the proxy server authentication information configured in the Intelligent Integrated Management Base.
If you use the proxy server for communications other than OpenID authentication of the Intelligent Integrated Management Base, you can skip this step.
For details about the `jddsetproxyuser` command, see *jddsetproxyuser* in *Chapter 1. Commands* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.
5. Edit the Intelligent Integrated Management Base definition file (`imdd.properties`) to remove the properties for the linked OpenID provider that is registered. Remove the properties when the proxy information is defined.
For details about the Intelligent Integrated Management Base definition file (`imdd.properties`), see *Intelligent Integrated Management Base definition file (imdd.properties)* in *Chapter 2. Definition Files* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.
6. Edit the single sign-on mapping definition file for the Intelligent Integrated Management Base to remove all mapping definitions.
7. Start the JP1/IM - Manager service.
8. Use the `jddupdatessomap` command or the single sign-on mapping definition application API (`im_api_v1_updateSsoMap`) for the definition to take effect.
The `KAJY52031-W` message is output, because the purpose is to clear the single sign-on mapping definitions.
For details about the `jddupdatessomap` command, see *jddupdatessomap* in *Chapter 1. Commands* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.
For details about the single sign-on mapping definition application API (`im_api_v1_updateSsoMap`), see *5.14.1 Single sign-on mapping definition application* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

4.12 Setting up the direct access URL

The URL for direct access should contain information for displaying the window you want as query parameters. Specify the query parameters for each function after `index` in the Integrated Operation Viewer window.

The format of the URL is as follows:

```
http://host-name-of-the-Intelligent-Integrated-Management-server:port-number/index?<query parameters>=<value>&<query parameters>=<value>&eou=1
```

Note: `https` is used for SSL communication.

4.12.1 Direct access URL

The table below shows query parameters specified in a direct access URL. Specify a URL-encoded value for each query parameter.

Table 4–3: Query parameters for the direct access URL

No.	Query parameter	Required/optional	Description
1	seqno	Optional	Specifies the serial number.
2	sid	Optional	Specifies the tree SID of the node that will be displayed in the selected state. If this parameter is omitted, the system assumes that the tree SID of All Systems at the beginning of the tree is selected. When <code>seqno</code> is specified, the <code>sid</code> value corresponding to the serial number is obtained and overwritten regardless of whether the <code>sid</code> parameter is specified.
3	dialog	Optional	Specifies to show the Event detail window when <code>detail</code> is specified. If this parameter is omitted, or if an invalid value is specified, the SID of a JP1 event is not obtained.
4	tab	Optional	Specifies the tab that will be displayed for direct access. You can specify one of the following values: <code>_HITACHIJP1PFMWC</code> It shows the Performance tab. <code>custom UI Id[#]</code> It shows the Custom UI tab. For <i>Id</i>, specify the value designated for the <code>jpl.imdd.gui.settings.contentView.<custom UI Id></code> property of the custom UI display function. <code>suggestion</code> It shows the Suggestion tab. <code>job</code> It shows the Job flow tab. <code>relation</code> It shows the Related node tab. <code>trend</code> It shows the Trends tab. If this parameter is omitted, the tabs are shown according to the priorities of the tabs to be displayed. For details, see Table 4-4 .

No.	Query parameter	Required/optional	Description
5	view	Optional	Specifies the format of the Operating status area in the Integrated Operation Viewer window to be displayed. You can specify one of the following formats: - sunburst: Sunburst chart format - tree: Tree chart format If the parameter is omitted, the system assumes sunburst.
6	eou	Required	URL terminal flag. Specify 1 at the end of a URL.

#

For details about the `jpl.imdd.gui.settings.contentView.<custom UI Id>` property of the custom UI display function, see 6.2 *Customization definition information of the Integrated Operation Viewer window* in the *JPI/Integrated Management 3 - Manager Command, Definition File and API Reference*.

Table 4–4: Priority of the tab to be displayed

Tab name	Priority
Performance	1
Custom UI [#]	2
Suggestion	3
Job flow	4
Related node	5
Trends	6

#

The window shows as many tabs as the number of the Custom UI tabs defined by the user. Note that the Custom UI tabs are displayed in the order of the definition in the Intelligent Integrated Management Base definition file (`imdd.properties`). For details, see *Intelligent Integrated Management Base definition file (imdd.properties)* in Chapter 2. *Definition Files* in the *JPI/Integrated Management 3 - Manager Command, Definition File and API Reference*.

Important

- If a serial number is changed due to a server replacement, a disk failure, or other reasons, the serial number might overlap in the integrated monitoring database of JPI/IM - Manager. If the serial number overlaps, the event information on the latest event is obtained by the `seqno` parameter. Thus, if the serial number retrieved from the information on an old incident is specified for the `seqno` parameter, an unwanted event might be obtained. If the serial number is changed, check that the details of the incident coincide with the ones of the event when specifying the parameter.
- Because the serial number specified for the `seqno` parameter is redirected after the `sid` value corresponding to the serial number is obtained, it does not remain in the Web browser address bar. Therefore, take measures so that the serial number is retained at the calling source and the event information can be checked.

4.12.2 Getting the direct access URL for node selection

Use **Copy tree URL** from **Operation menu** in the Integrated Operation Viewer window to get the direct access URL for node selection.

For details, see *2.1 Overview of the Integrated Operation Viewer window in the JPI/Integrated Management 3 - Manager GUI Reference*.

The direct access URL generated by **Copy tree URL** is formatted as:

```
http://server-host-name:port-number/index?sid=<sid>&view=<view>&eou=1
```

The following table shows the meanings of the values specified in the query parameters.

Table 4–5: Query parameters for getting the direct access URL for node selection

Query parameter	Meaning
sid	The tree SID corresponding to the node that was selected when you clicked the Copy tree URL button.
view	The format of the Operating status area that was displayed when you clicked the Copy tree URL button. - sunburst: Sunburst chart format - tree: Tree chart format
eou	It always shows 1.

The following direct access URL is an example when the node on the host HOSTB that belongs to the system SYSTEM01 is selected if the area is displayed in the sunburst chart format, obtained by clicking the **Copy tree URL** button:

```
http://HOSTA:20703/index?sid=%5FROOT%5FAllSystems%2F%5FSYSTEM%5FSYSTEM01%2F%5FHOST%5FHOSTB&view=sunburst&eou=1
```

4.12.3 OpenID authentication direct access URL

The OpenID authentication direct access URL function enables the direct access URL function to be used in single sign-on through OpenID authentication. You can specify it together with the query parameters for the direct access URL.

The table below shows the parameter specified in the query parameter. Specify a URL-encoded value for each parameter.

Table 4–6: Query parameter for the direct access URL for OpenID authentication

No.	Query parameter	Required/optional	Description
1	op	Optional	Specifies the name of an OpenID provider. The name of the OpenID provider must have the same value as the one of <i><key-name-of-the-OpenID-provider></i> defined in the Intelligent Integrated Management Base definition file (<i>imdd.properties</i>). When you specify this parameter, an authentication request is made to the authentication URL of the specified OpenID provider without the login window of the Intelligent Integrated Management Base. If the key name of the OpenID provider does not exist, the system assumes that no <i>op</i> parameter is specified for operation.

The following table shows how the OpenID authentication direct access URL function works based on whether the *op* parameter is specified, the *jp1.imdd.jp1LoginForm* parameter of Intelligent Integrated Management Base definition file (*imdd.properties*), and the number of OpenID provider definitions defined for the OpenID provider definition function.

Table 4–7: Relationship among the op parameter, the number of OP definitions, and the jp1.imdd.jp1LoginForm parameter

op parameter	Number of OP definitions	Specified jp1.imdd.jp1LoginForm value	
		true	false
Omitted	None	The login window is displayed.	The login window is displayed. (The JP1/Base authentication login form is displayed.)
	1		An authentication request is sent to the authentication URL of the OpenID provider.
	2 or more		The login window is displayed.
Specified	None	The login window is displayed. (The specification of the op parameter is ignored.)	
	1	An authentication request is sent to the authentication URL of the OpenID provider.	
	2 or more		

Note that if the jp1.imdd.jp1LoginForm parameter is set to false and only one OpenID provider is defined, authentication is performed directly through the defined OpenID provider even when the op parameter is omitted.

Important

The op parameter is not added to the URL obtained by **Copy tree URL** selected from **Operation menu** in the Integrated Operation Viewer window.

The following is an example of the direct access URL in the conditions below:

- Show the Integrated Operation Viewer window while the node on the host HOSTB that belongs to the system SYSTEM01 is selected.
- Okta authentication
- View format: Sunburst chart

```
http://host-name-of-the-Intelligent-Integrated-Management-server:port-number/index?op=okta&sid=%5FROOT%5FAllSystems%2F%5FSYSTEM%5FSYSTEM01%2F%5FHOST%5FHOSTB&view=sunburst&eou=1
```

4.12.4 Examples of specifying direct access URLs

This subsection describes some examples of specifying direct access URLs.

Note that if you have changed the port number on which HTTP communication is received in the Intelligent Integrated Management Base service, change the port number 20703 in the definition example to the changed one. In addition, if you use the communication encryption function of JP1/IM - Manager to encrypt communications between your Web browser and the Intelligent Integrated Management Base, change http to https.

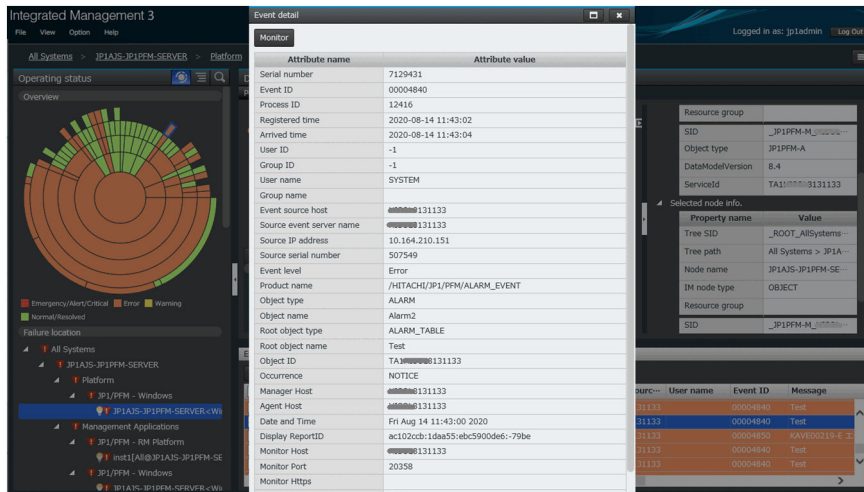
(1) When you make access by specifying the Event detail window

URL

```
http://server-host-name:port-number/index?seqno=3611&dialog=detail&eou=1
```

What window is displayed

The Event detail window appears with the IM management node having the applicable seqno (serial number) selected.



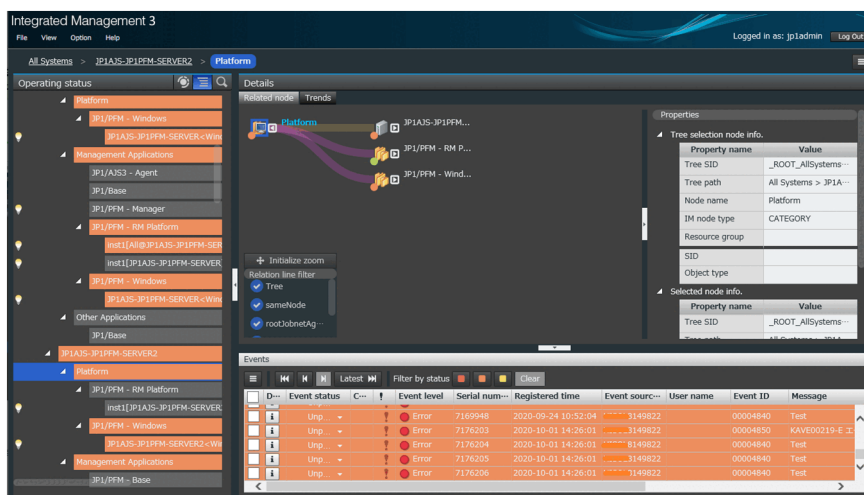
(2) When you make access by selecting a tab

URL

```
http://server-host-name:port-number/index?seqno=3611&tab=relation&eou=1
```

What window is displayed

The specified tab is displayed with the IM management node having the applicable seqno (serial number) selected.
The **Related node** tab is specified in the above URL.



(3) When you make access by specifying a tab and the Event detail window

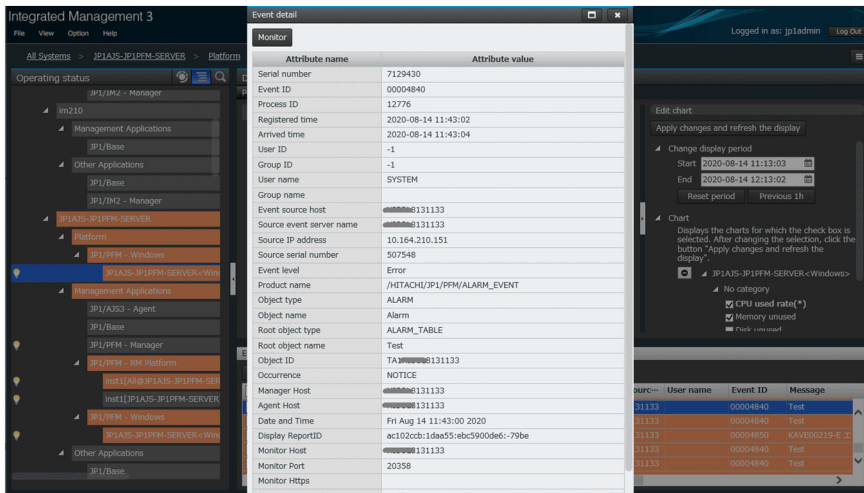
URL

```
http://server-host-name:port-number/index?seqno=3611&dialog=detail&tab=trend&eou=1
```

What window is displayed

The specified tab is displayed with the IM management node having the applicable `seqno` (serial number) selected, and the Event detail window also appears.

The **Trends** tab is specified in the above URL.



(4) Examples of defining automated actions

The following provides examples of using the direct access URL through the automated action function.

Example 1

In the Integrated Operation Viewer window, you send an email notification containing the URL for checking the business impact of a specific IM management node, to the person in charge (`userA`) via an automated action.

When the email recipient clicks the URL in the email body, the direct access URL function displays the Integrated Operation Viewer window, with the **Job flow** tab open.

Email definitions

From: `admin@xxxxxx.com`

To: `userA@xxxxxx.com`

Email subject: Check the impact on your business

Email body: `http://host-name-of-the-Intelligent-Integrated-Management-server:20703/index?seqno=73&tab=job&eou=1`

Command definition example

```
jimmail.exe -to userA@xxxxxx.com -s "Check the impact on your business" -b "http://$ACTHOST:20703/index?seqno=$EVSEQNO&tab=job&eou=1"
```

Example 2

In the Integrated Operation Viewer window of the Intelligent Integrated Management Base, you send an email notification containing the URL for checking the Event detail window on the applicable node, to the person in charge (userA) via an automated action when a failure occurs.

When the email recipient clicks the URL in the email body, the direct access URL function displays the Integrated Operation Viewer window, with the Event detail window open.

Email definitions

From: admin@xxxxxx.com

To: userA@xxxxxx.com

Email subject: [Severity:Error] Failure Notification

Email body: `http://host-name-of-the-Intelligent-Integrated-Management-server:20703/index?seqno=74&detail=1&eou=1`

Command definition example

```
jimmail.exe -to userA@xxxxxx.com -s "[Severity:$EVSEV] Failure Notification" -b "http://$ACTHOST:20703/index?seqno=$EVSEQNO&dialog=detail&eou=1"
```

4.13 Configuring the method for applying system configuration information

System configuration information can be viewed and managed from integrated operation viewer (WebGUI). It also provides the ability to modify setup by downloading and uploading manager and agent defined file from integrated operation viewer, and the ability to generate and reflect IM management node trees.

For detail, see *3.6 Operation using WebGUI (integrated operation viewer)* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

This section explains the method for applying system configuration information.

You specify the method for applying system configuration information by using options of the `jddupdatetree` command. Note that if you do not specify the options on the application method with the `jddupdatetree` command, it follows the definition of the `jp1.imdd.simt.updateMode` property in the Intelligent Integrated Management Base definition file (`imdd.properties`).

Specify the *new and rebuilding mode* in the following cases:

- When you create a new configuration
- When you backed up the IM database (`jimdbbackup` command) and then recovered it (`jimdbrecover` command)
- When you unset up the integrated monitoring database (`jcodbunsetup` command) and set it up again (`jcodbsetup` command)
- When you upgraded JP1/IM - Manager in the environment where the Intelligent Integrated Management Base was used

Specify the *configuration change mode* in the following case:

- When a managed target of the Intelligent Integrated Management Base is added, removed, or modified in addition to correction of misconfiguration

For details about the `jddupdatetree` command, see *jddupdatetree* in *Chapter 1. Commands* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*, and for details about the Intelligent Integrated Management Base definition file (`imdd.properties`), see *Intelligent Integrated Management Base definition file (imdd.properties)* in *Chapter 2. Definition Files* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

4.14 Migration procedure of the IM management node link definition file

This section describes the procedure for integrating the information that is displayed in **Scheduled date and time for linkage** of the Linked unit dialog box with automatically associated information through the association function of the root jobnet, when JP1/IM and JP1/AJS are upgraded to 12-50 or later.

This migration procedure only covers the environment where wait conditions and jobnet connectors are defined in the IM management node link definition file (`imdd_nodeLink_def.conf`).

For details about the IM management node link definition file (`imdd_nodeLink_def.conf`), see *IM management node link definition file (imdd_nodeLink_def.conf)* in *Chapter 2. Definition Files* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

For details about the Linked unit dialog box, see *3.14.2 Business impact determination support* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

1. Check that the IM management node link definition file (`imdd_nodeLink_def.conf`) exists.
2. Check that `type` (process target type) is set to `rootJobnetExecutionOrder` (relationship of execution order of a root jobnet) in the IM management node link definition file.
3. Check that the definition of `rootJobnetExecutionOrder` satisfies the items shown below.

If it satisfies them, you can skip step 4 and later.

- A relationship between the following units with the wait conditions is defined:
`from`: Unit whose end is being waited for
`to`: Unit with the wait condition
- A relationship with the following jobnet connectors is defined:
`from`: Destination root jobnet or a jobnet connector
`to`: Jobnet connector or a destination root jobnet

4. Remove the settings from the IM management node link definition file.

Remove the definitions that satisfied the conditions in step 3.

5. Execute the `jddcreatetree` command.

Execute the `jddcreatetree` command to get the configuration information. For details about the `jddcreatetree` command, see *jddcreatetree* in *Chapter 1. Commands* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

6. Execute the `jddupdatetree` command.

Execute the `jddupdatetree` command to create the tree information and link information of the IM management node. For details about the `jddupdatetree` command, see *jddupdatetree* in *Chapter 1. Commands* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

4.15 Web browser setup procedure to use the integrated operation viewer

To use the integrated operation viewer, perform the following procedure. You must set up your Web browser as follows before you can use Intelligent Integrated Management Base. For details about how to set up your web browser, see the documentation for your Web browser.

- Enable JavaScript.
- Enable cookies.
- Enable the display of images (GIF data).
- Check the pop-up blocker settings.

Enabling the pop-up blocker might block the display of dialog boxes. To prevent such problems, add the address of the integrated operation viewer to the permitted sites.

To use the communication encryption function of JP1/IM - Manager (communication between the Web browser and Intelligent Integrated Management Base is encrypted by HTTPS), you need to enable the SSL/TLS settings of your Web browser. If the root certificate of the Certificate Authority that issued a server certificate has not been imported, import it.

4.16 Dashboard Configuration

You can set the contents to be displayed on the Dashboard window and the **Dashboard** tab of the Integrated operation viewer according to your operation.

By setting a dashboard suitable for the monitored system, you can visualize the health of the IT system.

4.16.1 Customizing Auto-Generated Dashboards

Integrated operation viewer defaults to the auto-generated dashboard in the **Dashboard** tab for each IM management node selected in the **Operating status** area.

To customize this auto-generated dashboard, follow these steps:

1. Select the **Duplicate Dashboard** menu from the **Dashboard** tab operation menu.
2. Enter any dashboard name in the **Dashboard** tab edit screen.
3. After adding or editing a panel, click the **Save** button and then click the **Finish** button to exit.

If you want to edit a customized dashboard, you can edit it from the **Edit** menu.

4.16.2 Creating a new dashboard

In integrated operation viewer, you can create any new dashboard that is independent of a particular IM management node. After you create a dashboard, you can copy URL of the dashboard and use it as a separate **Dashboard** window.

In addition, by registering the created dashboard as a favorite, you can select any IM management node and view it from the side menu of the **Dashboard** tab.

To create a new dashboard, follow these steps:

1. Select **View-Dashboard List** from Integrated Operation Viewer window menu.
2. Click the **Add New** button in the **Dashboard List** dialog box.
3. Enter the desired dashboard name on the edit screen.
4. After adding a panel, click the **Save** button and then click the **Finish** button to exit.

4.16.3 Editing Dashboards

In the **Dashboard List** dialog box, you can edit a newly created dashboard or a dashboard customized with an auto-generated dashboard.

To edit a dashboard, follow these steps:

1. In the **Dashboard List** dialog box, check the dashboard to be edited and click the **Edit** button.

2. After editing the dashboard name or panel in the edit window, click the **Save** button, and then click the **Finish** button to exit.

4.16.4 Shared the Dashboard window

Automatically generated dashboards and newly created dashboards can be displayed in a separate window as the **Dashboard** window.

The steps to obtain URL for this window are as follows: By sharing URL, you can share the **Dashboard** window among several users/systems.

1. To share a newly created dashboard, check the target dashboard in the **Dashboard List** dialog box, and change it to **Share** in the public scope column.
2. Select the target title in the dashboard list to display the dashboard, or select IM management node in integrated operation viewer to display the target dashboard in the **Dashboard** tab.
3. Select the **Copy Dashboard URL** menu from the operation menu of the displayed dashboard.
4. In the **Copy Dashboard URL** dialog box, click the **Copy to Clipboard** button.

4.16.5 Deleting a dashboard

You can delete customized or newly created dashboards from an auto-generated dashboard.

To delete a dashboard, follow these steps: Note that if you remove the dashboard and there are no more dashboards associated with IM management node, the auto-generated dashboard will appear again.

1. In the **Dashboard List** dialog box, check the dashboard to be deleted, and click the **Delete** button.
2. Confirm the deletion in the **Delete dashboard** dialog. Then, click **OK**.

5

Setting Up Central Console

This chapter explains how to set up the functions of Central Console, such as JP1 event filtering and automated actions.

5.1 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 *3.11 System Environment Settings window* in the *JP1/Integrated Management 3 - 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.

5.1.1 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 $(\text{current-day} - (\text{set-number-of-days} - 1))$ 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 $(\text{current-day} - \text{set-number-of-days})$ 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 *4.17 Range of events to be collected at login* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

5.2 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.

5.2.1 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**, 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.

5.2.2 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 *4.1.4(2) Assigning a JP1 resource group and permission level to a JP1 user* in the *JP1/Integrated Management 3 - 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.

5.2.3 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 *4.1.4(2) Assigning a JP1 resource group and permission level to a JP1 user* in the *JP1/Integrated Management 3 - 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.

5.2.4 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 [5.2.4\(4\) 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 [4.1.4\(2\) Assigning a JP1 resource group and permission level to a JP1 user](#) in the *JP1/Integrated Management 3 - 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 *4.1.4(2) Assigning a JP1 resource group and permission level to a JP1 user* in the *JP1/Integrated Management 3 - 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 [5.2.4\(1\) 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 [6.5.3 Switching the event acquisition filter to be applied](#) in the *JP1/Integrated Management 3 - 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 [5.2.4\(3\)\(a\) 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 [6.5.4 Setting an additional common exclusion-condition to exclude a JP1 event from the monitoring target or action execution](#) in the *JP1/Integrated Management 3 - Manager Administration Guide*.

The method of editing an additional common exclusion-condition is the same as that of editing a common exclusion-condition. See [5.2.4\(3\)\(b\) 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 *JP1/Integrated Management 3 - Manager Command, Definition File and API 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 *4.1.4(2) Assigning a JP1 resource group and permission level to a JP1 user* in the *JP1/Integrated Management 3 - 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 *JP1/Integrated Management 3 - Manager GUI Reference*:

- System Environment Settings window
See 3.11 *System Environment Settings window*.
- Common Exclusion-Conditions Settings window
See 3.15 *Common Exclusion-Conditions Settings window*.
- Common Exclusion-Condition Settings (Extended) window
See 3.16 *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 *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

For details about the `jcochfilter` command, see `jcochfilter` in Chapter 1. *Commands* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API 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 *4.1.4(2) Assigning a JP1 resource group and permission level to a JP1 user* in the *JP1/Integrated Management 3 - 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.

5.3 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 *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

2. Restart JP1/IM - Manager.

3. Restart JP1/IM - View.

Monitoring of repeated events is now prevented.

5.4 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 *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

2. In the Event Console window, choose **Options**, and then **User Preferences**.

The Preferences window appears.

For details about the Preferences window, see *3.24 Preferences window* in the *JP1/Integrated Management 3 - 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.

5.5 Setting automated actions

This section describes the settings for using the automated action function.

5.5.1 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 *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

2. Terminate JP1/IM - Manager.
3. Execute the `jbssetcnf` command to apply the definitions.

In Windows:

```
jbssetcnf Console-path\conf\action.conf
```

In UNIX:

```
/opt/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 JP1 common definition information. For details about the `jbssetcnf` command, see the *JP1/Base User's Guide*.

4. Start JP1/IM - Manager.

5.5.2 Setting the execution conditions and details of automated actions

You can use the GUI of JP1/IM - View or the definition file to set the execution conditions and details of automated actions. This subsection describes both methods.

Note:

If you have upgraded your installation of Central Console from version 11-10 or earlier, you must update the definition file.

For details about the updating procedure, see [1.19.7\(2\) Updating the automated action definition file](#) (Windows) or [2.18.11\(3\) 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 [3.32 Action Parameter Definitions window](#) in the *JP1/Integrated Management 3 - Manager GUI Reference*.

For details about the Action Parameter Detailed Definitions window, see [3.33.1 Action Parameter Detailed Definitions window](#) in the *JP1/Integrated Management 3 - 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 5–1: 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 `jccache` 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 JP1/Integrated Management 3 - Manager Command, Definition File and API Reference.

5.5.3 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:

- 3.32 Action Parameter Definitions window in the JP1/Integrated Management 3 - Manager GUI Reference
- 3.33.1 Action Parameter Detailed Definitions window in the JP1/Integrated Management 3 - 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 JP1/Integrated Management 3 - Manager Command, Definition File and API 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 *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

5.5.4 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 *3.33.1 Action Parameter Detailed Definitions window* in the *JP1/Integrated Management 3 - 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 *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

5.5.5 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 [9.3.1 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=$EVMSG\n---\nFrom: I M-M Host ($ACTHOST) "
```

For details about the `jimmail` command, see *jimmail (Windows 3only)* in *Chapter 1. Commands in the JPI/Integrated Management 3 - Manager Command, Definition File and API 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: • 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: • 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

Parameter name	Setting item	Necessity to set	Description
			is supported. Multiple SMTP servers cannot be specified.
SmtPport	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. - NONE: No authentication - POP: POP-before-SMTP authentication - SMTP: SMTP-AUTH authentication (LOGIN/PLAIN) The default value is NONE.
SmtPAuthPort	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 <code>jimmailpasswd</code> 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. • 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. • 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 *JP1/Integrated Management 3 - Manager Command, Definition File and API 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 *JP1/Integrated Management 3 - Manager Command, Definition File and API 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
```

5.6 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

5.6.1 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 JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

5.6.2 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 5–2: 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 JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

We recommend that you store the created correlation event generation environment definition file in the following folder/directory:

Table 5–3: 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_spmd_reload` command or restart JP1/IM - Manager.

The defined information takes effect. For details about the `jco_spmd_reload` command, see *jco_spmd_reload* in *Chapter 1. Commands* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

5.6.3 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 *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

2. Either execute the `jco_spmd_reload` command or restart JP1/IM - Manager.

The defined information takes effect.

For details about the `jco_spmd_reload` command, see *jco_spmd_reload* in *Chapter 1. Commands* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

5.6.4 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 5–4: 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 .conf.

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 *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

We recommend that you store the created correlation event generation definition file in the following folder/directory:

Table 5–5: Folder/directory for storing the correlation event generation definition file

OS	Storage location#
Windows	For a physical host: <i>Console-path</i> \conf\evgen\define\
	For a logical host: <i>shared-folder</i> \jplcons\conf\evgen\define\
UNIX	For a physical host: /etc/opt/jplcons/conf/evgen/define/
	For a logical host: <i>shared-directory</i> /jplcons/conf/evgen/define/

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 *JP1/Integrated Management 3 - Manager Command, Definition File and API 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 *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

5.7 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 *3.24 Preferences window* in the *JP1/Integrated Management 3 - Manager GUI Reference*.

For details about how to edit memo entries, see *6.2.1 Editing JP1 memo entries* in the *JP1/Integrated Management 3 - Manager Administration Guide*.

5.8 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 *4.10 Event guide function* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.
- About the concept of event guides
See *13.1.10 Considerations for setting event guide information* in the *JP1/Integrated Management 3 - 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 *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

5.8.1 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 5–6: 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>

OS	Environment	Folder/directory for the sample file
	English	/etc/opt/jplcons/conf/guide/sample_jco_guide_en.txt
		<i>shared-directory</i> /jplcons/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 5–7: 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.

5.9 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 *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

5.10 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*.

5.11 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.

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 5–8: Storage locations of definition files for extended event attributes (extended file)

OS	Storage location	
Windows	Physical host	<i>Console-path</i> \conf\console\attribute\extend
	Logical host	<i>shared-folder</i> \JP1Cons\conf\console\attribute\extend
UNIX	Physical host	/etc/opt/jp1cons/conf/console/attribute/extend
	Logical host	<i>shared-folder</i> /jp1cons/conf/console/attribute/extend

The following table shows the file name for each operating language and the file name after the change.

Table 5–9: File names of definition files for extended event attributes (extended file)

Language	Stored file name	File name after the change
Japanese	template_extend_attr_ja.conf	extend_attr_ja.conf
English	template_extend_attr_en.conf	extend_attr_en.conf
Chinese	template_extend_attr_zh.conf	extend_attr_zh.conf

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 *JP1/Integrated Management 3 - Manager Command, Definition File and API 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 *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

3. Execute the `jco_spmc_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_spmc_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_spmc_reload` command, see `jco_spmc_reload` in *Chapter 1. Commands* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API 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 *6.9.1 Displaying program-specific extended attributes of JP1 events (displaying program-specific extended attributes)* in the *JP1/Integrated Management 3 - 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 *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

5.12 How to display user-defined event attributes

This section describes the procedures for displaying user-defined 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 *JP1/Base Function Reference*.

You can also use the `jevsend` and `jevsendd` commands in JP1/Base to issue user-specific events. In such cases, you might also need to specify information such as definition files for the extended event attributes. For details about how to set user-specific events to be issued by using the `jevsend` and `jevsendd` commands in JP1/Base, see the *JP1/Base User's Guide*.

To display user-defined 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-defined 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-defined 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 5–10: 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 5–11: 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
	Object ID	OBJECT_ID	SAMPLE_ID

Attribute type	Item	Attribute name	Description
	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

5.12.1 Creating the definition files

To display user-defined 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 *JP1/Integrated Management 3 - Manager Command, Definition File and API 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 *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

Example of definition:

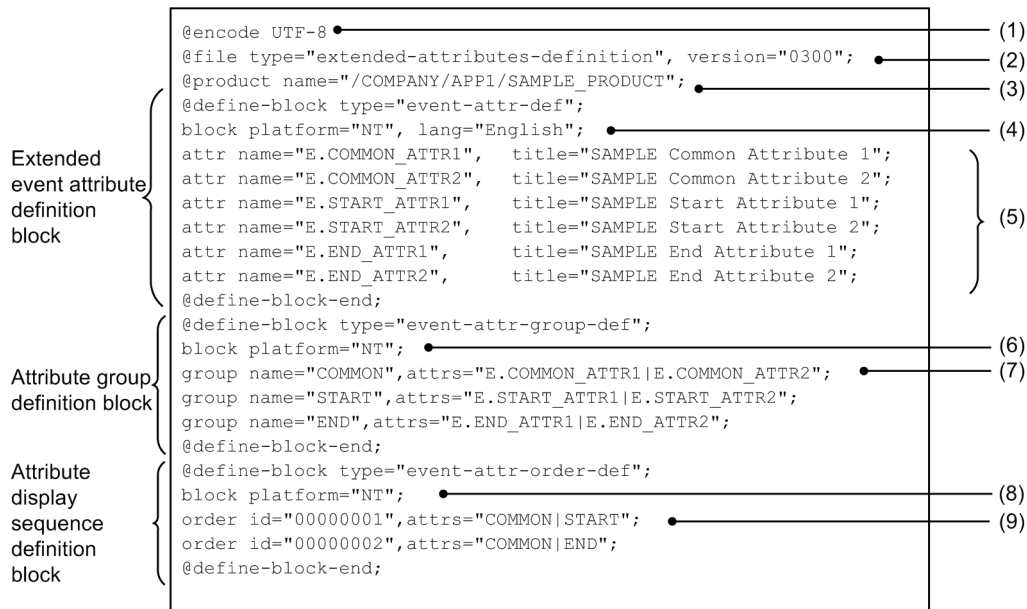
This example defines in the definition file for the extended event attributes the user-specific events that are issued by the **SAMPLE** application. This definition file defines the attributes of all JP1 events that are issued by a single application. This sample defines the JP1 events with event IDs 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 5–1: 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\jp1cons\conf\console\object_type*.

In UNIX:

```
/etc/opt/jp1cons/conf/console/object_type/
```

In the case of cluster operation, the storage location is *shared-directory*/jp1cons/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 *JP1/Integrated Management 3 - Manager Command, Definition File and API 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]
```

5.12.2 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 5–12: When the definition files take effect

Definition file	When it takes effect
Definition file for the extended event attributes	When the jco_spmc_reload command is executed or when JP1/IM - Manager is restarted
Definition file for objects types	When JP1/IM - View is restarted

5.13 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.

5.13.1 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 *JP1/Integrated Management 3 - Manager Command, Definition File and API 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 JP1/Integrated Management 3 - Manager Command, Definition File and API 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 JP1/Integrated Management 3 - Manager Command, Definition File and API 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.

5.13.2 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 JP1/Integrated Management 3 - Manager Command, Definition File and API Reference.

2. Edit the severity changing definition file.

For details about the information to be edited, see *6.9.4 Changing the severity level of JPI events* in the *JPI/Integrated Management 3 - Manager Administration Guide*.

3. Execute the `jco_spmd_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_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 *JPI/Integrated Management 3 - Manager Command, Definition File and API Reference*.

5.14 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.

5.14.1 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 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 *JP1/Integrated Management 3 - Manager Command, Definition File and API 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 JP1/Integrated Management 3 - Manager Command, Definition File and API 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 JP1/Integrated Management 3 - Manager Command, Definition File and API 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.

5.14.2 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 *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

2. Edit the display message change definition file.

For details about the contents to be edited, see 6.9.5(2) *Setting a display message change definition in the display message change definition file* in the *JP1/Integrated Management 3 - 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 *JP1/Integrated Management 3 - Manager Command, Definition File and API 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.

5.14.3 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 *JP1/Integrated Management 3 - Manager Command, Definition File and API 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 [5.2.4 Settings for event acquisition filters](#).

5.15 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 *JP1/Integrated Management 3 - Manager Command, Definition File and API 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 5–13: 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 <code>E.PPNAME</code> set to <code>/HITACHI/JP1/NTEVENT_LOGTRAP</code>	<code>B.SOURCESERVER</code>	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	<code>E.A1</code>	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	<code>E.SNMP_SOURCE</code>	--
4	JP1/AJS2 and JP1/AJS3	JP1 events with the following event IDs: • 4105 • 4106 • 4107 • 4109 • 410A • 4125 • 4126 • 4127	<code>E.C0</code>	--
5	JP1/PFM	JP1 events with the following product names: • <code>/PFM/ALARM_EVENT</code> • <code>/HITACHI/JP1/PFM/ALARM_EVENT</code>	<code>E.JPC_AGENT</code>	--

No	Product name	JP1 event to be mapped	Attribute name indicating event source host	Remarks
		/HITACHI/JP1/PFM/STATE_EVENT		
6		JP1 events with the following product name: /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: 3A80	The value of one of the following attributes containing a host name is mapped: - 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: /HITACHI/JP1/PAM	E.PAM_HOSTNAME	--
9	JP1/SCIM	JP1 events with the following event IDs: 432B 432C	E.SCIM_AGENT_ADDR	--
10	Cosminexus	JP1 events with the following event IDs: 12000 12080	E.HOST_NAME	--
11	JP1/ServerConductor	JP1 events with the following product name: /HITACHI/SYSTEM_MANAGER	E.HSM_SERVER	--
12	JP1/IM - EG for NNMi	JP1 events with the following event ID: 6100	E.NNMI_SRC_NODE_NAME	--
13	JP1/Console Agent for VOS3	- JP1 events with the following event IDs: 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
		• 10110 • 10112 • 10111 • 10410 • 10411 • 10412		
15		JP1 events with the following event IDs: • 10420 • 10421 • 10422	E.O3	--
16	JP1/IM - MO	JP1 events with the following event ID: • 6400	E.EVTSRC_INFO	--
17	JP1/IM - Manager	JP1 events with the following event ID: • 3A71	E.A1	--
18		JP1 events with the following event ID: • 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 *JP1/Integrated Management 3 - Manager Command, Definition File and API 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_spmc_reload` command to apply the definitions.

For details about the `jco_spmc_reload` command, see *jco_spmc_reload* in *Chapter 1. Commands* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

5.16 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.

5.16.1 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 *JP1/Integrated Management 3 - Manager Command, Definition File and API 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

5.16.2 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 3.24 *Preferences window* in the *JP1/Integrated Management 3 - 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 *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*. If such changes are made, JP1/IM - View might not function correctly.

5.17 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 and the Integrated Operation Viewer 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.

5.17.1 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 *JP1/Integrated Management 3 - Manager Command, Definition File and API 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 *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

3. Execute the `jco_spmd_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_spmd_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_spmd_reload` command, see `jco_spmd_reload` in *Chapter 1. Commands* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

4. From JP1/IM - View, log in to JP1/IM - Manager (Central Console). (This step is applicable when you are launching monitor startup from the Event Console window.)

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.

5. From web browser, log in to JP1/IM - Manager (This step is applicable when you are launching monitor startup from the Integrated Operation Viewer window.)

