HITACHI
Inspire the Next

JP1 Version 13

Integrated Management: Getting Started

3021-3-L01-40(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 or later

The above product includes the following:

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

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

P-CC842C-9GDL JP1/Integrated Management 3 - Agent 13-50 or later (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 or later (for Windows Server 2025, Windows Server 2022, Windows Server 2019, Windows Server 2016)

P-CC842C-6LDL JP1/Base 13-10 or later (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 or later (for AIX)

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

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

The above product includes the following:

P-CC842C-9MDL JP1/Integrated Management 3 - Manager 13-50 or later (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 or later (for SUSE Linux 15, SUSE Linux 12)

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

P-CC842C-9GDL JP1/Integrated Management 3 - Agent 13-50 or later (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 or later (for Windows Server 2025, Windows Server 2022, Windows Server 2019, Windows Server 2016)

P-CC842C-6LDL JP1/Base 13-10 or later (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 or later (for AIX)

■ Trademarks

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 (eay@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.

■ 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.

■ Issued

Sep. 2025: 3021-3-L01-40(E)

■ Copyright

Summary of amendments

The following table lists changes in this manual (3021-3-L01-40(E)) and product changes related to this manual.

Changes	Location
None	--

Legend:

--: Not applicable

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

Preface

This manual describes the main way of setting up and operating JP1/Integrated Management 3 - Manager, JP1/Integrated Management 3 - View, and JP1/Integrated Management 3 - Agent based on the system operation cycle. Users who want to learn about JP1/Integrated Management 3 - Manager functions based on the intended use of each function should read this manual first. JP1/Integrated Management 3 - Manager, JP1/Integrated Management 3 - View, and JP1/Integrated Management 3 - Agent might be generically referred to as *JP1/IM*.

■ How to read this manual

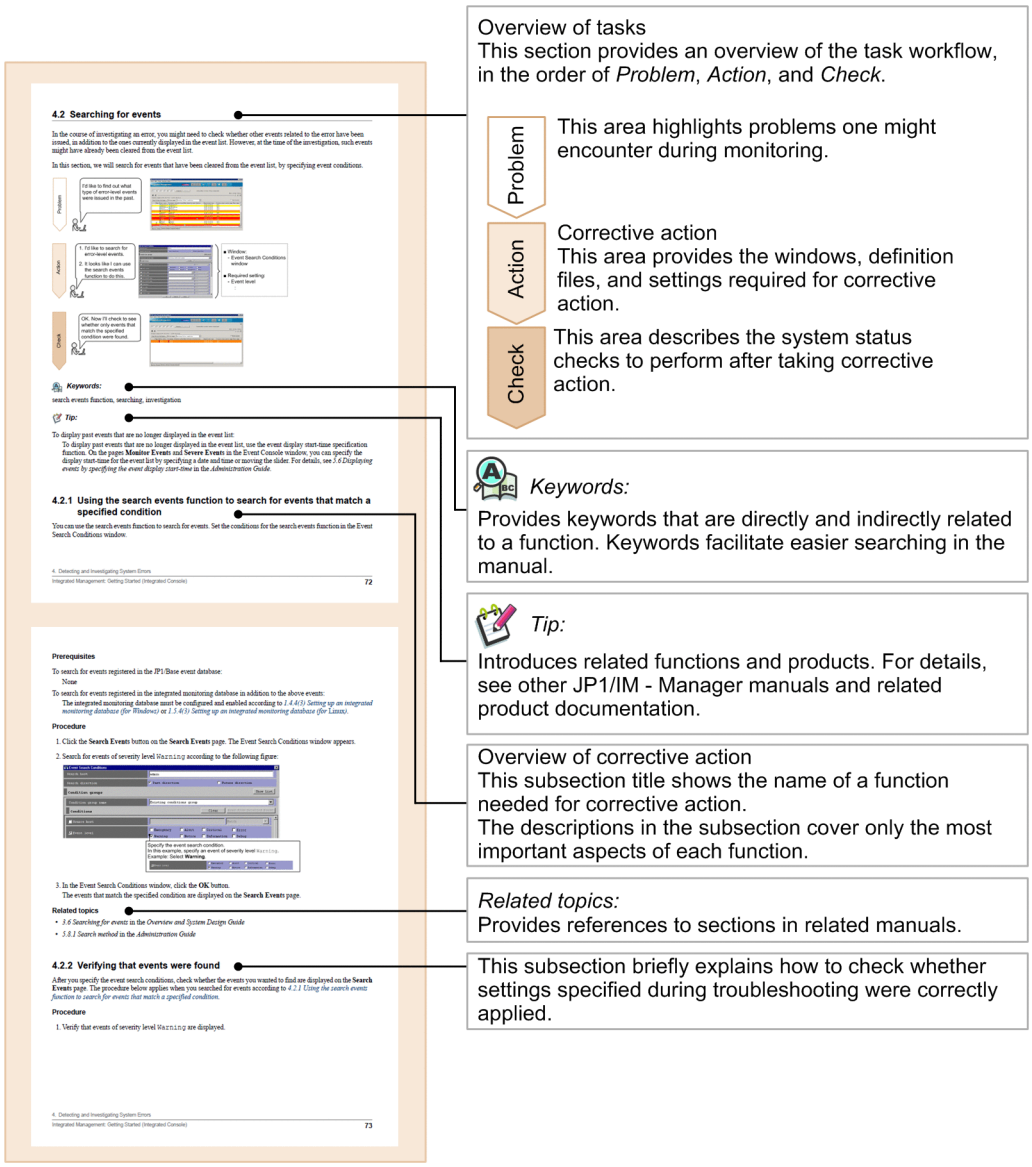
The following environments are required to perform the operations in each window.

Operations on the manager:

Environment in which Windows Server 2016 or Linux 7 is used

Operations on the viewer:

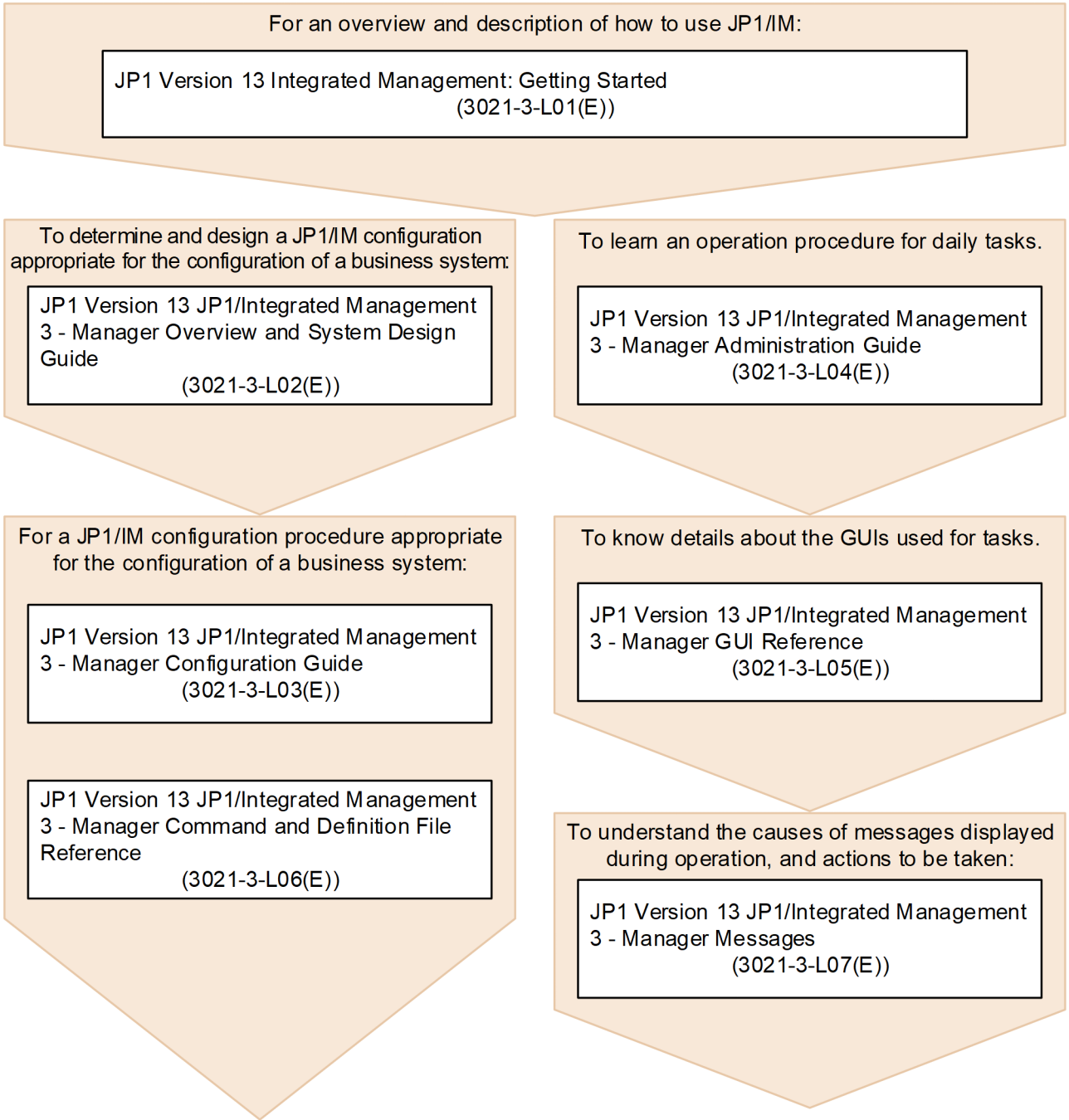
Environment in which Windows 10 is used



Some windows in this manual might differ from the windows of your product because of improvements made without prior notice.

The JP1/IM manual set consists of seven manuals, including this one. For details about the setup and operation methods introduced in this manual, read the pertinent descriptions in the manuals shown below.

The following shows an example of the reading sequence of manuals, based on user requirements:



In this manual, the term *Administrator permissions* means the Administrator permissions for a local PC. If the user has Administrator permissions for the local PC, operations are the same no matter whether they are performed with a local user account, a domain user account, or in an Active Directory environment.

This manual uses the following replacement characters to represent installation folders for Windows versions of JP1/IM and JP1/Base:

- View-path
- Manager-path
- Console-path

- Scope-path
- Agent-path
- Base-path

For details about these replacement characters, see *G. Reference Material for this Manual*.

■ Conventions: Fonts and symbols

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.
Italic	Italic characters indicate a placeholder for some actual text to be provided by the user or system. For example: • Write the command as follows: `copy` *source-file target-file* • The following message appears: `A file was not found. (file =` *file-name*`)` Italic characters are also used for emphasis. For example: • Do *not* 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 `dir`. • Use the `send` command to send mail. • The following message is displayed: `The password is incorrect.`

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:

Symbol	Convention
	`A, B, B, ...` means that, after you specify `A, B,` you can specify B as many times as necessary.

■ 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*.

Contents

1 Overview

This chapter helps you understand what is explained in this manual and what you can do with JP1/IM.

1.1 What is explained in this manual

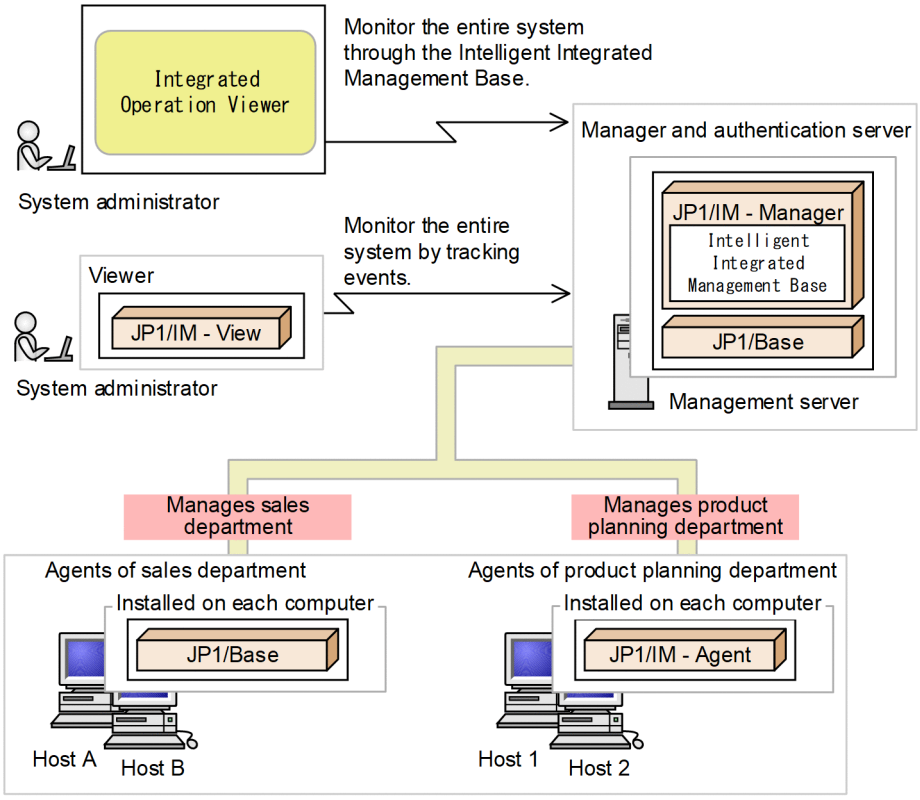
This manual is intended for professionals who want to use JP1/IM to manage and operate open platform systems, and those who are considering introducing JP1/IM. More specifically, it is intended for:

- System administrators and operators who want an overview of the basic use of JP1/IM
- Those who are considering implementation of JP1/IM to centrally monitor events that occur in their system

Users who have not purchased a support services contract can also use this manual.

This manual explains how to install, set up, and configure features that help the intended audience understand the health of the entire IT using the integrated operation viewer and begin monitoring and managing incidents. In addition, the following appendices show you the email notification functionality, visual monitoring, and functions for using JP1/IM as monitoring applications.

Operation procedures in this manual assume systems consisting of monitored hosts (agents) and management servers (managers) with JP1/Integrated Management 3 - Manager installed. Agents and managers are configured hierarchically in two levels, as shown in the following figure:



1.2 What you can do with JP1/IM

With the growing size and complexity of the systems underpinning an enterprise's business operations, management of system operation is a vital issue. While most routine tasks are automated to improve efficiency, non-routine tasks still depend on individual skills and require more efficient IT operation because such tasks involve collating various types of information and knowledge to infer and make decisions.

JP1/IM provides the Intelligent Integrated Management Base, which enables an integrated way to manage and collate various types of data and knowledge to improve system operations. JP1/IM optimizes system operations management by offering integrated management tailored to objectives and integration of operational tasks.

JP1/IM has the following features:

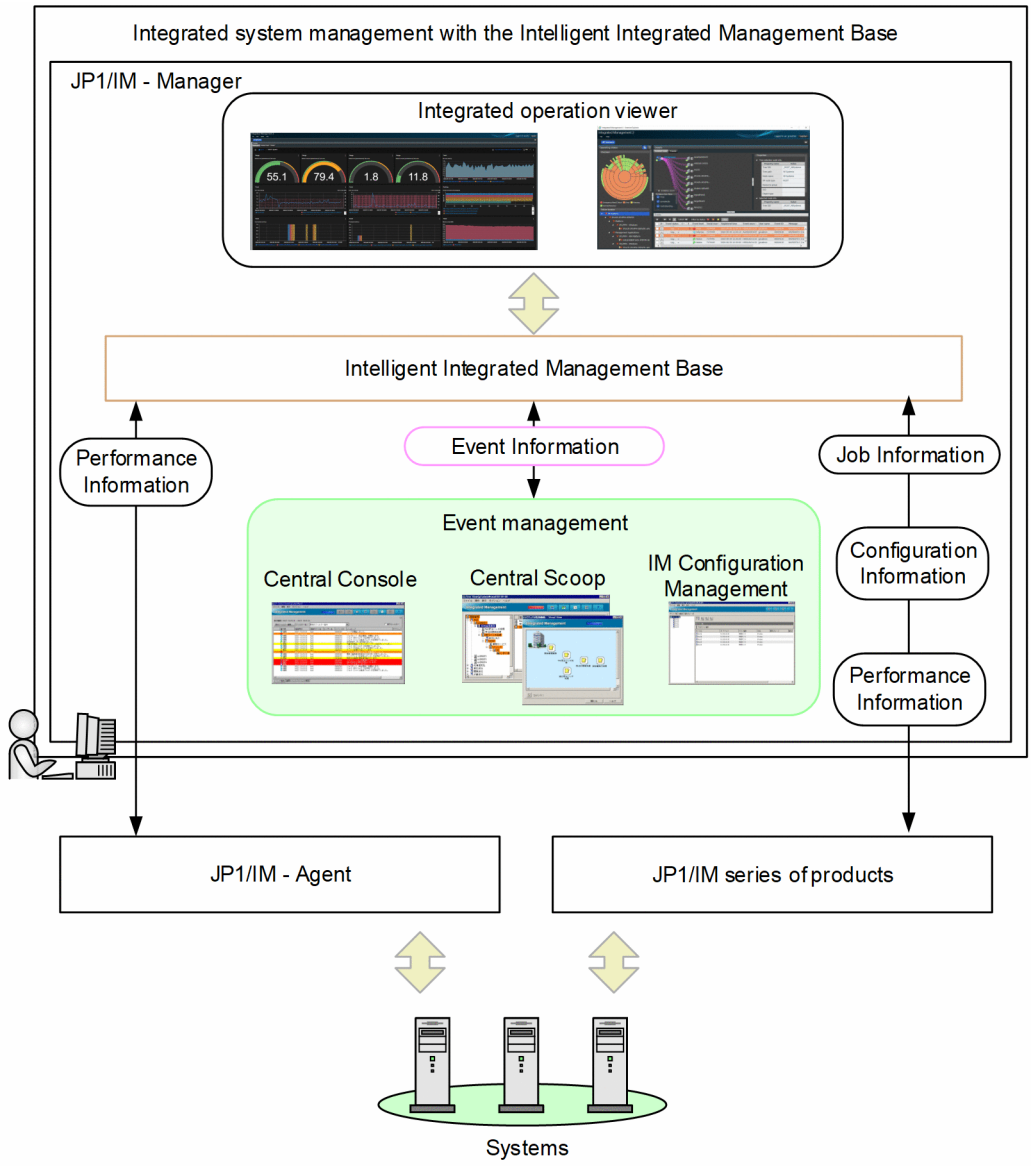
- Providing the viewer (integrated operation viewer) for JP1/IM - Manager (Intelligent Integrated Management Base) to understand the situation by visualizing the entire IT system, and to identify relationships between system components
- Integrated management using JP1 events (simply called *events* hereafter) and centralized system monitoring
- Error detection and reporting
- Integrating troubleshooting based on JP1/IM
- Integrated management of the system hierarchy and host settings

With the above features, JP1/IM integrates monitoring and operation into a unified management process based on JP1/IM, thus simplifying complex tasks.

The following figure shows the major JP1/IM functions.

The following figure illustrates the overview of JP1/IM.

Figure 1–1: Overview of JP1/IM



JP1/IM's Intelligent Integrated Management Base enables you to assess the health of your IT system from the context of your IT infrastructure, visualize the relevance of the data in your system, including impacted job information and operational information, in the integrated operation viewer (WWW browser), and take contextual actions. In addition, event management allows you to monitor and manage events based on events occurring in the system using a dedicated GUI.

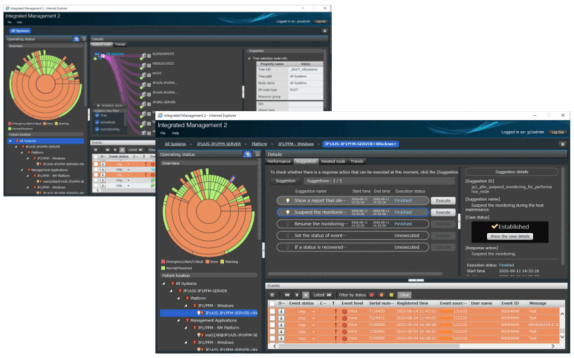
The following figures show the major JP1/IM functions.

Figure 1–2: Major functions of the Intelligent Integrated Management Base

■Major functions of the Intelligent Integrated Management Base

■Assess system health
(Integrated Operation Viewer
[**Dashboard**])
Assess the health of the entire IT system from the state of the IT infrastructure.

■Gain visibility into impactful IT resources
(Integrated Operation Viewer
[**Dashboard**])
Events and operating information for each IT resource
We collect and integrate the necessary information such as,
Analyze impacted IT resources.

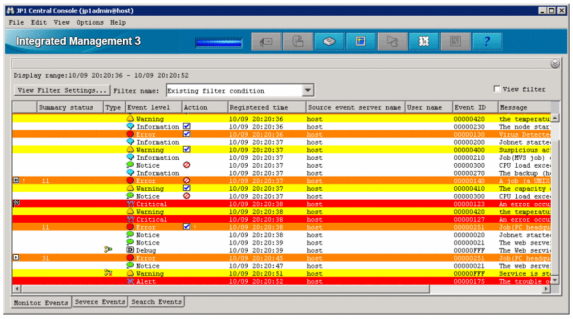


■Integrated system monitoring
(Integrated Operation Viewer)

Check the scope of impact based on the relevance of the data and take action according to the situation.

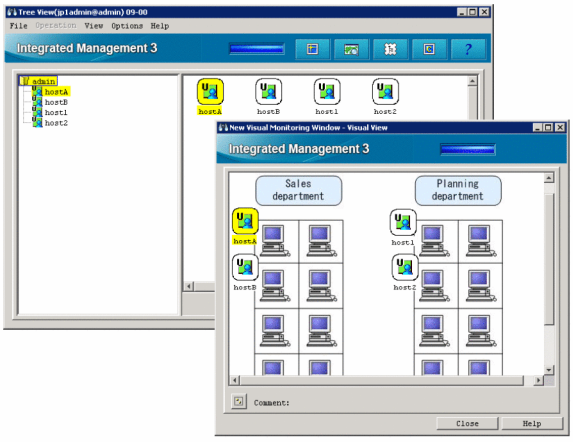
Figure 1–3: Major functions of event management

■Major functions of event management



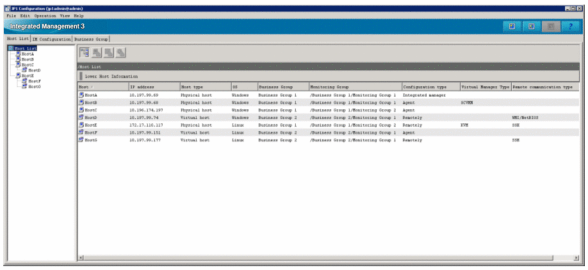
■Central monitoring (central console)

Centrally monitors the entire system by using JP1 events, and integrates all aspects of the operating cycle, from event monitoring to error detection, investigation, and resolution.



■Visual monitoring (central scope)

Implements visual object-oriented system monitoring, which the system administrator can customize based on what he or she wants to do.



■Configuration management (IM Configuration Management)

Allows the manager to centrally manage the system hierarchy managed by JP1/IM (IM configuration) and settings of the hosts that make up the system.

2 Installing and Setting Up JP1/IM

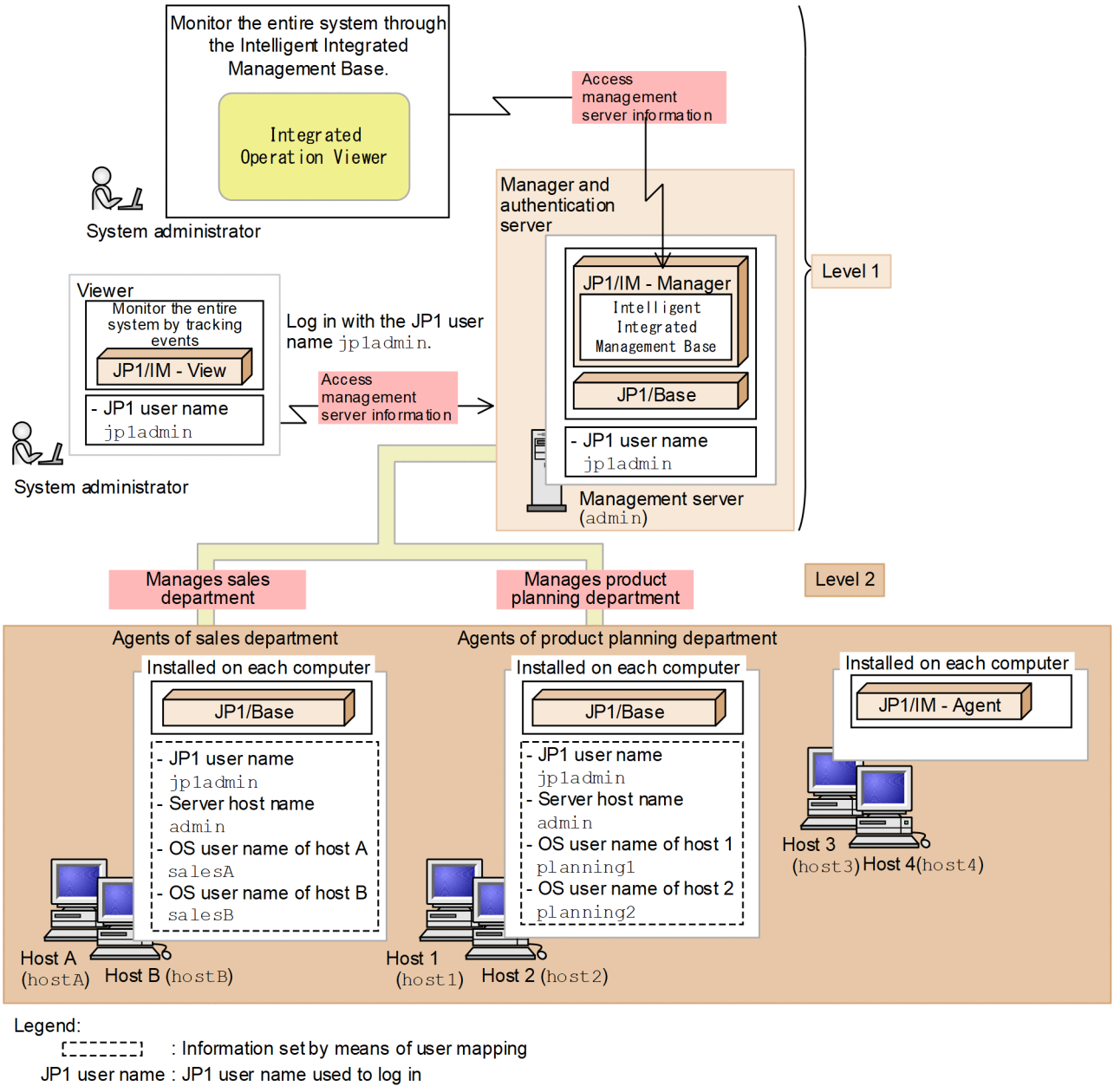
This chapter describes how to install and set up JP1/IM and JP1/Base.

2.1 Overview of a basic configuration system

This section describes a basic configuration system that will be built using this manual to install JP1/IM and start system monitoring. In this manual, the term *system* is used generally to indicate a system provided by JP1/IM - Manager.

A system consists of *managers* for managing events and hosts, *agents* that are monitored, and the *viewer* for monitoring and operating the system. In this manual, a basic configuration system is defined as a system that has a hierarchical two-level structure, with agents at a lower level than the manager).

Figure 2–1: Basic configuration system



In this example, the system administrator uses a viewer to log in with the JP1 user name `jp1admin`. Then, on the viewer, the system administrator monitors events that were transferred to the manager, which is a management server (`admin`), and events that were issued by the manager. The events issued by the agents (`hostA` and `hostB`) that belong to the sales department and the agents (`host1` and `host2`) that belong to the product planning department are transferred to the manager.

Each host in the figure has one NIC and only one IP address assigned. For details on settings if a host in the system has multiple NICs or if multiple IP addresses are assigned to an NIC, see the description of the communication protocols of JP1/Base in the *JP1/Base User's Guide*.

2.2 Preparation before installation

This section describes the preparations required before installing JP1/IM and its prerequisite product JP1/Base.

2.2.1 Preparing the products to be installed

Before you start installation, prepare the products listed below. Note that this manual assumes that the version of all products to be installed is 13-00 or later.

Manager

- JP1/Integrated Management 3 - Manager
- JP1/Base

Agent

One of the following is required:

- JP1/Integrated Management 3 - Agent
- JP1/Base

Viewer

- JP1/Integrated Management 3 - View#

#:

This is not required when you want to use only the Intelligent Integrated Management Base.

Related topics

- *1.5 JP1/IM - Manager system configuration* in the *Overview and System Design Guide*

2.2.2 Prerequisite OSs and OS environment configuration

(1) Prerequisite OSs

The following are the OSs required for managers, agents, and viewers. For details, see the *Release Notes* for the applicable products.

Manager

- Windows Server 2025, Windows Server 2022, Windows Server 2019, Windows Server 2016
- Linux

Agent

- Windows Server 2025, Windows Server 2022, Windows Server 2019, Windows Server 2016
- AIX#
- Linux

#: Not supported if agent is JP1/Integrated Management 3 - Agent.

Viewer

- Windows Server 2025, Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows 11, Windows 10

This manual describes how to install and set up Windows and Linux environments.

(2) Configuring the OS environment necessary for installation

You must perform the following according to the *Release Notes* for JP1/IM - Manager, JP1/IM - View, and JP1/Base:

- Apply the service packs and patches required by JP1/IM and JP1/Base to the OS.
- If the IM database is used, for the host name, specify a character string of no more than 32 characters consisting of half-width alphanumeric characters,hyphens (-), and periods(.).
- (Linux only) Adjust kernel parameters according to the configuration of JP1/IM.

Related topics

- *1.2.2 Configuring the system environment (for Windows)* in the *Configuration Guide*
- *2.2.2 Configuring the system environment (for UNIX)* in the *Configuration Guide*
- Description of the communication protocols of JP1/Base in the *JP1/Base User's Guide*

2.2.3 Required amounts of installation memory and disk space

The required amounts of installation memory and disk space vary depending on the operating environment. For details, see the *Release Notes* for JP1/IM - Manager, JP1/IM - View, and JP1/Base.