In the address bar (URL entry area) of the web browser, enter the URL of the login window to display the Integrated Operation Viewer window. If you are already logged in, log out and then log back in. You do not have to restart JP1/IM - Manager (Intelligent Integrated Management Base).

The following subsections provide details of each step.

5.17.2 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.

5.17.3 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 *JP1/Integrated Management 3 - Manager Command, Definition File and API 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 *JP1/Integrated Management 3 - Manager Command, Definition File and API 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 *JP1/Integrated Management 3 - Manager Command, Definition File and API 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 *JP1/Integrated Management 3 - Manager Command, Definition File and API 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 *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

5.18 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.

5.18.1 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 *8.3.2 Functions that can be operated from the Tool Launcher window* in the *JP1/Integrated Management 3 - 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 *5.18.4 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.

5.18.2 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.

5.18.3 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.

5.18.4 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 *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*. For details about the definition file for executing applications, see *Definition file for executing applications* in *Chapter 2. Definition Files* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

JP1/IM provides the `jcofuncfcheck` (Windows only) command for checking the definition file for the Tool Launcher window. For details about this command, see *jcofuncfcheck (Windows only)* in *Chapter 1. Commands* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

(b) Storage location

Store this file in the viewer's directory shown below. The definition takes effect when JP1/IM - View is restarted.

View-path\conf\function\en\

(c) Example of definition

This subsection presents the following example:

Application

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 5–2: Example definition in the definition file for the Tool Launcher window



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 *JP1/Integrated Management 3 - Manager Command, Definition File and API 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 *JP1/Integrated Management 3 - Manager Command, Definition File and API 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 5–3: 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.

5.18.5 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 *JP1/Integrated Management 3 - Manager Command, Definition File and API 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.

5.19 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 *JP1/Integrated Management 3 - Manager Command, Definition File and API 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 [4.1.4 Restrictions on viewing and operating business groups](#) in the *JP1/Integrated Management 3 - 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 [8.4 Managing business groups](#) in the *JP1/Integrated Management 3 - 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 [4.9 Mapping of the event source hosts](#) in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

- Setting event source host mapping

See [5.15 Setting event source host mapping](#).

6

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.

6.1 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.

6.1.1 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 3 - Manager Overview and System Design Guide*.

See *Chapter 2. Overview of Functions* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

- About the functions of Central Scope

See *Chapter 5. Objective-Oriented System Monitoring Using the Central Scope* in the *JP1/Integrated Management 3 - 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)*.

6.2 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:

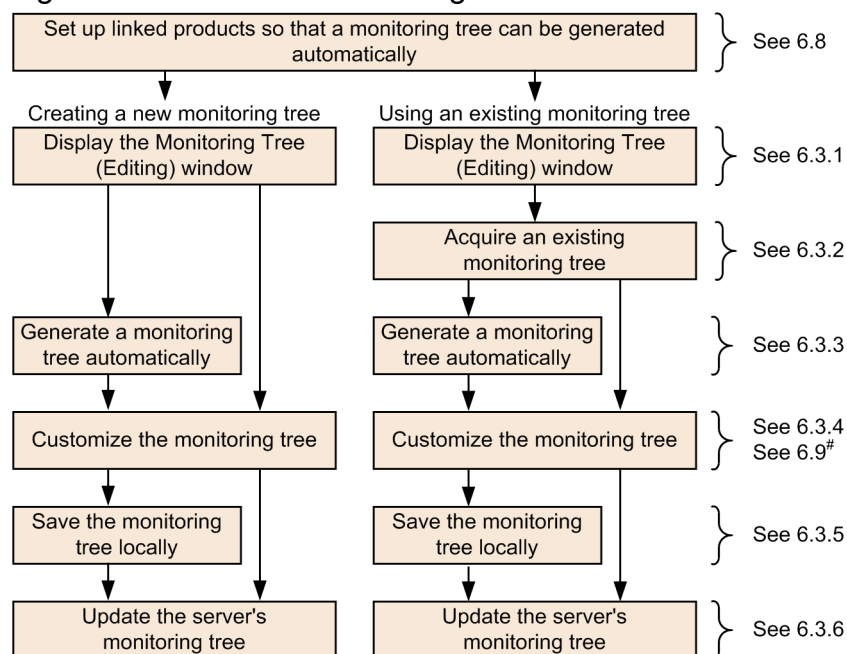
- About host information
See *5.11.2 Host information* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.
- About the format of host information file
See *Host information file (jcs_hosts)* in *Chapter 2. Definition Files* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.
- About the `jcshostsimport` command
See *jcshostsimport* in *Chapter 1. Commands* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

6.3 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 6–1: Procedure for using the GUI to create a monitoring tree



#: This section provides an example of monitoring object creation.

6.3.1 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 3- 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).

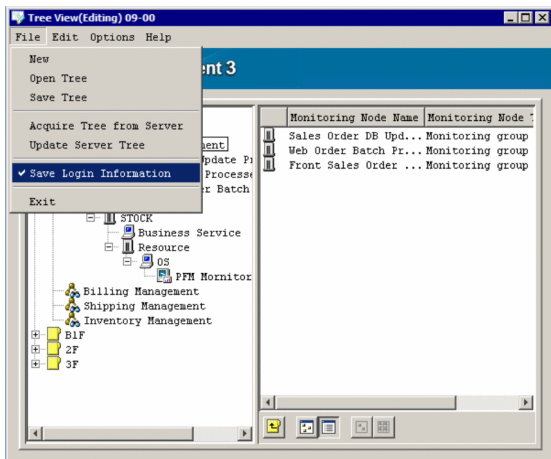
Saving the login information

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 6–2: Save Login Information menu



The following table lists and describes the operations that require login.

Table 6–1: 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.

6.3.2 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.

6.3.3 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 [6.8 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:

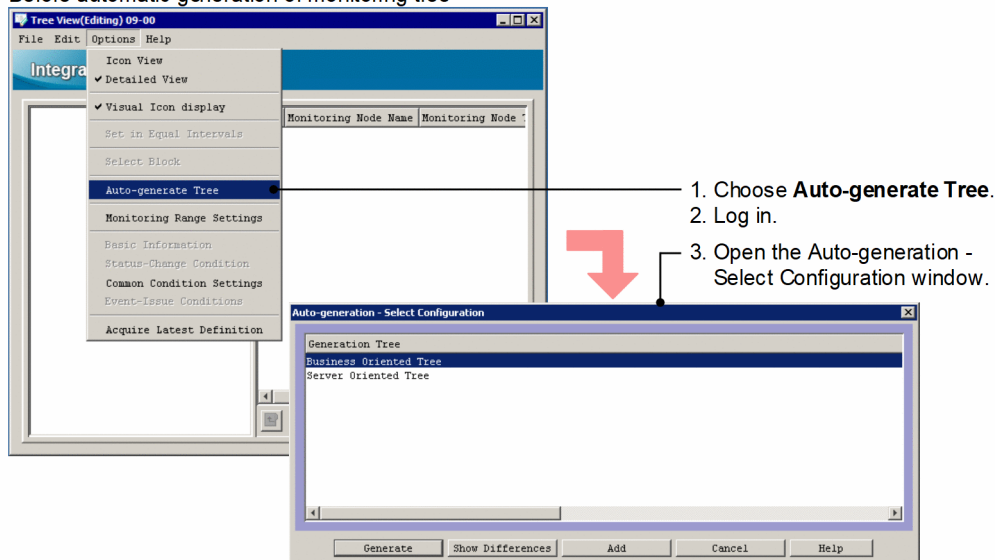
About monitoring tree automatic generation:

- About the monitoring tree automatic generation function
See 5.2 *Monitoring tree* in the *JPI/Integrated Management 3 - Manager Overview and System Design Guide*.
See 5.3 *Automatically generating a monitoring tree* in the *JPI/Integrated Management 3 - Manager Overview and System Design Guide*.
- About the monitoring tree model that is generated automatically
See *Chapter 9. Monitoring Tree Models (for Central Scope)* in the *JPI/Integrated Management 3 - Manager Command, Definition File and API Reference*.

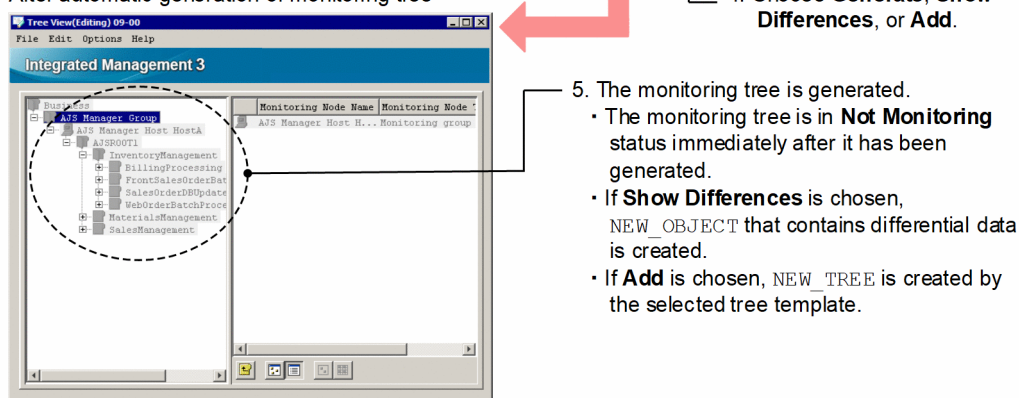
The following figure shows the procedure for generating a monitoring tree automatically.

Figure 6–3: 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.

6.3.4 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 5.2 *Monitoring tree* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

See 5.3 *Automatically generating a monitoring tree* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

See 5.4 *Editing a monitoring tree* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

See 5.11 *Central Scope* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

- About the settings for a monitoring tree

See 5.2 *Monitoring tree* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

- About the system-monitoring objects for which basic settings have been defined

See *Chapter 8. Lists of System-Monitoring Objects (for Central Scope)* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

If you set **Common condition** in the monitoring node attribute settings and use common conditions that have already been set, you must apply the operation described below to acquire those common conditions.

If you use a monitoring tree configuration file (CSV file), you can use the common conditions maintained by that configuration file. You can also use the common conditions maintained by JP1/IM - View when you generate a new monitoring tree.

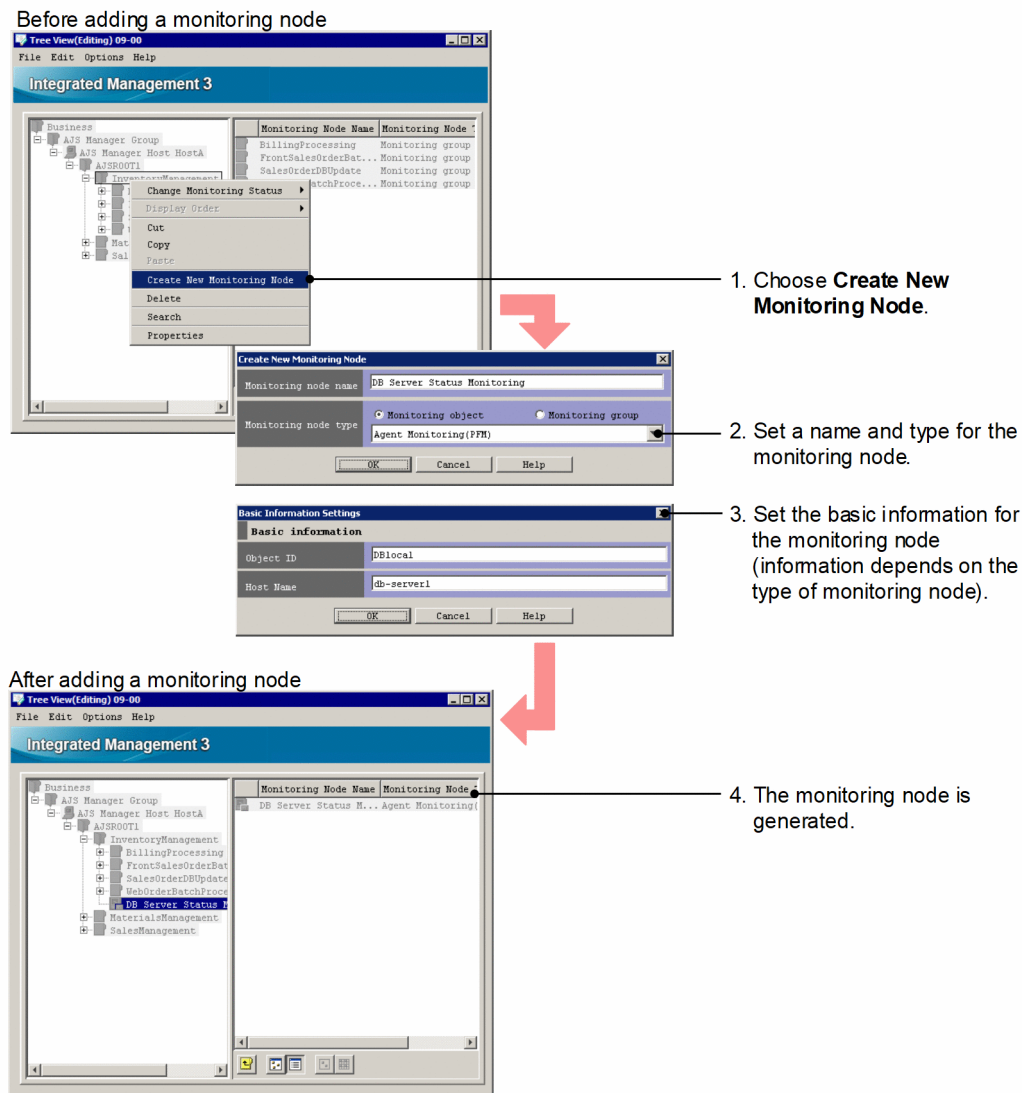
To acquire common conditions:

1. In the Monitoring Tree (Editing) window, from the menu bar, choose **Options**, and then **Acquire Latest Definition**.

(1) Adding monitoring nodes

The following figure shows the procedure for adding a monitoring node.

Figure 6–4: 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 8. Lists of System-Monitoring Objects (for Central Scope)* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API 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 8. Lists of System-Monitoring Objects (for Central Scope)* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API 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 [6.3.4\(7\) 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 [6.3.4\(6\) Setting the monitoring range](#).

The following provides an example of property settings.

Figure 6–5: Example of using the General page to set a monitoring node's monitoring status to Monitoring

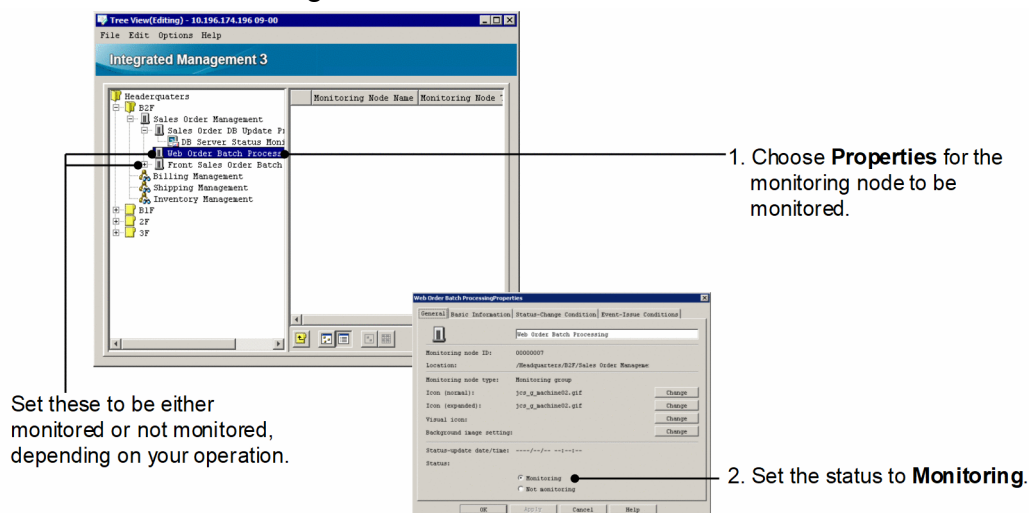


Figure 6–6: Example of settings on the Basic Information page

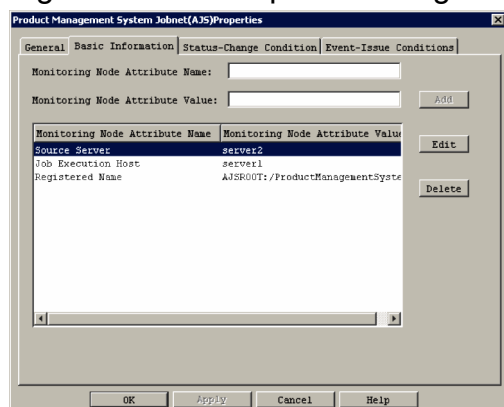


Figure 6–7: Example of using the Status-Change Condition page to set the status change condition for a monitoring node

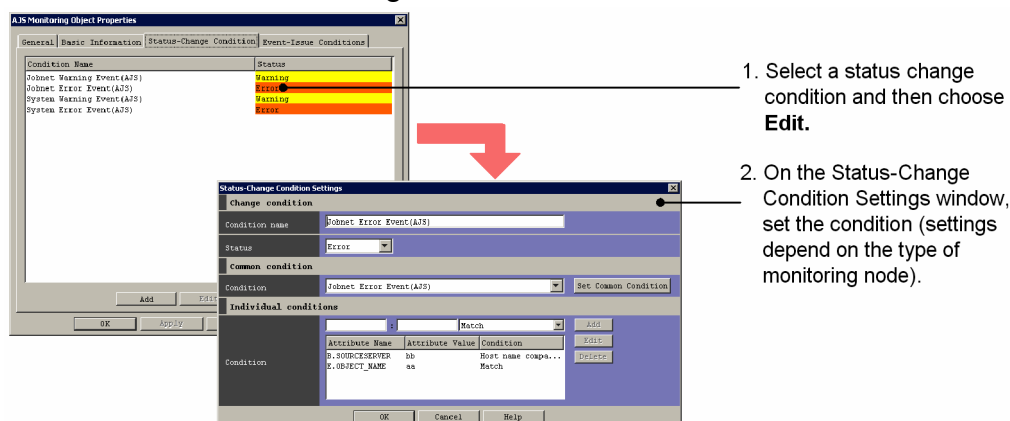
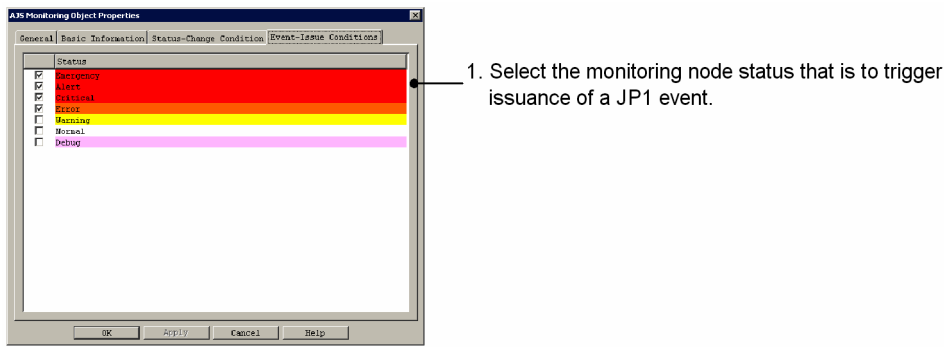


Figure 6–8: Example of setting JP1 event issuance on the Event-Issue Conditions page



(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 6–2: 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.

6.3.5 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.

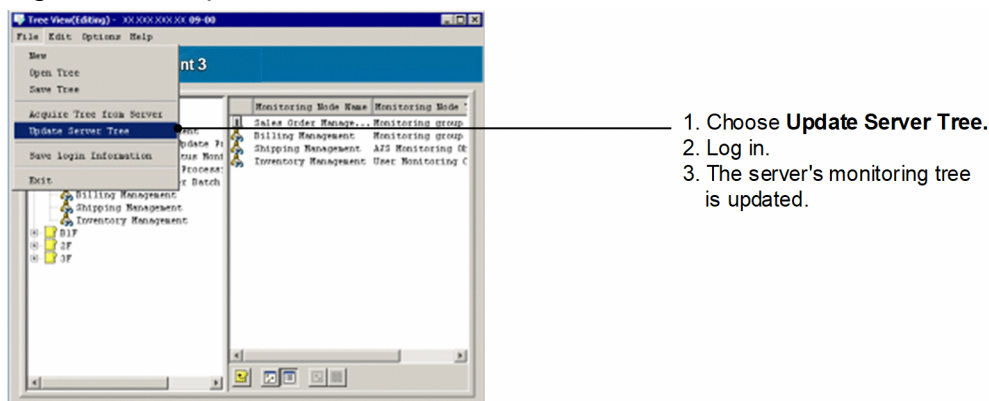
When the Save Tree window appears, specify a desired folder name and file name, and then save the monitoring tree.

6.3.6 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 6–9: 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.

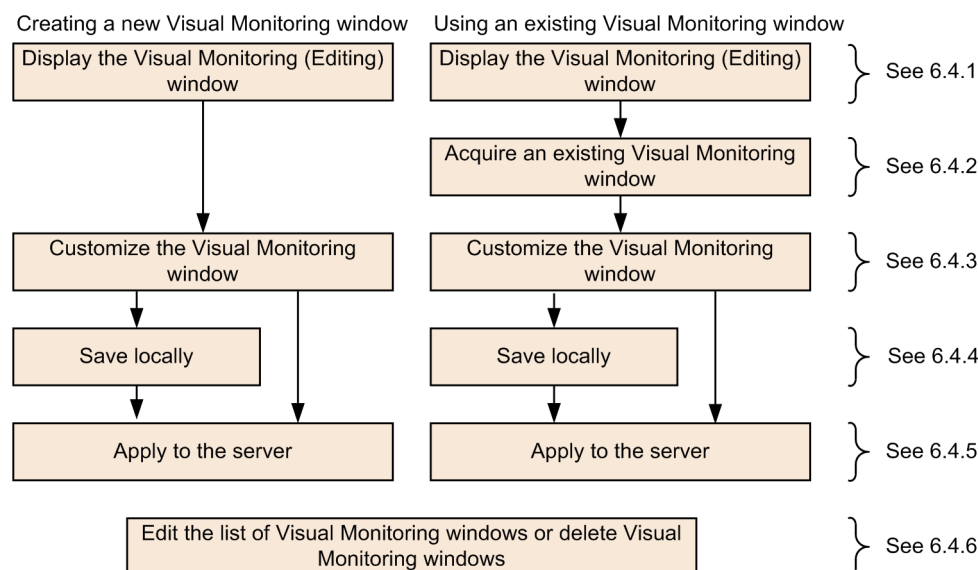
To check the applied monitoring tree, log in to JP1/IM - Manager (Central Scope), and then check the Monitoring Tree window.

6.4 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.

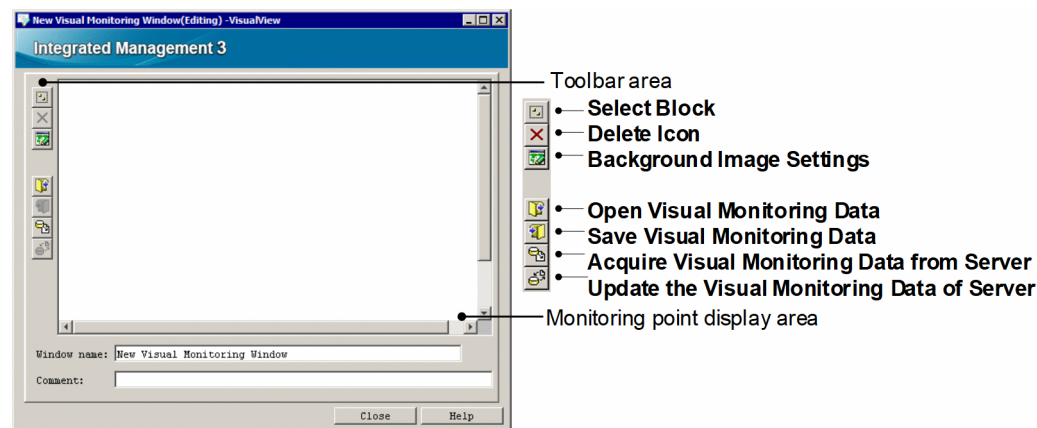
Figure 6–10: Procedure for using the GUI to create a Visual Monitoring window



6.4.1 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 6–11: 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.

6.4.2 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.

6.4.3 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:

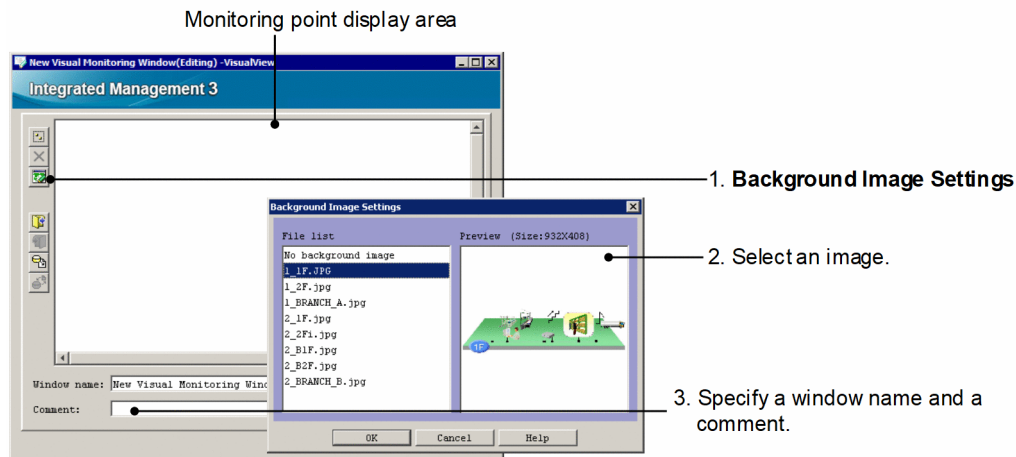
- Set a background image
- Add monitoring nodes
- Delete monitoring nodes
- Set attributes of monitoring nodes
- Change the monitoring status of monitoring nodes
- Search for monitoring nodes

(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 6–12: 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.

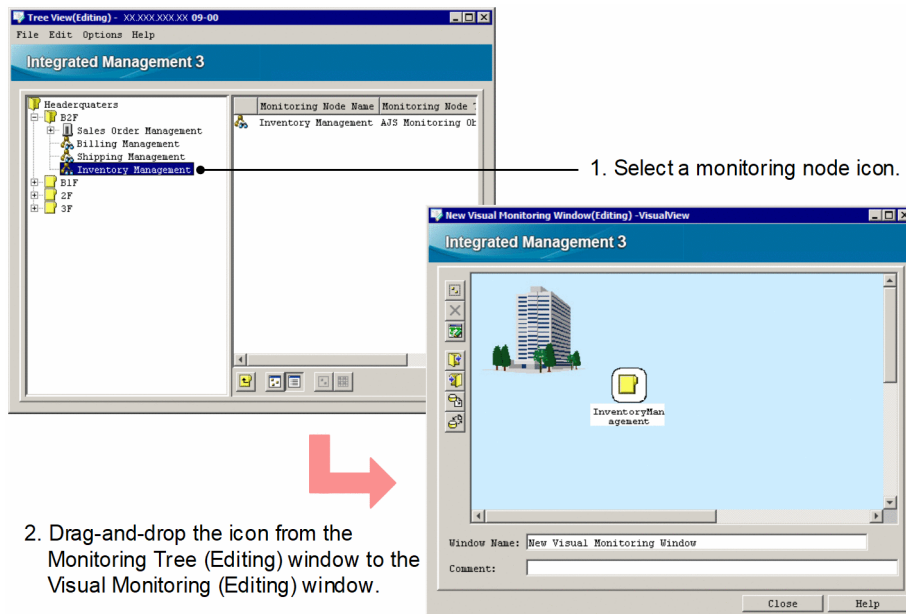
Hints on Visual Monitoring window operation

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 6–13: Adding monitoring nodes to a Visual Monitoring window



1. Select a monitoring node on the monitoring tree.

In the Monitoring Tree (Editing) window, display and select the monitoring node that you want to monitor by using the Visual Monitoring window.

2. Drag-and-drop the monitoring node in the Visual Monitoring window.

In the Monitoring Tree (Editing) window, drag (left-click) the monitoring node icon and drop it onto the Visual Monitoring (Editing) window.

In the case of a monitoring node icon added by the above method, the appropriate status color (such as red for failure) is displayed in the monitoring tree, thus reflecting the monitoring node's status.

There will be a delay before information in the Monitoring Tree window takes effect on the Visual Monitoring window.

(3) Deleting monitoring nodes from the Visual Monitoring window

To delete monitoring nodes from the Visual Monitoring window:

1. Select a monitoring node icon and then delete it.

Use one of the methods described below. To delete multiple icons in a batch, use  to select multiple icons.

- Select an icon, and then in the Visual Monitoring (Editing) window, on the toolbar, click .
- Select an icon, and then from the right-click pop-up menu, choose **Delete Icon**.

When a configuration dialog box appears, click the **Yes** button.

(4) Setting the attributes of monitoring nodes

If you set the attributes of a monitoring node in the Visual Monitoring (Editing) window, the specified settings are applied to the corresponding monitoring node in the Monitoring Tree (Editing) window.

To set attributes for a monitoring node that has been placed in the Visual Monitoring (Editing) window:

1. Open the Properties window for the monitoring node.

Select a monitoring node and then use the following method to open the Properties window:

- From the right-click pop-up menu, choose **Properties**.

2. Specify the settings on the **General** page.

Specify the monitoring node name, icon to be used, visual icon to be used,^{#1} background image settings (monitoring groups only), monitoring status, and JP1 resource group^{#2}.

3. Specify the settings on the **Basic Information** page.

Specify basic information for the monitoring node.

4. Specify the settings on the **Status-Change Condition** page.

Specify the JP1 events that are to change the status of the monitoring node when those events are received by JP1/IM - Manager.

For details about the settings for status change conditions, see *Chapter 8. Lists of System-Monitoring Objects (for Central Scope)* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API 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 [6.3.4\(7\) 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 [6.3.4\(2\) 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.

6.4.4 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.

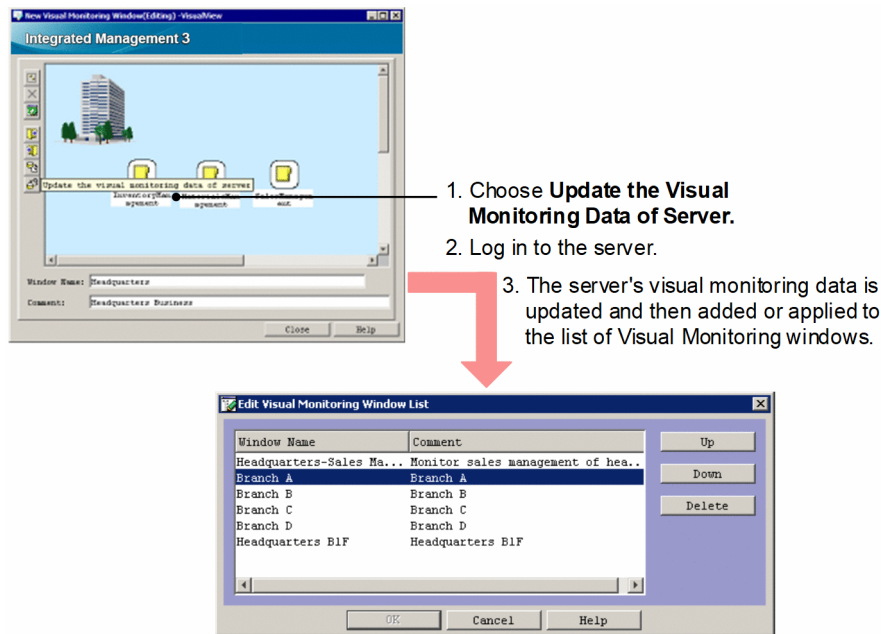
To save a customized Visual Monitoring window at the local host:

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.

6.4.5 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 6–14: 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.

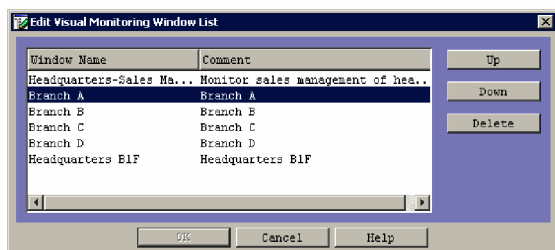
A dialog box is displayed while the processing is in progress. This dialog box closes when the processing is completed. When the Visual Monitoring window has been applied to the manager, the Visual Monitoring window is added or applied to the list of visual windows.

To check the applied Visual Monitoring window, log in to JP1/IM - Manager (Central Scope), and then check the Visual Monitoring window.

6.4.6 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 6–15: 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 **Top**, **End**, or **Delete** button.

To edit the list of Visual Monitoring windows and delete Visual Monitoring windows:

1. Open the Edit Visual Monitoring Window List window.
In the Monitoring Tree (Editing) window, from the menu bar, choose **Edit**, and then **Edit Visual Monitoring Window List**.
2. Log in to the server.
The Login window for logging in to JP1/IM - Manager (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.

6.5 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 [6.3.5 Saving a customized monitoring tree at the local host](#).
- Creating monitoring windows from the CSV files
See [6.3.4 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 *JPI/Integrated Management 3 - Manager Command, Definition File and API Reference*.

6.6 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 *5.8 Guide function* in the *JP1/Integrated Management 3 - 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 *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

6.6.1 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 6–3: 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> \jp1scope\conf\jcs_guide_sjis.txt
	English ^{#3}		<i>Scope-path</i> \conf\jcs_guide.txt
			<i>shared-folder</i> \jp1scope\conf\jcs_guide.txt
	Chinese ^{#4}		<i>Scope-path</i> \conf\jcs_guide_GB18030.txt ^{#5}
			<i>shared-folder</i> \jp1scope\conf\jcs_guide_GB18030.txt ^{#5}
UNIX ^{#1}	Japanese	Shift JIS	/etc/opt/jp1scope/conf/jcs_guide_sjis.txt
			<i>shared-directory</i> /jp1scope/conf/jcs_guide_sjis.txt
		EUC	/etc/opt/jp1scope/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		/etc/opt/jplscope/conf/jcs_guide.txt
			<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_spmd_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 6–4: 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.

6.7 Setting up a Central Scope operating environment

This section explains how to set up an operating environment for Central Scope.

6.7.1 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 *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

3. Start JP1/IM - Manager.

6.7.2 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 *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

3. Start JP1/IM - Manager.

6.7.3 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 *JP1/Integrated Management 3 - Manager Command, Definition File and API 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.

6.7.4 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 *JP1/Integrated Management 3 - Manager Command, Definition File and API 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.

6.7.5 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 *JP1/Integrated Management 3 - Manager Command, Definition File and API 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.

6.7.6 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\sovtool\exec\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\sovtool\item\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\sovtool\item\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 JP1/Integrated Management 3 - Manager Command, Definition File and API 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 JP1/Integrated Management 3 - Manager Command, Definition File and API 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 JP1/Integrated Management 3 - Manager Command, Definition File and API Reference.

6.7.7 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\jp1scope\conf
- In UNIX (physical host)
/etc/opt/jp1scope/conf
- In UNIX (logical host)
shared-directory/jp1scope/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 *JP1/Integrated Management 3 - Manager Command, Definition File and API 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 *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

6.7.8 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 JP1/Integrated Management 3 - Manager Command, Definition File and API 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 JP1/Integrated Management 3 - Manager Command, Definition File and API Reference.

6.7.9 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 JP1/Integrated Management 3 - Manager Command, Definition File and API Reference.

6.8 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.

6.8.1 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.

6.8.2 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/jplbase/conf/evtgw/snmpfilter.conf

- Sample file in Central Scope

In Windows:

Scope-path\conf\snmpfilter_im_sample.conf

In UNIX:

/etc/opt/jplscope/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*.

1. 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`.