2.2.4 Language settings in prerequisite OSs

Confirm that the same language is set in the OSs of the hosts on which JP1/IM - Manager, JP1/IM - View, JP1/IM - Agent, and JP1/Base will be installed.

The table below shows the language settings for prerequisite OSs. Make sure that you set the language as shown below. Otherwise, characters might be garbled.

OS	Items to check	Setting value		
		Japanese	English	Chinese
Windows	Region and language settings in the Control Panel	Japanese	English	Chinese (simplified)
Linux	Value of the LANG environment variable	ja_JP.UTF-8 or ja_JP.utf8	C, en_US.UTF-8, or en_US.utf8	zh_CN.gb18030

2.2.5 Setting ports used by JP1/IM

If you use JP1/IM on a host set up as a firewall, make sure that traffic in the local host through all ports used by JP1/IM can pass through the firewall. For details about port numbers, see *Appendix D Port Numbers*. For details about the direction of communication through a firewall, see *D.3 Direction of communication through a firewall*.

2.2.6 Setting name resolution

Setting name resolution

Make sure that the hosts in the system can perform unique name resolution with each other.

(Linux only) Confirming that the local host is available for name resolution

Use the `ping` command to confirm that the host name of the local host can be resolved with an IP address (other than a loopback address) in the connected LAN environment. If name resolution is not possible, JP1/IM - Agent, JP1/Base does not operate normally. Revise the `hosts` file settings.

Related topics

- Description of the communication protocols of JP1/Base in the *JP1/Base User's Guide*

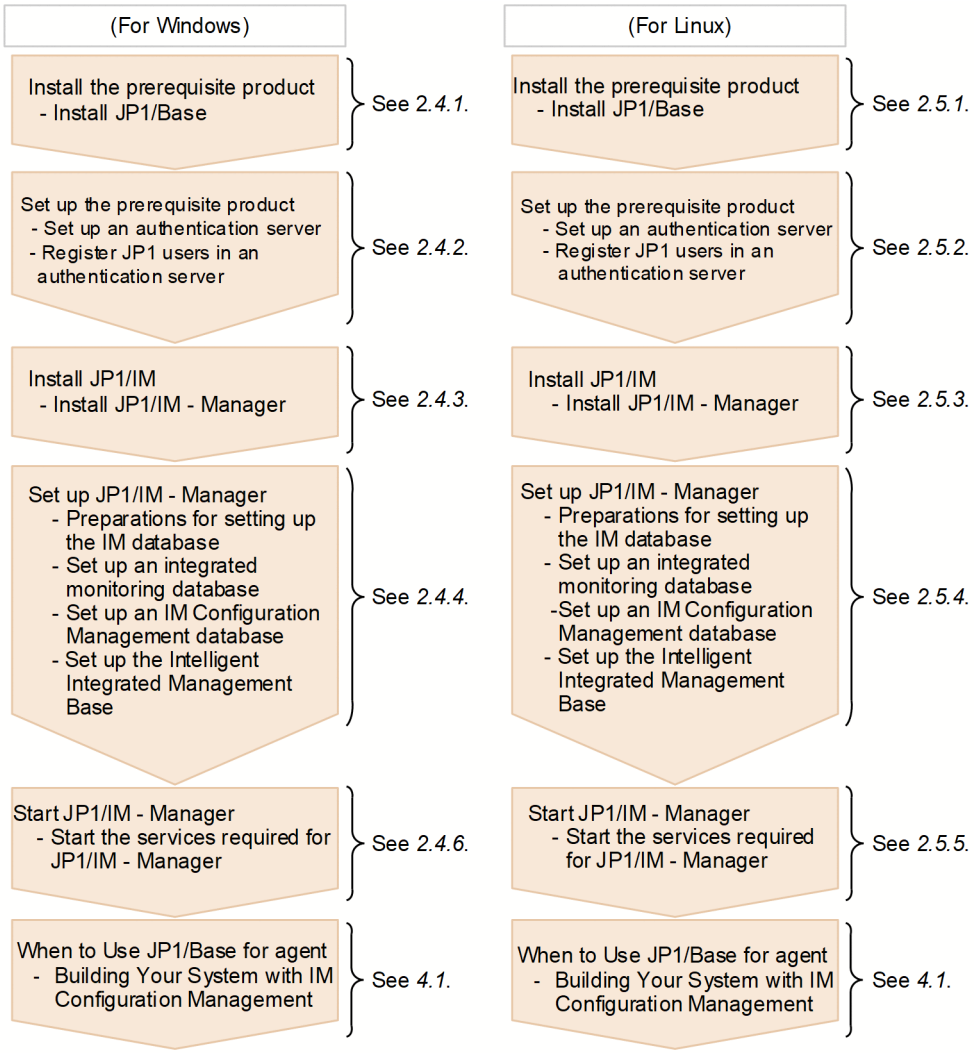
2.3 General procedures for installing and setting up JP1/IM

This section describes the installation and setup procedures, for each host type (manager, agent, or viewer).

For a manager:

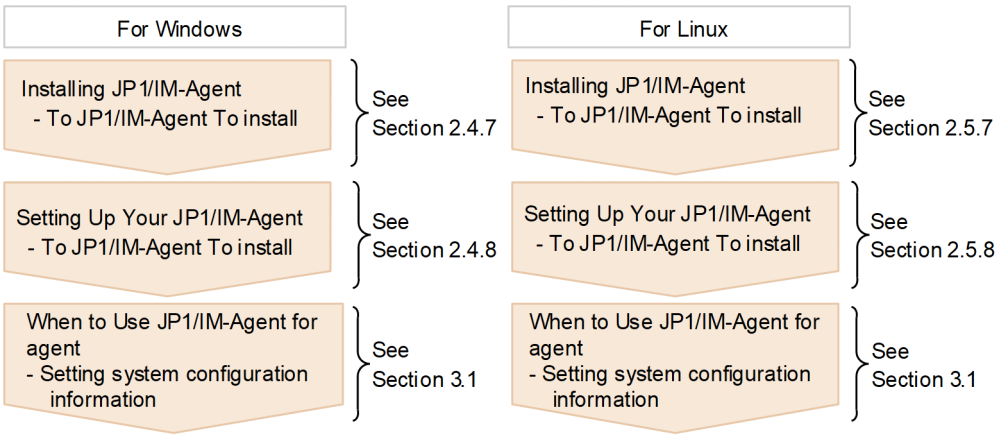
Install the prerequisite products, JP1/Base and JP1/IM - Manager. Set user authentication for JP1/Base to log in to JP1/IM - Manager, and then set up the IM database to use the JP1/IM - Manager functions described in this manual.

After installation and setup are complete, use IM Configuration Management to set the system hierarchy.



When agent is JP1/IM - Agent:

Install JP1/IM - Agent to manage the issued events with the manager.



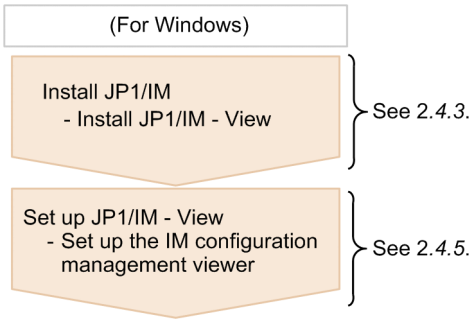
When agent is JP1/Base:

Install JP1/Base to allow the manager to manage events issued by the agent.

For a viewer (program that provides GUI):

Install JP1/IM - View to allow GUI operations for JP1/IM - Manager, and set up IM Configuration Management - View to allow GUI operations for IM Configuration Management.

Note that no viewer (program that provides GUI) is required to be installed when you want to use only the Intelligent Integrated Management Base.



2.4 Installation and setup (for Windows)

This section describes the installation and setup procedures required to start system monitoring with JP1/IM in Windows.

2.4.1 Installing the prerequisite product (for Windows)

Before you start system monitoring with JP1/IM, you need to install JP1/Base on the hosts used as managers. If you also use JP1/Base as an agent, install JP1/Base on agent hosts as well.

(1) Installing JP1/Base (for Windows)

On the hosts that will be used as the manager and agents in the system monitored by JP1/IM, perform a new installation of JP1/Base.

Prerequisites

The following conditions must be satisfied:

- JP1/Base supports the OS of the host on which the installation will be performed.
- The user who performs the installation has Administrator permissions.

Procedure

1. Insert the JP1/Base distribution media into the drive.
   Follow the instructions given by the installer after it starts. Specify the following items during installation:
   - User information
   - Installation folder
     The default installation folder is as follows:
     In an x86 environment:
     system-drive`:\Program Files\Hitachi\JP1Base`
     In an x64 environment:
     system-drive`:\Program Files (x86)\Hitachi\JP1Base`
     In an x64 environment, do not install JP1/Base under *system-drive*`:\Program Files\`. Problems might occur during operation if JP1/Base is in a `Program Files` folder that contains 64-bit modules. Do not install JP1/Base in the installation folder of any other product.
   - Automatic setup processing
     If the **Perform setup processing** check box is selected, initial setup is automatically performed so that you can use the program immediately after installation is complete. When the window for entering the OS user name and password for the installation target host appears, enter the OS user name and password. This OS user name and password will be used for user mapping with the JP1 user (`jp1admin`) registered during initial setup. For details about user mapping, see *4.2.1 Configuring user mapping*.
     This manual assumes that initial settings were configured by automatic setup unless otherwise indicated.
2. If you are prompted to restart the system, restart Windows.

2.4.2 Setting up the prerequisite product (for Windows)

This subsection describes the user authentication setup, which is included in the JP1/Base setup procedure.

(1) Setting up an authentication server (for Windows)

To log in to JP1/IM - Manager, you need to set up user authentication on the manager. You can set up a maximum of two authentication servers (primary and secondary).

If automatic setup processing was performed during installation of JP1/Base, the local host is set as the authentication server. If automatic setup processing was not performed, and you want to add and set up a host as an authentication server, or you want to set up a different host as an authentication server, perform the procedure below.

Prerequisites

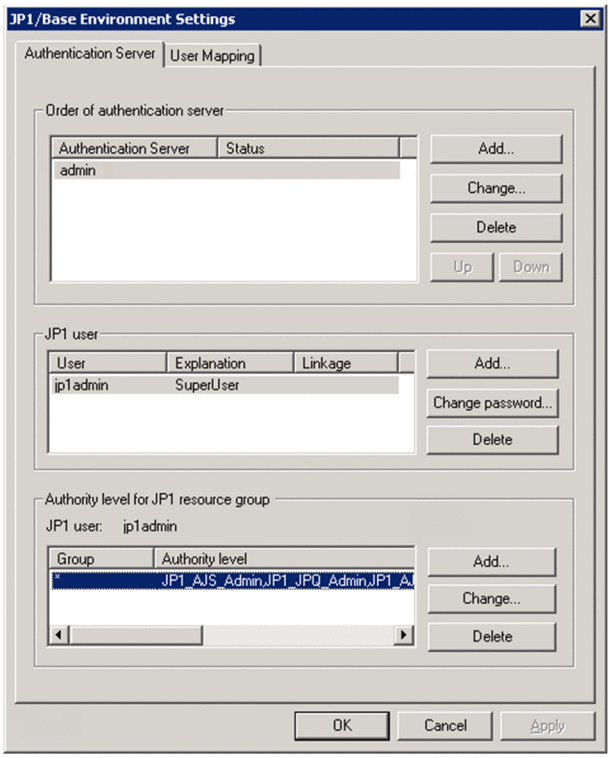
The host name of the host to be set up as an authentication server must be resolvable by using the `hosts` file or DNS server.

Procedure

1. From the Windows **Start** menu, select **All Programs**, **JP1_Base**, and then **JP1_Base Setup**. The JP1/Base Environment Settings dialog box appears.

2. In the **Order of authentication server** area, click the **Add** or **Change** button. The Authentication Server dialog box appears.

3. Enter the name of the host you want to set as the authentication server, and then click the **OK** button.
   In the **Order of authentication server** area, the host displayed at the top is the primary authentication server.



   If automatic setup processing was performed during installation of JP1/Base, the local host name has already been set as the authentication server name.

Related topics

- Description of user authentication settings in the *JP1/Base User's Guide*

(2) Registering JP1 users in an authentication server (for Windows)

Register JP1 users in the primary authentication server.

A JP1 user whose user name and password are `jp1admin` is automatically set during installation of JP1/Base. To add JP1 users, perform the procedure below.

Prerequisites

The primary authentication server must be specified.

Procedure

1. From the Windows **Start** menu, select **All Programs**, **JP1_Base**, and then **JP1_Base Setup**. The JP1/Base Environment Settings dialog box appears.
2. In the **Order of authentication server** area, click the host name of the primary authentication server to activate the **JP1 user** area.
3. In the **JP1 user** area, click the **Add** button to open the JP1 User dialog box.
4. Enter the JP1 user name and password, and then click the **OK** button.
   Register the JP1 user name and password according to the following rules:

Item	Number of bytes	Case-sensitive?	Permitted character string
JP1 user name	1 to 31 bytes	No	Alphanumeric characters and symbols (excluding * / \ " ' ^ [ ] { } ( ) : ; | = , + ? < > and spaces and tabs)
Password	6 to 32 bytes	Yes	Alphanumeric characters and symbols (excluding \ " : and spaces and tabs)

Related topics

- The procedure for using the GUI to set JP1 users in the *JP1/Base User's Guide*

(3) Operation permissions for JP1 users (for Windows)

Each JP1 user is assigned an operating permission called a *JP1 permission level*.

This manual assumes that the JP1 permission level for the system administrator (`jp1admin`) is `JP1_Console_Admin` and `JP1_CF_Admin`.

`JP1_Console_Admin` permission is needed to operate a central console and central scope.

`JP1_CF_Admin` permission is needed to operate IM Configuration Management.

If automatic setup processing was performed during installation of JP1/Base, the JP1 permission level required for the system administrator has already been set. If automatic setup processing was not performed or you want to register a JP1 user other than the system administrator, see the description of the operation permissions for JP1 users in the *JP1/Base User's Guide*.

Related topics

- *9.4.1 Managing JP1 users* in the *Overview and System Design Guide*

2.4.3 Installing JP1/IM (for Windows)

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

(1) Installing JP1/IM - Manager (for Windows)

After you log on with Administrator permissions to the machine on which JP1/IM - Manager will be installed, terminate all programs, and then install JP1/IM - Manager.

Prerequisites

The following conditions must be satisfied:

- JP1/IM - Manager supports the OS of the host on which the installation will be performed.
- The user who performs the installation has Administrator permissions.
- JP1/Base is installed.

Procedure

1. Terminate all programs.
   Before you start the installation, terminate all programs, and stop the JP1/Base services.
2. Insert the distribution media into the 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
   - Installation folder
     The following installation folders are created when you install JP1/IM - Manager:

Product	Folder that is created#	Description
JP1/IM - Manager	*installation-folder*\JP1IMM\	Stores JP1/IM - Manager information.
	installation-folder\JP1Cons\	Stores central console information.
	installation-folder\JP1Scope\	Stores central scope information.

     #: For the default *installation-folder*, see *G. Reference Material for this Manual*.
     Note that the drive specified as the installation folder for JP1/IM - Manager must be a fixed disk. You cannot install JP1/IM - Manager on a removable disk, network drive, or UNC path.
3. If you are prompted to restart the system, restart Windows.

(2) Installing JP1/IM - View (Windows only)

After you log on with Administrator permissions to the machine on which JP1/IM - View will be installed, terminate all programs, and then install JP1/IM - View.

Note that JP1/IM - View is not required to be installed when you want to use only the Intelligent Integrated Management Base.

Prerequisites

The following conditions must be satisfied:

- JP1/IM - View supports the OS of the viewer on which the installation will be performed.
- The user who performs the installation has Administrator permissions.

Procedure

1. Terminate all programs.
   Before you start the installation, terminate all programs.

2. Insert the distribution media into the 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 folder
     In an x64 environment, do not install JP1/IM under *system-drive*`:\Program Files\` (the `Program Files` folder that is not (`x86`) compatible).
     The following installation folder is created when you install JP1/IM - View:

Product	Folder that is created#	Description
JP1/IM - View	*installation-folder*`\JP1CoView\`	Stores JP1/IM - View information.

     #: For the default *installation-folder*, see *G. Reference Material for this Manual*.
     Note that the drive specified as the installation folder for JP1/IM - View must be a fixed disk. You cannot install JP1/IM - View on a removable disk, network drive, or UNC path.

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

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

You need to create and set up an integrated monitoring database to change the severity of events or consolidate a large number of events into one event. You also need to create and set up an IM Configuration Management database to use IM Configuration Management to manage the system hierarchy. These databases are generically called *IM databases*. This subsection describes how to create and set up IM databases.

The number of arguments for a command to be executed varies depending on whether the integrated monitoring database or the IM Configuration Management database is set up first. This manual describes the command arguments when the integrated monitoring database is installed first.

(1) Settings of the setup information file to be created (for Windows)

The following provides details about the settings specified in the setup information file that is created in *2.4.4(2) Preparations for setting up the IM database (for Windows)*.

Specification details

Specification	Description
`#IM DATABASE SERVICE - DB Size` `IMDBSIZE=S`	Specifies the size of the IM database to be created as `S`, `M`, or `L`. At installation, `S` is set.
`#IM DATABASE SERVICE - Data Storage Directory` `IMDBDIR=`*manager-path*`\database`	Specifies the absolute path of the directory in which data for the IM database is to be stored. Use a string of no more than 95 characters. At installation, *manager-path*`\database` is set. To change the value of `IMDBDIR`, do not specify a network drive (displayed in a list by `net use` executed from the command prompt) or Windows reserved device file (`AUX`, `CON`, `NUL`, `PRN`, `CLOCK$`, `COM[0-9]`, or `LPT[0-9]`).
`#IM DATABASE SERVICE - Port Number` `IMDBPORT=20700`	Specifies the port number used by the IM database. The range of permitted port numbers is from 5001 to 65535. At installation, `20700` is set.
`#IM DATABASE SERVICE - DB Install Directory` `IMDBENVDIR=`*manager-path*`\dbms`	Specifies the absolute path of the directory in which the IM database is to be installed. Use a string of no more than 195 characters. At installation, *manager-path*`\dbms` is set. To change the value of `IMDBENVDIR`, do not specify a network drive (displayed in a list by `net use` executed from the command prompt) or Windows reserved device file (`AUX`, `CON`, `NUL`, `PRN`, `CLOCK$`, `COM[0-9]`, or `LPT[0-9]`).

Related topics

- *14.1.3 Estimating IM database capacity requirements* in the *Overview and System Design Guide*

(2) Preparations for setting up the IM database (for Windows)

You need to prepare a *setup information file* that specifies the size of the database area required to set up an IM database and information about the database storage directory.

Prerequisites

The following conditions must be satisfied:

- JP1/IM - Manager is installed on the manager.
- The OS user has Administrator permissions.

Procedure

1. Edit the setup information file (`jimdbsetupinfo.conf`).

   The setup information file is created during installation of JP1/IM - Manager. However, you do not have to change the default settings unless you want to do something not covered by this manual.

   The setup information file is stored in:

   Manager-path`\conf\imdb\setup\`

Related topics

- *1.4.1 Preparations for creating IM databases (for Windows)* in the *Configuration Guide*
- *Setup information file (jimdbsetupinfo.conf)* in *2. Definition Files* in the *Command, Definition File and API Reference*

(3) Setting up an integrated monitoring database (for Windows)

Create an integrated monitoring database and set it up for use with the central console functions.

Prerequisites

The following conditions must be satisfied:

- Sufficient disk space for creating an integrated monitoring database is allocated to the drive on which JP1/IM - Manager is installed.
- The OS user who will execute the `jcodbsetup` and `jcoimdef` commands has Administrator permissions.

Procedure

1. Execute the following `jcodbsetup` command to create an integrated monitoring database:
   `"`*Console-path*`\bin\jcodbsetup" -f` *setup-information-file-name* `-q`
   If the UAC function is enabled, execute the command from the administrator console.
   It might take a long time to execute this command.
   The IM database service is created at this time.
2. Execute the following `jcoimdef` command to enable the integrated monitoring database:
   `"`*Console-path*`\bin\jcoimdef" -db ON`
3. Restart the JP1/IM3-Manager service.

Related topics

- *1.4.2 Setting up the integrated monitoring database (for Windows)* in the *Configuration Guide*
- *jcodbsetup* in *1. Commands* in the *Command, Definition File and API Reference*
- *jcoimdef* in *1. Commands* in the *Command, Definition File and API Reference*

(4) Setting up an 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.

Prerequisites

The following conditions must be satisfied:

- Sufficient disk space for creating an IM Configuration Management database is allocated to the drive on which JP1/IM - Manager is installed.
- The OS user who will execute the `jcodbsetup` and `jcoimdef` commands has Administrator permissions.

If the integrated monitoring database has already been set up according to *2.4.4(3) Setting up an integrated monitoring database (for Windows)* (the setup procedure described in this manual), the following condition must also be satisfied:

- The status of the IM database service is **Running**.

Procedure

1. Stop the JP1/IM3-Manager service.
2. Execute the following `jcfdbsetup` command to create an IM Configuration Management database:
   `"`*Manager-path*`\bin\imdb\jcfdbsetup" -s -q`
   If the UAC function is enabled, execute the command from the administrator console.
   It might take a long time to execute this command.

3. Execute the following `jcoimdef` command to enable the IM Configuration Management service (`jcfmain`):
   "*Console-path*\bin\jcoimdef" -cf ON
4. Start JP1/IM - Manager.

Related topics

- *1.4.3 Setting up the IM Configuration Management database (for Windows)* in the *Configuration Guide*
- *jcfdbsetup* in *1. Commands* in the *Command, Definition File and API Reference*
- *jcoimdef* in *1. Commands* in the *Command, Definition File and API Reference*

(5) Setting Up Intelligent Integrated Management Database (for Windows)

Create a Intelligent Integrated Management Database and configure it to use Intelligent Integrated Management Database with Intelligent Integrated Management Base.

Prerequisites

The following conditions must be met:

- The amount of disk space required to create an Intelligent Integrated Management Database is reserved on the drive where JP1/IM - Manager is installed.
- OS that executes `jimgndbsetup` command-user has Administrators privileges.

Operating procedure

1. Shut down JP1/IM3-Manager servicing.
2. Edits Intelligent Integrated Management Database setup information file (`jimgndbsetupinfo.conf`).
3. Run the following `jimgndbsetup` command to create an Intelligent Integrated Management Base database.
   "*Manager-path*\bin\imgndb\jimgndbsetup" -f *Intelligent-Integrated-Management-Database-setup-information-file-name* -q
4. Start JP1/IM3-Manager service.

Related topics

- *1.5 Construction of Intelligent Integrated Management Database (for Windows)* in the *Configuration Guide*
- *1. jimgndbsetup* in the *Command, Definition File and API Reference*

(6) Setting up the Intelligent Integrated Management Base (for Windows)

Configure the service of the Intelligent Integrated Management Base (`jddmain`) so that it can be started from process management.

Prerequisites

The following conditions must be satisfied:

- An integrated monitoring database is set up.
- Intelligent Integrated Management Database is set up.
- The OS user who will execute the `jcoimdef` command has Administrator permissions.

Procedure

1. Stop the JP1/IM3-Manager service.
2. Execute the following `jcoimdef` command to enable the service of the Intelligent Integrated Management Base (`jddmain`):
   `"`*Console-path*`\bin\jcoimdef" -dd ON -hostmap ON`
3. Ensure that the integrated monitoring database is running.
4. Setup the Intelligent Integrated Management Base definition file (`imdd.properties`) In the intelligent integrated management infrastructure definition file (`imdd.properties`),specify the value specified in IMDBPORT of the setup information file (`jimdbsetupinfo.conf`) used when setting up the integrated monitoring database.
   If there is no change from the IMDBPORT default value of `20700`,addition to the integrated management infrastructure definition file is unnecessary.
   `jp1.im.db.DEFAULT.portNo =` *IMDBPORT-setting-value*
5. Define the hierarchical structure of the system in the system node definition file (`imdd_systemnode.conf`).
6. Define the names of the IM management nodes in the management group that are used when collected data is displayed in the sunburst or tree chart, in the category name definition file for IM management nodes (`imdd_category_name.conf`).
7. Restart the JP1/IM3 - Manager service.
8. Execute the `jddsetaccessuser` command to configure the users who can access the monitored products when system configuration information is collected.
9. Define the linked products and the name of the hosts from which configuration information of the monitoring objects in the linked products is collected, in the target host definition file for configuration collection (`imdd_target_host.conf`).
10. Execute the `jddcreatetree` command.
11. Define the relationships between IM management nodes in the IM management node link definition file (`imdd_nodeLink_def.conf`).
12. Execute the `jddupdatetree` command.

Related topics

- *1.4.2 Setting up the integrated monitoring database (for Windows)* in the *Configuration Guide*
- *1.5.2 Settings of Intelligent Integrated Management Database (for Windows)* in the *Configuration Guide*
- *jcoimdef* in *1. Commands* in the *Command, Definition File and API Reference*
- *jddsetaccessuser* in *1. Commands* in the *Command, Definition File and API Reference*
- *jddcreatetree* in *1. Commands* in the *Command, Definition File and API Reference*
- *jddupdatetree* in *1. Commands* in the *Command, Definition File and API Reference*
- *System node definition file (imdd_systemnode.conf)* in *2. Definition Files* in the *Command, Definition File and API Reference*
- *Category name definition file for IM management nodes (imdd_category_name.conf)* in *2. Definition Files* in the *Command, Definition File and API Reference*

- *Target host definition file for configuration collection (imdd_target_host.conf)* in *2. Definition Files* in the *Command, Definition File and API Reference*
- *IM management node link definition file (imdd_nodeLink_def.conf)* in *2. Definition Files* in the *Command, Definition File and API Reference*

2.4.5 Setting up JP1/IM - View (Windows only)

No specific setup procedure is required to use JP1/IM - View.

2.4.6 Starting JP1/IM - Manager (for Windows)

To use the JP1/IM - Manager functions normally, you need to start the services in the predefined order. This subsection describes how to start JP1/IM - Manager.

(1) Starting the services required for JP1/IM - Manager (for Windows)

To start system monitoring on the manager, start the JP1/Base services, and then start the JP1/IM - Manager services. Skip the step for any service that is already running.

Prerequisites

The following conditions must be specified:

- JP1/Base is installed and set up on the manager.
- JP1/IM - Manager is installed and set up on the manager.
- If you use JP1/IM - Agent for agent, JP1/IM - Agent must be installed and set up.
- The OS user has Administrator permissions.

Procedure

1. From the Windows **Start** menu, select **Control Panel**, **Administrative Tools**, and then **Services**. Then start the Service Control Manager.
2. Start the JP1/Base Event service.
3. Start the JP1/Base EventlogTrap service.
4. Start the JP1/Base LogTrap service.
5. Start the JP1/Base service.
6. Start the JP1/IM3 - Manager DB Server service.
7. Start JP1/IM3 - Manager Trend Data Management Services servicing.
   JP1/IM3-Manager Intelligent Integrated DB Server services are started automatically in conjunction with each other.
8. Start the JP1/IM3 - Manager service.

2.4.7 Installing JP1/IM - Agent (for Windows)

Install JP1/IM - Agent on agent. This section describes how to install a new JP1/IM - Agent.

(1) Install from agent package (for Windows)

Inside the system monitored by JP1/IM, JP1/IM - Agent is newly installed on the host to be agent. To install, use agent package downloaded from the manager.

Agent package is registered automatically when the manager is installed.

Prerequisites

The following conditions must be met:

- OS of hosts to be installed is JP1/IM - Agent premise OS.
- OS person who performs the install has Administrators privileges.
- The Intelligent Integrated Management Base is set up.
- JP1/IM3 - Manager servicing is running.
- JP1 user used to log in has the required permissions assigned.

Operating procedure

1. Log in to the host where you want to install JP1/IM - Agent.
2. Run REST API to download agent package that is registered with the manager.
   The following shows a sample file-retrieval using curl command.
   `curl -OL -H "Authorization: Bearer` *token*`" -H "Cookie: JSESSIONID=`*Session-ID*`" -v http://`*JP1/IM-Manager-hostname*`:20703/download/imagent/`*agent-package-filename*
   Tokens and session ID are obtained by issuing a login REST API.
   `curl -X POST -H "Content-Type: application/json" -d "{\"user\": \"`*username*`\", \"password\": \"`*password*`\"}" -v http://`*JP1/IM-Manager-hostname*`:20703/im/api/v1/login`
   It is recommended to issue a logout REST API immediately after completion.
   `curl -X POST -H "Content-Type: application/json" -H "Cookie: JSESSIONID=`*Session ID*`" -v http://`*JP1/IM-Manager-hostname*`:20703/im/api/v1/logout`
3. Unzip the downloaded agent package.
   Here is an example of how to decompress:
   `Expand-Archive-Path jp1_pc_agent_windows_`*Version-number-of-JP1/IM(VVRRSS-format)*`.zip`
4. Start the installer.
   Follow the instructions of the booted installer to proceed with the installation. During installation, set the following items:
   - User information
   - Installation folder
     The default installation folder settings are as follows:
     System-drive`\Program Files\Hitachi\`

The characters that can be specified as the install destination are 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 for folder name.

#2: Characters used to separate drives and folders. Cannot be used for folder name.

- Installation Mode

  Select [Normal Install Mode].

  The following need to be configured.

  - Host name of the destination manager host

  Specify the host name of the destination manager host that manages integrated agent to be newly installed.

  - Initial secret

  Initial secret is checked (issued) from the integrated operation viewer using the following steps.

  1. Log in to the integrated operation viewer and click **Issue initial secret** from the **Option** menu to open the Show Initial Secret window.

  2. Click the **Issue** button in the Show Initial Secret window, and click the **OK** button in the window for confirming the issuance of initial secret. Clicking the **OK** button issues initial secret.

  3. You can store the issued initial secret in any file. You can use it to install JP1/IM - Agent on other agent hosts.

5. If you are prompted to restart, restart Windows.

Related topics

- *1.3.1(3)(c) Initialization environment variable used by the installer* in the *Configuration Guide*
- *1.3.1 Installation procedure (for Windows)* in the *Configuration Guide*
- *1.2.1 Login window of the Intelligent Integrated Management Base* in the *GUI Reference*
- *2.1 Overview of the Integrated Operation Viewer window* in the *GUI Reference*
- *2.2.3 Show Initial Secret window* in the *GUI Reference*

(2) Install from the provided media (for Windows)

Inside the system monitored by JP1/IM, install a new JP1/IM - Agent on agent host.