6.8.3 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)
```

6.8.4 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 *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/jplbase/conf/evtgw/snmpfilter.conf

- Sample file of Central Scope

In Windows:

Scope-path\conf\snmpfilter_im_sample.conf

In UNIX:

/etc/opt/jplscope/conf/snmpfilter_im_sample.conf

Important

- 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*.

6.8.5 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.

6.8.6 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 *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`

:

6.8.7 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.

6.8.8 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 *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 *For Windows Systems HiRDB Version 8 System Definition* or *For UNIX Systems HiRDB Version 8 System Definition*.

6.8.9 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.

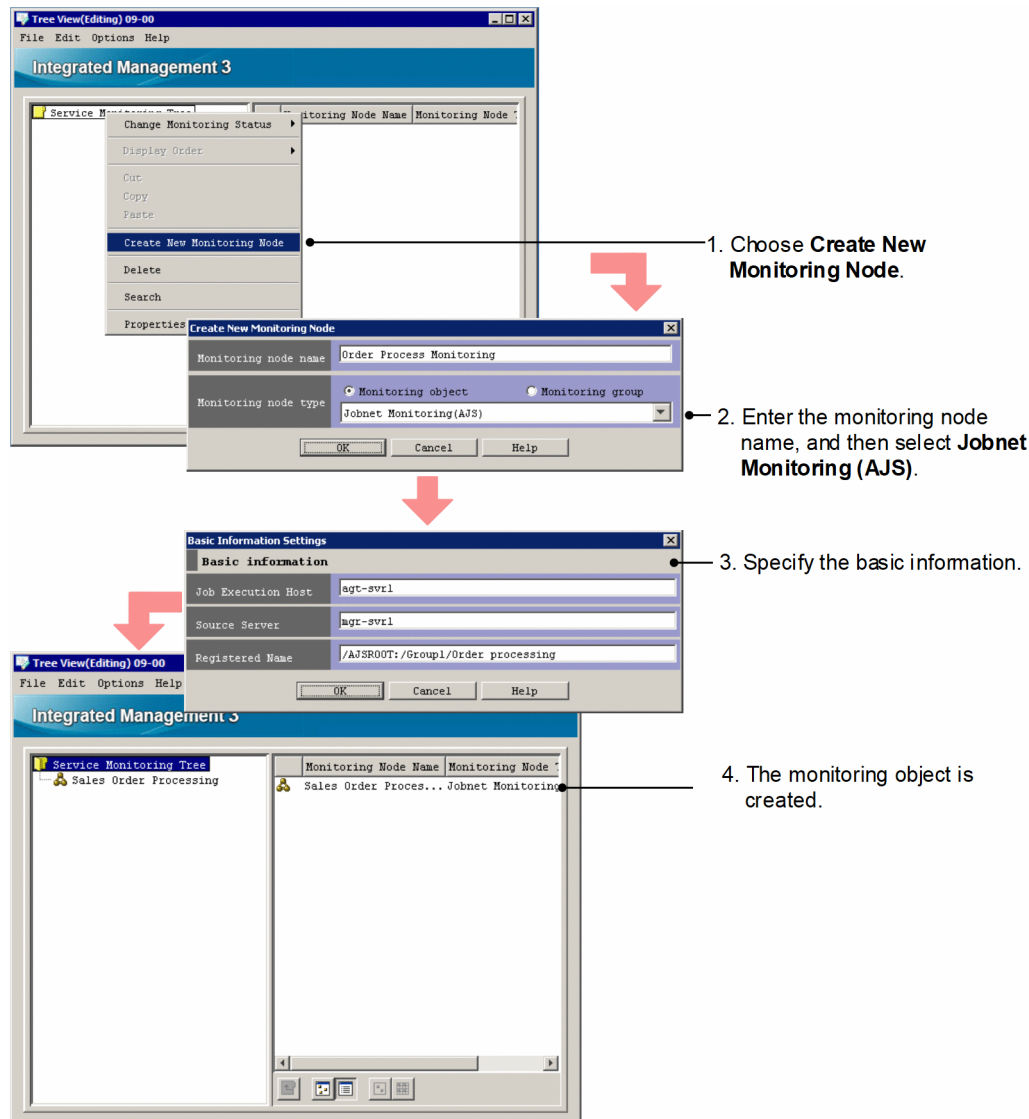
6.9 Examples of monitoring object creation

This section provides examples of manual creation of monitoring objects.

6.9.1 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 6–16: 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 6–5: 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.

6.9.2 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 6–6: 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*.

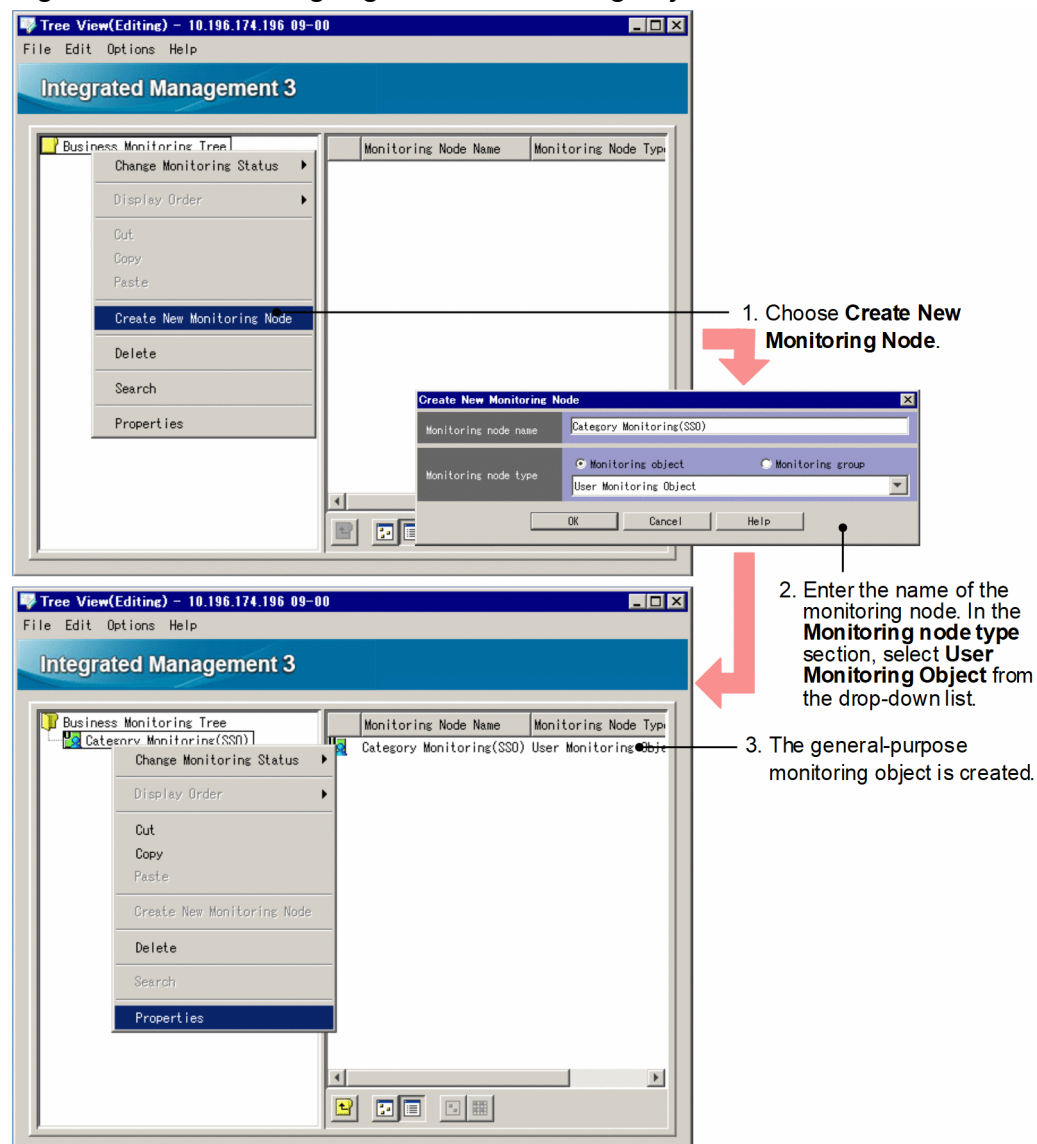
(2) Confirmation before creating a monitoring object

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 6–17: 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 6–7: 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 6–18: Setting up the general monitoring object (adding a status change condition - 1)

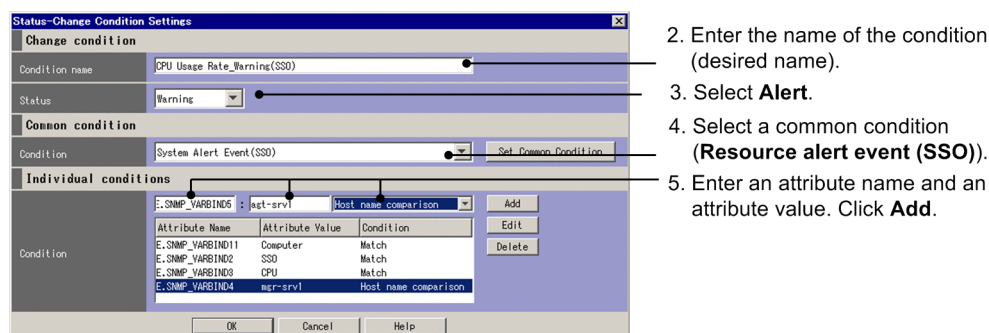
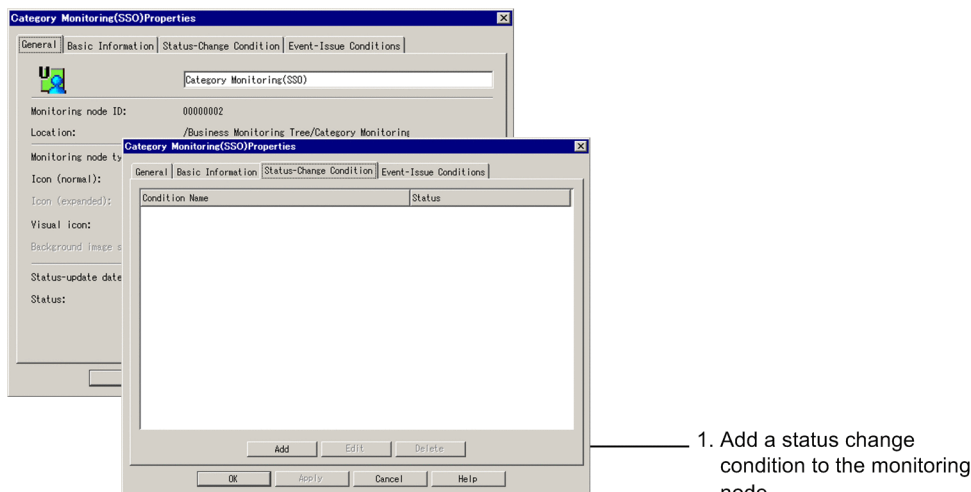
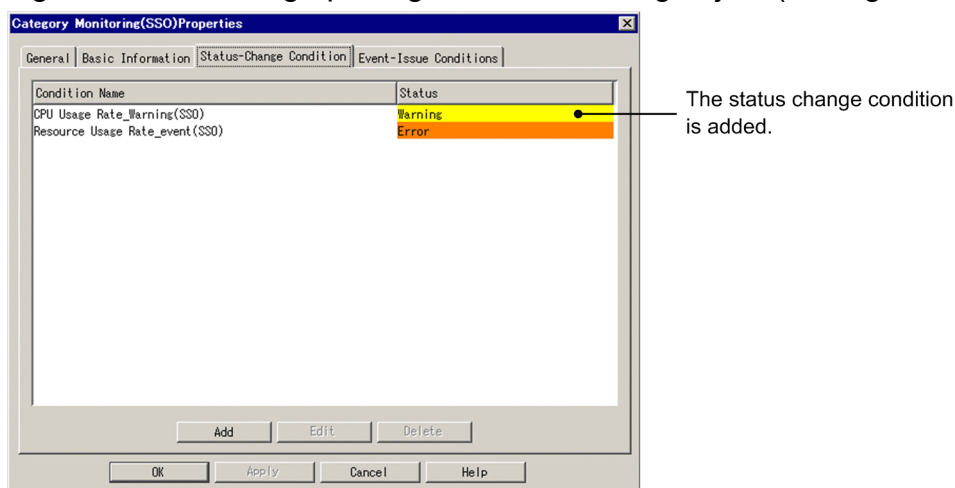


Figure 6–19: Setting up the general monitoring object (adding a status change condition - 2)



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.

2. 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.

3. 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 6–8: 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 6–9: 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.

4. 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.

6.9.3 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

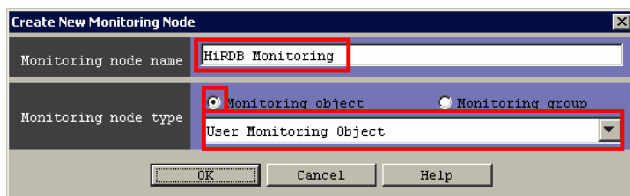
HiRDB version 07-02 or later can issue JP1 events, not JP1/SES events (the output settings are required at HiRDB). In this case, use the system-monitoring object provided by Central Scope to create a monitoring object for HiRDB.

(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 6–20: Create New Monitoring Node window



The settings in the Create New Monitoring Node window are as follows.

Table 6–10: 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:

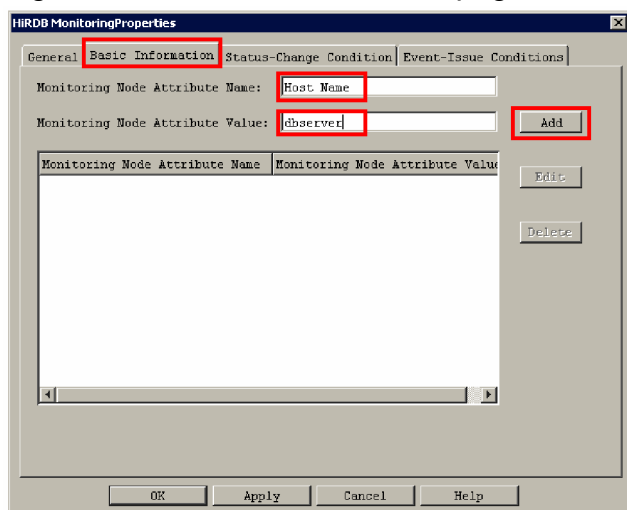
1. Select the newly created monitoring object.

2. From the **Edit** menu, choose **Properties**.

The Properties window appears.

3. Choose the **Basic Information** page.

Figure 6–21: Basic Information page



The settings on the **Basic Information** page are as follows.

Table 6–11: 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 HiRDB.

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.

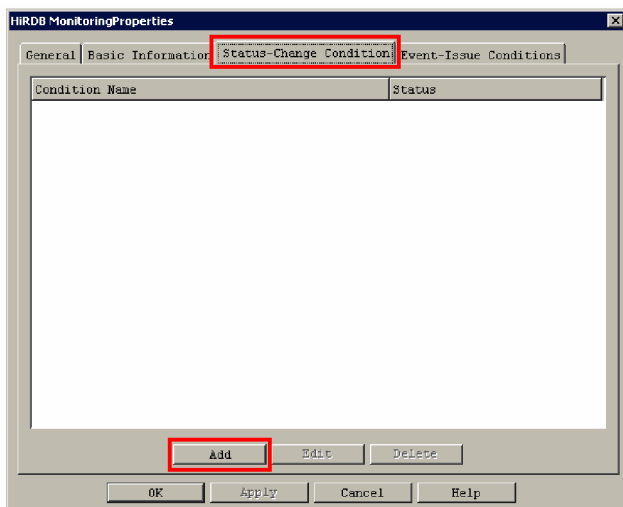
The basic information is set for the monitoring object.

(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.

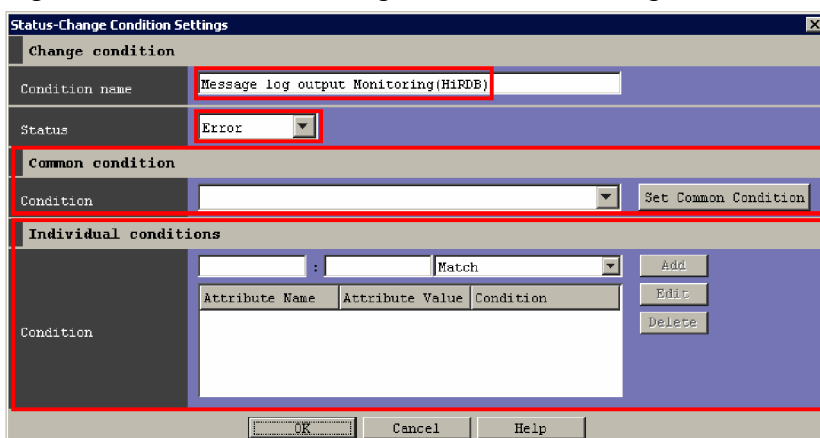
Figure 6–22: Status-Change Condition page



4. Click the **Add** button.

The Status-Change Condition Settings window appears.

Figure 6–23: Status-Change Condition Settings window



The settings in the Status-Change Condition Settings window are as follows.

Table 6–12: Settings in the Status-Change Condition Settings window

Item	Setting
Condition name	Specify a name for the condition.
Status	From the list box, select the status to which the monitoring object is to change when an event is received.
Common condition	Specify information needed to identify the event or the product that caused the event. The details are provided below.
Individual conditions	Specify information needed to identify the location where the event occurred. The details are provided below.

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 6–24: Common Condition Detailed Settings window

The settings in the Common Condition Detailed Settings window are as follows.

Table 6–13: Settings in the Common Condition Detailed Settings window

Item	Setting
Common condition name	Specify a name for the common condition.

Item	Setting
Message	Specify the message for the JP1 event (in this example, a JP1/SES event). Specify this information if you want to monitor only a specific message. In the case of HiRDB, specify a JP1/SES event message that is issued by HiRDB. For example, if you enter <code>KFPS01222-I</code> and select Match prefix , you can monitor only the HiRDB log swap messages.
Event ID	Specify the event ID of the JP1 event (in this example a JP1/SES event) to be monitored. For a product that issues JP1/SES events such as HiRDB, specify the basic code of JP1/SES events (<code>00010C03</code>).

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 6–14: 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.

6.9.4 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 6–15: 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 6–16: 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 6–17: 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	E.SNMP_VARBIND3	<u>Server</u>	<u>Match</u>
		Instance name	E.SNMP_VARBIND6	^DefaultDomain: J2EE_SV1(:.* \$)	<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	E.SNMP_VARBIND3	<u>Scheduler (CTM)</u>	<u>Match</u>
		Instance name	E.SNMP_VARBIND6	^DefaultDomain: CTM_SV1(:.* \$)	<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	E.SNMP_VARBIND6	^DefaultDomain: SFO_SV1(:.* \$)	<u>Regular expression</u>
J2EE Application 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	E.SNMP_VARBIND6	^DefaultDomain: J2EE_SV1:API(:.* \$)	<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 6-16 Information about the Cosminexus servers and applications to be monitored.](#))

Figure 6–25: Creating a J2EE Server Resource Monitoring (SSO) a monitoring object (steps 1 to 4)

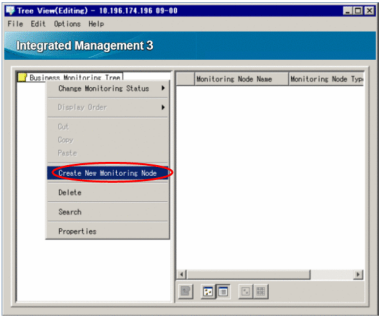
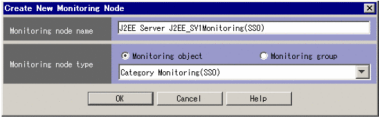
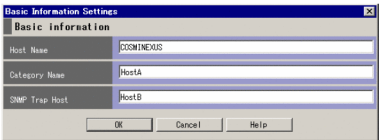
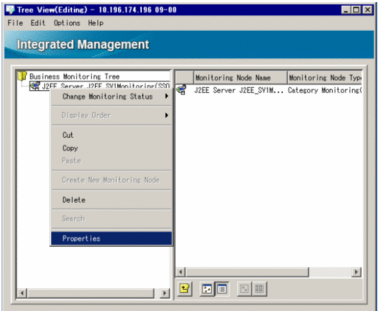
JP1/IM - View window	Step
	Step 1: Operation in the Monitoring Tree (Editing) window Select the monitoring group to which the monitoring object is to belong. Right-click the monitoring group to display a pop-up menu. Choose Create New Monitoring Node.
	Step 2: Operation in the Create New Monitoring Node window - 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
	Step 3: Operation in the Basic Information Settings window - 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
	Step 4 Click the OK button to return to the Monitoring Tree (Editing) window.

Figure 6–26: Creating a J2EE Server Resource Monitoring (SSO) a monitoring object (steps 5 to 8)

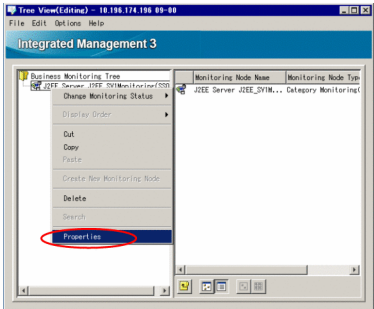
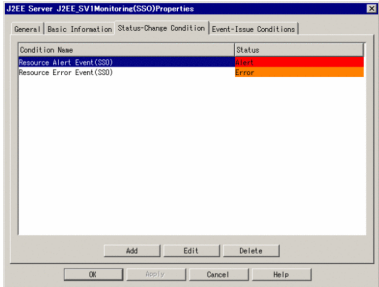
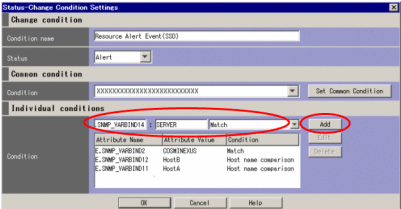
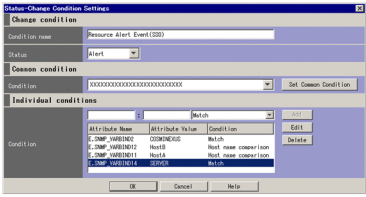
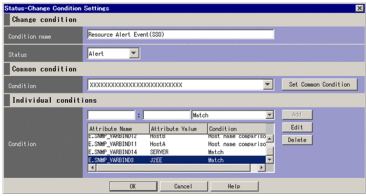
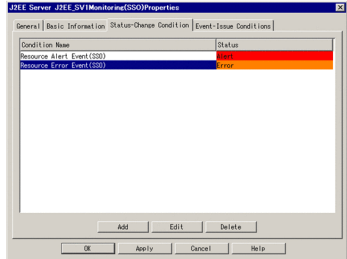
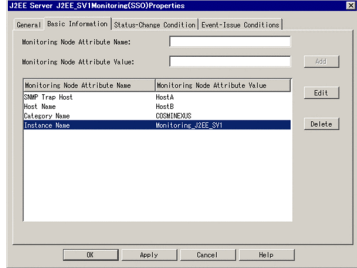
JP1/IM - View window	Step
	Step 5: Operation in the Monitoring Tree (Editing) window Select and right-click the monitoring object created in steps 1 to 4 to display a pop-up menu. Choose Properties.
	Step 6: Operation in the Properties window Click the Status-Change Condition tab. On the Status-Change Condition page, select Resource alert event (SSO). Then click the Edit button.
	Step 7: Operation in the Status-Change Condition Settings window See Table 6-17 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(. * \$)
	Step 8 When you click the Add button, the KAVB6083-W message appears. Click Yes.

Figure 6–27: Creating a J2EE Server Resource Monitoring (SSO) a monitoring object (steps 9 to 12)

JP1/IM - View window	Step
	Step 9: Operation in the Status-Change Condition Settings window Add other conditions as necessary (the dialog box in step 8 will not appear later).
	Step 10 Click the OK button to close the Status-Change Condition Settings window.
	Step 11: Operation in the Properties window Repeat steps 7, 9, and 10 for Resource Error Event (SSO) and to also add individual conditions.
	Step 12: Operation in the Properties window (optional) Click the Basic Information tab. On the Basic Information page, enter the attribute name of the monitoring node and the attribute value [#] . # 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.



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**).

7

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 3 - Manager Administration Guide*.

Before you use this function, make sure that your cluster software supports JP1/IM - Manager.

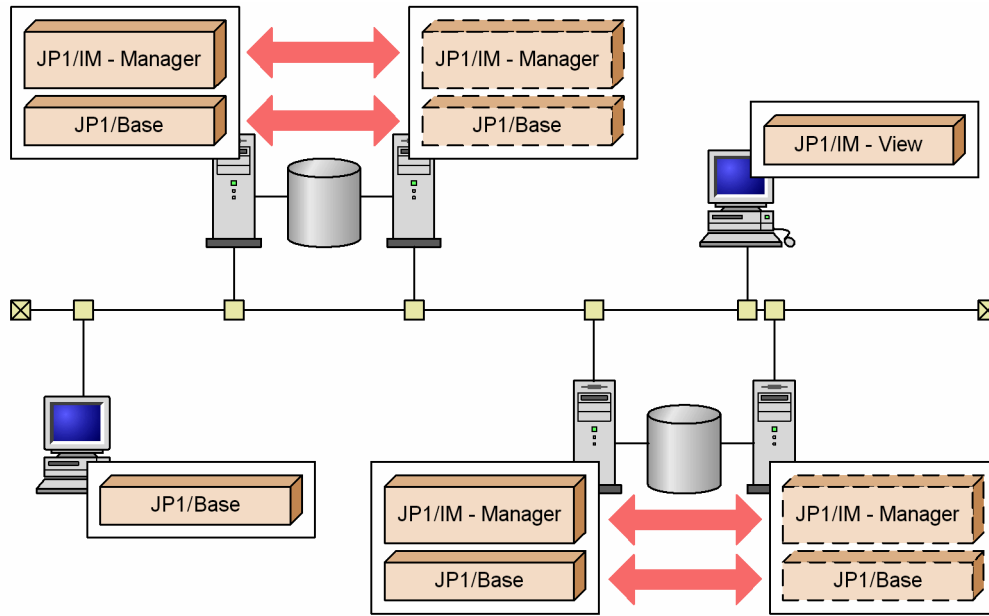
7.1 Overview of cluster operation (for Windows)

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 7–1: 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.

When a JP1/IM - Agent is used in a cluster, the modules that operate in the manager are the same as those that are supported in JP1/IM - Manager. For details about the cluster configuration supported by JP1/IM - Agent operating as agent, see 14.3.7(2) *Configuration for operating JP1/IM - Agent on a cluster system* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

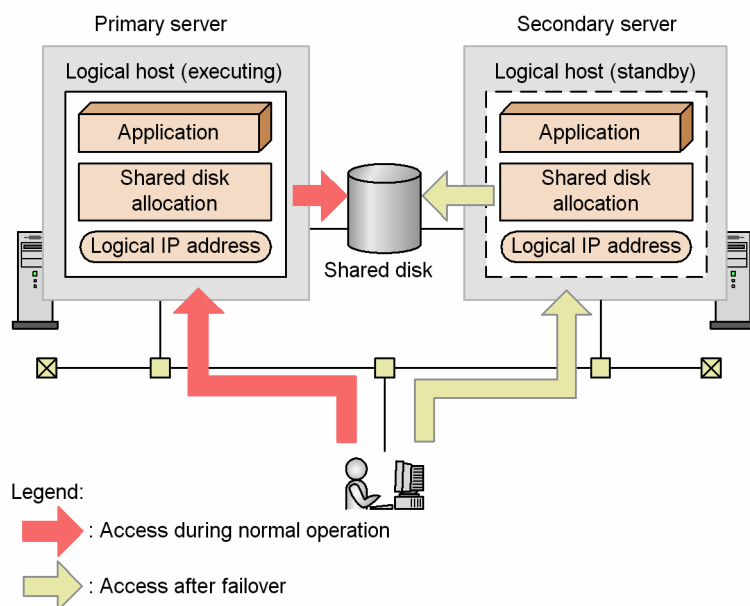
7.1.1 Overview of a cluster system (for Windows)

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 7–2: 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.

7.1.2 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 7–1: Prerequisites for the logical host environment

Logical host component	Prerequisites
Shared disk	• 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	• 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 7–2: Prerequisites for the physical host environment

Physical host component	Prerequisites
Server core	- 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	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	- 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	- 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	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, `-`, and `.` (period).

(5) Logical host names

Note the following when you specify a logical host name in JP1/IM - Manager:

- 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 (-).

When specifying logical host in JP1/IM - Agent, check the following points.

- The logical host name must be specified in the `hosts` file or on the name server to enable TCP/IP communication.
- Logical host name must be 63 characters or less and consist of single-byte alphanumeric characters and hyphens (-).

(6) Other Conditions

When using JP1/IM - Agent, note the following:

- When installing JP1/IM - Agent on primary server and secondary server in Windows, the installation destination must be the same folder.
- When installing JP1/IM - Agent on primary server and secondary server, make version the same.
- When installing the SAP system log extract command, perform the same setup on the running server and the standby server. The I/O file # of the SAP system log extract command, must be placed on the shared disk.

#

The command input and output files are as follows.

- Environment parameters file
- Log file of SAP system log extract command
- Trace file of SAP system log extract command
- Trace file output by RFC library
- When using the Web scenario monitoring function, place the same Web scenario file on the primary and secondary server.
- When copying Web scenario files between hosts in a clustered environment, follow the steps described in *1.5.1(9)(c) Migrating Web Scenario Files to another host* in the *JP1/Integrated Management 3 - Manager Administration Guide* and perform to be able to run the scenario without problems in the Web exporter of the destination host.

7.1.3 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 7–3: JP1/IM configuration in a cluster system

Product name	JP1/IM configuration in a cluster system
JP1/IM - View	• 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	• 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.

Product name	JP1/IM configuration in a cluster system
	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 7–4: File organization on the shared disk (Windows)

Function	Type of shared file	Folder name
Central Console	Definition file	<i>shared-folder\jplcons\conf\</i>
	Log file	<i>shared-folder\jplcons\log\</i>
	Temporary file	<i>shared-folder\jplcons\tmp\</i>
	History file [#]	<i>shared-folder\jplcons\operation\</i>
Central Scope	Definition file	<i>shared-folder\jplscope\conf\</i>
	Log file	<i>shared-folder\jplscope\log\</i>
	Temporary file	<i>shared-folder\jplscope\tmp\</i>
	Database	<i>shared-folder\jplscope\database\</i>
IM Configuration Management	Definition file	<i>shared-folder\JP1IMM\conf\imcf\</i>
	Log file	<i>shared-folder\JP1IMM\log\imcf\</i>
	Temporary file	<i>shared-folder\JP1IMM\tmp\</i>
	IM configuration data and profile data	<i>shared-folder\JP1IMM\data\imcf\</i>
IM database	Database	<i>user-specified-folder-on-shared-disk\imdb</i>
Intelligent Integrated Management Database	Execution file	See <i>Storage destination of the executable file of the Intelligent Integrated Management database in 2.7.1(1)(d) Where related files are stored in the JP1/Integrated Management 3 - Manager Overview and System Design Guide.</i>
	Logging file	See <i>Storage destination for individual logs of operation commands and Storage location of trend data management service logs in 2.7.1(1)(d) Where related files are stored in the JP1/Integrated Management 3 - Manager Overview and System Design Guide.</i>
	Data file	See <i>Storage destination for data files of Intelligent Integrated Management Database in 2.7.1(1)(d) Where related files are stored in the JP1/Integrated Management 3 - Manager Overview and System Design Guide.</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.

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 7–5: Services of JP1/IM - Manager (Windows)

Displayed name	Service name
JP1/IM3-Manager_ <i>logical-host-name</i>	JP1_Console_ <i>logical-host-name</i>
JP1/IM3-Manager DB Server_ <i>logical-host-name</i> ^{#1}	HiRDBEmbeddedEdition_JM ^{#2}
JP1/IM3-Manager DB Cluster Service_ <i>logical-host-name</i> ^{#1}	HiRDBClusterService_JM ^{#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 *JP1/Integrated Management 3 - Manager Command, Definition File and API 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.

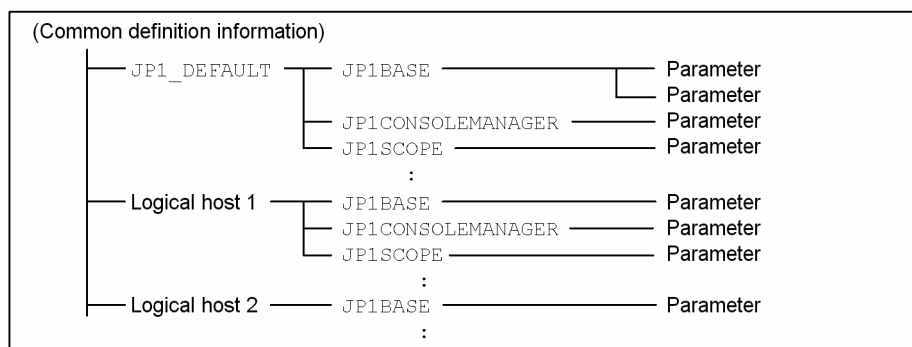
For details about the communication methods, see the descriptions of the JP1/Base communication methods in the *JP1/Base User's Guide*. JP1/IM - Manager uses the same communication methods as JP1/Base.

(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 7–3: 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.

7.2 Environment setup procedure for cluster operation (for Windows)

This section describes the environment setup for JP1/IM - Manager and JP1/IM - Agent that supports cluster operation.

The following figure shows the setup procedure.

For details about how to set a cluster system for the Intelligent Integrated Management Base, see [7.4 Creating a cluster environment for the Intelligent Integrated Management Base \(for Windows\)](#).

Figure 7–4: Setup procedure (when setting up a new environment (JP1/IM - Manager))

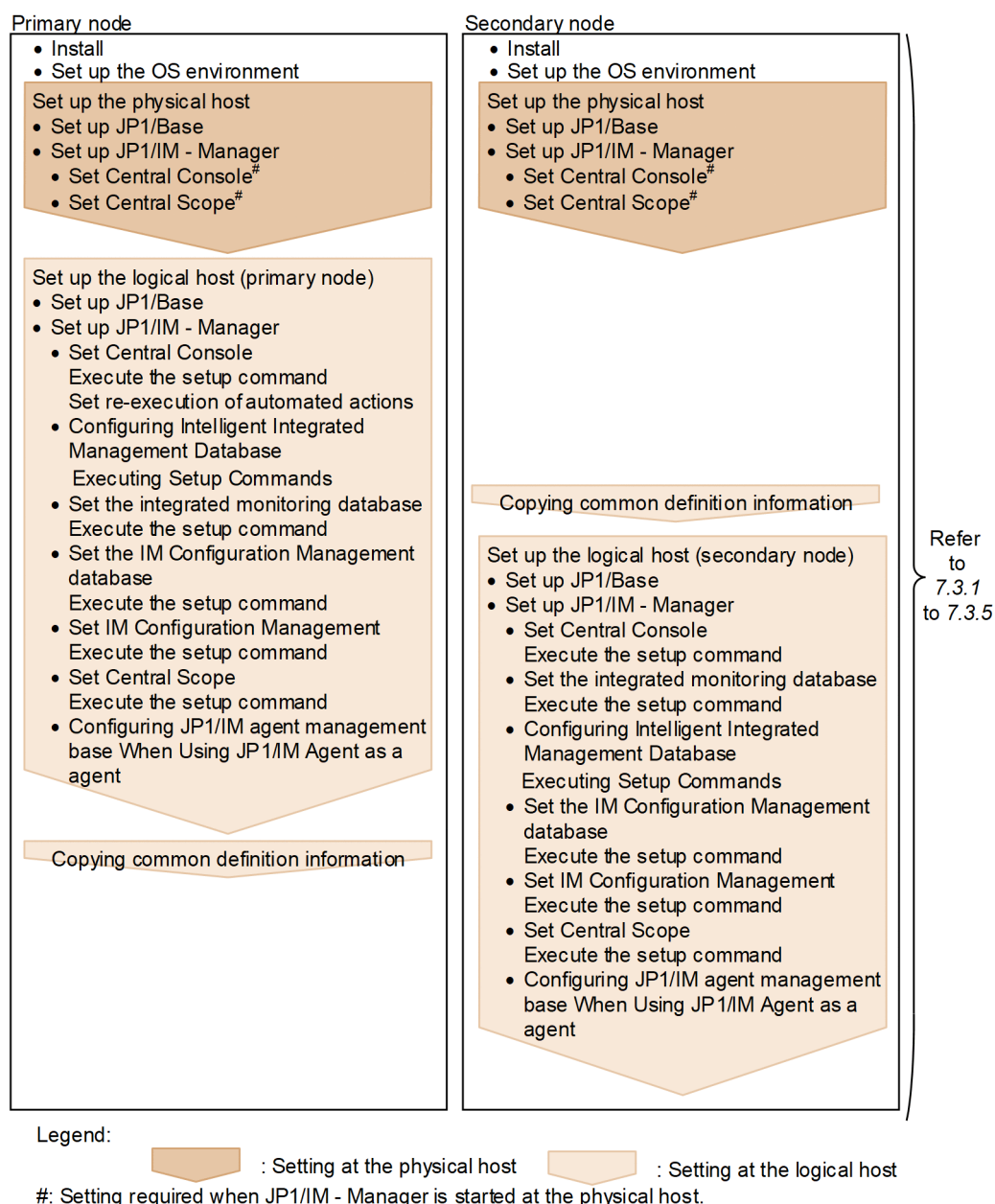


Figure 7–5: Setup procedure (when setting up a new environment (JP1/IM - Agent))

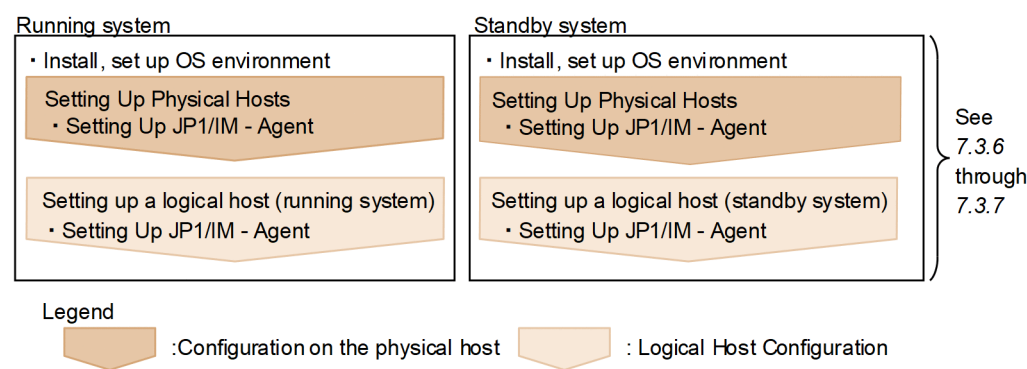
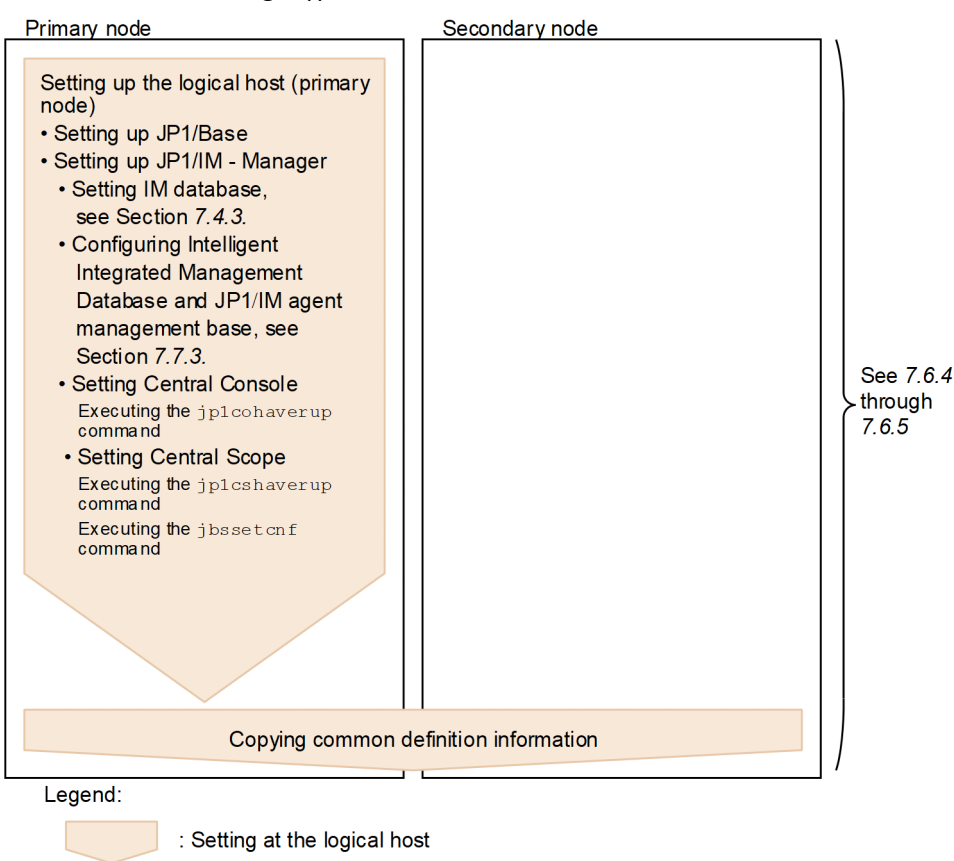


Figure 7–6: Setup procedure (when upgrading the existing logical host environment (JP1/IM - Manager))



7.3 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 and JP1/IM - Agent. It also describes the setup of JP1/Base because JP1/Base must be set up on the same logical host with JP1/IM - Manager.

Before you start the procedure, check the following information about the cluster system.

Table 7–6: 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 [7.1.2 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 [7.7.1 Deleting logical hosts \(for Windows\)](#).

7.3.1 Newly installing JP1/Base and JP1/IM - Manager (for Windows)

Install JP1/IM - Manager and JP1/Base on the local disks of Execute system Server and standby system Server.

If you install JP1/IM - Manager, JP1/IM agent management base for using JP1/IM - Agent is also installed.

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.

Perform the following steps related to JP1/IM agent management base when performing encrypted communication between JP1/IM agent management base and JP1/IM agent control base:

1. Deploy server certificate and the key file of server certificate.
If cryptographic communication (HTTPS) is set to enable, place server certificate and key file (private key file) of the cluster environment in the shared folder.

7.3.2 Setting up the physical host environment during new installation of JP1/IM - Manager (for Windows)

After installing JP1/Base and JP1/IM - Manager on both the active server and the standby server, set up the physical host environment for JP1/Base and JP1/IM - Manager.

If you install JP1/IM - Manager, JP1/IM agent management base for using JP1/IM - Agent is also installed.

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.

7.3.3 Setting up the logical host environment (primary node) during new installation of JP1/IM - Manager (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

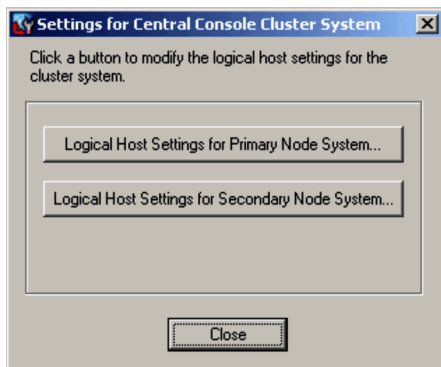
To set up JP1/Base:

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)

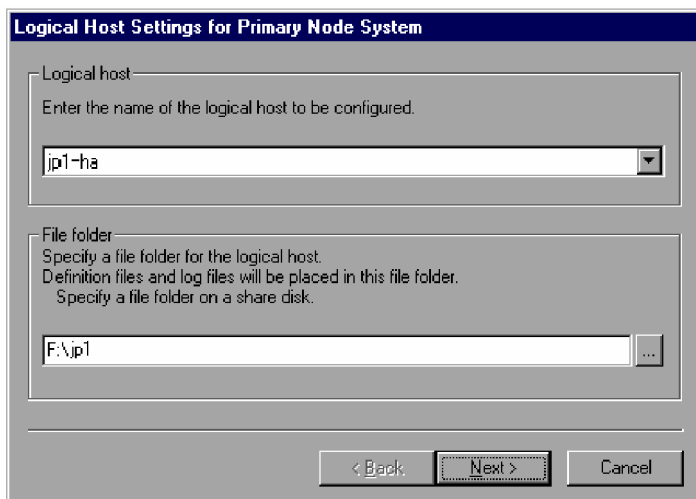
To set JP1/IM - Manager (Central Console):

1. Open the setup window for the logical host of JP1/IM - Manager (Central Console).
When you execute `Console-path\bin\jp1cohasetup.exe`, the following window appears.



2. Click the **Logical Host Settings for Primary Node System** button.

The following window appears.



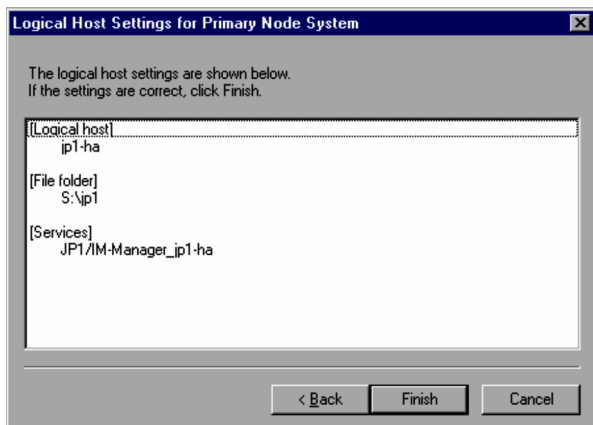
Specify the logical host name and file folder.

- 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.



Check the settings. If the settings are correct, click the **Finish** button.

Note that the environment settings of JP1/IM - Manager on the logical host inherit the settings of the physical host. Customize the environment settings of the logical host, with the `jcoimdef` command (`-h` option) if necessary.

For details about the `jcoimdef` command, see *jcoimdef* in *Chapter 1. Commands* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

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. The definition information of the physical host is inherited to the system environment configuration information to be specified in the command. Check the system environment configuration information of the physical host, and if necessary, set the system environment of the logical host.