Prerequisites

The following conditions must be met:

- OS of hosts to be installed is JP1/IM - Agent premise OS.
- OS person who performs the install has Administrators privileges.

Operating procedure

1. Shut down JP1/IM - Agent servicing.
2. Put JP1/IM - Agent offering medium into the drive.

   Follow the instructions of the booted installer to proceed with the installation. During installation, set the following items:

   - User information
   - Installation folder

     The default installation folder settings are as follows:

System-drive\Program Files\Hitachi\

Do not specify folders that contain symbols (such as ; # ' %) or character codes outside SJIS character code range (JIS level 3 and level 4) in the install location.

- Installation Mode

  Select [Normal Install Mode].

  The following need to be configured.

  - Host name of the destination manager host

  Specify the host name of the destination manager host that manages integrated agent to be newly installed.

  - Initial secret

  Initial secret is checked (issued) from the integrated operation viewer using the following steps.

  1. Log in to the integrated operation viewer and click **Issue initial secret** from the **Option** menu to open the Show Initial Secret window.

  2. Click the **Issue** button in the Show Initial Secret window, and click the **OK** button in the window for confirming the issuance of initial secret. Clicking the **OK** button issues initial secret.

  3. You can store the issued initial secret in any file. You can use it to install JP1/IM - Agent on other agent hosts.

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

Related topics

- *1.3.1(3)(c) Initialization environment variable used by the installer* in the *Configuration Guide*
- *1.3.1 Installation procedure (for Windows)* in the *Configuration Guide*
- *1.2.1 Login window of the Intelligent Integrated Management Base* in the *GUI Reference*
- *2.1 Overview of the Integrated Operation Viewer window* in the *GUI Reference*
- *2.2.3 Show Initial Secret window* in the *GUI Reference*

2.4.8 Setting up JP1/IM - Agent (for Windows)

Enables JP1/IM - Agent services (jpc_imagent) to be started from Process Management.

Prerequisites

The following conditions must be met:

- OS that executes the jpc_service command-user has Administrators privileges.

Operating procedure

1. Stop JP1/IM - Agent servicing by running the following command:
   jpc_service_stop -s all

2. Run the following command to enable servicing for JP1/IM - Agent:
   Agent-path\tools\jpc_service -on [*service-name*]
   The service name specifies the service name of JP1/IM - Agent to register.

3. Verify that JP1/IM - Agent serviceis registered by running the following command:
   services.msc
   You can check the services in management console. If the service exists, the service is valid.

4. Run the following command to start JP1/IM - Agent services:
   ```
   jpc_service_start -s all
   ```

Related topics

- *1.21 Setup for JP1/IM - Agent (for Windows)* in the *Configuration Guide*
- *1. Commands related to the JP1/IM - Agen*t in the *Command, Definition File and API Reference*

2.5 Installation and setup (for Linux)

This section describes the installation and setup procedures required to start system monitoring with JP1/IM in Linux.

2.5.1 Installing the prerequisite product (for Linux)

Prior to monitoring the system with JP1/IM, you must install JP1/Base on the host you are managing. If you also use JP1/Base as an agent, install JP1/Base on agent host as well.

(1) Installing JP1/Base (for Linux)

On the hosts that will be used as the manager and agents in the system monitored by JP1/IM, perform a new installation of JP1/Base.

Prerequisites

The following conditions must be satisfied:

- JP1/Base supports the OS of the host on which the installation will be performed.
- The OS user who performs the installation has `root` permissions.
- The host name at the installation destination can be resolved with an IP address in the connected LAN environment.

Procedure

1. Terminate all programs.
   Before you install JP1/Base, terminate all JP1 programs.
2. Insert the JP1/Base distribution media into the drive.
3. Execute the following command to install and start the Hitachi Program Product Installer:
   /cdrom/XXXX/`setup` */cdrom*
   XXXX varies depending on your OS. For */cdrom*, specify the device special file name for the drive on which the distribution media is automatically mounted.
   When the Hitachi Program Product Installer starts, the following initial window appears:

```
    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.
    +-------------------------------------------------------------------+
```

4. In the initial window of the Hitachi Program Product Installer, enter **I** to display a list of software programs.
5. In the list of software programs, move the cursor to `JP1/Base`, and then press the space bar to select it.
6. In the Hitachi Program Product Installer window, enter **I** to start installation of JP1/Base.

Initial setup is automatically performed so that you can use JP1/Base immediately after installation is completed.

7. After installation is completed, enter **Q** to return to the initial window.

8. Terminate the Hitachi Program Product Installer, and then create an automated startup script for JP1/Base.
   Execute the command as follows:
   ```
   cd /etc/opt/jp1base
   cp -p jbs_start.model jbs_start
   ```

2.5.2 Setting up the prerequisite product (for Linux)

The following describes how to set up an authentication server when JP1/Base has been installed in Linux.

(1) Setting up an authentication server (for Linux)

To log in to JP1/IM - Manager, you need to set up user authentication on the manager. You can set a maximum of two authentication servers (primary and secondary).

The local host is set as an authentication server during installation of JP1/Base. To set a different host as an authentication server, perform the procedure below.

Prerequisites

The following conditions must be satisfied:

- The host name of the host to be set up as an authentication server can be resolved by using the `hosts` file or DNS server.
- The OS user who will execute the `jbssetusrsrv` command has `root` permissions.

Procedure

1. Specify the following `jbssetusrsrv` command on the host you want to specify as the authentication server:
   `/opt/jp1base/bin/jbssetusrsrv` *primary-authentication-server* [*secondary-authentication-server*]

Related topics

- Description of the settings of user authentication in the *JP1/Base User's Guide*

(2) Registering JP1 users in an authentication server (for Linux)

Register JP1 users in the primary authentication server.

A JP1 user whose user name and password are `jp1admin` is automatically set during installation of JP1/Base. To add JP1 users, perform the procedure below.

Prerequisites

The following conditions must be satisfied:

- The primary authentication server is specified.
- The OS user who will execute the `jbsadduser` command has `root` permissions.

Procedure

1. On the host specified as the primary authentication server, execute the following `jbsadduser` command to register a JP1 user to the authentication server:

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

   Specify the JP1 user name according to the following rules:

Item	Number of bytes	Case-sensitive?	Permitted character string
JP1 user name	1 to 31 bytes	No	Alphanumeric characters and symbols (excluding * / \ " ' ^ [ ] { } ( ) : ; | = , + ? < > and spaces and tabs)

2. After executing the `jbsadduser` command, follow the instructions to enter the password.

   Specify the password according to the following rules:

Item	Number of bytes	Case-sensitive?	Permitted character string
Password	6 to 32 bytes	Yes	Alphanumeric characters and symbols (excluding \ " : and spaces and tabs)

   Note that `jp1admin` is automatically set for both the JP1 user name and password during installation of JP1/Base.

Related topics

- Description about the `jbsadduser` command in the *JP1/Base User's Guide*

(3) Operation permissions for JP1 users (for Linux)

Each JP1 user is assigned an operating permission called a *JP1 permission level*.

This manual assumes that the JP1 permission level for the system administrator (`jp1admin`) is `JP1_Console_Admin` and `JP1_CF_Admin`.

`JP1_Console_Admin` permission is needed to operate a central console and central scope.

`JP1_CF_Admin` permission is needed to operate IM Configuration Management.

The JP1 permission level required for the system administrator is automatically set during installation of JP1/Base. To register a JP1 user other than the system administrator, see the description of the operation permissions for JP1 users in the *JP1/Base User's Guide*.

Related topics

- *9.4.1 Managing JP1 users* in the *Overview and System Design Guide*

2.5.3 Installing JP1/IM (for Linux)

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

(1) Installing JP1/IM - Manager (for Linux)

After you log on with `root` permissions to the machine on which JP1/IM - Manager will be installed, terminate all programs, and then install JP1/IM - Manager.

Prerequisites

The following conditions must be satisfied:

- JP1/IM - Manager supports the OS of the host on which the installation will be performed.
- The OS user who performs the installation has `root` permissions.
- JP1/Base is installed.

Procedure

1. Terminate all programs.
   Before you start the installation, terminate all programs, and stop the JP1/Base services.
2. Insert the JP1/IM - Manager distribution media into the drive.
3. Execute the following command to install and start the Hitachi Program Product Installer:

   ```
   /cdrom/XXXX/setup /cdrom
   ```

   XXXX varies depending on your operating environment. For */cdrom*, specify the device special file name for the drive on which the distribution media is automatically mounted.
   When the Hitachi Program Product Installer starts, the following initial window appears.

   ```
   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.
   +-------------------------------------------------------------------+
   ```

4. In the initial window of the Hitachi Program Product Installer, enter **I** to display a list of software programs.
5. In the list of software programs, move the cursor to `JP1/Integrated Manager 3 - Manager`, and then press the space bar to select it.
6. In the Hitachi Program Product Installer window, enter **I** to start installation of JP1/IM - Manager.
7. After installation is complete, enter **Q** to return to the initial window.
8. Terminate the Hitachi Program Product Installer, and then create an automated startup script for JP1/IM - Manager.
   Execute the command as follows:

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

2.5.4 Setting up JP1/IM - Manager (for Linux)

You need to create and set up an integrated monitoring database to change the severity of events or consolidate a large number of events into one event. You also need to create and set up an IM Configuration Management database to use

IM Configuration Management to manage the system hierarchy. These databases are generically called *IM databases*. This subsection describes how to create and set up IM databases.

The number of arguments for a command to be executed varies depending on whether the integrated monitoring database or the IM Configuration Management database is set up first. This manual describes the command arguments when the integrated monitoring database is installed first.

(1) Settings of the setup information file to be created (for Linux)

The following provides details about the settings specified in the the setup information file that is created in *2.5.4(2) Preparations for setting up the IM database (for Linux)*.

Specification details

Specification	Description
`#IM DATABASE SERVICE - DB Size` `IMDBSIZE=S`	Specifies the size of the IM database to be created as `S`, `M`, or `L`. At installation, `S` is set.
`#IM DATABASE SERVICE - Data Storage Directory` `IMDBDIR=/var/opt/jp1imm/database`	Specifies the absolute path of the directory in which data for the IM database is to be stored. Use a string of no more than 95 characters. At installation, `/var/opt/jp1imm/database` is set. To change the value of `IMDBDIR`, do not specify a path that contains a symbolic link (a file that is retrieved by executing `find / -type l`).
`#IM DATABASE SERVICE - Port Number` `IMDBPORT=20700`	Specifies the port number used by the IM database. The range of permitted port numbers is from 5001 to 65535. At installation, `20700` is set.
`#IM DATABASE SERVICE - DB Install Directory` `IMDBENVDIR=/var/opt/jp1imm/dbms`	Specifies the absolute path of the directory in which the IM database is to be installed. Use a string of no more than 123 characters. At installation, `/var/opt/jp1imm/dbms` is set. To change the value of `IMDBENVDIR`, do not specify a path that contains a symbolic link (a file that is retrieved by executing `find / -type l`).

Related topics

- *15.1.3 Estimating IM database capacity requirements* in the *Overview and System Design Guide*

(2) Preparations for setting up the IM database (for Linux)

The following describes s preparations for setting up the IM database in Linux. You need to prepare a *setup information file* that specifies the size of the database area required to set up an IM database and information about the database storage directory.

Prerequisites

JP1/IM - Manager must be installed on the manager.

Procedure

1. Edit the setup information file (`jimdbsetupinfo.conf`).

   The setup information file is created during installation. For activities described in this manual, you do not need to change the settings created during installation.

   The setup information file is stored in:
   `/etc/opt/jp1imm/conf/imdb/setup/`

Related topics

- *2.4.1 Preparations for creating IM databases (for UNIX)* in the *Configuration Guide*
- *Setup information file (jimdbsetupinfo.conf)* in *2. Definition Files* in the *Command, Definition File and API Reference*

(3) Setting up an integrated monitoring database (for Linux)

Create an integrated monitoring database and set it up for use with the central console functions.

Prerequisites

The following conditions must be satisfied:

- Sufficient disk space for creating an integrated monitoring database is allocated.
- The OS user who will execute the `jcodbsetup` and `jcoimdef` commands has `root` permissions.

Procedure

1. Execute the following `jcodbsetup` command to create an integrated monitoring database.
   `/opt/jp1cons/bin/jcodbsetup -f` *setup-information-file-name* `-q`
   It might take a long time to execute this command. The IM database service is created at this time.
2. Execute the following `jcoimdef` command to enable the integrated monitoring database:
   `/opt/jp1cons/bin/jcoimdef -db ON`
3. Restart the JP1/IM3-Manager service.

Related topics

- *2.4.2 Setting up the integrated monitoring database (for UNIX)* in the *Configuration Guide*
- *jcodbsetup* in *1. Commands* in the *Command, Definition File and API Reference*
- *jcoimdef* in *1. Commands* in the *Command, Definition File and API Reference*

(4) Setting up an IM Configuration Management database (for Linux)

Create an IM Configuration Management database and set it up so that the IM Configuration Management service can be started from process management.

Prerequisites

The following conditions must be satisfied:

- JP1/IM - View has stopped.
- Sufficient disk space for creating an IM Configuration Management database is allocated.
- The OS user who will execute the `jcfdbsetup` and `jcoimdef` commands has `root` permissions.

If the integrated monitoring database has already been set up according to the setup procedure in *2.5.4(3) Setting up an integrated monitoring database (for Linux)*, the following condition must also be satisfied:

- The status of the IM database service is **Running**.

Procedure

1. Stop the JP1/IM3 - Manager service.
2. Execute the following `jcfdbsetup` command to create an IM Configuration Management database:
   `/opt/jp1imm/bin/imdb/jcfdbsetup -s -q`
   It might take a long time to execute this command.
3. Execute the following `jcoimdef` command to enable the IM Configuration Management service (`jcfmain`):
   `/opt/jp1cons/bin/jcoimdef -cf ON`
4. Start JP1/IM - Manager.

Related topics

- *2.4.3 Setting up the IM Configuration Management database (for UNIX)* in the *Configuration Guide*
- *jcfdbsetup* in *1. Commands* in the *Command, Definition File and API Reference*
- *jcoimdef* in *1. Commands* in the *Command, Definition File and API Reference*

(5) Setting Up Intelligent Integrated Management Database (for Linux)

Create an Intelligent Integrated Management Database and configure it to use Intelligent Integrated Management Database with Intelligent Integrated Management Base.

Prerequisites

The following conditions must be met:

- The amount of disk space required to create an Intelligent Integrated Management Database is reserved on the drive where JP1/IM - Manager is installed.
- OS that executes `jimgndbsetup` command-user has root privileges.

Operating procedure

1. Shut down JP1/IM3 - Manager servicing.
2. Edits Intelligent Integrated Management Database setup information file (`jimgndbsetupinfo.conf`).
3. Run the following `jimgndbsetup` command to create Intelligent Integrated Management Base database.
   `/opt/jp1imm/bin/imgndb/jimgndbsetup" -f` *Intelligent-Integrated-Management-Database-setup-information-file-name* `-q`
4. Restart JP1/IM3-Manager service.

Related topics

- *2.5 Construction of Intelligent Integrated Management Database (for UNIX)* in the *Configuration Guide*
- *jimgndbsetup* in *1. Commands* in the *Command, Definition File and API Reference*

(6) Setting up the Intelligent Integrated Management Base (for Linux)

Configure the service of the Intelligent Integrated Management Base (`jddmain`) so that it can be started from process management.

Prerequisites

The following conditions must be satisfied:

- Integrated Monitoring DB and Intelligent Integrated Management Database are set up.
- The OS user who will execute the `jcoimdef` command has `root` permissions.

Procedure

1. Stop the JP1/IM3-Manager service.
2. Execute the following `jcoimdef` command to enable the service of the Intelligent Integrated Management Base:
   `/opt/jp1cons/bin/jcoimdef -dd ON -hostmap ON`
3. Ensure that the integrated monitoring database is running.
4. Edit the Intelligent Integrated Management Base definition file.
   Specify the value specified for "IMDBPORT" in the setup information file (`jimdbsetupinfo.conf`) used when setting up the integrated monitoring DB in the Intelligent Integrated Management Platform Definition File (`imdd.properties`).
   If there is no change from the IMDBPORT default value of 20700, it is not necessary to specify it in the Intelligent Integrated Management Platform definition file.
5. Define the hierarchical structure of the system in the system node definition file (`imdd_systemnode.conf`).
6. Define the names of the IM management nodes in the management group that are used when collected data is displayed in the sunburst or tree chart, in the category name definition file for IM management nodes (`imdd_category_name.conf`).
7. Restart the JP1/IM3 - Manager service.
8. Execute the `jddsetaccessuser` command to configure the users who can access the monitored products when system configuration information is collected.
9. Define the linked products and the name of the hosts from which configuration information of the monitoring objects in the linked products is collected, in the target host definition file for configuration collection (`imdd_target_host.conf`).
10. Execute the `jddcreatetree` command.
11. Define the relationships between IM management nodes in the IM management node link definition file (`imdd_nodeLink_def.conf`).
12. Execute the `jddupdatetree` command.

Related topics

- *2.4.2 Setting up the integrated monitoring database (for UNIX)* in the *Configuration Guide*
- *2.5.2 Settings of Intelligent Integrated Management Database (for UNIX)* in the *Configuration Guide*
- *jcoimdef* in *1. Commands* in the *Command, Definition File and API Reference*
- *jddsetaccessuser* in *1. Commands* in the *Command, Definition File and API Reference*
- *jddcreatetree* in *1. Commands* in the *Command, Definition File and API Reference*
- *jddupdatetree* in *1. Commands* in the *Command, Definition File and API Reference*

- *System node definition file (imdd_systemnode.conf)* in *2. Definition Files* in the *Command, Definition File and API Reference*
- *Category name definition file for IM management nodes (imdd_category_name.conf)* in *2. Definition Files* in the *Command, Definition File and API Reference*
- *Target host definition file for configuration collection (imdd_target_host.conf)* in *2. Definition Files* in the *Command, Definition File and API Reference*
- *IM management node link definition file (imdd_nodeLink_def.conf)* in *2. Definition Files* in the *Command, Definition File and API Reference*

2.5.5 Starting JP1/IM - Manager (for Linux)

In order to use the JP1/IM - Manager functions normally, you need to start the services in the predefined order. This subsection describes how to start JP1/IM - Manager.

(1) Starting the services required for JP1/IM - Manager (for Linux)

To start system monitoring on the manager, execute the automated startup script for JP1/Base, and then start the automated startup script for JP1/IM - Manager. Skip the step for a product that is already running.

Prerequisites

The following conditions must be specified:

- JP1/Base is installed and set up on the manager.
- JP1/IM - Manager is installed and set up on the manager.
- The OS user has `root` permissions.

Procedure

1. Execute the `/etc/opt/jp1base/jbs_start` script.
   JP1/Base starts.
2. Execute the `/etc/opt/jp1cons/jco_start` script.
   JP1/IM - Manager starts.

2.5.6 Installing JP1/IM - Agent (for Linux)

Install JP1/IM - Agent on agent. This section describes how to install a new JP1/IM - Agent.

(1) Install from agent package (for Linux)

Inside the system monitored by JP1/IM, JP1/IM - Agent is newly installed on the host to be agent. To install, use agent package downloaded from the manager.

Agent package is registered automatically when the manager is installed.

Prerequisites

The following conditions must be met:

- OS of hosts to be installed is JP1/IM - Agent premise OS.
- OS person who performs the install has root privileges.
- The default environment variable is set for the host to be installed.
- The Intelligent Integrated Management Base is set up.
- JP1/IM - Manager is running.
- JP1 user used to log in has the required permissions assigned.

Operating procedure

1. Log in to the host where you want to install JP1/IM - Agent.
2. Run REST API to download agent package that is registered with the manager.
   The following shows a sample file-retrieval using curl command.
   ```
   curl -OL -H "Authorization: Bearer token" -H "Cookie: JSESSIONID=Session ID"
   -v http://JP1/IM - Manager hostname:20703/download/imagent/ JP1/IM - Agent
   package filename
   ```
   Tokens and session ID are obtained by issuing a login REST API.
   ```
   curl -X POST -H "Content-Type: application/json" -d '{"user":
   "username", "password": "password"}' -v http://JP1/IM - Manager
   hostname:20703/im/api/v1/login
   ```
   It is recommended to issue a logout REST API immediately after completion.
   ```
   curl -X POST -H "Content-Type: application/json" -H "Cookie:
   JSESSIONID=Session ID" -v http://JP1/IM - Manager hostname:
   20703/im/api/v1/logout
   ```
3. Unzip the downloaded agent package.
   Here is an example of how to decompress:
   ```
   tar -zxvf jp1_pc_agent_linux_JP1/IM - Agent version number
   (VVRRSS format).tar.gz
   ```
4. Start the installer.
   Follow the instructions of the booted installer to proceed with the installation.
5. After the installation is complete, configure JP1/IM - Agent servicing.

Related topics

- *1.3.1(3)(c) Initialization environment variable used by the installer* in the *Configuration Guide*
- *2.3.1 Installation Procedure (for UNIX)* in the *Configuration Guide*

(2) Install from the provided media (for Linux)

Inside the system monitored by JP1/IM, install a new JP1/IM - Agent on agent host.

Prerequisites

The following conditions must be met:

- OS of hosts to be installed is JP1/IM - Agent premise OS.
- OS person who performs the install has root privileges.

- Intelligent Integrated Management Base is set up.
- The default environment variable is set for the host to be installed.

Operating procedure

1. Exit the program.
2. Put JP1/IM - Agent offering medium into the drive.
3. Install and start Hitachi PP Installer by running the following command:
   `/cdrom/XXXX/setup/cdrom`
   The part of XXXX depends on your OS. In addition, specify the device special name that is automatically mounted in "/cdrom" of the device special name.
   When Hitachi PP Installer starts up, the Welcome page appears. The following is an example of the initial screen that is displayed.

```
    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.
    +-------------------------------------------------------------------------+
```

4. Enter **I** in the default Hitachi PP Installer window to open the software list.
5. Move the cursor in the software list to `JP1/Integrated Management 3 - Agent` and select it with the spacebar.
6. Type **I** in Hitachi PP Installer to begin installing JP1/IM - Agent.
   The initial setup settings are automatically configured so that JP1/IM - Agent can operate as soon as it is installed.
7. After the installation is complete, enter **Q** to return to the initial screen.
8. After you finish Hitachi PP Installer, create JP1/IM - Agent autostart scripting.
   Run the command as follows:
   jpc_service_autostart -on

Related topics

- *1.3.1(3)(c) Initialization environment variable used by the installer* in the *Configuration Guide*
- *2.3.1 Installation Procedure (for UNIX)* in the *Configuration Guide*

2.5.7 Setting up JP1/IM - Agent (for Linux)

Enables JP1/IM - Agent services (jpc_imagent) to be started from Process Management.

Prerequisites

The following conditions must be met:

- OS that executes the `jpc_service` command-user has root privileges.

Operating procedure

1. Stop JP1/IM - Agent servicing by running the following command:
   `jpc_service_stop -s all`
2. Run the following command to enable servicing for JP1/IM - Agent:
   `/opt/jp1ima/tools/jpc_service -on [`*service-name-of-JP1/IM-Agent*`]`
3. Verify that JP1/IM - Agent serviceis enabled by running the following command:
   `systemctl list-unit-files`
   Valid if STATE of the corresponding service is not "masked".
4. Run the following command to start JP1/IM - Agent services:
   `jpc_service_start -s all`

Related topics

- *2.19 Setup for JP1/IM - Agent (for UNIX)* in the *Configuration Guide*
- *1. Commands related to the JP1/IM - Agen*t in the *Command, Definition File and API Reference*

2.6 Logging in to JP1/IM - Manager from the integrated operation viewer

To start system monitoring by using the Intelligent Integrated Management Base, log in to JP1/IM - Manager from the integrated operation viewer.

Prerequisites

The following conditions must be satisfied:

- The Intelligent Integrated Management Base is set up.
- JP1/IM - Manager is installed and set up on the manager.
- The primary authentication server is specified in JP1/Base of the manager.
- A JP1 user is registered on the primary authentication server.
- The IM database is set up.
- JP1/Base, JP1/IM - Manager, and IM database are running on the manager.
- The event-source-host mapping function is enabled.

Procedure

1. Start a Web browser and access the URL representing the host of JP1/IM - Manager (the Intelligent Integrated Management server) to display the Login window.

   The URL is defined in the following syntax:

   ```
   http://host-name-of-the-Intelligent-Integrated-Management-server:port-number/login
   ```

   Note: The URL starts with `https` if SSL communication is used.

   For the port number, specify the value set in server.port in the Intelligent Integrated Management Base Definition File (imdd.properties) of JP1/IM - Manager (Intelligent Integrated Management Server). The default value is 20703.

   For details about the Intelligent Integrated Management Base definition file, see the *Command, Definition File and API Reference*.

2. In the Login window, enter the user name and password.

3. Click the **Log In** button.

   The Integrated Operation Viewer window appears.

2.7 Logging in to JP1/IM - Manager from JP1/IM - View

To start system monitoring by using event management, log in to JP1/IM - Manager from JP1/IM - View. The Event Console window appears.

Prerequisites

The following conditions must be satisfied:

- JP1/IM - View is installed and set up on the viewer.
- JP1/IM - Manager is installed and set up on the manager.
- The primary authentication server is specified in JP1/Base of the manager.
- A JP1 user is registered on the primary authentication server.
- JP1/Base, JP1/IM - Manager, and IM database (if used) are running on the manager.

Procedure

1. From the Windows **Start** menu, select **All Programs**, **JP1_Integrated Management - View**, and then **Integrated View**. The Login window appears.
2. In the Login window, enter data for **User name**, **Password**, and **Host to connect**.
3. Select the **Central Console** check box.
4. Click the **OK** button.

3 Setting Up Monitoring Targets (When using JP1/IM - Agent for the agent)

This section describes how to define system configuration information and how to set categories.

This chapter assumes that the system is monitored by using integrated operation viewer.

3.1 Setting system configuration information

To monitor agent using JP1/IM - Agent, you define the system configuration.

Prerequisites

The following conditions must be met:

- *2.4.4(6) Setting up the Intelligent Integrated Management Base (for Windows)* or *2.5.4(6) Setting up the Intelligent Integrated Management Base (for Linux)* to set up and enable Intelligent Integrated Management Base.
- You have installed and set up.

Related topics

- *1.21. Setup for JP1/IM - Agent (for Windows)* in the *Configuration Guide*
- *2.19. Setup for JP1/IM - Agent (for UNIX)* in the *Configuration Guide*

3.1.1 Define system configuration information

Defines which system configuration information, such as hosts and jobs, that Intelligent Integrated Management Base collects from monitored systems are grouped by defined host and non-host object roots and placed on which systems.

Intelligent Integrated Management Base creates a hierarchical structure by distributing host and non-host object roots under the system as defined here and displays them in the form of a sunburst or tree in integrated operation viewer.

Operating procedure

1. Defines the hierarchical structure of the system, system node definition file (`imdd_systemnode.conf`) #. (optional)
2. Category name definition file for IM management nodes (`imdd_category_name.conf`) # defines IM management node of management group and the order in which the collected data is displayed in a hierarchical fashion. (optional)
3. If you are configuring IM management node with a product that allows hostnames to be aliased, define a mapping between the alias name and actual host name in host name definition file (`imdd_host_name.conf`) #. (optional)
4. Start JP1/IM - Manager, JP1/ IM database and Intelligent Integrated Management database.
5. Execute the `jddsetaccessuser` command. Set the user accessing the product to be monitored.
6. When linking with the product to be monitored, target host definition file for configuration collection (`imdd_target_host.conf`) # defines the hostname to acquire the configuration information of the linkage product and the monitoring object of the linkage product. (optional)
7. Run the `jddcreatetree` command to generate IM management node-related files.
8. IM management node link definition file (`imdd_nodeLink_def.conf`) # defines the relationship between IM management node. (optional)
9. Execute the `jddupdatetree` command. Intelligent Integrated Management server reflects the defined information.

#

The directory where the definition file is stored is shown below.

- For Windows
  For physical hosts: *Manager-path*\conf\imdd\
  For logical hosts: *shared-folder*\jp1imm\conf\imdd\
- For UNIX
  For physical host: /etc/opt/jp1imm/conf/imdd/
  For logical hosts: *shared-directory*/jp1imm/conf/imdd/

Related topics

- *4.2 Setting system configuration information* in the *Configuration Guide*
- *3.1 Starting JP1/IM - Manager* in the *Administration Guide*
- *System node definition file (imdd_systemnode.conf)* in *2. Definition Files* in the *Command, Definition File and API Reference*
- *Category name definition file for IM management nodes (imdd_category_name.conf)* in *2. Definition Files* in the *Command, Definition File and API Reference*
- *jddsetaccessuser* in *1. Commands* in the *Command, Definition File and API Reference*
- *jddcreatetree* in *1. Commands* in the *Command, Definition File and API Reference*
- *jddupdatetree* in *1. Commands* in the *Command, Definition File and API Reference*
- A chapter describing IM management node-related files in the *Overview and System Design Guide*

3.1.2 Check whether the system configuration information is reflected

After importing the information defined in Intelligent Integrated Management server, check whether integrated operation viewer can correctly monitor the status of system configuration information such as hosts/jobs collected from the monitored system.

Prerequisites

- Integrated operation viewer is set up in the viewer.

Operating procedure

1. In the address bar (URL entry area) of Web browser, enter URL of the log-in window.

   ```
   http://Intelligent-Integrated-Management-server-hostname:port-number/login
   ```

2. Enter your JP1 username (jp1admin) and password (jp1admin) to log in to Intelligent Integrated Management Base.
3. Select the **Dashboard** tab.
4. Make sure that the system you set is displayed on the Home window.