```
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 *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

(4) Setting JP1/IM - Manager (integrated monitoring database)

This setting is required when 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 *JP1/Integrated Management 3 - Manager Command, Definition File and API 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 *JP1/Integrated Management 3 - Manager Command, Definition File and API 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 *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

(5) JP1/IM - Manager (Intelligent Integrated Management Database) Setup

If you are using Intelligent Integrated Management Database, the steps to build logical host infrastructure for Intelligent Integrated Management Database (Trend data Management Database) are as follows:

1. Build JP1/IM - Manager's logical host infrastructure.

Prior to building Intelligent Integrated Management Database's logical host environment, logical host environment of JP1/IM - Manager (central console) must be built because logical host environment of the created JP1/IM - Manager must be referenced. You must also build Intelligent Integrated Management Base, which is a prerequisite feature of integrated operation viewer, and setup, which is an integrated monitoring DB. If you have already built it, continue to the next step.

For details on how to build JP1/IM - Manager (central console) logical host environment, see [7.3.3\(3\) Setting JP1/IM - Manager \(Central Console\)](#). For details about building Intelligent Integrated Management Base, see [4.4 Creating a cluster environment for the Intelligent Integrated Management Base](#). For details about Setup of the integrated monitoring DB, see [7.3.3\(4\) Setting JP1/IM - Manager \(integrated monitoring database\)](#).

2. Prepare cluster environment Intelligent Integrated Management Database setup information file.

In cluster environment Intelligent Integrated Management Database setup information file, describe the required definitions, such as the data directory, port number, and so on.

see *Cluster environment Intelligent Integrated Management Database setup information file* (`jimgndbclustersetupinfo.conf`) in *Chapter 2. Definition Files* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference* for editing Intelligent Integrated Management Database setup information file.

3. Execute `jimgndbsetup` command.

Execute the following command:


```
jimgndbsetup -f cluster-environment-Intelligent-Integrated-Management-Data
base-setup-information-file -h logical-host-name -c online
```

4. Setup the service-dependency.

To run JP1/IM - Manager in a cluster, you register JP1/IM - Manager and JP1/Base of logical host into the cluster software and setup them to start and stop under the control of the cluster software.

Configuration file contents to register JP1/IM - Manager into clusters is as follows:

Table 7–7: Configuration file contents for registering to the cluster software (Windows)

Item number	NAME	Service name	Dependency
1	JP1/Base Event <i>logical-host-name</i>	JP1_Base_Event <i>logical-host-name</i>	IP address Resources Physical disk resources
2	JP1/Base_ <i>logical-host-name</i>	JP1_Base_ <i>logical-host-name</i>	Cluster resource in item 1
3	JP1/IM3-Manager DB Server_ <i>logical-host-name</i> ^{#1}	HiRDBEmbeddedEdition_JM ⁿ ₂	Cluster resources in item 1 and 2
4	JP1/IM3-Manager DB Cluster Service_ <i>logical-host-name</i> ^{#1}	HiRDBClusterService_JM ⁿ ₂	Cluster resources in item 1, item 2, and item 3
5	JP1/IM3-Manager_ <i>logical-host-name</i>	JP1_Console_ <i>logical-host-name</i>	Cluster Resource ^{#3,#4} in Item 1, Item 2, Item 3, Item 4, Item 6 and Item 7
6	JP1/IM3-Manager Intelligent Integrated DB Server_ <i>logical-host-name</i>	JP1_IMGNDDB_Service_ <i>logical-host-name</i>	Cluster resources in item 1, item 2, and item 3
7	JP1/IM3-Manager Trend Data Management Service_ <i>logical-host-name</i>	promscale_ <i>logical-host-name</i>	Cluster resources in item 1, item 2, item 3, and item 6

#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 *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

5. Starting JP1/IM - Manager services from cluster software

Start the following services from the cluster software:

```
JP1/IM3-Manager Intelligent Integrated DB Server_ logical-host-name
```

```
JP1/IM3-Manager Trend Data Management Service_ logical-host-name
```

(6) 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 *JP1/Integrated Management 3 - Manager Command, Definition File and API 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 *JP1/Integrated Management 3 - Manager Command, Definition File and API 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 *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

(7) 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\jplcfhasetup.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.

(8) 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\jplcshasetup.exe*.

2. Click the **Logical Host Settings for Primary Node System** button.

In the Logical Host Settings for Primary Node System window, specify the logical host name and file folder.

- Logical host name

The logical host names created in JP1/Base are displayed. Select the logical host name.

- File folder

Specify a folder on the shared disk. A set of JP1/IM - Manager files for the logical host is created under the *specified-folder-name\jplscope* folder.

After you have specified the above information, click the **Next** button.

3. Check the settings.

(9) Setup when using JP1/IM - Agent as an agent

(a) Setup changes for JP1/IM agent management base

The following describes how to change setup of JP1/IM agent management base (imbase,imbaseproxy).

■ Changing JP1/IM agent management base ports

Perform the following steps:

1. Shut down JP1/IM agent management base.

2. Change the listen port number of JP1/IM agent management base.

Setting of the listen port number is setup to port membership of imbase configuration file (*jpc_imbase.json*) and imbaseproxy configuration file (*jpc_imbaseproxy*) in JP1/IM agent management base. Change this to the new port number.

For detail on imbase configuration file and imbaseproxy configuration file, see the appropriate file in *Chapter 2. Definition Files* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

3. Starts JP1/IM agent management base.

■ Setup the certificate

Perform the following steps:

1. Shut down JP1/IM agent management base.

2. Change server certificate and keying file for JP1/IM agent management base.

The listen port number is setup to imbase configuration file (`jpc_imbase.json`) or imbaseproxy configuration file (`jpc_imbaseproxy.json`) `cert_file` or `key_file` member.

Updates setup value of `cert_file` or `key_file`, or file that you are setup.

For detail of imbase configuration file and imbaseproxy configuration file, see the appropriate file in *Chapter 2. Definition Files* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

3. Starts JP1/IM agent management base.

7.3.4 Copying the common definition information during new installation of JP1/IM - Manager (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
```

7.3.5 Setting up the logical host environment (secondary node) during new installation of JP1/IM - Manager (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

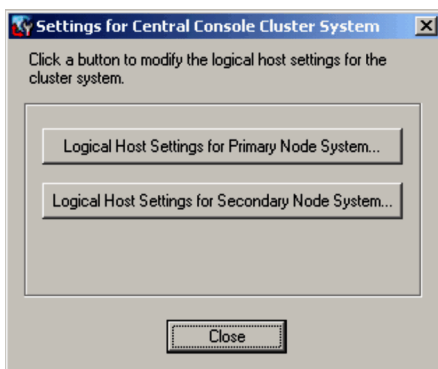
To set up JP1/Base:

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*.

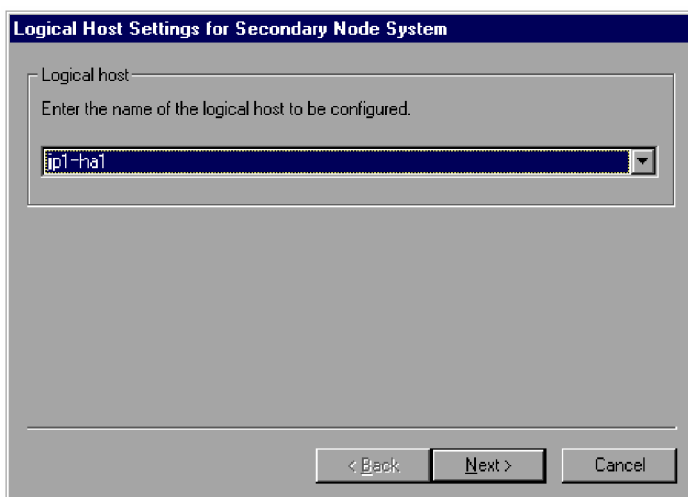
(3) Setting JP1/IM - Manager (Central Console)

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.



2. Click the **Logical Host Settings for Secondary Node System** button.
The following window appears.



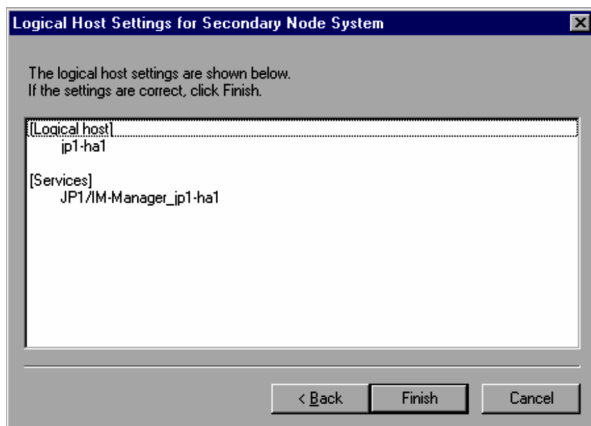
Specify the logical host name.

- 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.



Check the settings. If the settings are correct, click the **Finish** button.

(4) Setting JP1/IM - Manager (integrated monitoring database)

This setting is required when 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 [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 *JP1/Integrated Management 3 - Manager Command, Definition File and API 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 *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

(5) Setting JP1/IM - Manager (Intelligent Integrated Management Database)

If you are using Intelligent Integrated Management Database, the steps to build logical host infrastructure for Intelligent Integrated Management Database (Trend data Management Database) are as follows:

1. Build JP1/IM - Manager's logical host infrastructure.

Prior to building Intelligent Integrated Management Database's logical host environment, logical host environment of JP1/IM - Manager (central console) must be built because logical host environment of the created JP1/IM - Manager must be referenced. You must also build Intelligent Integrated Management Base, which is a prerequisite feature of integrated operation viewer, and setup, which is an integrated monitoring DB. If you have already built it, continue to the next step.

For details about how to build a JP1/IM - Manager (central console) logical host environment, see [7.3.5\(3\) Setting JP1/IM - Manager \(Central Console\)](#). For details about building Intelligent Integrated Management Base, see [4.4 Creating a cluster environment for the Intelligent Integrated Management Base](#). For details about setup of the integrated monitoring DB, see [7.3.5\(4\) Setting JP1/IM - Manager \(integrated monitoring database\)](#).

2. Prepare cluster environment Intelligent Integrated Management Database setup information file.

In cluster environment Intelligent Integrated Management Database setup information file, describe the required definitions, such as the data directory, port number, and so on.

See *Cluster environment Intelligent Integrated Management Database setup information file (jimgnbdbclustersetupinfo.conf)* in *Chapter 2. Definition Files* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference* for editing Intelligent Integrated Management Database setup information file.

3. Execute jimgnbdbsetup command.

Execute the following command:

```
jimgnbdbsetup -f cluster-environment-Intelligent-Integrated-Management-Data  
base-setup-information-file -h logical-host-name -c standby
```

4. Setup the service-dependency.

To run JP1/IM - Manager in a cluster, you register JP1/IM - Manager and JP1/Base of logical host into the cluster software and setup them to start and stop under the control of the cluster software.

For JP1/IM - Manager to register to the cluster, see configuration file contents in [7.5 Registering into the cluster software during new installation and setup \(for Windows\)](#).

5. Starting JP1/IM - Manager services from cluster software

Start the following services from the cluster software:

JP1/IM3-Manager Intelligent Integrated DB Server_ *logical-host-name*

JP1/IM3-Manager Trend Data Management Service_ *logical-host-name*

(6) 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 [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 *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

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

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

Use arguments to specify the cluster setup information file name, logical host name, 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 `jcfdbsetup` command, see `jcfdbsetup` in *Chapter 1. Commands* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

(7) 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.

(8) 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.

(9) Setup when using JP1/IM - Agent as an agent

This is the same as the procedure that is performed for primary server. For instructions, see [7.3.3\(9\) Setup when using JP1/IM - Agent as an agent](#).

7.3.6 Newly installing JP1/IM - Agent with integrated agent host (for Windows)

Install the JP1/IM - Agent on the local disk of the primary server and the secondary server.

1. Newly installing JP1/IM - Agent.

For details on how to install the software, see [1.3.1\(3\) Procedure of JP1/IM - Agent installation](#).

Select "Normal installation mode" for the installation mode.

This command is executed for both the primary server and the secondary server.

In the case of Windows, the installation destination folder must be the same path on the executable server and the standby server.

Do not start the JP1/IM - Agent service on the physical host. If it is running, stop it.

2. Create a configuration file for the new setup command for the logical host.

For details about configuration file, see *Configuration file of the logical host new setup (any-file-name)* in *Chapter 2. Definition Files* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

In addition, configuration file's sample filename is stored in the following path: You can copy and create.

```
JP1/IM-Agent-Installation-destination-folder\jplima\conf\sample\jpc_lhsetup.properties
```

3. Run a new setup command for the logical host.

```
jimalhsetup -h logical-hostname -d shared-folder -c {online|standby} -f setup-configuration-file [-q]
```

For details about the new setup command for logical hosts, see *jimalhsetup* in *Chapter 1. Commands* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

This command is executed on both the running server and the standby server.

4. Verify that Windows has registered to servicing.

On both the primary server and the secondary server, display the service of Windows to confirm that the service for logical host has been registered.

The name of the service for the logical host is the name appended with *_logical-host-name*.

5. Configure TLS settings.

When operating with TLS enabled, place the CA certificate file in the *shared-folder\jplima\conf\user\cert*.

Also, enter the full path of the CA certificate in the *immgr.tls_config.ca_file* of the *shared-folder\jplima\conf\jpc_imagentcommon.json*.

6. Perform the required setup.

7.3.7 Setting up the JP1/IM - Agent during new installation (for Windows), 1.21.2 Settings of JP1/IM - Agent to make the required configuration changes.

7. Reister the service for logical host in the cluster software.

For JP1/IM - Agent service's registration to the clustered software, see *7.5 Registering into the cluster software during new installation and setup (for Windows)*.

8. Setup JP1/IM - Agent to determine if it has stopped servicing for one minute on setup of the clusters.

If you upload the definition file to integrated operation viewer, restart of the service might occur after you deploy the definition file.

Also, if the content of the uploaded definition file is invalid and the service fails to start, the definition file is restored and the service is started.

As described above, you should setup the clusters to prevent them from detecting a temporary service outage because service might be temporarily stopped.

9. When using the data distribution function to multiple manager hosts, perform the following procedure before checking the operation.

Execute *New setting* in *7.3.7(2)(a) Setting the data delivery function to multiple manager hosts (for Windows) (optional)*.

10. Check for problems in operation.

- Start the service from the cluster software.
- Causes a failover.

7.3.7 Setting up the JP1/IM - Agent during new installation (for Windows)

In a cluster configuration, note the following:

- Files and folders on the shared disc may be the target of JP1/IM - Agent's files and folders.
- Starting and stopping JP1/IM - Agent services in integrated agent host is done from the clustered software.
- To change setup of service definition file, you must use both the primary server and the secondary server. You must also setup the same value on value that you want to setup.
- The security-product exception setup must also exclude *shared-folder/jplima*.

(1) Auto-start Setup

Because this is controlled by the cluster software, setup is not executed when OS is started automatically.

(2) Configuring JP1/IM agent control base

(a) Setting the data delivery function to multiple manager hosts (for Windows) (optional)

■ New settings

1. Shut down JP1/IM - Agent services from the cluster software.

The service key of the service to be stopped is shown below.

- jpc_imagent
- jpc_imagentaction
- jpc_imagentproxy
- jpc_alertmanager
- jpc_prometheus_server
- jpc_fluentd

2. Create folders for JP1/IM agent management base secondary.

Create the following folders as secondary folders for JP1/IM agent management base:

- *shared-folder\jplima\tmp\download-imagent-group-identifier*
- *shared-folder\jplima\tmp\upload-imagent-group-identifier*
- *shared-folder\jplima\tmp\jbsfwd-imagent-group-identifier*
- *shared-folder\jplima\tmp\imagent-imagent-group-identifier*
- *shared-folder\jplima\tmp\imagentproxy-imagent-group-identifier*
- *shared-folder\jplima\tmp\imagentaction-imagent-group-identifier*

To create the above folder, use the following command:

```
mkdir folder
```

3. Create a file for JP1/IM agent management base secondary.

This command is executed on both the running server and the standby server.

Source file name	Destination file name
jpc_imagent_service.exe	jpc_imagent-imagent-group-identifier_service_logical-hostname.exe
jpc_imagent_service_logical-hostname.xml	jpc_imagent-imagent-group-identifier_service_logical-hostname.xml
jpc_imagentproxy_service.exe	jpc_imagentproxy-imagent-group-identifier_service_logical-hostname.exe
jpc_imagentproxy_service_logical-hostname.xml	jpc_imagentproxy-imagent-group-identifier_service_logical-hostname.xml

Source file name	Destination file name
jpc_imagentaction_service.exe	jpc_imagentaction-imagent-group-identifier_service_logical-hostname.exe
jpc_imagentaction_service_logical-hostname.xml	jpc_imagentaction-imagent-group-identifier_service_logical-hostname.xml

4. Configure the service startup settings.

This command is executed on both the running server and the standby server.

See 3.15.7(5)(c) *Setting up secondary service startup* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

5. Configure settings for JP1/IM agent control base secondary.

This command is executed on the running server.

See 3.15.7(5)(d) *Configuration file of JP1/IM agent control base* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

6. Register a secret for the secondary of JP1/IM agent control base.

This command is executed on the running server.

Obtain and register initial secret of JP1/IM - Manager to which the secondary JP1/IM agent control base connects.

For the keys of initial secret to register, see 3.15.7(5)(e) *Initial secret, client secret, and HTTP proxy password keys* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

7. Perform settings other than JP1/IM agent control base.

This command is executed on the running server.

See 3.15.7(5)(f) *Sending settings of programs other than JP1/IM agent control base* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

8. Activate the services defined in service definition file by running the following command:

This command is executed on both the running server and the standby server.

```
Agent-path\tools\jpc_service -on service-key -h logical-hostname
```

For the service key, use the service key with *-imagent group identifier* among the JP1/IM - Agent service keys in the Windows environment described in 10.1 *Service of JP1/IM - Agent* in the *JP1/Integrated Management 3 - Manager Administration Guide*.

9. Register services for logical hosts in the cluster software.

The following services are registered in the cluster software.

Service	Dependency
jpc_imagent-imagent-group-identifier_service_logical-hostname	- IP Address Resources - Physical Disk Resources
jpc_imagentproxy-imagent-group-identifier_service_logical-hostname	jpc_imagent-imagent-group-identifier_service_logical-hostname
jpc_imagentaction-imagent-group-identifier_service_logical-hostname	jpc_imagentproxy-imagent-group-identifier_service_logical-hostname

For details about the command to register with the cluster software, see Step 7 *Reister the service for logical host in the cluster software* in 7.3.6 *Newly installing JP1/IM - Agent with integrated agent host (for Windows)*.

■ Setting at the time of version upgrade

If you are upgrading from a version that has data delivery function to multiple manager hosts enabled, perform the steps below.

Perform the following procedure after step 5 (before step 6) of [1.3.1\(3\)\(b\) Install instructions](#) at the time of version upgrade installation.

1. Create a file for JP1/IM agent management base secondary.

Copy the source file in *Agent-path\bin* and rename it to the destination file name.

Source file name	Destination file name
jpc_imagent_service.exe	jpc_imagent-imagent-group-identifier_service_logical-hostname.exe
jpc_imagentproxy_service.exe	jpc_imagentproxy-imagent-group-identifier_service_logical-hostname.exe
jpc_imagentaction_service.exe	jpc_imagentaction-imagent-group-identifier_service_logical-hostname.exe

(b) Deactivating the data delivery function to multiple manager hosts (for Windows) (optional)

The following describes the procedure for setting the data delivery function to multiple manager hosts when the data delivery function is no longer used.

Perform one of the following depending on your operating environment.

- Remove only data delivery function to multiple manager hosts without uninstalling logical hosts
- Uninstall the logical host

■ When deleting only the data delivery function to multiple manager hosts without uninstalling the logical host

1. Shut down JP1/IM - Agent running on the logical host.

This command is executed only for the running system server.

Stop the service running on the logical host from the cluster software.

2. Cancel the service registered in the cluster software.

This command is executed only for the running system server.

Cancel the service registered in step 8 of [7.3.7\(2\)\(a\) Setting the data delivery function to multiple manager hosts \(for Windows\) \(optional\)](#).

Check your cluster software documentation for instructions on how to remove the service.

3. Cancel the service of the secondary registered in Windows.

This command is executed on both the running server and the standby server.

For details about how to cancel, see step 3 in [7.7.3 Uninstall JP1/IM - Agent \(for Windows\)](#).

4. Delete the secret that you created to use the data delivery to multiple manager hosts feature.

This command is executed on the running server.

For the key of the secret to be deleted, see [3.15.7\(5\)\(e\) Initial secret, client secret, and HTTP proxy password keys](#) in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

This step is not necessary for secrets that have already been deleted.

5. Restore the settings for using the data delivery function to multiple manager hosts.

7.3.7(2)(a) Setting the data delivery function to multiple manager hosts (for Windows) (optional). Restore the settings for JP1/IM agent control base secondary set in steps 4 and 7 under *New settings*.

6. Delete the files copied to use the data delivery function to multiple manager hosts.

In *7.3.7(2)(a) Setting the data delivery function to multiple manager hosts (for Windows) (optional)*, delete the files for the secondary JP1/IM agent management base that you copied in step 2 of *New settings*.

7. Delete the folder created to use the data delivery function to multiple manager hosts.

After saving the required files such as logs, delete the folders for the secondary JP1/IM agent management base created in step 1 of *New settings* in *7.3.7(2)(a) Setting the data delivery function to multiple manager hosts (for Windows) (optional)*.

8. Delete integrated agent data registered on JP1/IM - Manager to which the disabled secondary service is connected.

This command is performed on both the running server and the standby server of JP1/IM - Manager. This command is not executed on the running server and the standby server of JP1/IM - Agent.

For details on deleting integrated agent data, see *2.2.1 List of Integrated Agents window in the JP1/Integrated Management 3 - Manager GUI Reference*.

■ When uninstalling the logical host

Perform step 4 to step 8 in *To remove only the data delivery function to multiple manager hosts without uninstalling the logical host* above between step 1 and step 2 in *7.7.3 Uninstall JP1/IM - Agent (for Windows)*.

Follow step 9 in *To remove only data delivery function to multiple manager hosts without uninstalling the logical host* above.

(3) Setup for Auto-Stop on OS Shutdown

Because it is controlled by the cluster software, setup is not performed when the service is stopped during OS shutdown.

(4) Additional Setup

The steps for changing setup in a clustered configuration are essentially the same as for a regular-host setup change. For details about changing setup of a persistent host, see *1.21 Setup for JP1/IM - Agent (for Windows)*.

7.4 Creating a cluster environment for the Intelligent Integrated Management Base (for Windows)

This section describes how to create a cluster environment for the Intelligent Integrated Management Base when the JP1/IM - Manager host managed by the cluster system is to be supported.

Note that once you configure the cluster environment for the Intelligent Integrated Management Base, it will take longer for the JP1/IM - Manager service to start. If your clustering software monitors the start-up time of the JP1/IM - Manager service or the startup control of JP1/Base is used to start the JP1/IM - Manager service, you need to check and, if necessary, revise the timeout value of the software. After configuring the Intelligent Integrated Management Base, check the start-up time of the service and adjust the timeout value.

The following table describes the organization of the files stored on the shared disk of the Intelligent Integrated Management Base.

Table 7–8: Organization of the files stored on the shared disk

OS	Shared file type	Folder name
Windows	Definition file	<code>shared-folder\jplimm\conf\imdd\</code> <code>shared-folder\jplimm\conf\imgndb\</code> <code>shared-folder\jplimm\conf\ssl\#</code>
	Log file	<code>shared-folder\jplimm\log\imdd\</code>
	Plug-in	<code>shared-folder\jplimm\plugin\imdd\</code>
	Data file	<code>shared-folder\jplimm\data\imdd\</code>
	Response action execution history	<code>shared-folder\jplimm\log\suggestion</code>

The `ssl` folder is created by enable the communication encryption function and the JP1/IM3-Manager service has started.

7.4.1 Creating a new cluster environment (For Windows)

The procedure for creating a cluster environment for the Intelligent Integrated Management Base is provided below.

For details about how to start JP1/IM - Manager after the setup, see *Chapter 3. Starting and Stopping JP1/IM - Manager* in the *JP1/Integrated Management 3 - Manager Administration Guide*.

Before performing the procedure described below, make sure that a cluster environment has already been created for both Central Console and the integrated monitoring database.

1. Stop JP1/IM - Manager.

Stop all JP1/IM - Managers in both the physical and the logical host environments.

2. Copy the folder of definition files.

Copy the `imdd` folder of the definition files on the physical host to the shared folder. Execute the following command:

```
xcopy Manager-path\conf\imdd shared-folder\jplimm\conf\imdd /s/e/i
```

3. Copy the plug-ins folder.

Copy the plugin folder of the plug-ins folder on the physical host to the shared folder. Execute the following command:

```
xcopy Manager-path\plugin shared-folder\jplimm\plugin /s/e/i
```

4. Create of the output folder of data files.

Create of the output folder of data files as *shared-folder\jplimm\data\imdd*.

Execute the following command:

```
mkdir shared-folder\jplimm\data\imdd\
```

5. Create an event-forwarding relay information folder.

Create *shared-folder/jplimm/data/imdd/eventForward/*. Execute the following command:

```
mkdir -p shared-folder/jplimm/data/imdd/eventForward/
```

6. Edit the intelligent integrated management infrastructure definition file (*imdd.properties*).

Specify the values specified for LOGICALHOSTNUMBER parameter and IMDBPORT parameter of the cluster setup information file (*jimdbclustersetupinfo.conf*) used when setting up the integrated monitoring database of the logical host in the intelligent integrated management infrastructure definition file (*imdd.properties*).

For example, you can set these values as follows:

```
jpl.im.db.DEFAULT.logicalHostNum=value-set-for-LOGICALHOSTNUMBER  
jpl.im.db.DEFAULT.portNo=value-set-for-IMDBPORT
```

For details, see *Cluster setup information file (jimdbclustersetupinfo.conf)* in *Chapter 2. Definition Files* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

In addition, as an interval when performing trend data deletion, in the setting item

jpl.imdd.trenddata.deleteInterval in the Description example of the Intelligent Integrated Management Base definition file (*imdd.properties*), set twice the value specified in *Interval to monitor* in [7.5.3 Setting Cluster Soft Parameters \(for Windows\)](#).

For details, see 1. in *Notes on Deleting Trend Data* in [2.7.2\(3\)\(g\) Deleting Trend Data Manually \(Specify integrated agent, user-defined Prometheus, and user-defined Fluentd host names and Delete\)](#) in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

7. Execute the following *jcoimdef* command to enable the service of the Intelligent Integrated Management Base:

```
Console-path\bin\jcoimdef -dd ON -hostmap ON -h logical-host-name
```

For details about the *jcoimdef* command, see *jcoimdef* in *Chapter 1. Commands* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

8. Create the output folder of operation logs.

Create the output folder of operation logs as *shared-folder\jplimm\operation\imdd\suggestion*.

Execute the following command:

```
mkdir shared-folder\jplimm\operation\imdd\suggestion\
```

9. Set up Intelligent Integrated Management Database.

Build Logical host infrastructure for intelligent integrated databases.

- For Active host

For details about the build process, see [7.3.3\(5\) JP1/IM - Manager \(Intelligent Integrated Management Database\) Setup](#).

- For Standby host
For details about the build process, see [7.3.5\(5\) Setting JP1/IM - Manager \(Intelligent Integrated Management Database\)](#).

10. Start the service.

Start the following services from the cluster software:

- JP1/IM3-Manager_ *logical-host-name*
- JP1/IM3-Manager DB Server_ *logical-host-name*
- JP1/IM3-Manager DB Cluster Service_ *logical-host-name*
- JP1/IM3-Manager Intelligent Integrated DB Server_ *logical-host-name*
- JP1/IM3-Manager Trend Data Management Service_ *logical-host-name*

7.4.2 Creating a cluster environment to which a corrected version is applied (For Windows)

This subsection describes how to create a cluster environment to which a corrected version is applied. If you apply the corrected version to a cluster environment, you have to relocate plug-ins.

1. Stop JP1/IM - Manager.

Stop all JP1/IM - Managers in both the physical and the logical host environments.

2. Copy the plug-ins folder.

Copy the `plugin` folder of the `plug-ins` folder on the physical host to the shared folder. Execute the following command:

```
xcopy Manager-path\plugin shared-folder\jplimm\plugin /s/e/i
```

3. Copy the definition file

Copy the `imdd_system.properties` file on the physical host to the shared folder. Execute the following command:

```
xcopy Manager-path\conf\imdd\system\imdd_system.properties shared-folder\jplimm\conf\imdd\system /s /e /i
```

4. Start the service.

From the cluster software, start the JP1/IM3-Manager_ *logical-host-name* service.

7.4.3 Creating a cluster environment after upgrading (For Windows)

This subsection describes how to upgrade the Intelligent Integrated Management Base that is currently in use in a cluster environment.

Also, if you want to upgrade the linked product at the same time, perform the version upgrade of the linked product before performing step 9.

1. Stop JP1/IM - Manager.

Stop all JP1/IM - Managers in both the physical and the logical host environments.

2. Copy the plug-ins folder.

Copy the plugin folder of the plug-ins folder on the physical host to the shared folder. Execute the following command:

```
xcopy Manager-path\plugin shared-folder\jplimm\plugin /s/e/i
```

3. Copy the definition file.

Copy the definition file for the physical host to a shared folder. Execute the following command:

```
robocopy Manager-path\conf\imdd shared-folder\jplimm\conf\imdd /e /xn /xo /xc
xcopy Manager-path\conf\imdd\*.model shared-folder\jplimm\conf\imdd /y
xcopy Manager-path\conf\imdd\system\*.model shared-folder\jplimm\conf\imdd\system /y
xcopy Manager-path\conf\imdd\system\*.update shared-folder\jplimm\conf\imdd\system /y
xcopy Manager-path\conf\imdd\system\fileoperation\*.update shared-folder\jplimm\conf\imdd\system\fileoperation /y
xcopy Manager-path\conf\imdd\responseaction\*.model shared-folder\jplimm\conf\imdd\responseaction /y
xcopy Manager-path\conf\imdd\fileoperation\*.model shared-folder\jplimm\conf\imdd\fileoperation /y
xcopy Manager-path\conf\imdd\suggestion\*.model shared-folder\jplimm\conf\imdd\suggestion /y
xcopy Manager-path\conf\imdd\plugin shared-folder\jplimm\conf\imdd\plugin /s/e/i/y
xcopy Manager-path\conf\imgndb\postgresql.conf.model shared-folder\jplimm\conf\imgndb/y
echo f | xcopy shared-folder\jplimm\conf\imdd\system\imdd_system.properties.update shared-folder\jplimm\conf\imdd\system\imdd_system.properties /y
echo f | xcopy shared-folder\jplimm\conf\imdd\system\fileoperation\imdd_product_deffile_list.json.update shared-folder\jplimm\conf\imdd\system\fileoperation\imdd_product_deffile_list.json /y
```

4. Create an event-forwarding relay information folder.

Create *shared-folder/jplimm/data/imdd/eventForward/*. Execute the following command:

```
mkdir -p shared-folder/jplimm/data/imdd/eventForward/
```

5. Set up Intelligent Integrated Management Database.

When upgrading from JP1/IM - Manager of V12, build Logical host infrastructure for intelligent integrated databases.

- For Active host
For details about the build process, see [7.3.3\(5\) JP1/IM - Manager \(Intelligent Integrated Management Database\) Setup](#).
- For Standby host
For details about the build process, see [7.3.5\(5\) Setting JP1/IM - Manager \(Intelligent Integrated Management Database\)](#).

6. Add a new setting.

Add the newly added setting value according to the function to be used.[#]

#

When upgrading JP1/IM - Manager from 13-00 or 13-01 to 13-10 or later, add three lines ("web-enable-admin-api: true", "db-connections-max: 50", "db-writer-connection-concurrency: 1" (underlined part of "after change" below) to the end of the following file in a text editor. When the Intelligent Integrated Management database is rebuilt, this procedure is not required because it is added automatically.

shared-folder/jplimm/conf/imgndb/config.yml

<Example of change>

- Before change

```
db-host: localhost
db-name: imgndb
db-user: imuser
db-password: rCKsdJ8vSQn2
db-port: 20705
web-listen-address: localhost:20706
log-level: info
db-ssl-mode: allow
promql-max-points-per-ts: 30001
```

- After change