Related topics

- *1.2.1 Login window of the Intelligent Integrated Management Base* in the *GUI Reference*
- *2. Integrated Operation Viewer Window* in the *GUI Reference*

4 Setting Up Monitoring Targets(When using JP1/Base for agent)

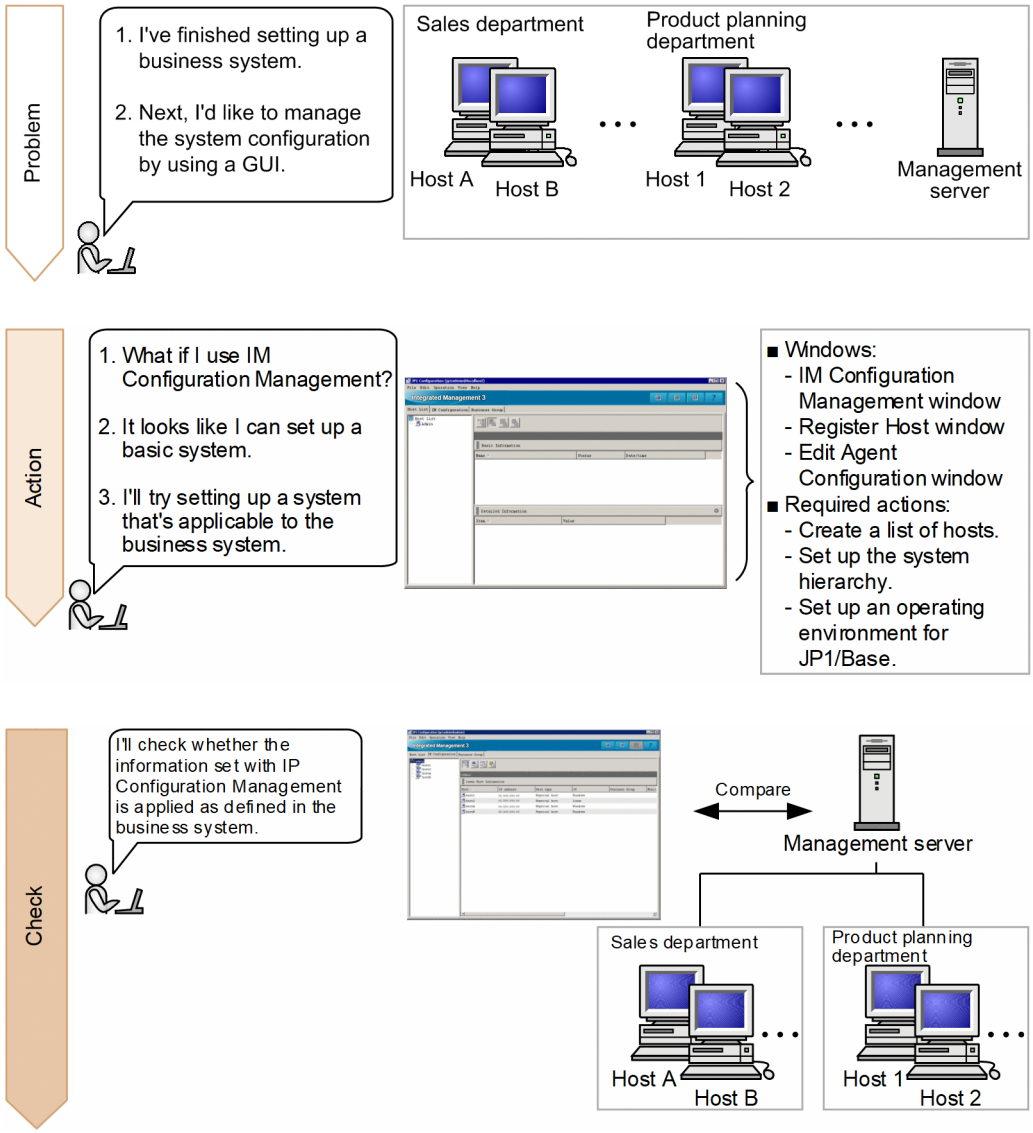
This chapter explains how to define and manage a system configuration, and the preparations that are necessary for monitoring events.

This chapter assumes that the system is monitored by using JP1/IM - View.

4.1 What is IM Configuration Management?

IM Configuration Management allows you to use a viewer (GUI program) to define a hierarchical configuration for a system. You can also use IM Configuration Management to centrally manage the hierarchical configuration of each host comprising a system.

In this section, we will use IM Configuration Management to define a basic system hierarchy so that events can be centrally managed.



This manual describes how to use IM Configuration Management to define the hierarchy for a basic configuration system for a new installation of JP1/IM - Manager.

The following describes how to define the basic configuration system shown in *2.1 Overview of a basic configuration system*.

To define a system hierarchy:

1. Register hosts into IM Configuration Management.
2. Use IM Configuration Management to define the system hierarchy.

***Keywords*:**

GUI, configuration management, configuration, system, IM Configuration Management, monitoring

4.1.1 Registering the hosts into IM Configuration Management

You need to register the manager and agents into IM Configuration Management to define a system hierarchy.

Prerequisites

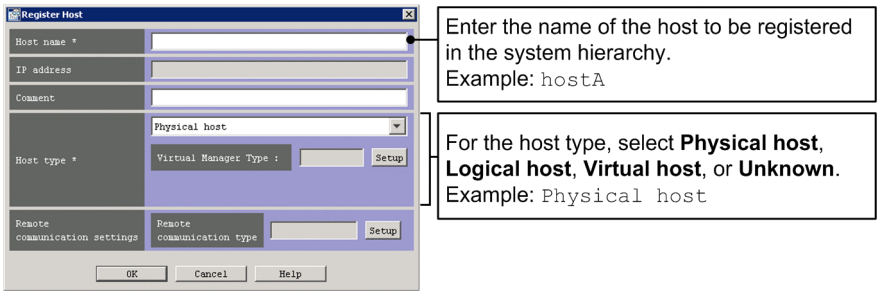
The following conditions must be satisfied:

- The IM Configuration Management database has been configured and enabled according to *2.4.4(4) Setting up an IM Configuration Management database (for Windows)* or *2.5.4(4) Setting up an IM Configuration Management database (for Linux)*.
- JP1/Base is installed on each agent.
- IM Configuration Management - View is set up on the viewer.

Procedure

1. From the Windows **Start** menu, select **Programs**, **JP1_Integrated Management 3 - View**, and then **Configuration Management**. The Login window appears.
2. Enter `jp1admin` for **User name**, `jp1admin` for **Password**, and `admin` for **Host to connect**, and then log in. The IM Configuration Management window appears.
3. In the IM Configuration Management window, select the **Host List** tab, and then select **Edit**, and then **Register Host**. The Register Host window appears.
4. Register the host to IM Configuration Management according to the system hierarchy described in *2.1 Overview of a basic configuration system*.

   Because `admin` is the local host, it has already been registered. Register hosts A, B, 1, and 2 to IM Configuration Management according to the following figure.



   Similarly, register all the hosts contained in the basic configuration system.

Related topics

- *8. System Hierarchy Management Using IM Configuration Management* in the *Overview and System Design Guide*
- *1.4.4 Settings for using the functions of IM Configuration Management (for Windows)* in the *Configuration Guide*
- *1.20.3 Setting up and customizing IM Configuration Management - View (for Windows)* in the *Configuration Guide*
- *9. Managing the System Hierarchy Using IM Configuration Management* in the *Administration Guide*
- *5. IM Configuration Management Window* in the *GUI Reference*

4.1.2 Using IM Configuration Management to define the system hierarchy

On the **IM Configuration** page in the IM Configuration Management window, you can check the systems that were built by using IM Configuration Management. The following describes how to define the basic configuration system shown in *2.1 Overview of a basic configuration system*.

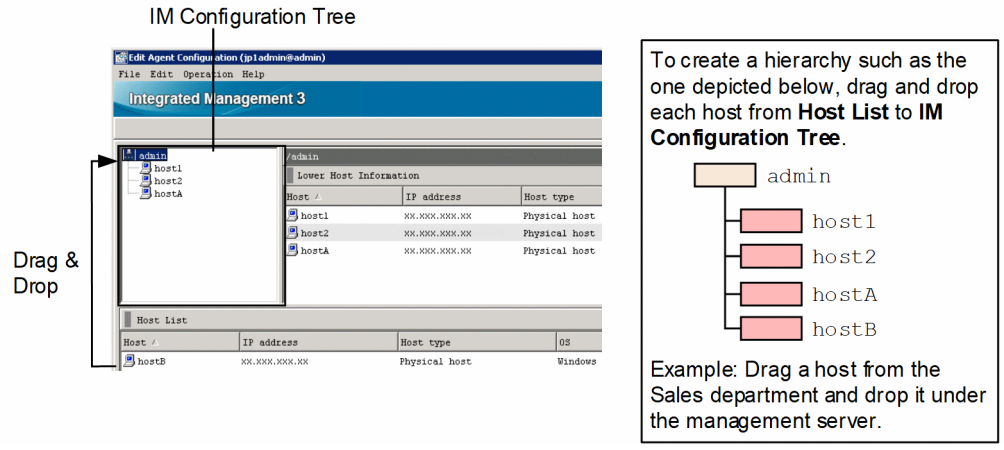
Prerequisites

The hosts must be registered in IM Configuration Management.

Procedure

1. In the IM Configuration Management window, select **Edit**, and then **Edit Agent Configuration**. The Edit Agent Configuration window appears.

2. Configure the hosts to match the system hierarchy according to the following figure.



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

4. In the Edit Agent Configuration window, select **Operation**, and then **Apply IM Configuration** to reflect the definitions of the system hierarchy to JP1/IM - Manager.

Related topics

- *1.9 Setting the system hierarchy (when IM Configuration Management is used) (for Windows)* in the *Configuration Guide*
- *3. Using IM Configuration Management to Set the System Hierarchy* in the *Configuration Guide*
- *9. Managing the System Hierarchy Using IM Configuration Management* in the *Administration Guide*

4.1.3 Verifying that the system has been correctly set up by IM Configuration Management

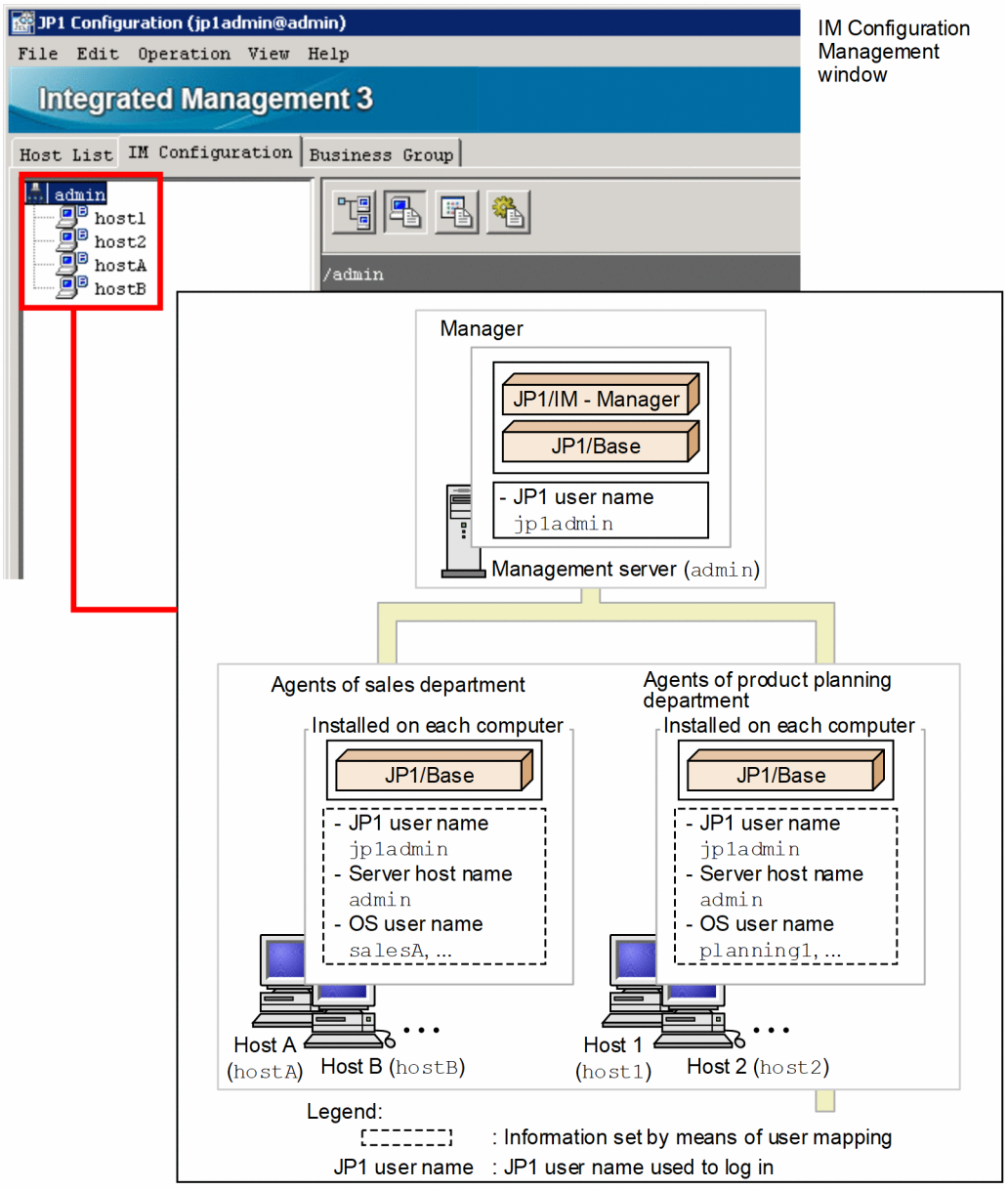
To use JP1/IM to centrally manage events issued in a business system, verify that the system has been set up correctly by IM Configuration Management. The following describes how to verify that the basic configuration system shown in *2.1 Overview of a basic configuration system* has been set up.

Prerequisites

The basic configuration system must be set up according to *4.1 What is IM Configuration Management?*.

Procedure

1. In the IM Configuration Management window, select the **IM Configuration** page.
2. Verify that the system hierarchy has been defined as shown in *2.1 Overview of a basic configuration system*.