```
db-host: localhost
db-name: imgndb
db-user: imuser
db-password: rCKsdJ8vSQn2
db-port: 20705
web-listen-address: localhost:20706
log-level: info
db-ssl-mode: allow
promql-max-points-per-ts: 30001
web-enable-admin-api: true
db-connections-max: 50
db-writer-connection-concurrency: 1
```

If you do not add a "web-enable-admin-api: true" line, deleting the trend data and deleting integrated agent info will fail.

For details about deleting trend data and integrated agent information, see *2.2.1 List of Integrated Agents window* in the *JP1/Integrated Management 3 - Manager GUI Reference* and see *5.11.4 Delete Trend Data* and *5.18.2 Delete integrated agent info* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

If you do not add the "db-connections-max: 50" and "db-writer-connection-concurrency: 1" rows, the following events may occur when collecting a large amount of performance data (when the sum of sample collected by integrated agent in the system (in the system of lower manager in a multi-stage configuration) exceeds 10,000 seconds):

- Performance data is not saved in Intelligent Integrated Management Database and cannot be displayed and retrieved
- Trend data management service memory usage increases

7. Setup the service-dependency.

Register JP1/IM agent management base and Intelligent Integrated Management Database services to the cluster software and setup them to start and stop under the control of the cluster software.

For details about setting dependencies, see [7.3.5\(5\) Setting JP1/IM - Manager \(Intelligent Integrated Management Database\)](#).

8. Start the service.

Start the following services from the cluster software:

- JP1/IM3-Manager_ *logical-host-name*
- JP1/IM3-Manager Intelligent Integrated DB Server_ *logical-host-name*
- JP1/IM3-Manager Trend Data Management Service_ *logical-host-name*
- JP1/IM3-Agent Base Server_ *logical-host-name*
- JP1/IM3-Agent Base Proxy Server_ *logical-host-name*

9. By executing the `jddcreatetree` command, generate the IM management node-related files.

For details about the `jddcreatetree` command, see `jddcreatetree` in *Chapter 1. Commands in the JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

10. By executing the `jddupdatetree` command in new and rebuilding mode, apply the definitions to the Intelligent Integrated Management server.

For details about the `jddupdatetree` command, see `jddupdatetree` in *Chapter 1. Commands in the JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

7.5 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, JP1/Base and JP1/IM - Agent on the logical host into the cluster software, and then set them to be started and terminated by the cluster software.

Start the services in the order of resource, JP1/Base, JP1/IM - Manager and JP1/IM - Agent for startup.

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 7–9: Settings for registering JP1/IM - Manager to 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/IM3-Manager DB Server <i>logical-host-name</i> ^{#1}	HiRDBEmbeddedEdition_JM ^{#2}	Cluster resources of Nos. 1 and 2
4	JP1/IM3-Manager DB Cluster Service <i>logical-host-name</i> ^{#1}	HiRDBClusterService_JM ^{#2}	Cluster resources of Nos. 1, 2, and 3
5	JP1/IM3-Manager <i>logical-host-name</i>	JP1_Console <i>logical-host-name</i>	Cluster resources of Nos. 1, 2, 3, 4, 6 and 7 ^{#3,5}
6	JP1/IM3-Manager Intelligent Integrated DB Server <i>logical-host-name</i> ^{#4}	JP1_IMGNDDB_Service <i>logical-host-name</i>	Cluster resources of Nos. 1, 2, and 3
7	JP1/IM3-Manager Trend Data Management Service <i>logical-host-name</i> ^{#4}	promscale <i>logical-host-name</i>	Cluster resources of Nos. 1, 2, 3 and 6

#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 *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

#3

If you do not use the IM database, remove the cluster resources of Nos. 3 and 4 from the dependencies.

#4

Register to the clustered software only if you are using Intelligent Integrated Management Database.

#5

If you do not use Intelligent Integrated Management Database, remove the cluster resources in Item 6 and Item 7 from the dependencies.

Configuration file contents to register JP1/IM - Agent into the clustered software is as follows:

When you register the cluster software, setup it so that it has the following dependencies: Register only the services you want to use into the clustered software.

Table 7–10: Settings for registering JP1/IM - Agent with cluster software (Windows)

Service	Dependency
<i>jpc_windows_exporter_service_logical-host-name</i>	• IP address resources • Physical disk resources
<i>jpc_blackbox_exporter_service_logical-host-name</i>	• IP address resources • Physical disk resources
<i>jpc_ya_cloudwatch_exporter_service_logical-host-name</i>	• IP address resources • Physical disk resources
<i>jpc_imagent_service_logical-host-name</i>	• IP address resources • Physical disk resources
<i>jpc_imagentproxy_service_logical-host-name</i>	• <i>jpc_imagent_service_logical-host-name</i>
<i>jpc_imagentaction_service_logical-host-name</i>	• <i>jpc_imagentproxy_service_logical-host-name</i>
<i>jpc_alertmanager_service_logical-host-name</i>	• <i>jpc_windows_exporter_service_logical-host-name</i> • <i>jpc_blackbox_exporter_service_logical-host-name</i> • <i>jpc_ya_cloudwatch_exporter_service_logical-host-name</i> • <i>jpc_script_exporter_service_logical-host-name</i> • <i>jpc_promitor_resource_discovery_service_logical-host-name</i> • <i>jpc_promitor_scraper_service_logical-host-name</i> • <i>jpc_imagentaction_service_logical-host-name</i>
<i>jpc_prometheus_server_service_logical-host-name</i>	• <i>jpc_alertmanager_service_logical-host-name</i>
<i>jpc_fluentd_service_logical-host-name</i>	• <i>jpc_imagentaction_service_logical-host-name</i>
<i>jpc_web_exporter_service_logical-host-name</i>	• IP Address Resources • Physical Disk Resources
<i>jpc_vmware_exporter_service_logical-host-name</i>	• IP Address Resources • Physical Disk Resources
<i>jpc_windows_exporter_hyperv_service_logical-host-name</i>	• IP Address Resources • Physical Disk Resources

7.5.1 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 [8.5 Registering into the cluster software during new installation and setup \(for UNIX\)](#).

7.5.2 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.

7.5.3 Setting Cluster Soft Parameters (for Windows)

Configure the following settings for JP1/IM3-Manager Trend Data Management Service *_logical-host-name* described in [Table 7-9 Settings for registering JP1/IM - Manager to cluster software \(Windows\)](#) in [7.5 Registering into the cluster software during new installation and setup \(for Windows\)](#). For details of the values to set, see 1. in

Notes on Deleting Trend Data in 2.7.2(3)(g) Deleting Trend Data Manually (Specify integrated agent, user-defined Prometheus, and user-defined Fluentd host names and Delete) in the JP1/Integrated Management 3 - Manager Overview and System Design Guide.

- Interval to monitor: more than 14 seconds
- Number of times to be judged to have hesitation: 2 or more times in a row

7.6 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 and JP1/IM - Agent. It also describes the setup of JP1/Base because JP1/Base must be set up on the same logical host with JP1/IM - Manager.

Before you start the procedure, check the following information about the cluster system.

Table 7–11: 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 [7.1.2 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 [7.7.1 Deleting logical hosts \(for Windows\)](#).

7.6.1 Upgrade installation of 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. 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.

Important

If you have already set up Intelligent Integrated Management Database and have upgraded JP1/IM - Manager from version 13-10 or earlier to version 13-11 or later, run `jimgndbupdate` command to update

7.6.2 Upgrade installation of JP1/IM - Agent (for Windows)

When upgrading JP1/IM - Agent from version 13-00 or 13-01, also refer to [1.3.3\(14\) Notes on upgrading JP1/IM - Agent from version 13-00 or 13-01](#).

1. Stop JP1/IM - Agent servicing.

Stop JP1/IM - Agent of logical host from the cluster software.

If physical host is also used, JP1/IM - Agent of physical host is stopped.

2. Upgrade installation of JP1/IM - Agent.

For details about how to install the software, see [1.3.1\(3\) Procedure of JP1/IM - Agent installation](#).

This command is executed for both primary server and secondary server.

3. Create a configuration file for the version upgrade setup command for the logical host.

For details about configuration file, see *Configuration file of the logical host version upgrade setup command (any-file-name)* in Chapter 2. Definition Files in the JP1/Integrated Management 3 - Manager Command, Definition File and API Reference.

In addition, configuration file's sample filename is stored in the following path: You can copy and create.

```
JP1/IM-Agent-Installation-destination-folder\jplima\conf\sample\jpc_lhupdate.properties
```

4. Execute the version upgrade setup command for the logical host.

```
jimalhupdate -h logical-hostname -d shared-folder -c {online|standby} -f setup-configuration-file [-q]
```

For details about the upgrade setup command for logical hosts, see *jimalhupdate* in Chapter 1. Commands in the JP1/Integrated Management 3 - Manager Command, Definition File and API Reference.

This command is executed on both the running server and the standby server.

5. Verify that Windows has registered to servicing.

On both the primary server and the secondary server, display the service of Windows to confirm that the service for logical host has been registered.

The name of the service for the logical host is the name appended with *_logical-host-name*.

6. Perform the required setup for the added add-on program.

When using the added add-on program, see [1.21.2\(13\) Setting up Web scenario monitoring function](#), [1.21.2 \(14\) Setting up VMware exporter](#), [1.21.2\(3\)\(i\) Add a Web exporter scrape job \(for Windows\) \(optional\)](#), and [1.21.2\(3\)\(j\) Add a VMware exporter scrape job \(for Windows only\) \(optional\)](#) to make the necessary settings.

7. Reister the service for logical host in the cluster software.

When you register the cluster software, setup it so that it has the following dependencies: Register only the services you want to use into the clustered software.

Service	Dependency
jpc_web_exporter_service_logical-host-name	• IP address resources • Physical disk resources
jpc_vmware_exporter_service_logical-host-name	• IP address resources • Physical disk resources
jpc_windows_exporter_hyperv_service_logical-host-name	• IP address resources • Physical disk resources

8. If you are using the data distribution function to multiple manager hosts, perform the following steps before starting the service.

Execute *Setting at the time of version upgrade* in [7.3.7\(2\)\(a\) Setting the data delivery function to multiple manager hosts \(for Windows\) \(optional\)](#).

9. Start JP1/IM - Agent servicing.

Start JP1/IM - Agent of logical host service from the cluster software.

If you are also using physical host, start JP1/IM - Agent service of physical host.

7.6.3 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 [1.19.7 Specifying settings for upgrading \(for Windows\)](#).

7.6.4 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 7–12: 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.
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
```

7.6.5 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
```

7.7 Uninstalling logical hosts (for Windows)

This section describes how to uninstall logical hosts of JP1/IM - Manager and JP1/IM - Agent. The subsections below first explain how to delete logical hosts and then explain how to uninstall JP1/IM - Manager, JP1/Base and JP1/IM - Agent from the logical disk on the active server and the standby server.

7.7.1 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 3 - 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/IM3-Manager and JP1/IM3-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:

- JP1/IM - Manager DB Cluster Service (JP1/IM3-Manager DB Cluster Service_ *logical-host-name*) on the logical host
Stop the service.
- IM database service (JP1/IM3-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 *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

4. 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 *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

5. Delete the following files and folders.

Files under *shared-folder*\data\imcf\imconfig

Files and folders under *shared-folder*\data\imcf\profiles

(2) Delete for Intelligent Integrated Management Database

If you are using Intelligent Integrated Management Database, turn `jimgndbunsetup` command to execute and Intelligent Integrated Management Database logical host's Trend data Management Database to delete.

For details of `jimgndbunsetup` command, see *jimgndbunsetup* in *Chapter 1. Commands* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

For details about logical host as a whole deletion, see [7.7.1\(3\) Deleting the logical host](#).

If you are using cluster software and delete only Intelligent Integrated Management Database, review setup of the cluster software so that failover does not occur even if Intelligent Integrated Management Database is stopped.

(3) Deleting the logical host

To delete a logical host in Windows, use the `jplbshasetup.exe` command of JP1/Base.

To delete the logical host:

1. Execute the `jplbshasetup.exe` command.
2. In the Settings for Base Node Switching System window, click the **Delete Logical Host** button.
3. Select the name of the logical host that you want to delete.
4. Click the **Next** button.
5. Check the deletion details and then click the **Finish** button.

The logical host is now deleted. Note that when you delete the logical host, JP1/Base, JP1/IM - Manager, JP1/AJS, and JP1/Power Monitor (06-02 or later) are all deleted in batch mode.

Shared files and shared folders on the shared disk are not deleted. You must delete them manually.

(4) 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 [7.7.1\(1\) 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.
`spmsetsvccon -d -h logical-host-name`

7.7.2 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.

If you uninstall JP1/IM - Manager, JP1/IM agent management base for using JP1/IM - Agent is also uninstalled.

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

7.7.3 Uninstall JP1/IM - Agent (for Windows)

Uninstall JP1/IM - Agent on the local disks of active server and standby server.

1. Shut down JP1/IM - Agent running on logical host.
Shut down the services running in logical host from the cluster software.

2. If you are using the data distribution function to multiple manager hosts, perform the following procedure after stopping the service.

Perform *When uninstalling the logical host* described in 7.3.7(2)(b) *Deactivating the data delivery function to multiple manager hosts (for Windows) (optional)*.

3. Delete the services that have been registered to the cluster software.

Check your clustered software documentation for details about how to delete the service.

4. Delete the services that have been registered to Windows.

For services used on logical hosts, the services for logical hosts on both the active system and the standby system are canceled from Windows.

To remove service for a logical host, use the following command:

```
Agent-Path\tools\jpc_service -off service-key -h logical-host-name
```

The following shows an example of register servicing a Alertmanager.

```
Agent-Path\tools\jpc_service -off jpc_alertmanager -h logical-host-name
```

5. Delete service definition file for logical host.

Delete service definition file for logical host at the bottom of *Agent-Path\bin*.

File name to delete: *jpc_service_name_service_logical-host-name.xml*

The following shows a sample Alertmanager.

File name to delete
<i>jpc_alertmanager_service_logical-host-name.xml</i>

6. Delete Windows service program for logical host.

Delete Windows service program for logical host at the bottom of *Agent-path\bin*.

File name to delete: *jpc_service-name_service_logical-host-name.exe*

The following shows a sample Alertmanager.

File name to delete
<i>jpc_alertmanager_service_logical-host-name.exe</i>

7. Delete shared folders.

7.8 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.

7.8.1 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 (`jplcf_applyconfig.conf`)
- Remote log trap environment definition file (`jplcf_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 (`jplcf_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 of JP1/IM - Manager \(for Windows\)](#).

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.

7.8.2 Using commands to change settings (for Windows)

If you have used the `jcochafmode`, `jcochcfmode`, or `jcocmddef` command to change settings, you must also specify the same settings at the primary and secondary servers.

- When the `jcochafmode` command was executed

If you have changed the location of the event acquisition filter by specifying the `-h` option, you must copy the common definition information from the primary server to the secondary server.

Copy the common definition information using the setup procedure described in [7.3.4 Copying the common definition information during new installation of JP1/IM - Manager \(for Windows\)](#).

- 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 [7.3.4 Copying the common definition information during new installation of JP1/IM - Manager \(for Windows\)](#).

- 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.

7.8.3 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. Check the following service statuses:

If the status are different from the following status, stop the services to create the following status.

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

2. By operating the cluster software on the active host, place the following services offline and stop them by order:

- JP1/IM - Manager Service on the logical host (service name that is displayed: `JP1/IM3-Manager_logical-hostname`)
- JP1/IM - Manager DB Cluster Service on the logical host (service name that is displayed: `JP1/IM3-Manager DB Cluster Service_logical-host-name`)
- The IM database service on the logical host (service name that is displayed: `JP1/IM3-Manager DB Server_logical-host-name`)

3. In addition to transferring the shared disk and the logical IP address assigned to the active host to the standby host, make sure that the shared disk and the logical IP address can be used on the logical host.

4. On the standby host, start the following service from the service window of the OS by order:

- The IM database service on the logical host (service name that is displayed: `JP1/IM3-Manager DB Server_logical-host-name`)
- JP1/IM - Manager DB Cluster Service on the logical host (service name that is displayed: `JP1/IM3-Manager DB Cluster Service_logical-host-name`)

5. On standby host, execute the `jimdbstatus` command.

- Check that the IM database service is operational (the KNAN11182-I message is output).
KNAN11182-I The IM database service is running.
- If the IM database service is not operational, execute the `jimdbstatus` command every 10 seconds, and then wait until the service is operational.
`jimdbstatus -h logical-host-name`

6. Execute the `jimdbstop` command to stop the IM databases on the standby host:

```
jimdbstop -h logical-host-name
```

7. On the standby host, stop the following service from the service window of the OS:

JP1/IM - Manager DB Cluster Service on the logical host (service name that is displayed: JP1/IM3-Manager DB Cluster Service_ *logical-host-name*)

8. In addition to transferring the shared disk and the logical IP address assigned to the standby host to the active host, make sure that the shared disk and the logical IP address can be used on the logical host.

9. 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 11:
KNAN11201-I The IM database service is the latest.
- If the following message is output, perform the procedure beginning with step 10:
KNAN11202-I The overwrite is necessary for the IM database.
KNAN11211-I An update of the configuration files of an IM database service is required.

The following message will be output on the standby host, but it is not a problem.

KNAN11210-W The table schema could not be checked because a common disk could not be accessed.

10. Execute the `jimdbupdate` command to update the IM databases on the standby host:

```
jimdbupdate -h logical-host-name -i
```

The following message will be output on the standby host, but it is not a problem.

KNAN11210-W The table schema could not be checked because a common disk could not be accessed.

11. On the standby host, stop the following service from the service window of the OS:

The IM database service on the logical host (service name that is displayed: JP1/IM3-Manager DB Server_ *logical-host-name*)

12. On the active host, stop the following service from the service window of the OS:

The IM database service on the logical host (service name that is displayed: JP1/IM3-Manager DB Server_ *logical-host-name*)

13. Execute the `jimdbupdate` command on the active host:

```
jimdbupdate -h logical-host-name
```

- If the following message is output, perform step 16:
KNAN11201-I The IM database service is the latest.
- If the following message is output, perform the procedure beginning with step 14:

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.

KNAN11211-I An update of the configuration files of an IM database service is required.

14. 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
```

15. Execute the `jimdbupdate` command to update the IM databases on the active host:

```
jimdbupdate -h logical-host-name -i
```

16. On the active host, stop the following service from the service window of the OS:

The IM database service on the logical host (service name that is displayed: JP1/IM3-Manager DB Server_*logical-host-name*)

17. By operating the cluster software on the active host, place the following services online and start them by order:

JP1/IM - Manager Service on the logical host (service name that is displayed: JP1/IM3-Manager_*logical-host-name*)

JP1/IM - Manager DB Cluster Service on the logical host (service name that is displayed: JP1/IM3-Manager DB Cluster Service_*logical-host-name*)

18. Start the services stopped in step 1.

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.

7.9 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.
- 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 *2.2.4 Tasks to be performed before a logical host name is changed in a cluster system* in the *JP1/Integrated Management 3 - Manager Administration Guide* and perform the required tasks.
- When you create a logical host in a cluster system, or when you change the binding method, make sure to stop "JP1/IM3-Manager" service that is running on the physical host. If you create a logical host, or configure settings to change the binding method, the service of the logical host will not work correctly. In this situation, after checking the configuration, reboot the server machine to restore the service.
- If you are using JP1/Base on the physical host and you are not going to start JP1/IM - Manager on the physical host, delete (comment out) the definition for JP1/IM - Manager from the start sequence definition file for JP1/Base (`Base-path\JP1Base\conf\boot\JP1SVPRM.DAT`).
- If you execute "`jbsrt_get -h logical-host`" on a standby host that uses a cluster, the message "KAVB3113-I Definition does not exist. " is displayed. If that happens, execute "`jbsrt_get -h logical-host`" on an active host.
- For details on supported cluster software and notes on cluster software, see the following URL.

```
http://www.hitachi.com/products/it/software/prod/jpl/products/envionents/cluster/index.html
```

7.10 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.

7.10.1 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.

7.10.2 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 7. 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 3 - Manager Administration Guide*.

7.10.3 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.

8

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 3 - Manager Administration Guide*.

Before you use this function, make sure that your cluster software supports JP1/IM - Manager.

8.1 Overview of cluster operation (for UNIX)

The overview of cluster operation is the same as for Windows. For details, see [7.1 Overview of cluster operation \(for Windows\)](#).

8.1.1 Overview of a cluster system (for UNIX)

The overview of a cluster system is the same as for Windows. For details, see [7.1.1 Overview of a cluster system \(for Windows\)](#).

8.1.2 Prerequisites for cluster operation (for UNIX)

The prerequisites for cluster operation are the same as for Windows. For details, see [7.1.2 Prerequisites for cluster operation \(for Windows\)](#).

8.1.3 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 8–1: JP1/IM configuration in a cluster system

Product name	JP1/IM configuration in a cluster system
JP1/IM - View	• 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	• 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 8–2: File organization on the shared disk (UNIX)

Function	Type of shared file	Directory name
Central Console	Definition file	<i>shared-directory/jp1cons/conf/</i>
	Log file	<i>shared-directory/jp1cons/log/</i>

Function	Type of shared file	Directory name
	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>
Intelligent Integrated Management Database	Execute file	See <i>Storage destination of the executable file of the Intelligent Integrated Management Database in 2.7.1(1)(d) Where related files are stored in the JP1/Integrated Management 3 - Manager Overview and System Design Guide.</i>
	Logging file	See <i>Storage destination for individual logs of operation commands and Storage location of trend data management service logs in 2.7.1(1)(d) Where related files are stored in the JP1/Integrated Management 3 - Manager Overview and System Design Guide.</i>
	Data file	See <i>Storage destination for data files of Intelligent Integrated Management Database in 2.7.1(1)(d) Where related files are stored in the JP1/Integrated Management 3 - Manager Overview and System Design Guide.</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 3 - 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.

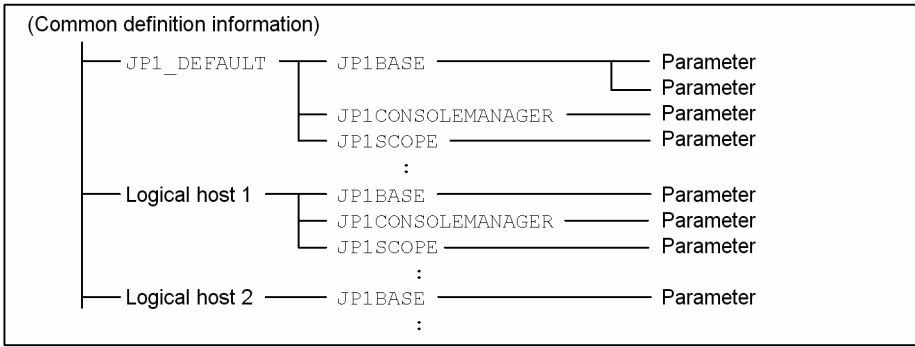
For details about the communication methods, see the descriptions of the JP1/Base communication methods in the *JP1/Base User's Guide*. JP1/IM - Manager uses the same communication methods as JP1/Base.

(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 8–1: 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.

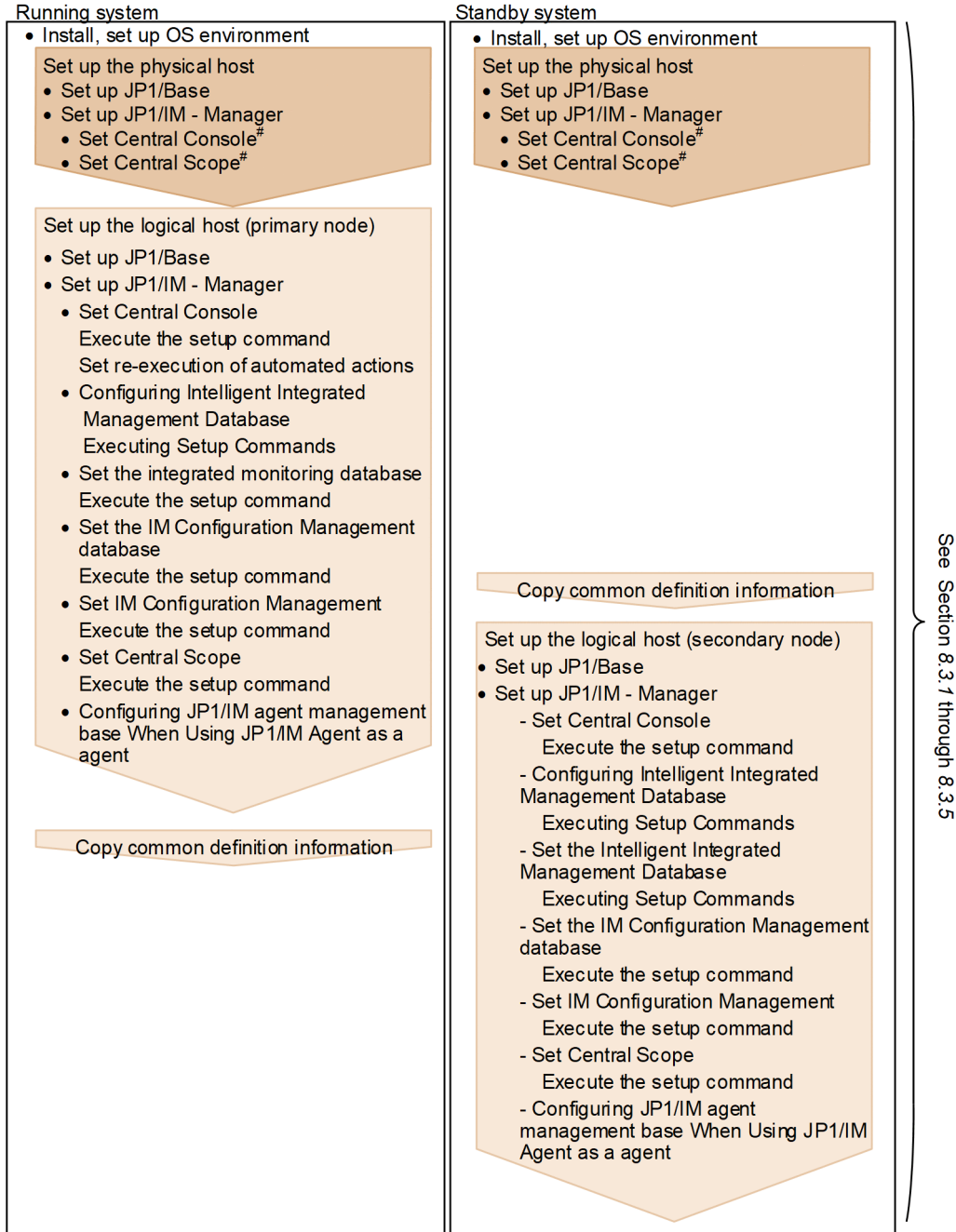
JP1/IM - Manager, JP1/Base, JP1/AJS, and JP1/Power Monitor (06-02 or later) use the common definition information to store the settings.

8.2 Environment setup procedure for cluster operation (for UNIX)

This section describes the environment setup for JP1/IM - Manager and JP1/IM - Agent that supports cluster operation.

For details about how to set a cluster system for the Intelligent Integrated Management Base, see [8.4 Setup for Intelligent Integrated Management Base's cluster environment \(for UNIX\)](#).

Figure 8–2: Setup procedure (when setting up a new environment (JP1/IM - Manager))



Legend: : Setting at the physical host : Setting at the logical host

[#]: Setting required when JP1/IM - Manager is started at the physical host.

Figure 8–3: Setup workflow (new environmental Setup (JP1/IM - Agent))

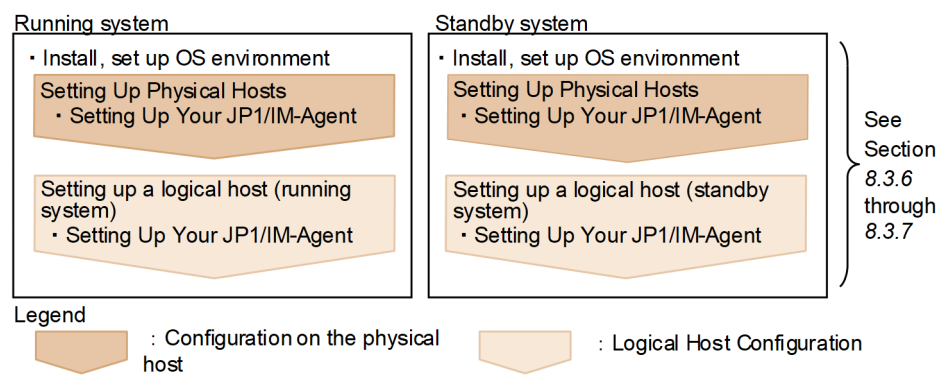
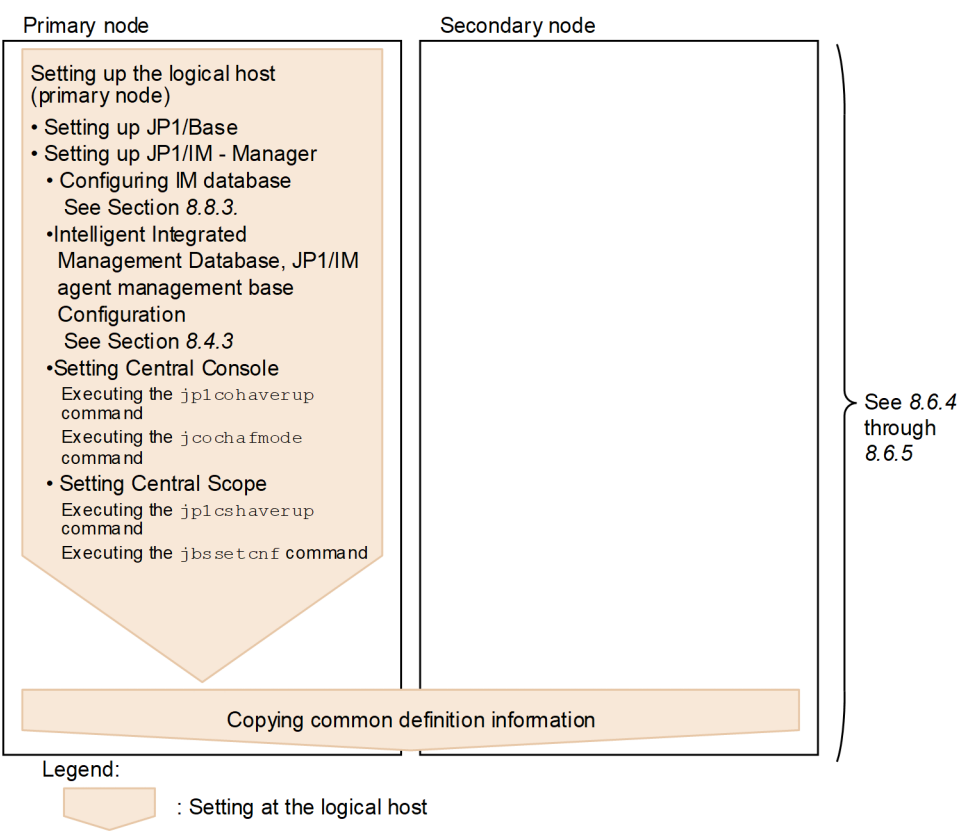


Figure 8–4: Setup procedure (when upgrading the existing logical host environment (JP1/IM - Manager))



8.3 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 and JP1/IM - Agent. It also describes the setup of JP1/Base because JP1/Base must be set up on the same logical host with JP1/IM - Manager.

Before you start the procedure, check the following information about the cluster system.

Table 8–3: 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 [7.1.2 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 [8.7.1 Deleting logical hosts \(for UNIX\)](#).

8.3.1 Newly installing JP1/Base and JP1/IM - Manager (for UNIX)

Install JP1/IM - Manager and JP1/Base on the local disks of the primary server and the secondary server.

If you install JP1/IM - Manager, JP1/IM agent management base for using JP1/IM - Agent is also installed.

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.

Perform the following steps related to JP1/IM agent management base when performing encrypted communication between JP1/IM agent management base and JP1/IM agent control base:

1. Deploy server certificate and the key file of server certificate.
If cryptographic communication (HTTPS) is set to enable, place server certificate and key file of the cluster environment in the shared directory.

8.3.2 Setting up the physical host environment during new installation of JP1/IM - Manager (for UNIX)

After installing JP1/Base and JP1/IM - Manager on both the active server and the standby server, set up the physical host environment for JP1/Base and JP1/IM - Manager.

If you install JP1/IM - Manager, JP1/IM agent management base for using JP1/IM - Agent is also installed.

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.

8.3.3 Setting up the logical host environment (primary node) of JP1/IM - Manager 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/jplcons/bin/jplcc_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*/jplcons/ directory is created and a set of JP1/IM - Manager (Central Console) files for the logical host is created.

Note that the environment settings of JP1/IM - Manager on the logical host inherit the settings of the physical host. Customize the environment settings of the logical host, with the `jcoimdef` command (`-h` option) if necessary.

For details about the command, see *jplcc_setup_cluster (UNIX only)* in *Chapter 1. Commands* and *jcoimdef* in *Chapter 1. Commands* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API 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. The definition information of the physical host is inherited to the system environment configuration information to be specified in the command. Check the system environment configuration information of the physical host, and if necessary, set the system environment of the logical host.:

```
/opt/jplcons/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 *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

(4) Setting JP1/IM - Manager (integrated monitoring database)

This setting is required when 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 *JP1/Integrated Management 3 - Manager Command, Definition File and API 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 [8.3.3\(2\) 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 *JP1/Integrated Management 3 - Manager Command, Definition File and API 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 *JP1/Integrated Management 3 - Manager Command, Definition File and API 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) JP1/IM - Manager (Intelligent Integrated Management Database) Setup

If you are using Intelligent Integrated Management Database, the steps to build logical host infrastructure for Intelligent Integrated Management Database (Trend data Management Database) are as follows:

1. Build JP1/IM - Manager's logical host infrastructure.

Prior to building Intelligent Integrated Management Database's logical host environment, logical host environment of JP1/IM - Manager (central console) must be built because logical host environment of the created JP1/IM - Manager must be referenced. You must also build Intelligent Integrated Management Base, which is a prerequisite feature of integrated operation viewer, and setup, which is an integrated monitoring DB. If you have already built it, continue to the next step.

For details on how to build JP1/IM - Manager (central console) logical host environment, see [8.3.3\(3\) Setting JP1/IM - Manager \(Central Console\)](#). For details about building Intelligent Integrated Management Base, see [4.4 Creating a cluster environment for the Intelligent Integrated Management Base](#). For details about setup of the integrated monitoring DB, see [8.3.3\(4\) Setting JP1/IM - Manager \(integrated monitoring database\)](#).

2. Create an OS user other than root.

You must have an OS user (a user with login other than root) other than root from which you want to start Intelligent Integrated Management Base database (PostgreSQL).

Use OS's `useradd` command to create them as needed. If you have already created one, skip to the next step.

Here is a sample Execute for `useradd` command when you create a user `imsrvuser`:

```
useradd imsrvuser
```

If you have already created one, continue to the next step.

3. Prepare cluster environment Intelligent Integrated Management Database setup information file.

In cluster environment Intelligent Integrated Management Database setup information file, describe the required definitions, such as the data directory, port number, and so on.

See *Cluster environment Intelligent Integrated Management Database setup information file* (*jimgndbclustersetupinfo.conf*) in *Chapter 2. Definition Files* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference* for editing Intelligent Integrated Management Database setup information file.

4. Execute jimgndbsetup command.

Execute the following command:

```
jimgndbsetup -f cluster-environment-Intelligent-Integrated-Management-Data
base-setup-information-file -h logical-host-name -c online
```

5. Starting JP1/IM - Manager services from cluster software

Start the following services from the cluster software:

```
jp1_cons_logical-host-name.service
```

(6) 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 *JP1/Integrated Management 3 - Manager Command, Definition File and API 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 [8.3.3\(2\) 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 *JP1/Integrated Management 3 - Manager Command, Definition File and API 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 *JP1/Integrated Management 3 - Manager Command, Definition File and API 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.

(7) Setting JP1/IM - Manager (IM Configuration Management) (optional)

This subsection describes the setting procedure 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 -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 `jplcf_setup_cluster`, the following directories are created:

- *shared-directory*/jplimm/conf/imcf
- *shared-directory*/jplimm/tmp
- *shared-directory*/jplimm/log/imcf
- *shared-directory*/jplimm/data/imcf

For details about the command, see *jplcf_setup_cluster (UNIX only)* in *Chapter 1. Commands* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

(8) Setting JP1/IM - Manager (Central Scope) (optional)

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 -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*/jplscope/ 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 *jplcs_setup_cluster (UNIX only)* in *Chapter 1. Commands* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

(9) Setup when using JP1/IM - Agent as a agent

(a) Setting changes for JP1/IM agent management base

The following describes how to change setting of JP1/IM agent management base (imbase,imbaseproxy).

■ Changing JP1/IM agent management base ports

Perform the following steps:

1. Shut down JP1/IM agent management base.
2. Change the listen port number of JP1/IM agent management base.
Setup of the listen port number is setup to port membership of imbase configuration file (`jpc_imbase.json`) and imbaseproxy configuration file (`jpc_imbaseproxy.json`) in JP1/IM agent management base. Change this to the new port number.
For detail on imbase configuration file and imbaseproxy configuration file, see the appropriate file in *Chapter 2. Definition Files in the JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.
3. Starts JP1/IM agent management base.

■ Setup the certificate

Perform the following steps:

1. Stop JP1/IM agent management base.
2. Change server certificate and keying file for JP1/IM agent management base.
The listen port number is setup to imbase configuration file (`jpc_imbase.json`) or imbaseproxy configuration file (`jpc_imbaseproxy.json`) `cert_file` or `key_file` member.
Updates setup value of `cert_file` or `key_file`, or file that you are setting.
For detail of imbase configuration file and imbaseproxy configuration file, see the appropriate file in *Chapter 2. Definition Files in the JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.
3. Starts JP1/IM agent management base.

8.3.4 Copying the common definition information during new installation of JP1/IM - Manager (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/jplbase/bin/jbssetcnf common-definition-information-backup-file-name`

8.3.5 Setting up the logical host environment (secondary node) during new installation of JP1/IM - Manager (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/jplimm/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/jplcons/bin/jplcc_setup_cluster -h logical-host-name`
Specify the logical host name by using an argument.
 - *logical-host-name* (-h option)
Specify the logical host name that was set up at the primary server.For details about the command, see `jplcc_setup_cluster` (UNIX only) in *Chapter 1. Commands in the JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

(4) Setting JP1/IM - Manager (integrated monitoring database)

This setting is required when 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 [8.3.5\(1\) 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 JP1/Integrated Management 3 - Manager Command, Definition File and API 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 JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

(5) JP1/IM - Manager (Intelligent Integrated Management Database) Setup

If you are using Intelligent Integrated Management Database, the steps to build logical host infrastructure for Intelligent Integrated Management Database (Trend data Management Database) are as follows:

1. Build JP1/IM - Manager's logical host infrastructure.

Prior to building Intelligent Integrated Management Database's logical host environment, logical host environment of JP1/IM - Manager (central console) must be built because logical host environment of the created JP1/IM - Manager must be referenced. You must also build Intelligent Integrated Management Base, which is a prerequisite feature of integrated operation viewer, and setup, which is an integrated monitoring DB. If you have already built it, continue to the next step.

For details on how to build JP1/IM - Manager (central console) logical host environment, see [8.3.3\(3\) Setting JP1/IM - Manager \(Central Console\)](#). For details about building Intelligent Integrated Management Base, see [4.4 Creating a cluster environment for the Intelligent Integrated Management Base](#). For details about setup of the integrated monitoring DB, see [8.3.3\(4\) Setting JP1/IM - Manager \(integrated monitoring database\)](#).

2. Create an OS user other than root.

You must have an OS user (a user with login other than root) other than root from which you want to start Intelligent Integrated Management Base database (PostgreSQL).

Use OS's `useradd` command to create them as needed. If you have already created one, skip to the next step.

Here is a sample execution for `useradd` command when you create a user `imsrvuser`:

```
useradd imsrvuser
```


If you have already created one, continue to the next step.

3. Prepare cluster environment Intelligent Integrated Management Database setup information file.

In cluster environment Intelligent Integrated Management Database setup information file, describe the required definitions, such as the data directory, port number, and so on.

See *Cluster environment Intelligent Integrated Management Database setup information file* (*jimgndbclustersetupinfo.conf*) in *Chapter 2. Definition Files* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference* for editing Intelligent Integrated Management Database setup information file.

4. Execute jimgndbsetup command.

Execute the following command:

```
jimgndbsetup -f cluster-environment-Intelligent-Integrated-Management-Data  
base-setup-information-file -h logical-host-name -c standby
```

5. Starting JP1/IM - Manager services from cluster software

Start the following services from the cluster software:

```
jp1_cons_logical-host-name.service
```

(6) 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 [8.3.5\(1\) 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 *JP1/Integrated Management 3 - Manager Command, Definition File and API 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 *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

(7) 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 JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

(8) 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 JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

Setup of the secondary node is now complete.

(9) Setup when using JP1/IM - Agent as a agent

This is the same as the procedure that is performed for the primary server. For instructions, see [8.3.3\(9\) Setup when using JP1/IM - Agent as a agent](#).

8.3.6 Newly installing JP1/IM - Agent with integrated agent host (for UNIX)

Install the JP1/IM - Agent on the local disk of the primary server and the secondary server.

1. Newly installing JP1/IM - Agent.

For details on how to install the software, see [2.3.1\(2\) Procedure of JP1/IM - Agent installation](#).

Select "Normal installation mode" for the installation mode.

This command is executed for both the primary server and the secondary server.

Do not start the JP1/IM - Agent service on the physical host. If it is running, stop it.

2. Create a configuration file for the command.

For details about configuration file, see *Configuration file of the logical host new setup command (any-file-name)* in *Chapter 2. Definition Files in the JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

In addition, configuration file's sample filename is stored in the following path: You can copy and create.

JP1/IM-Agent-Installation-destination-folder\jplima/conf/sample/jpc_lhsetup.properties

3. Run a new setup command for the logical host.

```
jimalhsetup -h logical-hostname -d shared-directory -c {online|standby}  
-f setup-configuration-file [-q]
```

For details about the new setup command for logical hosts, see *jimalhsetup* in *Chapter 1. Commands* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

This command is executed on both the running server and the standby server.

4. Verify that systemd has registered to servicing.

On both the primary server and the secondary server, display the service list of systemd to confirm that the service for logical host has been registered.

The name of the service for logical host is file name of unit definition file.

5. Configure TLS settings.

When operating with TLS enabled, place the CA certificate file in the *shared-directory*/jplima/conf/user/cert.

Also, enter the full path of the CA certificate in the *immgr.tls_config.ca_file* of the *shared-directory*/jplima/conf/jpc_imagentcommon.json.

6. Perform the required setup.

[8.3.7 Setting up the JP1/IM - Agent during new installation \(for UNIX\)](#) and [2.19.2 Settings of JP1/IM - Agent](#) to make the required configuration changes.

7. Reister the service for logical host in the cluster software.

For JP1/IM - Agent service's registration to the clustered software, see [8.5 Registering into the cluster software during new installation and setup \(for UNIX\)](#).

8. Setup JP1/IM - Agent to determine if it has stopped servicing for one minute on setup of the clusters.

If you upload the definition file to integrated operation viewer, restart of the service might occur after you deploy the definition file.

Also, if the content of the uploaded definition file is invalid and the service fails to start, the definition file is restored and the service is started.

As described above, you should setup the clusters to prevent them from detecting a temporary service outage because service might be temporarily stopped.

9. When using the data distribution function to multiple manager hosts, perform the following procedure before checking the operation.

Execute *New settings* in [8.3.7\(2\)\(a\) Setting the data delivery function to multiple manager hosts \(for Linux\) \(optional\)](#).

10. Check for problems in operation.

- Start the service from the cluster software.
- Causes a failover.

8.3.7 Setting up the JP1/IM - Agent during new installation (for UNIX)

In a cluster configuration, note the following:

- Files and directories on the shared disc may be the target of JP1/IM - Agent's files and directories.

- Starting and stopping JP1/IM - Agent services in integrated agent host is done from the clustered software.
- To change setup of unit definition file, you must use both the primary server and the secondary server. You must also setup the same value on value that you want to setup.
- The security-product exception setup must also exclude shared-directory/jplima.

(1) Auto-start Setup

Because this is controlled by the cluster software, setup is not executed when OS is started automatically.

(2) Configuring JP1/IM agent control base

(a) Setting the data delivery function to multiple manager hosts (for Linux) (optional)

■ New settings

1. Shut down JP1/IM - Agent services from the cluster software.

The service key of the service to be stopped is shown below.

- jpc_imagent
- jpc_imagentaction
- jpc_imagentproxy
- jpc_alertmanager
- jpc_prometheus_server

jpc_fluentd

2. Create folders for JP1/IM agent management base secondary.

Create the following folders as secondary folders for JP1/IM agent management base:

- *shared-directory/jplima/tmp/download-imagent-group-identifier*
- *shared-directory/jplima/tmp/upload-imagent-group-identifier*
- *shared-directory/jplima/tmp/jbsfwd-imagent-group-identifier*
- *shared-directory/jplima/tmp/imagent-imagent-group-identifier*
- *shared-directory/jplima/tmp/imagentproxy-imagent-group-identifier*
- *shared-directory/jplima/tmp/imagentaction-imagent-group-identifier*

To create the above folder, use the following command:

```
mkdir -m 700 directory
```

3. Create a unit definition file for JP1/IM agent management base secondary.

Copy the source unit definition file at the bottom of `/usr/lib/systemd/system` and rename it to the destination filename.

The owner and owner group of the created unit definition file must have `root`, accessibility of `644`.

Source file name	Destination file name
<code>jpc_imagent_logical-hostname.service</code>	<code>jpc_imagent-imagent-group-identifier_logical-hostname.service</code>

Source file name	Destination file name
<code>jpc_imagentproxy_logical-hostname.service</code>	<code>jpc_imagentproxy-imagent-group-identifier_logical-hostname.service</code>
<code>jpc_imagentaction_logical-hostname.service</code>	<code>jpc_imagentaction-imagent-group-identifier_logical-hostname.service</code>

4. Configure the service startup settings.

This command is executed on both the running server and the standby server.

See 3.15.7(5)(c) *Setting up secondary service startup* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

5. Configure settings for JP1/IM agent control base secondary.

This command is executed on the running server.

See 3.15.7(5)(d) *Configuration file of JP1/IM agent control base* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

6. Register a secret for the secondary of JP1/IM agent control base.

This command is executed on the running server.

Obtain and register initial secret of JP1/IM - Manager to which the secondary JP1/IM agent control base connects.

For the keys of initial secret to register, see 3.15.7(5)(e) *Initial secret, client secret, and HTTP proxy password keys* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

7. Perform settings other than JP1/IM agent control base.

This command is executed on the running server.

See 3.15.7(5)(f) *Sending settings of programs other than JP1/IM agent control base* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

8. Activate the services defined in service definition file by running the following command:

This command is executed on both the running server and the standby server.

```
systemctl daemon-reload
```

9. Register services for logical hosts in the cluster software.

The following services are registered in the cluster software.

Service
<code>jpc_imagent-imagent-group-identifier</code>
<code>jpc_imagentproxy-imagent-group-identifier</code>
<code>jpc_imagentaction-imagent-group-identifier</code>

For details about the dependencies of the above services and the command to register with the cluster software, see Step 7 *Register the service for logical host in the cluster software* in 8.3.6 *Newly installing JP1/IM - Agent with integrated agent host (for UNIX)*.

(b) Deactivating the data delivery function to multiple manager hosts (for Linux) (optional)

The following describes the procedure for setting the data delivery function to multiple manager hosts when the data delivery function is no longer used.

Perform one of the following depending on your operating environment.

- Remove only data delivery function to multiple manager hosts without uninstalling logical hosts
- Uninstall the logical host

■ When deleting only the data delivery function to multiple manager hosts without uninstalling the logical host

1. Shut down JP1/IM - Agent running on the logical host.
This command is executed only for the running system server.
Stop the service running on the logical host from the cluster software.
2. Cancel the service registered in the cluster software.
This command is executed only for the running system server.
Cancel the service registered in step 8 of [8.3.7\(2\)\(a\) Setting the data delivery function to multiple manager hosts \(for Linux\) \(optional\)](#).
3. Activate to deactivate the services on the secondary registered with systemd.
This command is executed on both the running server and the standby server.
For how to enable it, see step 3 in [8.7.3 Uninstalling JP1/IM - Agent \(for UNIX\)](#).
4. Delete the secret that you created to use the data delivery to multiple manager hosts feature.
This command is executed on the running server.
For the key of the secret to be deleted, see [3.15.7\(5\)\(e\) Initial secret, client secret, and HTTP proxy password keys](#) in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.
This step is not necessary for secrets that have already been deleted.
5. Restore the settings for using the data delivery function to multiple manager hosts.
[8.3.7\(2\)\(a\) Setting the data delivery function to multiple manager hosts \(for Linux\) \(optional\)](#). Restore the settings for JP1/IM agent control base secondary set in steps 4 and 7 under *New settings*.
6. Delete the files copied to use the data delivery function to multiple manager hosts.
In [8.3.7\(2\)\(a\) Setting the data delivery function to multiple manager hosts \(for Linux\) \(optional\)](#), delete the files for the secondary JP1/IM agent management base that you copied in step 2 of *New settings*.
7. Delete the folder created to use the data delivery function to multiple manager hosts.
After saving the required files such as logs, delete the folders for the secondary JP1/IM agent management base created in step 1 of *New settings* in [8.3.7\(2\)\(a\) Setting the data delivery function to multiple manager hosts \(for Linux\) \(optional\)](#).
8. Refresh systemd.
This command is executed on both the running server and the standby server.
For details about how to update, see step 5 in [8.7.3 Uninstalling JP1/IM - Agent \(for UNIX\)](#).
9. Delete integrated agent data registered on JP1/IM - Manager to which the disabled secondary service is connected.
This command is performed on both the running server and the standby server of JP1/IM - Manager. This command is not executed on the running server and the standby server of JP1/IM - Agent.
For details on deleting integrated agent data, see [2.2.1 List of Integrated Agents window in the JP1/Integrated Management 3 - Manager GUI Reference](#).

■ When uninstalling the logical host

Perform step 4 to step 8 in *When deleting only the data delivery function to multiple manager hosts without uninstalling the logical host* above between step 1 and step 2 in [8.7.3 Uninstalling JP1/IM - Agent \(for UNIX\)](#).

Follow step 10 in *When deleting only the data delivery function to multiple manager hosts without uninstalling the logical host* above.

(3) Setup for Auto-Stop on OS Shutdown

Because it is controlled by the cluster software, setup is not performed when the service is stopped during OS shutdown.

(4) Additional Setup

The steps for changing setup in a clustered configuration are essentially the same as for a regular-host setup change. For details about changing setup of a persistent host, see [2.19 Setup for JP1/IM - Agent \(for UNIX\)](#).

8.4 Setup for Intelligent Integrated Management Base's cluster environment (for UNIX)

This section describes how to create a cluster environment for the Intelligent Integrated Management Base when the JP1/IM - Manager host managed by the cluster system is to be supported.

Note that once you configure the cluster environment for the Intelligent Integrated Management Base, it will take longer for the JP1/IM - Manager service to start. If your clustering software monitors the start-up time of the JP1/IM - Manager service or the startup control of JP1/Base is used to start the JP1/IM - Manager service, you need to check and, if necessary, revise the timeout value of the software. After configuring the Intelligent Integrated Management Base, check the start-up time of the service and adjust the timeout value.

The following table describes the organization of the files stored on the shared disk of the Intelligent Integrated Management Base.

Table 8–4: Organization of the files stored on the shared disk

OS	Shared file type	Directory name
UNIX	Definition file	<i>shared-directory/jplimm/conf/imdd/ shared-directory/jplimm/conf/imgndb/ shared-directory/jplimm/conf/ssl/#</i>
	Log file	<i>shared-directory/jplimm/log/imdd/</i>
	Plug-in	<i>shared-directory/jplimm/plugin/imdd/</i>
	Data file	<i>shared-directory/jplimm/data/imdd/</i>
	Response action execution history	<i>shared-directory/jplimm/log/suggestion</i>

The `ssl` directory is created by enable the communication encryption function and the JP1/IM3-Manager service has started.

8.4.1 Creating a new cluster environment (for UNIX)

The procedure for creating a cluster environment for the Intelligent Integrated Management Base is provided below.

For details about how to start JP1/IM - Manager after the setup, see *Chapter 3. Starting and Stopping JP1/IM - Manager* in the *JP1/Integrated Management 3 - Manager Administration Guide*.

Before performing the procedure described below, make sure that a cluster environment has already been created for both Central Console and the integrated monitoring database.

1. Stop JP1/IM - Manager.

Stop all JP1/IM - Managers in both the physical and the logical host environments.

2. Copy the directory of the definition files.

Copy the `imdd` directory of the definition files on the physical host to the shared directory. Execute the following command:

```
cp -a /etc/opt/jplimm/conf/imdd shared-directory/jplimm/conf/
```

3. Copy the plug-ins directory.

Copy the plugin directory of plug-ins directory on the physical host to the shared directory. Execute the following command:

```
cp -a /etc/opt/jplimm/plugin shared-directory/jplimm/
```

4. Create of the output directory of data files.

Create of the output folder of data files as *shared-directory/jplimm/data/imdd/*.

Execute the following command:

```
mkdir -p shared-directory/jplimm/data/imdd/
```

5. Create an event-forwarding relay information directory.

Create *shared-directory/jplimm/data/imdd/eventForward/*. Execute the following command:

```
mkdir -p shared-directory/jplimm/data/imdd/eventForward/
```

6. Edit the intelligent integrated management infrastructure definition file (*imdd.properties*).

Specify the values specified for LOGICALHOSTNUMBER parameter and IMDBPORT parameter of the cluster setup information file (*jimdbclustersetupinfo.conf*) used when setting up the integrated monitoring database of the logical host in the intelligent integrated management infrastructure definition file (*imdd.properties*).

For example, you can set these values as follows:

```
jpl.im.db.DEFAULT.logicalHostNum=value-set-for-LOGICALHOSTNUMBER
```

```
jpl.im.db.DEFAULT.portNo=value-set-for-IMDBPORT
```

For details, see *Cluster setup information file (jimdbclustersetupinfo.conf)* in *Chapter 2. Definition Files in the JPI/Integrated Management 3 - Manager Command, Definition File and API Reference*.

In addition, as an interval when performing trend data deletion, in the setting item

jpl.imdd.trenddata.deleteInterval in the Description example of the Intelligent Integrated Management Base definition file (*imdd.properties*), set twice the value specified in *Interval to monitor* in [8.5.3 Setting Cluster Soft Parameters \(for Linux\)](#).

For details, see 1. in *Notes on Deleting Trend Data* in *2.7.2(3)(g) Deleting Trend Data Manually (Specify integrated agent, user-defined Prometheus, and user-defined Fluentd host names and Delete)* in the *JPI/Integrated Management 3 - Manager Overview and System Design Guide*.

7. Execute the following *jcoimdef* command to enable the service of the Intelligent Integrated Management Base:

```
/opt/jplcons/bin/jcoimdef -dd ON -hostmap ON -h logical-host-name
```

For details about the *jcoimdef* command, see *jcoimdef* in *Chapter 1. Commands in the JPI/Integrated Management 3 - Manager Command, Definition File and API Reference*.

8. Create the output directory of operation logs.

Create the output directory of operation logs as *shared-directory/jplimm/operation/imdd/suggestion/*.

Execute the following command:

```
mkdir -p shared-directory/jplimm/operation/imdd/suggestion/
```

9. Set up Intelligent Integrated Management Database.

Build logical host infrastructure for intelligent integrated databases.

- For active host

For details about the build process, see [8.3.3\(5\) JPI/IM - Manager \(Intelligent Integrated Management Database\) Setup](#).

- For standby host

For details about the build process, see [8.3.5\(5\) JP1/IM - Manager \(Intelligent Integrated Management Database\) Setup](#).

10. Start the service.

Start the following services from the cluster software:

- JP1/IM3-Manager_logical-host-name

8.4.2 Creating a cluster environment to which a corrected version is applied (for UNIX)

This subsection describes how to create a cluster environment to which a corrected version is applied. If you apply the corrected version to a cluster environment, you have to relocate plug-ins.

1. Stop JP1/IM - Manager.

Stop all JP1/IM - Managers in both the physical and the logical host environments.

2. Copy the plug-ins directory.

Copy the `plugin` directory of `plug-ins` directory on the physical host to the shared directory. Execute the following command:

```
cp -a /etc/opt/jplimm/plugin shared-directory/jplimm/
```

3. Copy the definition file

Copy the `imdd_system.properties` file on the physical host to the shared directory. Execute the following command:

```
cp -a /etc/opt/jplimm/conf/imdd/system/imdd_system.properties shared-directory/jplimm/conf/imdd/system/
```

4. Start the service.

From the cluster software, start the JP1/IM3-Manager.

8.4.3 Creating a cluster environment after upgrading (for UNIX)

This subsection describes how to upgrade the Intelligent Integrated Management Base that is currently in use in a cluster environment.

Also, if you want to upgrade the linked product at the same time, perform the version upgrade of the linked product before performing step 8.

1. Stop JP1/IM - Manager.

Stop all JP1/IM - Managers in both the physical and the logical host environments.

2. Copy the plug-ins directory.

Copy the `plugin` directory of `plug-ins` directory on the physical host to the shared directory. Execute the following command:

```
cp -a /etc/opt/jplimm/plugin shared-directory/jplimm/
```


3. Copy the definition file.

Copy the definition file for the physical host to a shared directory. Execute the following command:

```
cp -a -n /etc/opt/jplimm/conf/imdd/ shared-directory/jplimm/conf/imdd/
cp -a /etc/opt/jplimm/conf/imdd/*.model shared-directory /jplimm/conf/imdd/
cp -a /etc/opt/jplimm/conf/imdd/system/*.model shared-directory /jplimm/conf/imdd/system/
cp -a /etc/opt/jplimm/conf/imdd/system/*.update shared-directory /jplimm/conf/imdd/system/
cp -a /etc/opt/jplimm/conf/imdd/system/fileoperation/*.update shared-directory /jplimm/conf/imdd/system/fileoperation
cp -a /etc/opt/jplimm/conf/imdd/responseaction/*.model shared-directory/jplimm/conf/imdd/responseaction
cp -a /etc/opt/jplimm/conf/imdd/fileoperation/*.model shared-directory/jplimm/conf/imdd/fileoperation
cp -a /etc/opt/jplimm/conf/imdd/suggestion/*.model shared-directory/jplimm/conf/imdd/suggestion
cp -a /etc/opt/jplimm/conf/imdd/plugin shared-directory/jplimm/conf/imdd/
cp -a /etc/opt/jplimm/conf/imgndb/postgresql.conf.model shared-directory/jplimm/conf/imgndb/
cp shared-directory/jplimm/conf/imdd/system/imdd_system.properties.update shared-directory/jplimm/conf/imdd/system/imdd_system.properties
cp shared-directory/jplimm/conf/imdd/system/fileoperation/imdd_product_def file_list.json.update shared-directory/jplimm/conf/imdd/system/fileoperation/imdd_product_deffile_list.json
```

4. Create an event-forwarding relay information directory.

Create *shared-directory/jplimm/data/imdd/eventForward/*. Execute the following command:

```
mkdir -p shared-directory/jplimm/data/imdd/eventForward/
```

5. Setup Intelligent Integrated Management Database.

When upgrading from JP1/IM - Manager of V12, build logical host infrastructure for intelligent integrated databases.

- For active host
For details about the build process, see [8.3.3\(5\) JP1/IM - Manager \(Intelligent Integrated Management Database\) Setup](#).
- For standby host
For details about the build process, see [8.3.5\(5\) JP1/IM - Manager \(Intelligent Integrated Management Database\) Setup](#).

6. Add new settings.

Add new settings corresponding to the new functions you are going to use.#

```
#
When upgrading JP1/IM - Manager from 13-00 or 13-01 to 13-10 or later, add three lines ("web-
enable-admin-api: true", "db-connections-max: 50", "db-writer-connection-
concurrency: 1" (underlined part of "after change" below) to the end of the following file in a text editor.
When the Intelligent Integrated Management database is rebuilt, this procedure is not required because it is
added automatically.
shared-directory/jplimm/conf/imgndb/config.yml
<Example of change>
- Before change
```

```
db-host: localhost
db-name: imgndb
db-user: imuser
db-password: rCKsdJ8vSQn2
db-port: 20705
web-listen-address: localhost:20706
log-level: info
db-ssl-mode: allow
promql-max-points-per-ts: 30001
```

- After change

```
db-host: localhost
db-name: imgndb
db-user: imuser
db-password: rCKsdJ8vSQn2
db-port: 20705
web-listen-address: localhost:20706
log-level: info
db-ssl-mode: allow
promql-max-points-per-ts: 30001
web-enable-admin-api: true
db-connections-max: 50
db-writer-connection-concurrency: 1
```

If you do not add a "web-enable-admin-api: true" line, deleting the trend data and deleting integrated agent info will fail.

For details about deleting trend data and integrated agent information, see *2.2.1 List of Integrated Agents window* in the *JP1/Integrated Management 3 - Manager GUI Reference* and see *5.11.4 Delete Trend Data* and *5.18.2 Delete integrated agent info* in the *JP1/Integrated Management 3 -Manager Command, Definition File and API Reference*.

If you do not add the "db-connections-max: 50" and "db-writer-connection-concurrency: 1" rows, the following events may occur when collecting a large amount of performance data (when the sum of sample collected by integrated agent in the system (in the system of lower manager in a multi-stage configuration) exceeds 10,000 seconds):

- Performance data is not saved in Intelligent Integrated Management Database and cannot be displayed and retrieved
- Trend data management service memory usage increases

7. Start the service.

Start the following services from the cluster software:

- JP1/IM3-Manager_ *logical-host-name*
- JP1/IM3-Manager Intelligent Integrated DB Server_ *logical-host-name*
- JP1/IM3-Manager Trend Data Management Service_ *logical-host-name*
- JP1/IM3-Agent Base Server_ *logical-host-name*
- JP1/IM3-Agent Base Proxy Server_ *logical-host-name*

8. By executing the `jddcreatetree` command, generate the IM management node-related files.

For details about the `jddcreatetree` command, see *jddcreatetree* in *Chapter 1. Commands in the JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

9. By executing the `jddupdatetree` command in new and rebuilding mode, apply the definitions to the Intelligent Integrated Management server.

For details about the `jddupdatetree` command, see *jddupdatetree* in *Chapter 1. Commands in the JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

8.5 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, JP1/Base and JP1/IM - Agent 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, JP1/IM - Manager and JP1/IM - Agent.

There is more than one JP1/IM - Agent service. To prevent these services from starting and stopping at the same time, set up dependencies. The order of starting and stopping the services is arbitrary.

Also, set up dependencies to start JP1/IM - Agent service after the logical IP address resource and shared-directory are ready.

The services covered by JP1/IM - Agent are: registered only the services to be used to the clusters.

- `jpc_node_exporter`
- `jpc_blackbox_exporter`
- `jpc_ya_cloudwatch_exporter`
- `jpc_imagent`
- `jpc_imagentproxy`
- `jpc_imagentaction`
- `jpc_alertmanager`
- `jpc_prometheus_server`
- `jpc_fluentd`
- `jpc_vmware_exporter`

After you register the clusters, you do the following:

- Start

Start the service with the following command:

```
/opt/jplima/tools/jpc_service_start -s service-key -h logical-host
```

- Stop

Stop the service with the following command:

```
/opt/jplima/tools/jpc_service_stop -s service-key -h logical-host
```

- Forced stop

Stop the service forcibly with the following command:

```
/opt/jplima/tools/jpc_service_stop -s service-key -h logical-host -f
```

- Operational monitoring

Check the status of the service with the following command:

```
systemctl is-active service-key#_logical-host-name
```

- #
- Set the corresponding value below as the *service-key*.
- When monitoring the operation of Promitor Scraper: `promitor_scraper`
 - When monitoring the operation of Promitor Resource Discovery: `promitor_resource_discovery`

8.5.1 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 8–5: Detailed information for script design in cluster registration

Function to be registered	Description
Start	Starts JP1/IM - Manager. • 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 (300 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). For details about how to set the timeout period, see <i>14.7.11 Considering the timeout period during startup or stop of JP1/IM - Manager (in UNIX)</i> in the <i>JP1/Integrated Management 3 - Manager Overview and System Design Guide</i>. • 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	Terminates JP1/IM - Manager. • 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 (300 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). For details about how to set the timeout period, see <i>14.7.11 Considering the timeout period during startup or stop of JP1/IM - Manager (in UNIX)</i> in the <i>JP1/Integrated Management 3 - Manager Overview and System Design Guide</i>. • 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.

Function to be registered	Description
	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.
JP1/IM - Manager operation monitoring ^{#1}	Monitors normal operation of JP1/IM - Manager. - Command to be used <code>jco_spmd_status -h logical-host-name</code> To determine whether JP1/IM - Manager is running normally, check the return value of the <code>jco_spmd_status</code> command. This command determines the status from the operating status of each process. 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. - 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_spmd_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 (retrieable error): While the <code>jco_spmd_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}	Checks to see if the IM databases are running normally. - Command to be used <code>jimdbstatus -h logical-host-name</code> To determine the operating status, check the return value of the <code>jimdbstatus</code> command. - 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.
Verifying the Health of the Intelligent Integrated Management Database ^{#3}	If you are using the Intelligent Integrated Management database, verify that the Intelligent Integrated Management database is running normally. - Use this command <code>jimgndbstatus -h logical host name</code> - Determining the results of the operating status The following shows how to determine the return value: Return value=0: Running Returns=1: <code>jimgndbstatus</code> command terminated abnormally Return value=12: Stopping Return value=16: Intelligent Integrated Management Database is started and the Trend Data Management Service is stopped.

Function to be registered	Description
	Return value=17: Intelligent Integrated Management Database is stopped and the Trend Data Management Service is started. Return value=20: The Intelligent Integrated Management database is not set up
Forced termination	Forcibly terminates JP1/IM - Manager and releases the current resources. Command to be used <code>jco_killall.cluster logical-host-name</code> The <code>jco_killall.cluster</code> command forcibly terminates each process without performing JP1/IM - Manager termination processing. If you are using IM database service, also kill IM database service. If you are using Intelligent Integrated Management Database (Trend data Management Database), also forcibly terminates Intelligent Integrated Management Database service. <i>Note:</i> Before you execute forced termination, use the stop command to terminate JP1/IM - Manager.

#1

The commands used for JP1 operations related to operation checking are the same between UNIX and Windows, but the operations are different. Windows operations differ from UNIX operations due to their association with Windows service control. In Windows, when some of the processes terminate, the JP1 process management terminates each process automatically and places the service in stopped status. Treat service stop as an error or detect an error when a command such as `jco_spmc_status` returns a value of 8.

#2

Executed when the IM databases are used.

#3

Execute if you are using Intelligent Integrated Management Database.



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.

8.5.2 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
 - Allocate the shared disk and logical IP addresses, and make them available for use.
 - 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.

8.5.3 Setting Cluster Soft Parameters (for Linux)

Configure the following settings for *Verifying the Health of the Intelligent Integrated Management Database* (*jimgndbstatus* command) described in *Table 8-5 Detailed information for script design in cluster registration* in *8.5.1 Creating a script to be registered into the cluster software (for UNIX)*. For details of the values to set, see 1. in *Notes on Deleting Trend Data* in *2.7.2(3)(g) Deleting Trend Data Manually (Specify integrated agent, user-defined Prometheus, and user-defined Fluentd host names and Delete)* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

- Interval to monitor: more than 14 seconds
- Number of times to be judged to have hesitation: 2 or more times in a row

8.6 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 and JP1/IM - Agent. It also describes the setup of JP1/Base because JP1/Base must be set up on the same logical host of JP1/IM - Manager.

Before you start the procedure, check the following information about the cluster system.

Table 8–6: 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 [7.1.2 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 [8.7.1 Deleting logical hosts \(for UNIX\)](#).

8.6.1 Upgrade installation of 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.

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.

Important

If you have already set up Intelligent Integrated Management Database and have upgraded JP1/IM - Manager from version 13-10 or earlier to version 13-11 or later, run `jimgndbupdate` command to update Intelligent Integrated Management Database. If you have not updated Intelligent Integrated Management Database, JP1/IM - Manager might fail to start servicing.

8.6.2 Upgrade installation of JP1/IM - Agent (for UNIX)

When upgrading JP1/IM - Agent from version 13-00 or 13-01, also see [2.3.4\(9\) Notes on upgrading JP1/IM - Agent from version 13-00 or 13-01](#).

1. Shut down JP1/IM - Agent servicing.

Shut down JP1/IM - Agent of logical host from the cluster software. If physical host is also used, JP1/IM - Agent of physical host is stopped.

2. Upgrade and install JP1/IM - Agent.

For details about how to install the software, see [2.3.1\(2\) Procedure of JP1/IM - Agent installation](#).

This command is executed for both the primary server and the secondary server.

3. Create a configuration file for the version upgrade setup command for the logical host.

For details about configuration file, see *Configuration file of the logical host version upgrade setup command (any-file-name)* in *Chapter 2. Definition Files in the JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

In addition, configuration file's sample filename is stored in the following path: You can copy and create.

```
JP1/IM-Agent-Installation-destination-directory\jplima\conf\sample\jpc_lhu  
pdate.properties
```

4. Execute the version upgrade setup command for the logical host.

```
jimalhupdate -h logical-hostname -d shared-directory -c {online|standby}  
-f setup-configuration-file [-q]
```

For details about the upgrade setup command for logical hosts, see *jimalhupdate* in *Chapter 1. Commands in the JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

This command is executed on both the running server and the standby server.

5. Verify that the added service is registered with `systemd`.

On both the primary server and the secondary server, display the service list of `systemd` to confirm that the service for logical host has been registered.

The name of the service for logical host is file name of the unit definition file.

At the command prompt, execute the following command:

```
systemctl list-unit-files -t service
```

6. Perform the required setup for the added add-on program.

When using the added add-on program, see [2.19.2 \(14\) Setting up VMware exporter](#) and [2.19.2\(3\)\(i\) Add a VMware exporter scrape job \(for Linux\) \(optional\)](#) to make the necessary settings.

7. Reister the service for logical host in the cluster software.

Register the service for the logical host in the cluster software.

The following service is covered: registered only the services to use with the clusters.

```
jpc_vmware_exporter
```

- Start

Start the service with the following command:

```
/opt/jplima/tools/jpc_service_start -s jpc_vmware_exporter -h logical-host
-name
```

- Stop

Stop the service with the following command:

```
/opt/jplima/tools/jpc_service_stop -s jpc_vmware_exporter -h logical-host
-name
```

- Forced stop

Stop the service forcibly with the following command:

```
/opt/jplima/tools/jpc_service_stop -s jpc_vmware_exporter -h logical-host
-name -f
```

- Operational monitoring

Check the status of the service with the following command:

```
systemctl is-active jpc_vmware_exporter_logical-host-name
```

8. Check for problems in operation.

- Start the service from the cluster software.
- Causes a failover.

9. Start JP1/IM - Agent servicing.

Start JP1/IM - Agent of logical host service from the cluster software.

If you are also using physical host, start JP1/IM - Agent service of physical host.

8.6.3 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 [2.18.11 Specifying settings for upgrading \(for UNIX\)](#).

8.6.4 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 8–7: 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.
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
```

8.6.5 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`

8.7 Uninstalling logical hosts (for UNIX)

This section describes how to uninstall logical hosts of JP1/IM - Manager and JP1/IM - Agent. The subsections below first explain how to delete logical hosts and then explain how to uninstall JP1/IM - Manager , JP1/Base and JP1/IM - Agent from the logical disk on the active server and the standby server.

8.7.1 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 3 - 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 *JP1/Integrated Management 3 - Manager Command, Definition File and API 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 `jcfdbunsetup` command, see *jcfdbunsetup* in *Chapter 1. Commands* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API 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 Intelligent Integrated Management Database

If you are using the Intelligent Integrated Management database, run the `jimgndbunsetup` command to delete the Intelligent Integrated Management database (Trend Data Management DB) on the logical host.

For details about `jimgndbunsetup` command, see *jimgndbunsetup* in *Chapter 1. Commands* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

For details about Logical host as a whole Delete, see *8.7.1(3) Deleting the logical host*.

If you are using cluster software and want to delete only the Intelligent Integrated Management Database, review the settings of the cluster software so that failover does not occur even if the Intelligent Integrated Management Database stops.

(3) Deleting the logical host

To delete a logical host in UNIX, use the `jbsunsetcnf` command of JP1/Base. Execute the following command:

```
/opt/jplbase/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.

(4) 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 *8.7.1(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/jplbase/bin/jbsunsetcnf -h logical-host-name -c JP1CONSOLEMANAGER
```

- `[logical-host-name\JP1SCOPE\]` key
`/opt/jplbase/bin/jbsunsetcnf -h logical-host-name -c JP1SCOPE`
- `[logical-host-name\JP1CONFIG\]` key
`/opt/jplbase/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`).

8.7.2 Uninstalling JP1/IM - Manager and JP1/Base (for UNIX)

Uninstall JP1/IM - Manager and JP1/Base on the local disks on the active server and on the standby server.

If you uninstall JP1/IM - Manager, JP1/IM agent management base for using JP1/IM - Agent is also uninstalled.

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

8.7.3 Uninstalling JP1/IM - Agent (for UNIX)

Uninstall JP1/IM - Agent on the local disks of active server and standby server.

1. Shut down JP1/IM - Agent running on logical host.
 Shut down the services running in logical host from the cluster software.
2. If you are using the data distribution function to multiple manager hosts, perform the following procedure after stopping the service.
 Perform *When uninstalling the logical host described in 8.3.7(2)(b) Deactivating the data delivery function to multiple manager hosts (for Linux) (optional)*.
3. Delete the services that have been registered to the cluster software.
 Check your clustered software documentation for details about how to delete the service.
4. Enable to cancel services registered in systemd.
 For services used by logical hosts, enable services for logical hosts on both the running and standby systems to be released from systemd.
 To enable services for a logical host, use the following command:

```
/opt/jplima/tools/jpc_service -on service-key -h logical-host
```


 The following is an example of enabling the Alertmanager service:

```
/opt/jplima/tools/jpc_service -on jpc_alertmanager -h logical-host
```
5. Delete unit definition file for logical host.
 Delete unit definition file at the bottom of `/usr/lib/systemd/system`.
 File name to delete: `jpc_service-name_logical-host-name.service`

The following shows a sample Alertmanager.

File to delete
<code>jpc_alertmanager_logical-host-name.service</code>

6. Refresh systemd.

Execute the following to refresh systemd:

<code># systemctl daemon-reload</code>

7. Delete the shared directory.

8.8 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.

8.8.1 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 (`jplcf_applyconfig.conf`)
- Remote log trap environment definition file (`jplcf_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 (`jplcf_profile_manager.conf`)

Copy the common definition information using the setup procedure described in [8.3.4 Copying the common definition information during new installation of JP1/IM - Manager \(for UNIX\)](#).

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.

8.8.2 Using commands to change settings (for UNIX)

If you have used the `jcochafmode`, `jcochcfmode`, or `jcocmddef` command to change settings, you must also specify the same settings at the primary and secondary servers.

- When the `jcochafmode` command was executed

If you have changed the location of the event acquisition filter by specifying the `-h` option, you must copy the common definition information from the primary server to the secondary server.

Copy the common definition information using the setup procedure described in [8.3.4 Copying the common definition information during new installation of JP1/IM - Manager \(for UNIX\)](#).

- 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 [8.3.4 Copying the common definition information during new installation of JP1/IM - Manager \(for UNIX\)](#).

- 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.

8.8.3 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. Check the following service statuses:

If the status are different from the following status, stop the services to create the following status.

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

2. By operating the cluster software on the active host, stop JP1/IM - Manager on the logical host.

3. In addition to transferring the shared disk and the logical IP address assigned to the active host to the standby host, make sure that the shared disk and the logical IP address can be used on the logical host.

4. On standby host, execute `jimdbstart` command in `/opt/jplimm/bin/imdb` to start the IM database.

```
jimdbstart -h logical-host-name
```

5. On standby host, execute the `jimdbstatus` command.

- Check that the IM database service is operational (the `KNAN11182-I` message is output).
`KNAN11182-I The IM database service is running.`
- If the IM database service is not operational, execute the `jimdbstatus` command every 10 seconds, and then wait until the service is operational.

```
jimdbstatus -h logical-host-name
```

6. Execute the `jimdbstop` command to stop the IM databases on the standby host:

```
jimdbstop -h logical-host-name
```

7. In addition to transferring the shared disk and the logical IP address assigned to the standby host to the active host, make sure that the shared disk and the logical IP address can be used on the logical host.
8. 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 10:
KNAN11201-I The IM database service is the latest.
 - If the following message is output, perform the procedure beginning with step 9:
KNAN11202-I The overwrite is necessary for the IM database.
9. Execute the `jimdbupdate` command to update the IM databases on the standby host:
`jimdbupdate -h logical-host-name -i`

The following message will be output on the standby host, but it is not a problem.

KNAN11210-W The table schema could not be checked because a common disk could not be accessed.
10. Execute the `jimdbupdate` command on the active host:
`jimdbupdate -h logical-host-name`
 - If the following message is output, perform step 13:
KNAN11201-I The IM database service is the latest.
 - If the following message is output, perform the procedure beginning with step 11:
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.
KNAN11211-I An update of the configuration files of an IM database service is required.
11. 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`
12. Execute the `jimdbupdate` command to update the IM databases on the active host:
`jimdbupdate -h logical-host-name -i`
13. By operating the cluster software on the active host, start JP1/IM - Manager on the logical host.
14. Start the services stopped in step 1.

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.

8.9 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.
- 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-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 *2.2.4 Tasks to be performed before a logical host name is changed in a cluster system* in the *JP1/Integrated Management 3 - Manager Administration Guide* and perform the required tasks.
- If a logical host is created in a cluster system or the binding method is to be changed, be sure to stop the daemon of JP1/IM - Manager running on the physical host. If a logical host is created or the binding method is changed without stopping the daemon on the physical host, the daemon on the physical host will not operate normally. In this case, recover by rebooting the server machine.
- If JP1/IM - Manager is not used on the physical host, be sure to cancel the setting of the automatic startup and stop script.
- If you execute "`jbsrt_get -h logical-host`" on a standby host that uses a cluster, the message "KAVB3113-I Definition does not exist. " is displayed. If that happens, execute "`jbsrt_get -h logical-host`" on an active host.
- For details on supported cluster software and notes on cluster software, see the following URL.

<http://www.hitachi.com/products/it/software/prod/jp1/products/envionents/cluster/index.html>

8.10 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.

8.10.1 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.

8.10.2 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 8. Operation and Environment Configuration in a Cluster System (for UNIX)*, 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 3 - Manager Administration Guide*.

8.10.3 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.

9

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.

9.1 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

9.2 Operating in multiple networks

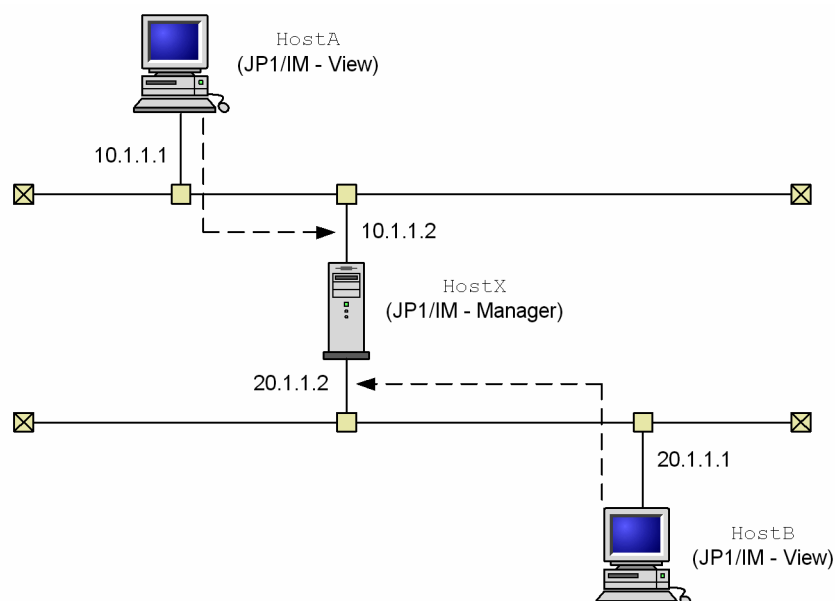
This section describes examples of system configurations that use multiple LANs (configurations in which multiple networks are connected), and the required communication settings based on the configuration examples.

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.

9.2.1 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 9–1: Connecting JP1/IM - View in a multi-LAN environment (non-cluster operation)



The following tables show the settings for each host.

Table 9–1: 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 9–2: Settings for HostA and HostB (JP1/IM - View)

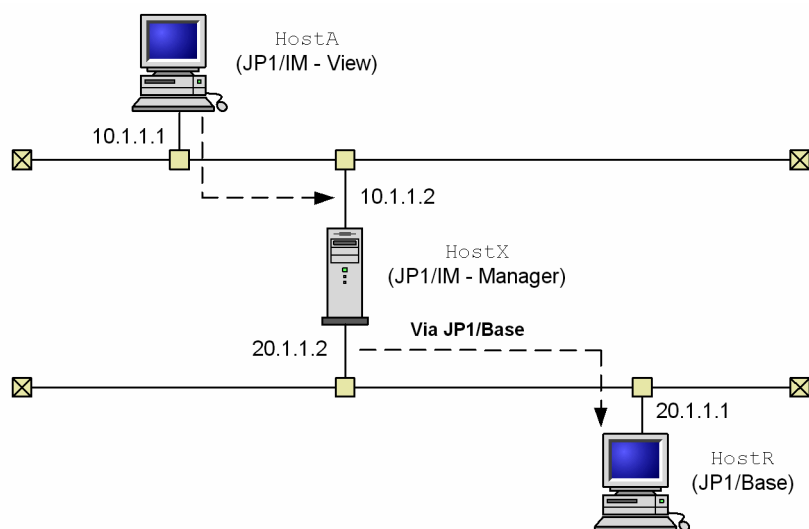
Host name	Host to connect	Other conditions [#]
HostA	HostX	Conversion from host name HostX to 10.1.1.2 must be possible.
HostB	HostX	Conversion from host name HostX to 20.1.1.2 must be possible.

[#]: Use the `hosts` file and DNS to resolve host names, because JP1/IM - View does not reference settings in the `jp1hosts` and `jp1hosts2` files.

9.2.2 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 9–2: Command execution in a multi-LAN environment (non-cluster operation)



The following tables show the settings for each host.

Table 9–3: 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).

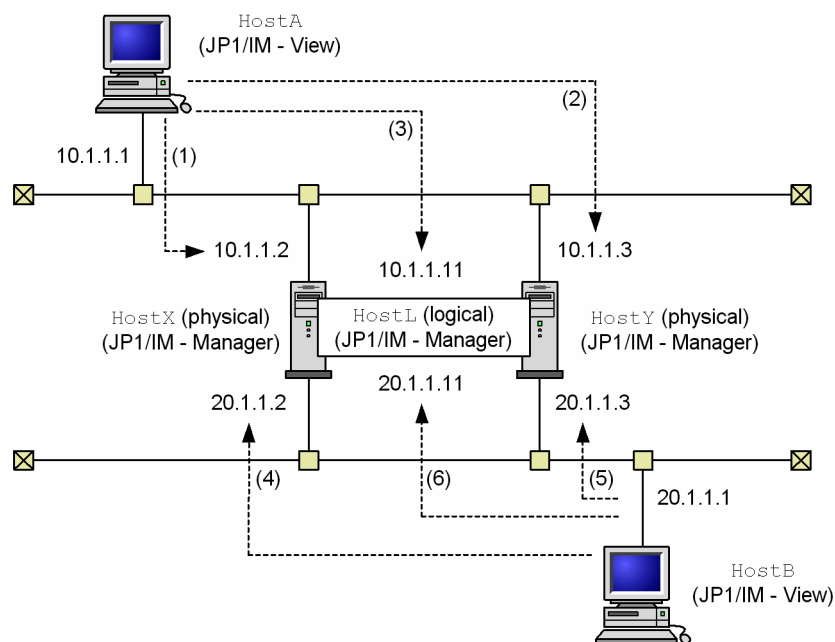
Table 9–4: Settings for HostA (JP1/IM - View)

Host name	Host to connect	Other conditions
HostA	HostX	Conversion from host name HostX to 10.1.1.2 must be possible.

9.2.3 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 9–3: Connecting JP1/IM - View in a multi-LAN environment (cluster operation)



The following tables show the settings for each host.

Table 9–5: 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 9–6: Settings for HostA (JP1/IM - View)

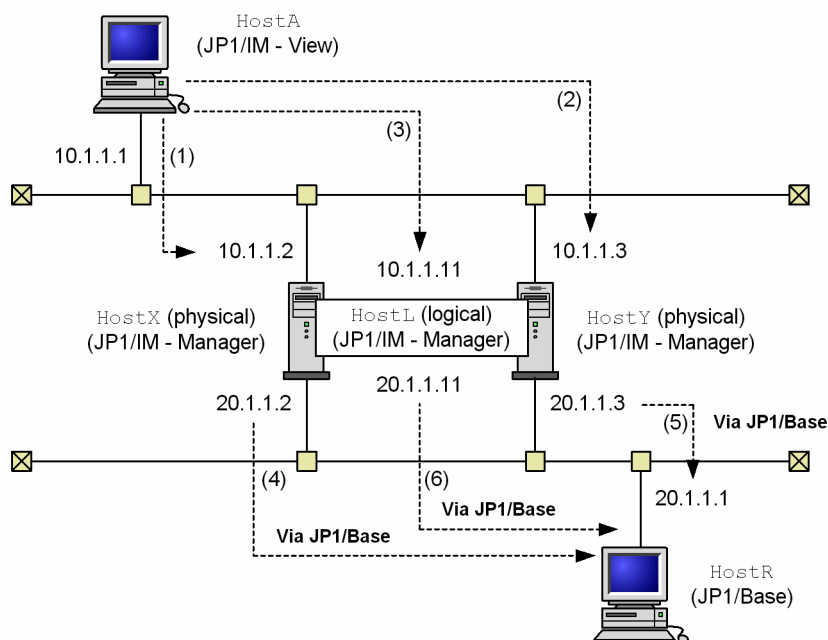
Host name	Host to connect	Other conditions	Correspondence to number in parentheses in figure
HostA	HostX	Conversion from host name HostX to 10.1.1.2 must be possible.	1

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

9.2.4 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 9–4: Command execution in a multi-LAN environment (cluster operation)



The following tables show the settings for each host.

Table 9–7: 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 9–8: 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

9.3 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.

9.3.1 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 3 - 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.

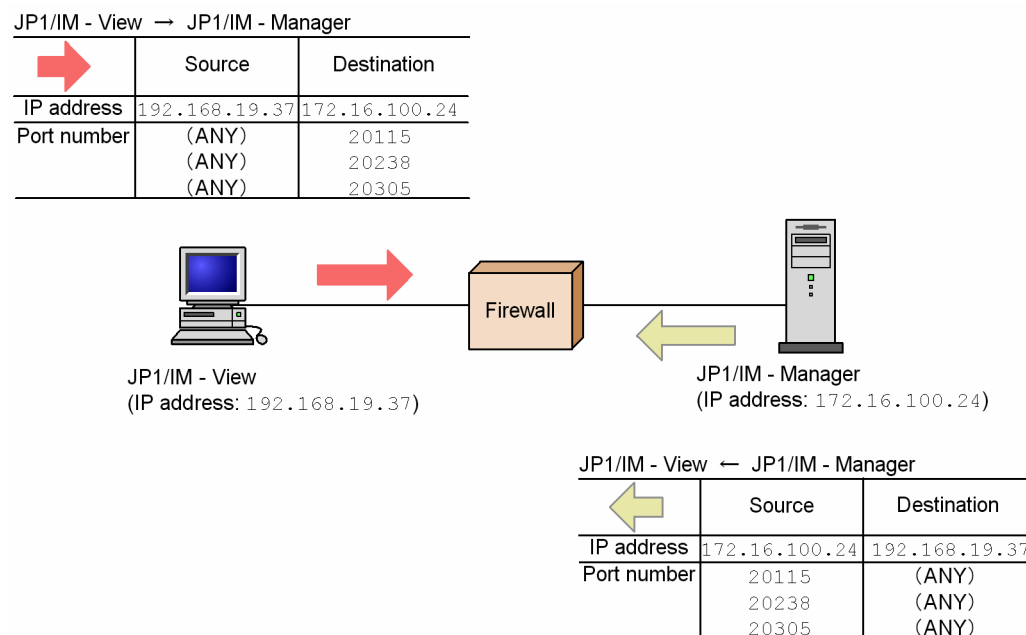
(b) Example of settings for JP1/IM

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 9–5: 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 3 - Manager Overview and System Design Guide*, the port numbers used by JP1/IM are described as shown in the following table.

Table 9–9: Firewall passage directions

Service name	Port number	Firewall passage direction
jplimevtcon	20115/tcp	JP1/IM - View → JP1/IM - Manager (Central Console)
jplimcmda	20238/tcp	JP1/IM - View → JP1/Base ^{#1} JP1/IM - Manager (Central Console) → JP1/Base ^{#1}
jplimcss	20305/tcp	JP1/IM - View → JP1/IM - Manager (Central Scope)
jplimegs	20383/tcp	Firewall setup is unnecessary because all communication takes place on the machine on which JP1/IM - Manager is installed.
jddmain	20703/tcp	Web browser → JP1/IM - Manager (Intelligent Integrated Management Base)
None ^{#2}	Port number of the IM database ^{#3}	JP1/IM - Manager (physical host) → JP1/IM - Manager (IM database (physical host))

Service name	Port number	Firewall passage direction
	Port number of the IM database ^{#4}	JP1/IM - Manager (logical host) → JP1/IM - Manager (IM database (logical host))
jplimcf	20702/tcp	JP1/IM - View → JP1/IM - Manager (IM Configuration Management)
jplimfcs	20701/tcp	Firewall setup is unnecessary because all communication takes place on the machine on which JP1/IM - Manager is installed.
jimmail	25/tcp ^{#5}	JP1/IM - Manager → mail server (SMTP) (without authentication)
	587/tcp ^{#5}	JP1/IM - Manager → mail server (SMTP) (with SMTP-AUTH authentication)
	110/tcp ^{#5}	JP1/IM - Manager → mail server (POP3) (with POP-before-SMTP authentication)

Legend:

→: Direction of the connection when established

#1: Refers to JP1/Base on the manager.

#2: Not registered in the `services` file.

#3: This is the port number for the IM database (physical host) that was set in the setup information file when the IM database was set up on the physical host.

#4: This is the port number for the IM database (logical host) that was set in the cluster setup information file when the IM database was set up on the logical host.

#5: The destination port number might differ depending on which port is used on the destination server.

#6: The port number might differ depending on the HTTP server settings.

This table assumes the following communication method:

- *Service name* and *Port number* columns

These are the service names and port numbers used by JP1 for communication. According to this table, port number 20115 (service name `jplimevtcon`), port number 20238 (service name `jplimcmda`), 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 9–10: 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
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

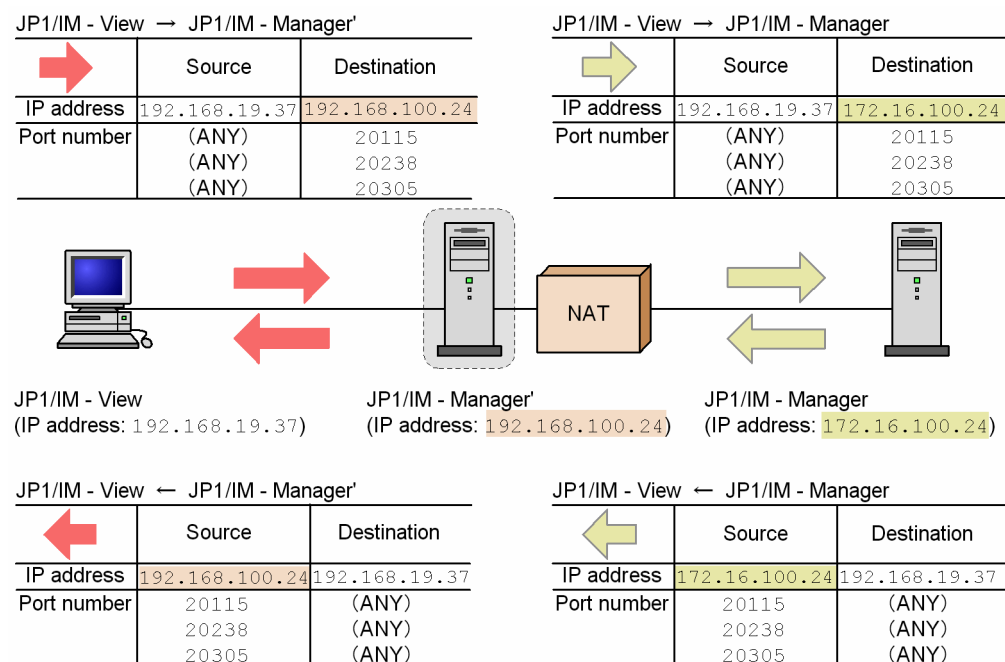
This subsection describes the NAT settings based on an example of an environment in which there is a firewall between JP1/IM - View and JP1/IM - Manager.

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 9–6: 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 9–11: 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.

9.3.2 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 3 - Manager Overview and System Design Guide*

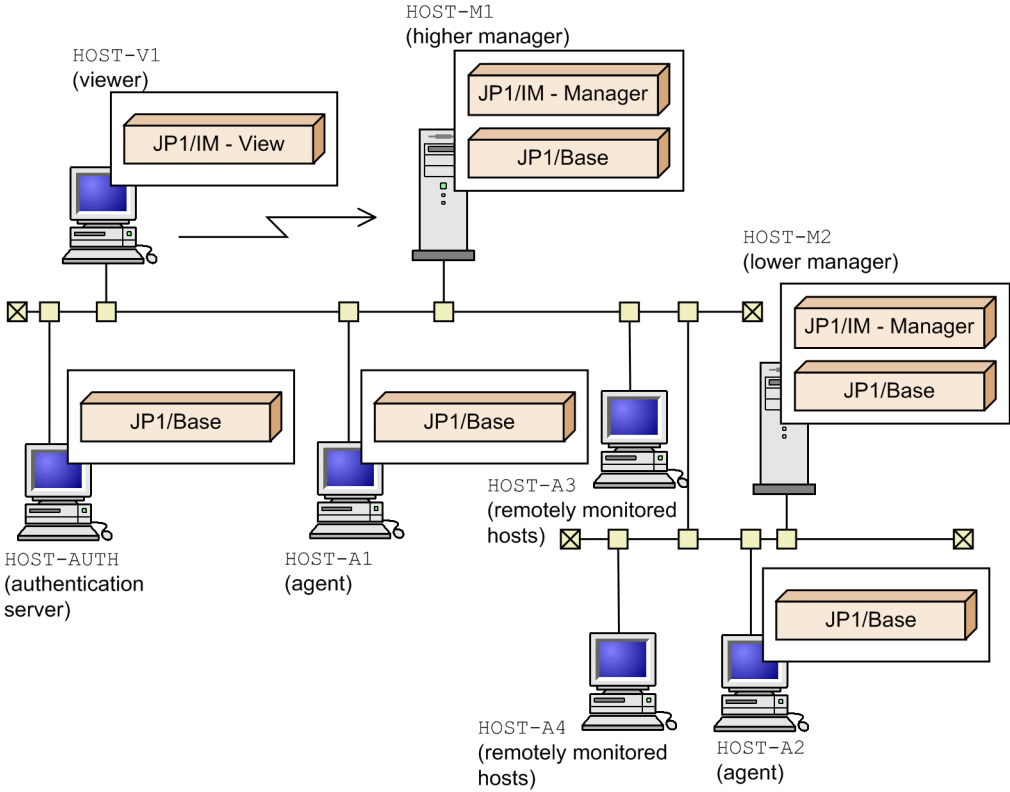
(b) Example of system configuration and communication

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 9–7: 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} 20702/tcp (jplimcf) ^{#2}

^{#1}: The port of jplimcss is used only when JP1/IM - Manager (Central Scope) is used.

^{#2}: The port of jplimcf is used only when JP1/IM - Manager (JP1/IM - Configuration) is used.

Integrated Operation Viewer Window	Passage direction	Manager (JP1/IM and JP1/Base)
(ANY)	→	20703/tcp (jddmain) [#]

[#]: The port of jddmain is used only when JP1/IM - Manager (Intelligent Integrated Management Base) is used.

This applies to communication between HOST-V1 and HOST-M1 in the example system configuration.

- 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 (jplimevtapi)

Manager (JP1/Base)	Passage direction	Agent (JP1/Base)
		20237/tcp (jplimrt) 20239/tcp (jplimcmdc) 20306/tcp (jplbsplugin) 20600/tcp (jplbscom)
20098/tcp (jplimev) 20239/tcp (jplimcmdc)	←	(ANY)
20600/tcp (jplbscom)	←	(ANY)

This table applies to communications between HOST-M1 and HOST-A1 and HOST-A2, and between HOST-M2 and HOST-A2.

- Communication between manager (Intelligent Integrated Management Base) and host of linked product

Manager (JP1/IM)	Passage direction	Host of linked product (JP1/Base, JP1/AJS, JP1/PFM and other linked products#2)
(ANY)	→	20306/tcp (jplbsplugin) 20358/tcp (PFM - Web Console#1)

#:1 This is used to link JP1/IM with JP1/PFM - Manager.

#:2 For details about how to set a port number for linking with the host of another linked product, see the section describing how to link with JP1/IM in the manual for the applicable linked product. For the JP1/PFM refers to the *version 12-10* or later manual.

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 [9.3.2\(2\)\(a\) For a normal system](#) and [9.3.2\(2\)\(b\) 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 `jplhosts` information or `jplhosts2` 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 [9.3.2\(2\)\(b\) For a cluster system](#), while the sender's operation is as discussed in [9.3.2\(2\)\(a\) For a normal system](#).

In addition, if host names and IP addresses are defined in the `jplhosts` information or the `jplhosts2` information when the `jplhosts` information or the `jplhosts2` 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 `jplhosts` information is defined as follows:

```
hostA 100.0.0.10 200.0.0.10
```

Also suppose that the `hosts` file contains the following definition:

```
100.0.0.10 hostA hostB
```

```
200.0.0.10 hostC
```


The `hosts` file is not referenced regarding `hostA` and IP addresses `100.0.0.10` and `200.0.0.10`. Therefore, if the configuration definition file contains `hostB` and `hostC` that are not defined in the `jplhosts` information, the system configuration cannot be defined.

(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.

9.3.3 Notes on Windows Firewall

(1) Configuring Windows Firewall settings

- If you are using the integrated management from JP1/IM - View in an environment where Windows Firewall is enabled, register programs or port numbers with "Exceptions" as required.

Follow these procedures to register programs and port numbers:

- Execute the following command. Change *Console-path* to the installation folder for the integrated console and then execute the command.
`netsh advfirewall firewall add rule name="JP1/IM3-Manager" dir=in action=allow program="Console-path\bin\evtcon.exe" enable=yes protocol=tcp`
- Make sure that **Programs and Services** or **Allow an app or feature through Windows Firewall** of **Windows Firewall** displays what has been registered in the above steps, and that the check box for the applicable item is selected.
- If you are using the integrated scope in an environment where Windows Firewall is enabled, register the programs or port numbers for the integrated scope with "Exceptions" as required, in addition to the settings described above (using the integrated management from JP1/IM - View).

Register the items with the exceptions list by either of the following procedures:

- Select **Exceptions** tab of **Windows Firewall** on **Control Panel** to register the following programs/ports.

Registering a program

Register the following information by selecting **Add Program** and then **Browse**.

File Name: *installation-folder*\JP1Scope\bin\jcsmain.exe

Registering a port number

Register the following information by selecting [Add Port].

Port Number: tcp 20305

Name: JP1/IM3-Manager

- Execute the following command. Additionally, change *Scope-path* to the installation folder for the integrated scope and then execute the command.

```
netsh advfirewall firewall add rule name="JP1/IM3-Manager" dir=in action=allow program="Scope-path\bin\jcsmain.exe" enable=yes protocol=tcp
```

- If you are using the IM configuration in an environment where Windows Firewall is enabled, register the programs or port numbers for the IM configuration with "Exceptions" as required, in addition to the settings described above (using the integrated management from JP1/IM - View).

Register the items with the exceptions list by either of the following procedures:

- Select **Exceptions** tab of **Windows Firewall** on **Control Panel** to register the following programs/ports.

Registering a program

Register the following information by selecting **Add Program** and then **Browse**.

File Name: *installation-folder\JP1Scope\bin\jcsmain.exe*

Registering a port number

Register the following information by selecting **Add Port**.

Port Number: tcp 20702

Name : JP1/IM3-Manager

- Execute the following command. Additionally, change *Manager-path* to the installation folder for the JP1/IM - Manager and then execute the command.

```
netsh advfirewall firewall add rule name="JP1/IM3-Manager" dir=in action=allow program="Manager-path\bin\imcf\jcfmain.exe" enable=yes protocol=tcp
```
- If you are using JP1/IM - View or the Integrated Operation Viewer window in an environment where Windows Firewall security is improved, and outbound connections that do not follow the rules are not blocked:
 - Do not block transmission from the following port numbers:
 - 20115/tcp
 - 20238/tcp
 - 20305/tcp
 - 20702/tcp
 - 20703/tcp
 - 22301/tcp
 - 22302/tcp
 - 22303/tcp
 - 22304/tcp
 - Do not block transmission from the following program:
 - View-path\bin\jdk\bin\java.exe*
 - Do not block transmission to the IP addresses used to connect to JP1/IM - Manager.
- If you are using JP1/IM - View in an environment where Windows Firewall security is improved, and outbound connections that do not follow the rules are blocked:

Select the **Windows Firewall with Advanced Security** tool in **Administrative Tools** in **Control Panel**, and then allow the program below to connect from the New **Outbound Rule** wizard under Outbound Rules.

File: *View-path\bin\jdk\bin\java.exe*

(2) Deleting information from Windows Firewall

To delete the registered information from Windows Firewall, select the applicable item from the items displayed under **Programs and Services** of Windows Firewall, and press **Delete** to delete the registered information.

(3) Temporarily disabling Windows Firewall

To temporarily disable the registered information from Windows Firewall, clear the checkbox for the items that are displayed under **Programs and Services** of Windows Firewall.

9.4 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 *14.10.7 Communication encryption function setting (enable/disable) and connectivity among product versions* and *Appendix H. Connectivity with Previous Versions* in the *JP1/Integrated Management 3 - 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(1) Backup (in Windows)* or *1.1.1(3) Backup (in UNIX)* in the *JP1/Integrated Management 3 - Manager Administration Guide*.

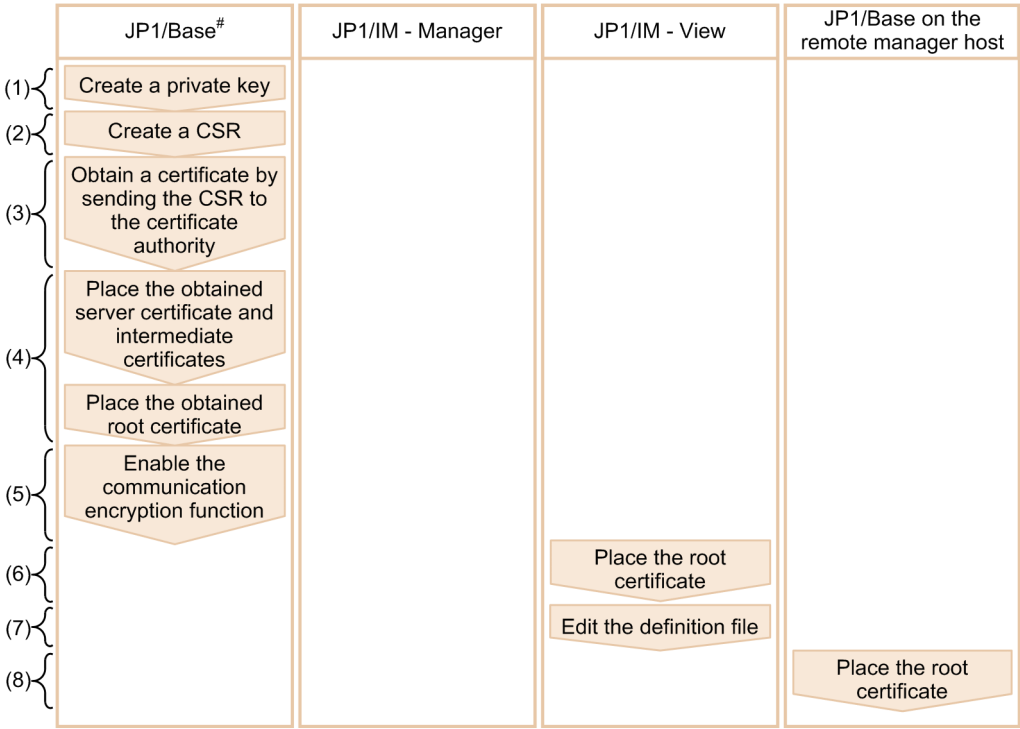
9.4.1 Newly using the communication encryption function

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 *14.10.6 System configuration* in the *JP1/Integrated Management 3 - 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.

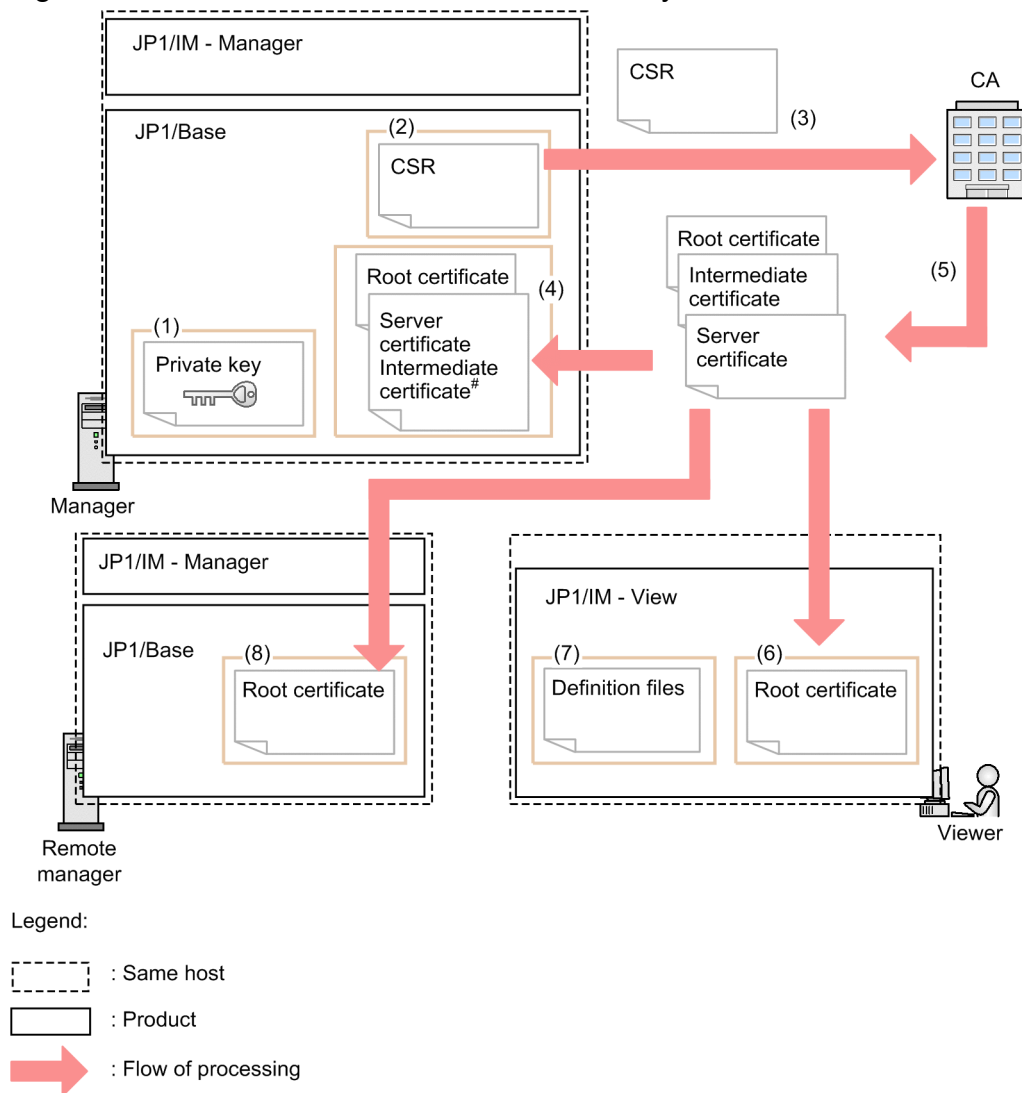
The following figures show the procedure for newly using the communication encryption function.

Figure 9–8: Procedure for newly using the communication encryption function



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

Figure 9–9: Overview of files that are edited by the user



#: 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 *14.10.4(2) Verifying host names (CN and SAN) in server certificates* in the *JP1/Integrated Management 3 - 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 *14.10.3(1) Encryption between a manager host and a viewer host* in the *JP1/Integrated Management 3 - 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 (nossllhost.conf)* in *Chapter 2. Definition Files* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API 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

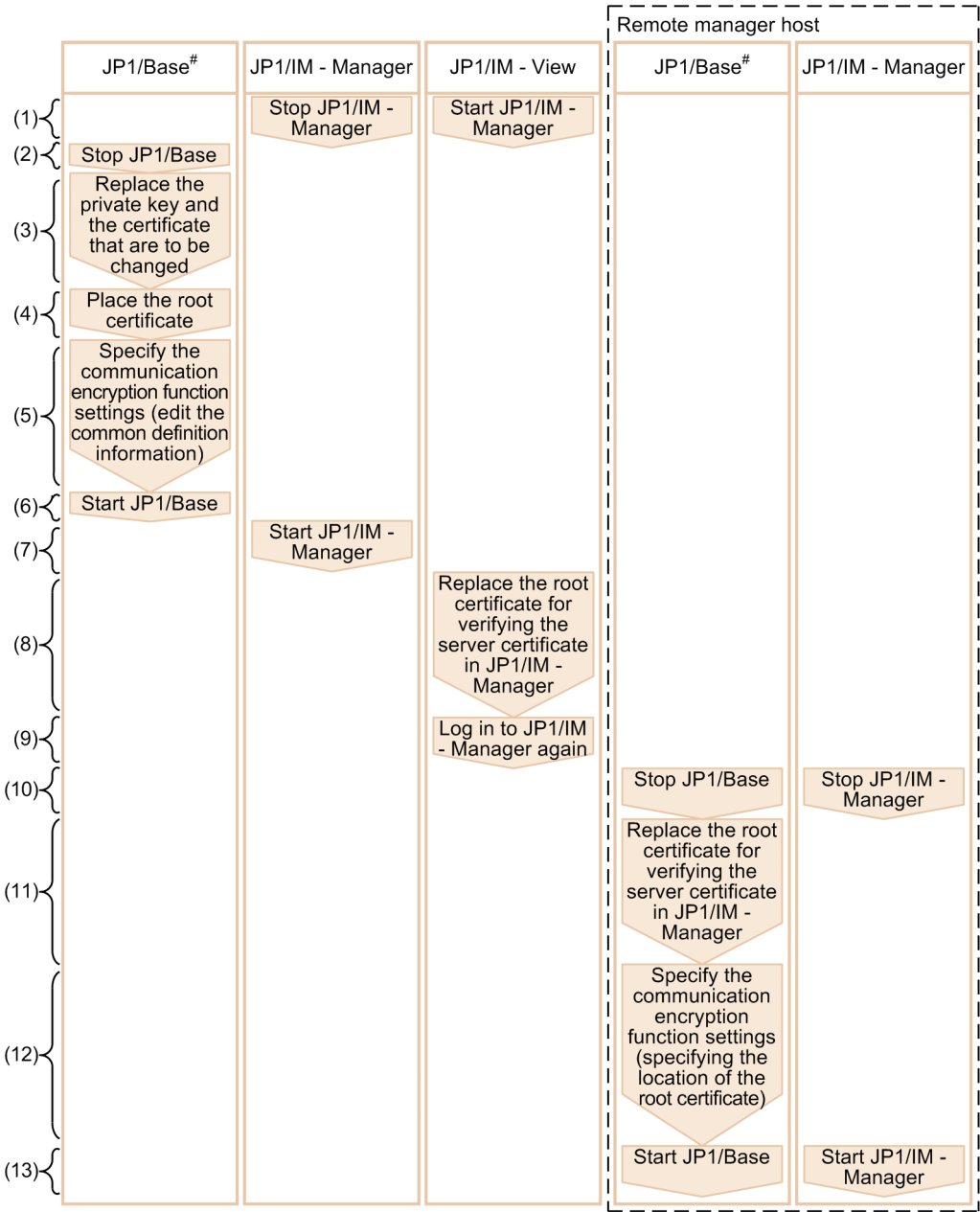
Communication encryption function settings cannot be changed while JP1/IM - Manager and JP1/Base are running. If you need to change communication encryption function settings for a reason such as to replace expired server or root certificates, you must first stop JP1/IM - Manager and JP1/Base.

After you have configured the communication encryption function, check that the function has been configured correctly. For details about the checking procedure, see [9.4.6 Checking whether the communication encryption function has been configured correctly](#).

9.4.2 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 9–10: 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 *14.10.3(1) Encryption between a manager host and a viewer host* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

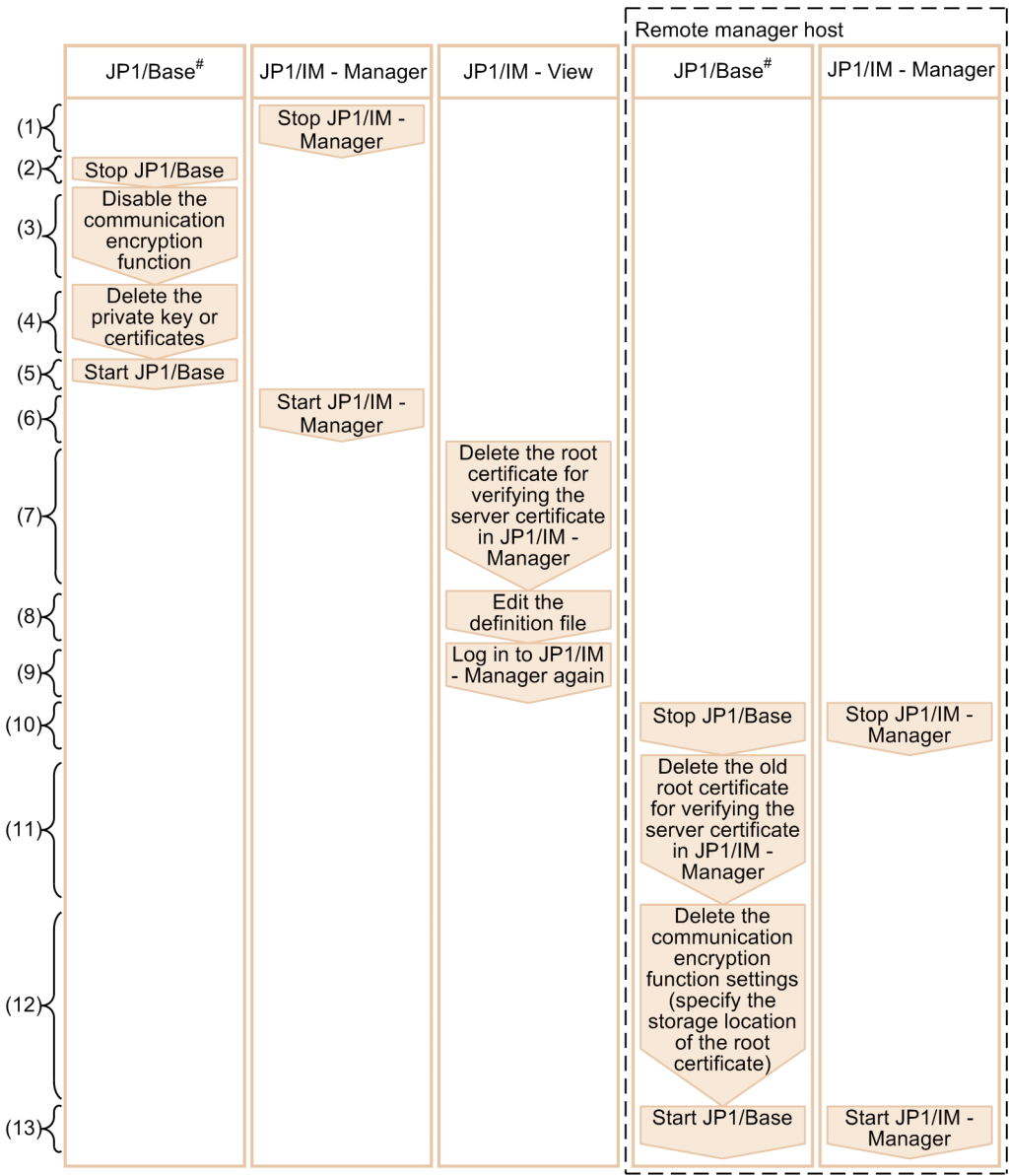
#3: To edit a certificate, use a text editor to open the certificate and edit its contents.

After you have configured the communication encryption function, check if the function has been configured correctly. For details about the checking procedure, see [9.4.6 Checking whether the communication encryption function has been configured correctly](#).

9.4.3 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 9–11: 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 *14.10.3(1) Encryption between a manager host and a viewer host* in the *JP1/Integrated Management 3 - 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 (nossllhost.conf)* in *Chapter 2. Definition Files* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API 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 [9.4.6 Checking whether the communication encryption function has been configured correctly](#).

9.4.4 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 [9.4.6 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

9.4.5 Settings for JP1/IM - Agent (JP1/IM agent control base)

To encrypt communication between JP1/IM agent management base and JP1/IM agent control base, the following setup is required:

(1) To verify the server certificate of JP1/IM agent management base

1. Place CA certificate.

Place CA certificate of authentication station that issued the server certificate of imbase you are connecting to in the following directory:

- For Windows
Agent-path\conf\cert\
- For Linux
/opt/jplima/conf/cert/

2. Write the path of CA certificate in the imagent configuration file (jpc_imagentcommon.json).

3. Restart imagent and imagentproxy.

(2) If you do not verify the server certificate for JP1/IM agent management base

1. Set "true" to `tls_config.insecure_skip_verify` of the imagent configuration file (jpc_imagentcommon.json).
2. Restart imAgent and ImagentProxy.

9.4.6 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 to JP1/IM - Manager from the Web browser.

If you are using the Intelligent Integrated Management Base, confirm that you can log in to the Intelligent Integrated Management Base.

For details about the login procedure, see *Chapter 4. JP1/IM - Manager Login and Logout* in the *JP1/Integrated Management 3 - Manager Administration Guide*.

3. 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 3 - Manager Administration Guide*.

4. 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 *8.1 Executing a command* in the *JP1/Integrated Management 3 - Manager Administration Guide*.

For details about how to execute commands by automated actions, see *5.5 Setting automated actions*.

5. 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*.

10

Settings for Linking to Other JP1 Products

This chapter describes the environment setup for linking JP1/IM to other JP1 products.

10.1 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.

10.1.1 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.

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_spmd_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 *JP1/Integrated Management 3 - Manager Command, Definition File and API 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 *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

10.2 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 *JP1/Integrated Management 3 - Manager Command, Definition File and API 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 10–1: 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.

10.3 Linking with JP1/AJS

This section explains the settings for linking with JP1/AJS.

10.3.1 Settings for launching a JP1/AJS window by monitor startup

For details about the settings for monitor startup, see [5.17 Setting monitor startup for linked products](#) and the JP1/AJS documentation.

10.3.2 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 [8.3.2 Functions that can be operated from the Tool Launcher window](#) in the *JP1/Integrated Management 3 - Manager Administration Guide*. For details about the settings for the Tool Launcher window, see [5.18 Setting the Tool Launcher window](#).

10.3.3 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.

10.3.4 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.

10.3.5 Settings for checking the association between root jobnets and their configuration information by using the Intelligent Integrated Management Base

If you are using the Intelligent Integrated Management Base to monitor JP1/AJS root jobnets, you need to collect system configuration management information from JP1/AJS. For details about the settings for linkage with JP1/AJS, see the JP1/AJS documentation.

Specifically, collect the following information from JP1/AJS:

- The name of the host on which JP1/AJS - Manager is installed
- JP1/AJS - Manager inside the host
- The name of the scheduler service
- The name of the job group
- The name of the root jobnets
- The name of the host on which JP1/AJS - Agent is installed under JP1/AJS - Manager
- JP1/AJS - Agent under JP1/AJS - Manager inside the host

From the JP1/AJS3 - Manager host, collect only the information on the root jobnets that have been registered for execution.

10.4 Linking with JP1/PFM

This section explains the settings for linking with JP1/PFM.

10.4.1 Settings for launching a JP1/PFM window by monitor startup

For details about the settings for monitor startup, see [5.17 Setting monitor startup for linked products](#) and the JP1/PFM documentation.

10.4.2 Settings for launching a JP1/PFM window from the Tool Launcher window

For details about the settings for the Tool Launcher window, see [5.18 Setting the Tool Launcher window](#) and the JP1/PFM documentation.

10.4.3 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.

10.4.4 Settings for checking operation information by using the Intelligent Integrated Management Base

To monitor the JP1/PFM operation information by using the Intelligent Integrated Management Base, you need to collect JP1/PFM system configuration management information by using both the configuration collection adapter command and the plug-ins for linking with other products. For details about the settings for linkage with JP1/PFM, see the JP1/PFM documentation.

The prerequisites for collecting system configuration management information of JP1/PFM are as follows:

- JP1/IM - Manager, JP1/PFM - Manager, and JP1/PFM - Web Console should be version 12-00 or later.
- JP1/IM - Manager should use the same authentication server as the one for the linked JP1/PFM - Web Console.
- The authentication mode of the linked JP1/PFM should be in JP1 authentication mode, in which JP1/Base centrally manages authentication.
- Linked JP1/PFM - Web Console should be able to be logged in to from the JP1/IM - Manager host.
- The JP1 user who has logged in to JP1/IM - Manager should have permissions to operate JP1/PFM.

Specifically, collect the following information from JP1/PFM:

- The name of the host on which JP1/PFM - Manager is installed
- JP1/PFM - Manager inside the host

- The name of the host on which JP1/PFM - Agent or JP1/PFM - RM is installed under JP1/PFM - Manager, or the name of the host to be monitored by JP1/PFM - RM
- JP1/PFM - Base installed on the host on which JP1/PFM - Agent or JP1/PFM - RM is installed under JP1/PFM - Manager
- The service ID of JP1/PFM - Agent or JP1/PFM - RM under JP1/PFM - Manager
- The service of JP1/PFM - Agent or JP1/PFM - RM under JP1/PFM - Manager

For details about the configuration collection adapter command and the plug-ins for linking with other products, see *Chapter 4. User-created Plug-ins* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

If you use the integrated operation viewer, see the section describing how to set up a Web browser to use the monitoring console in the *JP1/Performance Management Planning and Configuration Guide*.

Index

A

- acquiring existing Visual Monitoring window [554](#)
- action status change, setting JP1 event issuance during [504](#)
- adding
 - monitoring nodes to monitoring tree [543](#)
 - monitoring nodes to Visual Monitoring window [556](#)
- adding host to business group [416](#)
- adding or deleting profile (agent configuration) [423](#)
- adding or deleting profile (remote monitoring configuration) [433](#)
- adding profile (agent configuration) [423](#)
- adding profile (remote monitoring configuration) [433](#)
- addition of program-specific attribute, setting [505](#)
- address translation [710](#)
 - support of [717](#)
- applying
 - customized monitoring tree to manager [551](#)
 - customized Visual Monitoring window to manager [558](#)
- applying business group information and monitoring group information to monitoring tree of Central Scope [417](#)
- applying edited information in configuration file (remote monitoring configuration) [436](#)
- authentication server, specifying (UNIX) [294](#)
- authentication server, specifying (Windows) [61](#)
- automated action definition file, updating [114](#), [333](#)
- automated actions
 - setting [490](#)
 - setting details of [490](#)
 - setting execution conditions of [490](#)
 - settings for monitoring execution status of [492](#)
 - setting suppression of execution [493](#)
 - setting up execution environment for [490](#)
- automatic generation of monitoring tree [540](#)
- automatic startup (UNIX) [318](#)
- automatic stop (UNIX) [318](#)

B

- Before configuring an environment for the Intelligent Integrated Management Base [444](#)
- building container environments in JP1/IM - Agent (for UNIX) [358](#)
- building container environments in JP1/IM - Agent (for Windows) [207](#)

- business group

- setting reference and operation restrictions [533](#)

C

- Central Console, setting up [472](#)
- Central Scope
 - before starting environment setup for [536](#)
 - environment setup for [536](#)
 - executing upgrade command [114](#), [333](#)
 - registering host information [537](#)
 - settings for using functions (UNIX) [323](#)
 - settings for using functions (Windows) [109](#)
 - setting up [535](#)
 - setting up for linked products [572](#)
 - setting up operating environment for [565](#)
- changing communication type for vCenter [397](#)
- changing communication type for VMware ESX [397](#)
- changing configured certificates [724](#)
- changing settings in file (UNIX) [694](#)
- changing settings in file (Windows) [645](#)
- checking language environment setting of JP1/Base [278](#)
- Cloning a Virtual Machine (for UNIX) [283](#)
- Cloning a Virtual Machine (for Windows) [50](#)
- cluster operation [599](#)
 - JP1/IM configuration in [602](#), [653](#)
 - JP1's support range [601](#)
- cluster software [599](#)
- cluster system
 - environment setup procedure for cluster operation (UNIX) [656](#)
 - environment setup procedure for cluster operation (Windows) [606](#)
 - JP1/IM configuration (UNIX) [653](#)
 - JP1/IM configuration (Windows) [602](#)
 - logical host [599](#)
 - new installation and setup of logical host (UNIX) [658](#)
 - new installation and setup of logical host (Windows) [608](#)
 - notes about cluster operation (UNIX) [697](#)
 - notes about cluster operation (Windows) [649](#)
 - operation and environment configuration in cluster system (UNIX) [652](#)
 - operation and environment configuration in cluster system (Windows) [597](#)
 - overview (UNIX) [653](#)

- overview (Windows) 598
- overview of cluster operation (UNIX) 653
- overview of cluster operation (Windows) 598
- prerequisites for cluster operations (UNIX) 653
- prerequisites for cluster operations (Windows) 599
- registering into cluster software (new installation and setup) (UNIX) 680
- registering into cluster software (new installation and setup) (Windows) 633
- upgrade installation and setup of logical hosts (UNIX) 685
- upgrade installation and setup of logical hosts (Windows) 637
- collecting and distributing Event Service definition information when IM Configuration Management is not used (UNIX) 307
- collecting and distributing Event Service definition information when IM Configuration Management is not used (Windows) 75
- collecting and distributing Event Service definition information when IM Configuration Management is used (UNIX) 306
- collecting and distributing Event Service definition information when IM Configuration Management is used (Windows) 74
- collecting virtualization system configuration information 405
- command execution
 - setting up execution environment (UNIX) 308
 - setting up execution environment (Windows) 76
- common definition information, setting 604, 655
- communication encryption function
 - checking whether configured correctly 730
- communication encryption function, newly using 720
- communication encryption function, stop using 727
- communication method 604, 654
- communications, controlling by JP1/Base 701
- completed-action linkage, setting 565
- configuration definition
 - notes about setting information (UNIX) 301
 - notes about setting information (Windows) 69
- configuration definition information
 - changing (UNIX) 301
 - changing (Windows) 69
 - deleting (UNIX) 301
 - deleting (Windows) 69
 - setting (UNIX) 300
 - setting (Windows) 68
- configuration files
 - applying edited information in 425
 - editing 424
- configuring
 - automatic startup (UNIX) 318
 - automatic stop (UNIX) 318
 - changing cluster operating environment settings (UNIX) 694
 - changing cluster operating environment settings (Windows) 645
 - cluster operating environment (UNIX) 656
 - cluster operating environment (Windows) 606
 - command execution environment (JP1/Base) (UNIX) 308
 - command execution environment (JP1/Base) (Windows) 76
 - Event Service (JP1/Base) (UNIX) 303
 - Event Service (JP1/Base) (Windows) 71
 - installing each JP1/IM program (UNIX) 272
 - installing each JP1/IM program (Windows) 32
 - JP1/IM - View operation (Windows) 119
 - settings for handling JP1/IM - Manager failures (UNIX) 327
 - settings for handling JP1/IM - Manager failures (Windows) 110
 - settings for handling JP1/IM - View failures (Windows) 119
 - settings for using the functions of Central Scope (UNIX) 323
 - settings for using the functions of Central Scope (Windows) 109
 - startup sequence for services (JP1/Base) (Windows) 60
 - uninstalling each JP1/IM program (UNIX) 365
 - uninstalling each JP1/IM program (Windows) 259
 - upgrade installation, for (UNIX) 332
 - upgrade installation, for (Windows) 113
- configuring JP1/IM - Manager 729
- configuring SSH (UNIX) 311
- configuring SSH (Windows) 87
- Configuring the method for applying system configuration information 467
- configuring WMI (Windows) 80
- consolidated display of repeated events 524
- conventions
 - diagrams 10
 - version numbers 13
- copying common definition information during new installation of JP1/IM - Manager (UNIX) 664

- copying common definition information during new installation of JP1/IM - Manager (Windows) [616](#)
- copying common definition information during upgrade installation (UNIX) [689](#)
- copying common definition information during upgrade installation (Windows) [640](#)
- correlation event generation
 - creating and applying definition of [500](#)
 - history files, setting size and number of [498](#)
 - setting [498](#)
 - setting startup of [498](#)
 - setting startup options [499](#)
- Cosminexus, setup for linkage with [578](#)
- creating a new dashboard [470](#)
- creating IM database (UNIX) [285](#)
- creating IM database (Windows) [52](#)
- creating scripts to be registered into cluster software (UNIX) [681](#)
- customizing
 - monitoring tree [542](#)
 - toolbar for monitoring tree [567](#)
 - Visual Monitoring window [554](#)
- customizing auto-generated dashboards [470](#)
- customizing JP1/IM - View operation (Windows) [119](#)
- customizing operation
 - IM Configuration Management - View [121](#)
- customizing operation of Central Console viewer and Central Scope viewer (Windows) [119](#)

D

- dashboard configuration [470](#)
- data, preparations for collecting [110](#), [327](#)
- definition files
 - creating [510](#), [526](#), [529](#)
 - enabling [512](#)
- deleting a dashboard [471](#)
- deleting host from business group [417](#)
- deleting monitoring nodes [548](#)
- deleting profile (agent configuration) [424](#)
- deleting profile (remote monitoring configuration) [434](#)
- diagram conventions [10](#)
- display and specification of program-specific extended attribute, setting [506](#)
- displaying
 - event (by specifying event acquisition range at login) [473](#)
- displaying the Start the process automatically when the log file trap service starts check box [115](#), [335](#)

- display message change definition file, configuring from [518](#)
- Display Message Change Definition Settings window, configuring from [516](#)

E

- editing
 - event guide information [502](#)
 - guide information [562](#)
 - list of Visual Monitoring windows [559](#)
- editing configuration file of JP1/IM - Manager (for UNIX) [320](#)
- editing configuration file of JP1/IM - Manager (for Windows) [95](#)
- editing dashboards [470](#)
- Enabling calling the JP1/Service Support window [733](#)
- encrypted communication, configuring [720](#)
- event acquisition filter
 - changing location of [332](#)
 - setting, by switching filter conditions [482](#)
 - setting common exclusion-conditions [483](#)
 - setting only one [481](#)
 - settings for [481](#)
- event acquisition range
 - displaying event by specifying [473](#)
- event guide information, editing [502](#)
- event receiver filter
 - changing [479](#)
 - creating new [478](#)
 - deleting [479](#)
 - settings for [477](#)
- event report output format, specifying [115](#), [334](#)
- event service
 - setting up (UNIX) [303](#)
 - setting up (Windows) [71](#)
- event service definition information
 - collecting and distributing (UNIX) [306](#)
 - collecting and distributing (Windows) [74](#)
- Event Service definition information, collecting and distributing (UNIX) [307](#)
- Event Service definition information, collecting and distributing (Windows) [75](#)
- executing the setup program
 - JP1/IM - Manager (UNIX) [318](#)

F

- failover [599](#)

failure, preparations for collecting data in event of [110, 327](#)

filters, setting [475](#)

firewall

basic information about [707](#)

communication settings for JP1 that is run in [712](#)

environment, operating in [707](#)

filtering through [707](#)

G

general monitoring object

example of creating (Cosminexus resource monitoring by JP1/Cm2/SSO) [591](#)

example of creating (CPU monitoring by JP1/Cm2/SSO) [581](#)

general monitoring objects, example of creating [586](#)

generating correlation events

Settings [498](#)

GUI

using to create monitoring tree [538](#)

using to create Visual Monitoring window [553](#)

guide information, editing [562](#)

H

health check function, setting [112, 331](#)

HiRDB

example of creating general monitoring objects [586](#)

setup for linkage with [579](#)

Hitachi PP Installer (UNIX) [275](#)

Hitachi Program Product Installer

starting [275](#)

hosts

registering [376](#)

registering information of [537](#)

how to collect data in installing (for Windows) [48](#)

how to link with the auto scale function (for Windows) [49](#)

how to use Hitachi Program Product Installer (UNIX) [275](#)

HP NNM, setup for linkage with [576](#)

I

IM Configuration Management

importing and exporting management information in [442](#)

settings for using functions of (UNIX) [289](#)

settings for using functions of (Windows) [56](#)

setting system hierarchy by using [375](#)

setting using export and import functions of (UNIX) [299](#)

setting using export and import functions of (Windows) [67](#)

setting virtualization system configuration [391](#)

IM Configuration Management database, setting (UNIX) [287](#)

IM Configuration Management database, setting (Windows) [55](#)

IM Configuration Management - View

customizing operation [121](#)

setting using (UNIX) [297](#)

setting using (Windows) [65](#)

installation

notes (UNIX) [279](#)

notes (Windows) [44](#)

preparations required before (UNIX) [271](#)

preparations required before (Windows) [31](#)

prerequisite program (UNIX) [271](#)

prerequisite program (Windows) [31](#)

procedure (UNIX) [269, 272](#)

procedure (Windows) [28, 32](#)

types of [274](#)

UNIX [272](#)

Windows [32](#)

installation and setup procedure (UNIX) [269](#)

installation and setup procedure (Windows) [28](#)

installing certificate [394](#)

integrated monitoring database, setting (UNIX) [286](#)

integrated monitoring database, setting (Windows) [53](#)

Intelligent Integrated Management Base

Before configuring [444](#)

Compatible setting of the repeated event viewing suppression function [452](#)

Configuring the method for applying system configuration information [467](#)

Creating a cluster environment [449](#)

Defining links [453](#)

Migration procedure of the IM management node link definition file [468](#)

Overview of configuring [444](#)

Settings for linkage with an OpenID provider through single sign-on (linkage with external products) [457](#)

Settings for using the encryption function [448](#)

Settings necessary to use the custom UI display function [450](#)

Setting system configuration information [445](#)

Setting up the direct access URL [460](#)

Setting up the suggestion function for response actions depending on the system status 456

Setting work impact icons 454

IP addresses 715

support of 712

J

jcfview.conf 121

JP1/AJS

example of creating system-monitoring objects 580

setup for linkage with 572

JP1/Base

controlling communications by 701

copying primary authentication server settings (UNIX) 295

copying primary authentication server settings (Windows) 62

installing 31, 271

registering JP1 users (UNIX) 294

registering JP1 users (Windows) 62

setting operation permissions for JP1 users (UNIX) 294

setting operation permissions for JP1 users (Windows) 62

setting service startup sequence (Windows) 60

settings for handling failures (UNIX) 296

settings for handling failures (Windows) 64

settings for using the source host name of Event Service in the FQDN format (UNIX) 310

settings for using the source host name of Event Service in the FQDN format (Windows) 78

setting up command execution environment (UNIX) 308

setting up command execution environment (Windows) 76

setting up Event Service (UNIX) 303

setting up Event Service (Windows) 71

setting user authentication (UNIX) 293

setting user authentication (Windows) 61

setting user mapping (UNIX) 293

setting user mapping (Windows) 61

specifying authentication server (UNIX) 294

specifying authentication server (Windows) 61

JP1/Cm2/SSO

example of creating general monitoring object 581

example of creating general monitoring object (Cosminexus resource monitoring by JP1/Cm2/SSO) 591

setup for linkage 573

JP1/IM

Central Scope environment setup 536

communication 712

controlling communications by JP1/Base 701

creating IM database (UNIX) 285

creating IM database (Windows) 52

designing setup details (UNIX) 271

designing setup details (Windows) 31

using to create monitoring tree 561

environment setup procedure for cluster operation (UNIX) 656

environment setup procedure for cluster operation (Windows) 606

installation and setup procedure (UNIX) 269

installation and setup procedure (Windows) 28

installing (UNIX) 268, 272

installing (Windows) 27, 32

notes about cluster operation (UNIX) 697

notes about cluster operation (Windows) 649

operating in firewall environment 707

operating in multiple networks 702

operation and environment configuration depending on network configuration 700

operation and environment configuration in cluster system (UNIX) 652

operation and environment configuration in cluster system (Windows) 597

overview of cluster operation (UNIX) 653

overview of cluster operation (Windows) 598

preparations required before installing (UNIX) 271

preparations required before installing (Windows) 31

registering host information 537

setting automated actions 490

setting correlation event generation 498

setting monitor startup for linked products 525

settings for linking to other integrated management products 732

setting Tool Launcher window 528

setting up (UNIX) 268

setting up (Windows) 27

setting up Central Console 472

setting up Central Scope 535

setting up Central Scope operating environment 565

setting up IM Configuration Management View (Windows) 120

setting up JP1/IM - Agent (UNIX) 338

setting up JP1/IM - Agent (Windows) 122

setting up JP1/IM - Manager (UNIX) 318

- setting up JP1/IM - Manager (Windows) 95
- setting up JP1/IM - View (Windows) 119
- uninstalling (UNIX) 365
- uninstalling (Windows) 259
- JP1/IM - Agent
 - installing (Windows) 32
 - setup (Windows) 122
- JP1/IM - Agent
 - setup (UNIX) 338
- JP1/IM - Manager
 - automatic startup (UNIX) 318
 - automatic stop (UNIX) 318
 - executing the setup program (UNIX) 318
 - installing (UNIX) 272
 - installing (Windows) 32
 - services and processes of 603, 654
 - settings for handling failures (UNIX) 327
 - settings for handling failures (Windows) 110
 - setup (UNIX) 318
 - setup (Windows) 95
 - uninstalling (UNIX) 365
 - uninstalling (Windows) 259
- JP1/IM - View
 - customizing JP1/IM - View operation (Windows) 119
 - installing (Windows) 32
 - setting, for login user 523
 - settings for handling failures (Windows) 119
 - setup (Windows) 119
 - uninstalling (Windows) 259
- JP1/IM - View settings 523
- JP1/IM - View settings, procedure for specifying 524
- JP1/PAM, setup for linkage with 578
- JP1/PFM, setup for linkage with 575
- JP1/ServerConductor
 - setup for linkage 579
- JP1/Software Distribution
 - remote installation using 42, 275
 - setup for linkage with 577
- jp1cohasetup.exe 609
- jp1cshasetup.exe 615
- JP1 events
 - displaying attributes of user-defined 508
 - editing guide information of 502
 - setting filters for 475
 - setting forwarding of (UNIX) 305
 - setting forwarding of (Windows) 73
 - setting issuance of, during action status change 504

- settings for operations to be performed during acquisition of 473
- setting to issue, in event of abnormal process termination 112, 330

JP1 users

- setting operation permissions for (UNIX) 294
- setting operation permissions for (Windows) 62

L

- language encoding 277
- launching a JP1/AJS window by monitor startup 735
- launching a JP1/PFM window by monitor startup 737
- linked products
 - setting monitor startup for 525
 - setting up for 572
- linking to JP1/IM - Navigation Platform 734
- linking to JP1/Service Support 733
- linking with JP1/AJS 735
- linking with JP1/PFM 737
- logical host 599
 - common definition information 604, 655
 - creating scripts to be registered into cluster software (UNIX) 681
 - deleting (UNIX) 690
 - deleting (Windows) 641
 - new installation and setup (UNIX) 658
 - new installation and setup (Windows) 608
 - registering into cluster software (Windows) 634
 - resource start and stop sequence (UNIX) 683
 - resource start and stop sequence (Windows) 635
 - upgrade installation and setup (UNIX) 685
 - upgrade installation and setup (Windows) 637
- logical hosts
 - prerequisites for environment of 600
- logical IP address 599, 600
- login information, saving 538

M

- managing profile
 - displaying (remote monitoring configuration) 435
 - editing configuration file (remote monitoring configuration) 436
- map display settings 549
- mapping
 - event source host 520
- memory entries, setting 501

- Migration procedure of the IM management node link definition file [468](#)
- monitoring nodes
 - adding [543](#), [556](#)
 - changing monitoring status of [557](#)
 - deleting [548](#), [556](#)
 - moving [548](#)
 - searching for [551](#), [558](#)
 - setting attributes of [545](#), [557](#)
- monitoring object database, automatic backup and recovery settings for [113](#), [331](#)
- monitoring objects, examples of creating [580](#)
- monitoring tree
 - acquiring, from server [540](#)
 - acquiring, stored locally [540](#)
 - acquiring existing [539](#)
 - applying customized [551](#)
 - creating, by using GUI [538](#)
 - customizing [542](#)
 - customizing toolbar for [567](#)
 - generating automatically [540](#)
 - opening editing window [538](#)
 - saving customized [551](#)
 - searching for monitoring nodes in [551](#)
 - setting monitoring range [549](#)
 - settings for using visual icons [550](#)
 - setting up for linked products [572](#)
- Monitoring Tree (Editing) window, opening [538](#)
- monitoring tree window
 - creating, by editing the saved CSV file [561](#)
- monitor startup, setting [525](#)
- monitor windows
 - determining window to be used for opening [526](#)
 - opening [525](#)
- moving monitoring nodes [548](#)
- multi-LAN environment
 - command execution (cluster operation) [705](#)
 - command execution (non-cluster operation) [703](#)
 - JP1/IM - View connection (cluster operation) [704](#)
 - JP1/IM - View connection (non-cluster operation) [702](#)

N

- NAT [710](#)
 - support of [717](#)
- NetBIOS setting (NetBIOS over TCP/IP) (Windows) [86](#)
- networks
 - operating in firewall environment [707](#)

- operating in multiple [702](#)
- operation and environment configuration depending on [700](#)
- newly installing JP1/Base and JP1/IM - Manager (UNIX) [658](#)
- newly installing JP1/Base and JP1/IM - Manager (Windows) [608](#)
- non-cluster system
 - environment setup for running logical hosts (UNIX) [698](#)
 - environment setup for running logical hosts (Windows) [650](#)
 - evaluating configuration for running logical host (UNIX) [698](#)
 - evaluating configuration for running logical host (Windows) [650](#)
 - logical host operation and environment configuration (UNIX) [698](#)
 - logical host operation and environment configuration (Windows) [650](#)
 - notes about running logical hosts (UNIX) [699](#)
 - notes about running logical hosts (Windows) [651](#)
- notes
 - during cluster operation (UNIX) [697](#)
 - during cluster operation (Windows) [649](#)
 - setting configuration definition information (UNIX) [301](#)
 - setting configuration definition information (Windows) [69](#)
- notes about
 - installing (UNIX) [279](#)
 - installing and uninstalling (Windows) [44](#)
- notes about cluster operation (UNIX) [697](#)
- notes about cluster operation (Windows) [649](#)
- notes about setting configuration definition information (UNIX) [301](#)
- notes about setting configuration definition information (Windows) [69](#)
- notes on
 - uninstallation (UNIX) [368](#)
 - uninstallation (Windows) [262](#)
- number of connected-host log entries in Login window for IM Configuration Management [121](#)
- number of connected-user log entries in Login window for IM Configuration Management [121](#)
- number of events to acquire
 - at updating [523](#)
 - per search [523](#)

O

opening edit window for Visual Monitoring window 553
OS environment, configuring 31, 271
Overview of configuring an environment for the Intelligent Integrated Management Base 444

P

packet filtering 707
physical hosts 599
 prerequisites for environment of 600
port numbers 712
 support of 712
preparation for creating IM database (UNIX) 285
preparations for creating IM databases (for Windows) 52
prerequisite program
 installing (UNIX) 271
 installing (Windows) 31
preventing history of previously used JP1 login user names from appearing 119
preventing names of JP1 users who are currently logged in from appearing 120, 121
primary authentication server, copying settings for (UNIX) 295
primary authentication server, copying settings for (Windows) 62
procedure
 installation and setup (UNIX) 269
 installation and setup (Windows) 28
profiles
 collecting 420
 collecting list of 419
 displaying 422

R

refresh interval 523
registering JP1 users (UNIX) 294
registering JP1 users (Windows) 62
regular expressions, setting 490
remote installation 275
remote installation (Windows) 42
repeated events, consolidated display of 524
response timeout period when system hierarchy is applied 121

S

saving

 customized monitoring tree at local host 551
 customized Visual Monitoring window at local host 558
saving manuals to computer (UNIX) 364
saving manuals to computer (Windows) 257
server response timeout period 121
service startup sequence, setting (Windows) 60
setting
 abnormal process termination, restart settings in event of 111, 330
 attributes of monitoring nodes 545
 automated actions 490
 Central Console 472
 Central Scope 535
 Central Scope operating environment 565
 completed-action linkage function 565
 correlation event generation 498
 execution conditions and details of automated actions 490
 execution environment for automated action function 490
 health check function 112, 331
 host information 537
 JP1/IM - View for login user 523
 JP1 event filtering 475
 JP1 event issuance during action status change 504
 maximum number of status change events 565
 memo entries 501
 memory-resident status change condition function 567
 monitoring range 549
 monitor startup for linked products 525
 number of connected-host log entries in Login window 119
 path to start WWW browser 119
 system hierarchy (when IM Configuration Management is not used) (UNIX) 300
 system hierarchy (when IM Configuration Management is not used) (Windows) 68
 system hierarchy (when IM Configuration Management is used) (UNIX) 297
 system hierarchy (when IM Configuration Management is used) (Windows) 65
 Tool Launcher window 528
 whether List of Action Results window can start when Event Console window opens 119
 whether to allow copying to clipboard 119
 whether Tool Launcher window can start when Event Console window opens 119

Setting

- Intelligent Integrated Management Base (for UNIX) 320
- Intelligent Integrated Management Base (for Windows) 95
- setting business group 410
- setting common exclusion-conditions 483
- setting common exclusion-conditions (by using common-exclusion-conditions extended definition file and jcochfilter command) 486
- setting common exclusion-conditions (by using Common Exclusion-Conditions Settings window or Common Exclusion-Condition Settings (Extended) window 484
- setting display color of JP1 event 489
- setting event acquisition filter (for compatibility) 486
- setting event source host mapping 520
- setting for monitoring logs while remote monitoring is stopped 116, 335
- setting JP1 event forwarding when IM Configuration Management is not used (UNIX) 305
- setting JP1 event forwarding when IM Configuration Management is not used (Windows) 73
- setting JP1 event forwarding when IM Configuration Management is used (UNIX) 304
- setting JP1 event forwarding when IM Configuration Management is used (Windows) 72
- setting language code in common definition 278
- setting language code in environment variable file 277
- setting monitoring of repeated events to be prevented 488
- setting number of connected-host log entries in Login window 119
- setting path to start WWW browser 119
- setting profile on host in remote monitoring configuration 432
- setting reference and operation restrictions 533
- setting reference and operation restrictions on business group 533
- setting required immediately after installation (UNIX) 277
- setting required immediately after installation (Windows) 43
- settings for
 - automatic backup and recovery for monitoring object database 113, 331
 - changing location of event acquisition filter 332
 - deleting status change events when JP1 event handling is completed 566
 - event acquisition filters 481
 - event receiver filters 477
 - handling JP1/Base failures (UNIX) 296
 - handling JP1/Base failures (Windows) 64
 - initializing monitoring objects when JP1 events are received 566
 - issuing JP1 events in event of abnormal process termination 112, 330
 - linking to other integrated management products 732
 - operations to be performed during JP1/IM event acquisition 473
 - restarting process in event of abnormal termination 111, 330
 - severe events filters 479
 - status color of monitoring node name and monitoring node 569
 - suppressing display of monitoring node name and icon margin 568
 - suppressing movement of icon of monitoring node 571
 - user authentication (UNIX) 293
 - user authentication (Windows) 61
 - user mapping (UNIX) 293
 - user mapping (Windows) 61
 - using visual icons 550
 - view filters 475
- settings for checking operation information by using the Intelligent Integrated Management Base 737
- settings for checking the association between root jobnets and their configuration information by using the Intelligent Integrated Management Base 735
- settings for displaying event-source-host performance report 737
- settings for displaying the monitor window from an email sent by automated action 735
- settings for displaying the monitor window from event guide information 735
- settings for JP1/IM - Agent (JP1/IM agent control base) 730
- settings for launching a JP1/AJS window from the Tool Launcher window 735
- settings for launching a JP1/PFM window from the Tool Launcher window 737
- Settings for linkage with an OpenID provider through single sign-on (linkage with external products) 457
- settings for monitoring logs on remotely monitored host (UNIX) 311
- settings for monitoring logs on remotely monitored host (Windows) 80
- settings for upgrade installation (UNIX) 332
- settings for upgrade installation (Windows) 113
- settings for using the functions of the Intelligent Integrated Management Base (for UNIX) 320

- Settings for using the functions of the Intelligent Integrated Management Base (for Windows) [95](#)
- settings for using the source host name of Event Service in the FQDN format (UNIX) [310](#)
- settings for using the source host name of Event Service in the FQDN format (Windows) [78](#)
- settings of JP1/IM - Agent [126](#), [341](#)
- setting startup options [499](#)
- Setting the display message change function [516](#)
- setting up client application execution environment (UNIX) [309](#)
- setting up client application execution environment (Windows) [77](#)
- setting up command execution function for managed host (UNIX) [308](#)
- setting up command execution function for managed host (Windows) [76](#)
- setting up IM Configuration Management View [120](#)
- setting up IM Configuration Management View (Windows) [120](#)
- setting up JP1/IM - Agent during new installation (UNIX) [669](#)
- setting up logical host environment (primary node) during new installation of JP1/IM - Manager (Windows) [609](#)
- setting up logical host environment (primary node) during upgrade installation (UNIX) [687](#)
- setting up logical host environment (primary node) during upgrade installation (Windows) [639](#)
- setting up logical host environment (primary node) of JP1/IM - Manager during new installation (UNIX) [659](#)
- setting up logical host environment (secondary node) during new installation of JP1/IM - Manager (Windows) [616](#)
- setting up logical host environment (secondary node) during new installation of JP1/IM - Manager (UNIX) [665](#)
- setting up physical host environment during new installation (UNIX) [659](#)
- setting up physical host environment during new installation of JP1/IM - Manager (Windows) [609](#)
- setting up SSH connection with host started by KVM (in UNIX) [402](#)
- setting up SSH connection with host started by KVM (in Windows) [398](#)
- Setting up the direct access URL [460](#)
- Setting Up the Intelligent Integrated Management Base [443](#)
- Setting up the suggestion function for response actions depending on the system status [456](#)
- setting whether List of Action Results window can start when Event Console window opens [119](#)
- setting whether to allow copying to clipboard [119](#)
- setting whether Tool Launcher window can start when Event Console window opens [119](#)
- setup
 - JP1/IM - Agent (UNIX) [338](#)
 - JP1/IM - Manager (UNIX) [318](#)
 - JP1/IM - Manager (Windows) [95](#)
 - linked products [572](#)
 - procedure (UNIX) [269](#)
 - procedure (Windows) [28](#)
- setup
 - JP1/IM - Agent [122](#)
 - JP1/IM - View [119](#)
- setup for JP1/IM - Agent service [122](#)
- setup for JP1/IM - Agent servicing [338](#)
- setup when using JP1/IM - Agent as an agent [96](#), [321](#)
- severe events filters, setting [479](#)
- severity changing function, setting [513](#)
- shared disk [599](#), [600](#)
 - file organization on [603](#), [653](#)
- shared the Dashboard window [471](#)
- specifying the size of log information that can be collected per monitoring interval (for UNIX) [317](#)
- specifying the size of log information that can be collected per monitoring interval (for Windows) [94](#)
- starting JP1/Base and JP1/IM - Manager [279](#)
- starting log file trap [429](#)
- starting or stopping log file trap [429](#)
- status change events, setting for maximum number [565](#)
- stopping log file trap [430](#)
- suppressing message to be output to the system log (syslog) [326](#)
- switching between basic mode and extended mode for common exclusion-condition [484](#)
- system configurations using multiple LANs [702](#)
- system environment
 - configuring (UNIX) [271](#)
 - configuring (Windows) [31](#)
- system hierarchy
 - setting [375](#)
 - setting (when IM Configuration Management is not used) (UNIX) [300](#)
 - setting (when IM Configuration Management is not used) (Windows) [68](#)
 - setting (when IM Configuration Management is used) (UNIX) [297](#)
 - setting (when IM Configuration Management is used) (Windows) [65](#)
- system-monitoring objects, example of creating [580](#)

T

Tool Launcher window

- adding new menus [528](#)
 - determining window to be opened from [529](#)
 - setting [528](#)
 - settings for opening GUI of linked products from [528](#)
 - settings for opening Web page of linked products from [532](#)
- tuning.conf [120](#)

U

uninstallation

- notes (UNIX) [368](#)
- notes (Windows) [262](#)
- UNIX [365](#)
- Windows [259](#)

uninstallation procedure (UNIX) [365](#)

uninstallation procedure (Windows) [259](#)

uninstalling

- notes (Windows) [44](#)
- UNIX [365](#)
- Windows [259](#)

uninstalling JP1/IM - Manager and JP1/Base (UNIX) [692](#)

uninstalling JP1/IM - Manager and JP1/Base (Windows) [643](#)

uninstalling logical hosts (UNIX) [690](#)

uninstalling logical hosts (Windows) [641](#)

uninstall JP1/IM - Agent (for Windows) [643](#)

updated agent profile notification function [115](#), [335](#)

updating IM database (UNIX) [289](#)

updating IM database (Windows) [56](#)

updating IM database in a cluster environment (UNIX) [695](#)

updating IM database in a cluster environment (Windows) [646](#)

upgrade installation

- changing location of event acquisition filter [332](#)

upgrade installation of JP1/Base and JP1/IM - Manager (UNIX) [685](#)

upgrade installation of JP1/Base and JP1/IM - Manager (Windows) [637](#)

upgrade installation of JP1/IM - Agent (for Windows) [638](#)

upgrade installation of JP1/IM - Agent (UNIX) [686](#)

user authentication, setting (UNIX) [293](#)

user authentication, setting (Windows) [61](#)

user-defined event attributes, displaying [508](#)

user mapping, setting (UNIX) [293](#), [295](#)

user mapping, setting (Windows) [61](#), [63](#)

using Central Scope to monitor business group [417](#)

using commands to change settings (UNIX) [694](#)

using commands to change settings (Windows) [645](#)

using IM Configuration Management to manage a virtualization configuration [391](#)

V

variable binding

- loading to JP1 event [574](#)

version information, displaying [277](#)

version number conventions [13](#)

view filters

- changing [477](#)
- creating new [475](#)
- deleting [477](#)
- settings for [475](#)

virtualization system configuration

- setting [391](#)

virtualization system configuration (UNIX)

- settings for managing and monitoring (UNIX) [299](#)

virtualization system configuration (Windows)

- settings for managing and monitoring (Windows) [67](#)

visual icons, settings for using [550](#)

Visual Monitoring window

- acquiring, from server [554](#)
- acquiring existing [554](#)
- adding monitoring nodes to [556](#)
- applying customized [558](#)
- customizing [554](#)
- deleting [559](#)
- deleting monitoring nodes from [556](#)
- opening edit window for [553](#)
- saving customized [558](#)
- setting background image for [555](#)
- that has been saved locally, acquiring [554](#)
- using GUI to create [553](#)

W

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 [121](#)

work impact icons [454](#)



6-6, Marunouchi 1-chome, Chiyoda-ku, Tokyo, 100-8280 Japan