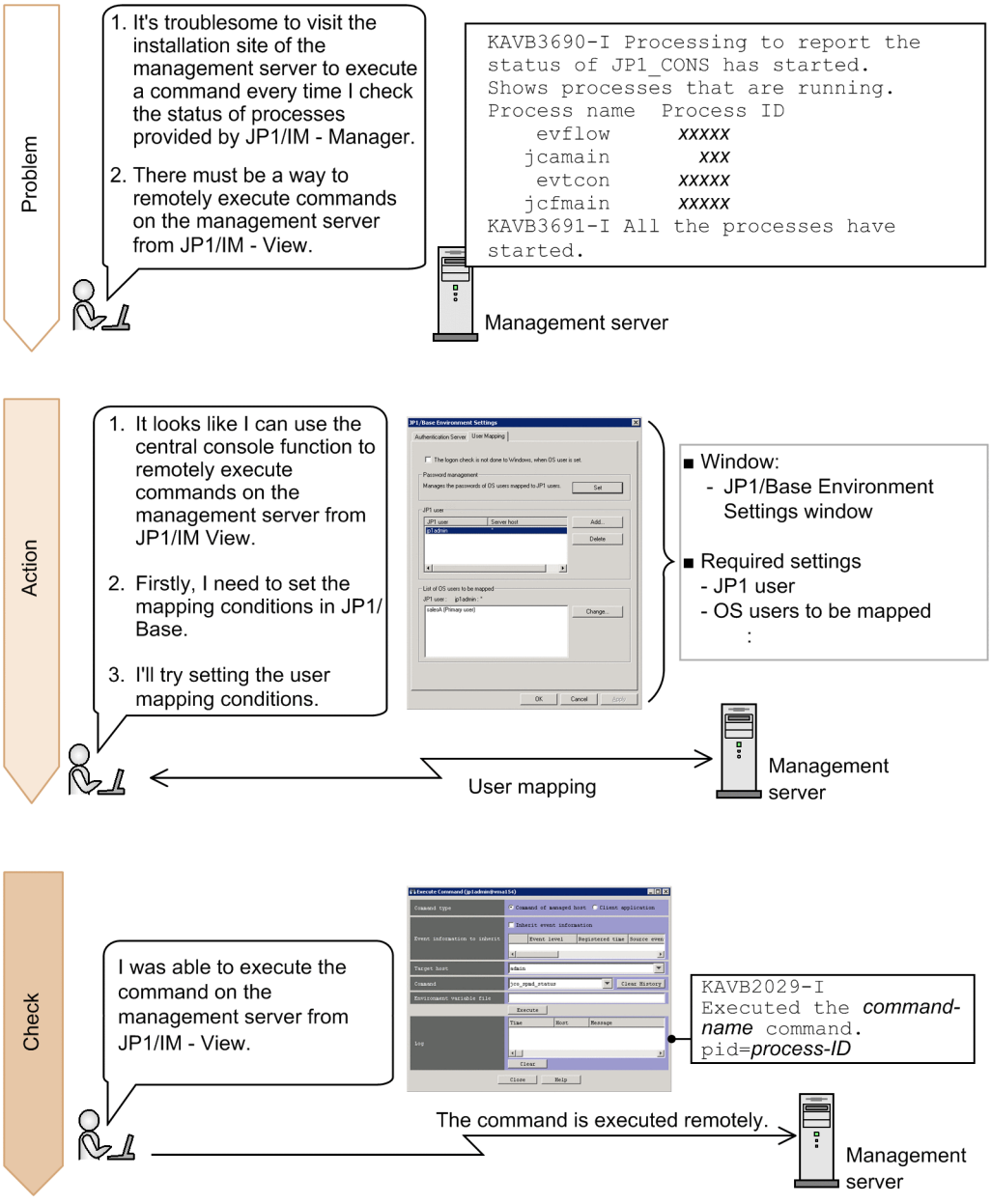


4.2 Settings for executing commands on monitored hosts from JP1/IM - View

You can use the JP1/IM - View command execution function to remotely execute commands on managed hosts. To use this function, you need to use JP1/Base to map a JP1 user who executes commands to an OS user account on the target host.

In this section, we will configure JP1/Base user mapping so that you can remotely execute commands on monitored hosts.

By configuring JP1/Base user mapping, you can also execute commands on the client host (the viewer host). This functionality is called *client application execution*, and the commands on the client host are called *client applications*. You can use the client application execution functionality without special settings.



Keywords:

user mapping, mapping, command, relationship

4.2.1 Configuring user mapping

To use the central console to execute commands on hosts in the system, you need to use JP1/Base user mapping to map a JP1 user account to an OS user account on a host. User mapping must be configured on each host on which commands are executed. This manual describes how to configure user mapping on host A in the basic configuration system shown in *2.1 Overview of a basic configuration system*. You can use the GUI or a command to configure user mapping.

(1) Using the GUI to configure user mapping (Windows only)

Because JP1 users can use the central console to execute commands on hosts in the system, you need to configure user mapping by using the JP1/Base GUI. This manual describes the user mapping procedure for the JP1 user `jp1admin` and the OS user `salesA`.

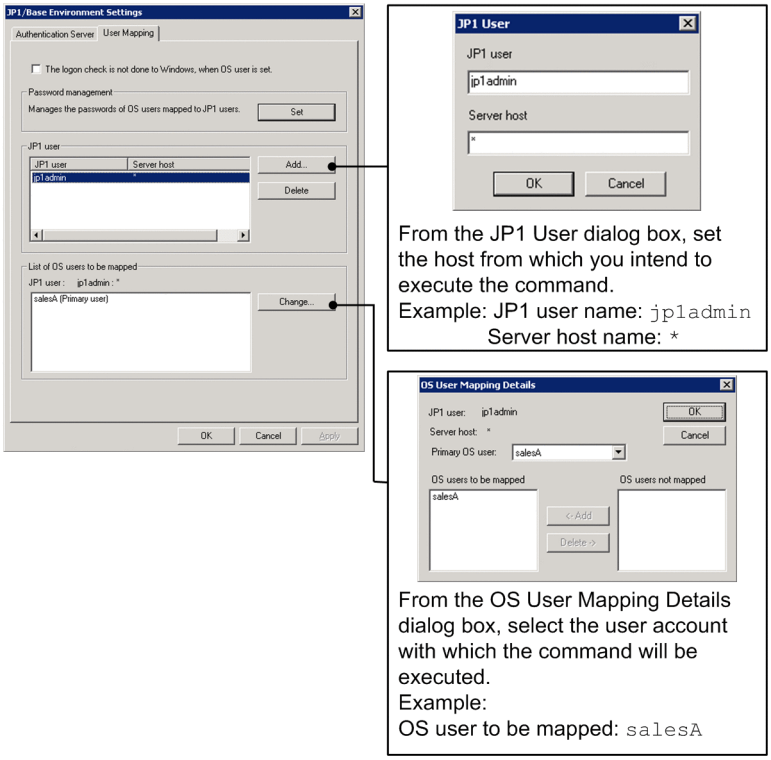
Prerequisites

The following conditions must be satisfied:

- The OS user to be mapped to the JP1 user has the following user permissions (Windows only):
  - **Log on locally**
  - **Log on as a service**
- The JP1 user who will execute commands from JP1/IM - View is registered in the authentication server.
- The JP1 user who will execute commands from JP1/IM - View has either of the following JP1 permission levels:
  - `JP1_Console_Admin`
  - `JP1_Console_Operator`
- The system is set up according to *2.1 Overview of a basic configuration system*.

Procedure

1. From the Windows **Start** menu, select **All Programs**, **JP1_Base**, and then **JP1_Base Setup**. The JP1/Base Environment Settings window dialog box appears.
2. Configure user mapping according to the following figure.



Related topics

- *9.4 Core functionality provided by JP1/Base* in the *Overview and System Design Guide*
- Descriptions of how to configure user mapping in the *JP1/Base User's Guide*

(2) Using a command to configure user mapping (Windows and Linux)

The following describes how to use the `jbssetumap` command to configure user mapping in order to allow commands to be executed on hosts in the system from the central console. This manual describes the user mapping procedure for the JP1 user `jp1admin` and the OS user `salesA`.

Prerequisites

The following conditions must be satisfied:

- The OS user to be mapped to the JP1 user has the following user permissions (Windows only):
  - **Log on locally**
  - **Log on as a service**
- The JP1 user who will execute commands from JP1/IM - View is registered in the authentication server.
- The JP1 user who will execute commands from JP1/IM - View has either of the following JP1 permission levels:
  - JP1_Console_Admin
  - JP1_Console_Operator
- The system is set up according to *2.1 Overview of a basic configuration system*.
- The user who will execute the `jbssetumap` command has Administrator or `root` permissions.

Procedure

1. Execute the following `jbssetumap` command on host A (`hostA`) to configure user mapping:

- In Windows:
  "*Base-path*\bin\jbssetumap" -u jp1admin -sha -o salesA
- In Linux:
  /opt/jp1base/bin/jbssetumap -u jp1admin -sha -o salesA

Execute the above command on each host.

Related topics

- Descriptions of how to configure user mapping in the *JP1/Base User's Guide*
- Description of the jbssetumap command in the *JP1/Base User's Guide*

4.2.2 Verifying that you can execute a command

After the command for configuring OS user mapping finishes, verify that you can execute a command on the manager.

Prerequisites

The following conditions must be satisfied:

- OS user mapping is configured according to the procedure in *4.2.1 Configuring user mapping*.
- The OS user who will execute the jco_spmd_status command (that is, the OS user mapped to the JP1 user by user mapping) has Administrator or root permissions.

Procedure

1. In the Event Console window, click the **Execute Command** button. The Execute Command window appears.
2. In the **Command type** area, select **Command of managed host**.
3. In the **Event information to inherit** area, clear the **Inherit event information** check box.
4. For **Target host**, specify the host as follows on which the command will be executed:
   admin
5. For **Command**, enter the jco_spmd_status command as follows to check whether the command can be executed:
   - In Windows:
     "*Console-path*\bin\jco_spmd_status"
   - In Linux:
     /opt/jp1cons/bin/jco_spmd_status
6. Click the **Execute** button.
7. Verify that the **Log** area displays the statuses of processes provided by JP1/IM - Manager.
   The following shows an example display for when the command is executed in Windows. Note that process IDs and running processes vary depending on the system environment.

```
----------------------------------------------------
2014/04/02 21:45:06,admin,"KAVB2012-I Received the ""C:\Program Files
(x86)\Hitachi\JP1Cons\bin\jco_spmd_status"" command."
```

```
2014/04/02 21:45:06,admin,"KAVB2029-I Executed the ""C:\Program Files
(x86)\Hitachi\JP1Cons\bin\jco_spmd_status"" command. pid=16592"
2014/04/02 21:45:06,admin,KAVB3690-I Processing to report the status of
JP1_CONS has started.
2014/04/02 21:45:06,admin,Shows processes that are running.
2014/04/02 21:45:06,admin,Process name Process ID
2014/04/02 21:45:06,admin, evflow 14256
2014/04/02 21:45:06,admin, jcamain 6292
2014/04/02 21:45:06,admin, evtcon 13308
2014/04/02 21:45:06,admin, jcfmain 13528
2014/04/02 21:45:06,admin,KAVB3691-I All the processes have started.
2014/04/02 21:45:06,admin,"KAVB2013-I Terminated the ""C:\Program Files
(x86)\Hitachi\JP1Cons\bin\jco_spmd_status""command. pid=16592 terminate
code=0 "
-----------------------------------------------------
```

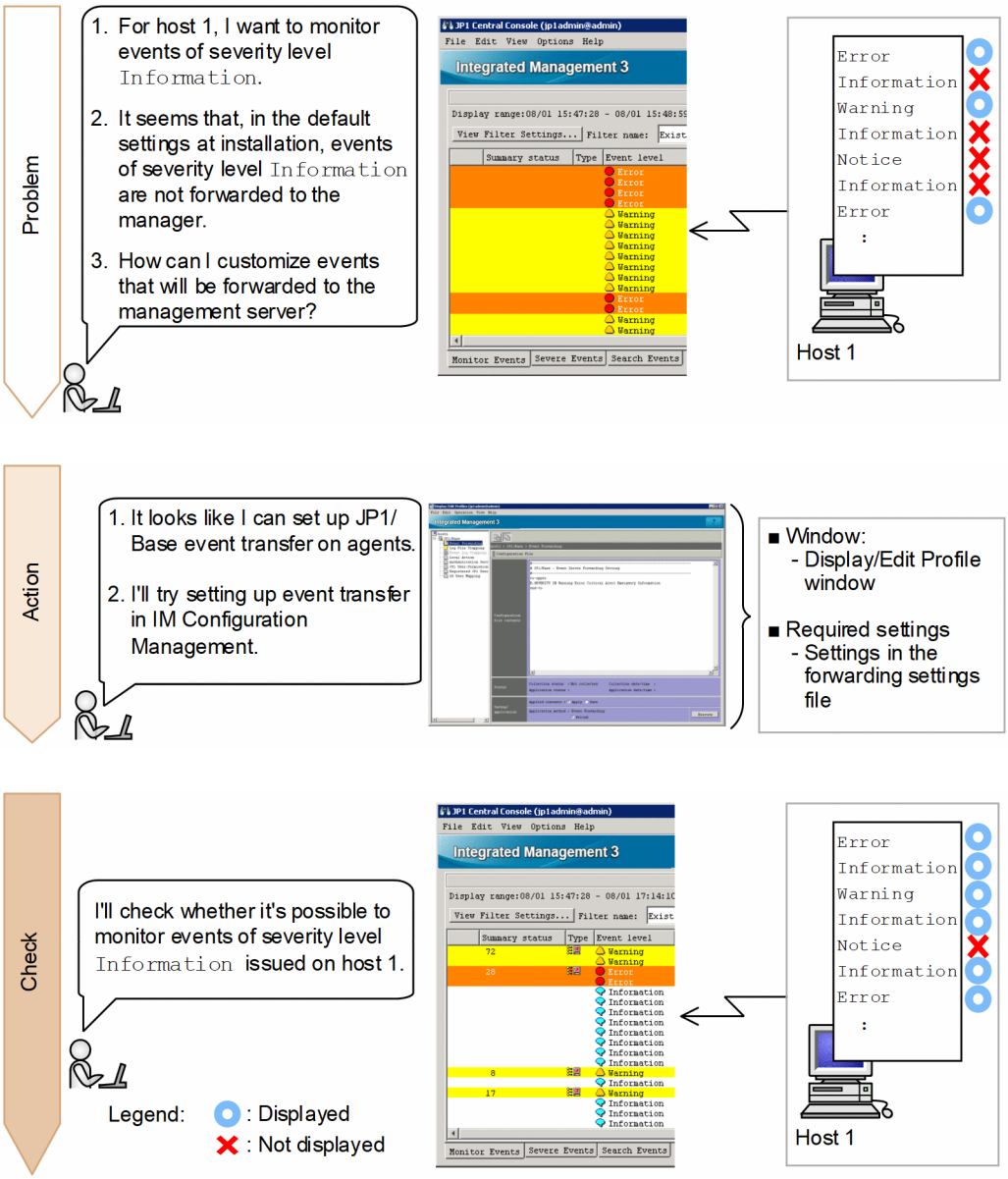
Related topics

- *jco_spmd_status* in *1. Commands* in the *Command, Definition File and API Reference*

4.3 Customizing settings for forwarding events from an agent to the manager

In the default settings at installation, events of severity level `Notice` or `Information` are not forwarded to the manager from monitored agents. To add these events as monitoring targets, you need to customize event forwarding settings in IM Configuration Management.

In this section, we will customize event forwarding settings in IM Configuration Management to monitor necessary events.



Keywords:

event, forwarding, monitoring target, forwarding filter

4.3.1 Using IM Configuration Management to set a forwarding filter

A forwarding filter, which is a JP1/Base function, specifies conditions for the events to be forwarded from JP1/Base and the destination manager to which they are sent. By setting forwarding filters on agents that forward events, you can customize event forwarding settings.

(1) Settings of the forwarding settings file to be created

The following table explains the detailed settings of the forwarding settings file that will be created in *4.3.1 (2) Creating a forwarding transfer settings file and using IM Configuration Management to set a forwarding filter*.

Specification details

Specification	Description

`to-upper`
`:`
`end-to`
	Specifies that events that match the conditions specified between `to-upper` and `end-to` are forwarded to the higher manager in the system hierarchy.

`E.SEVERITY IN Warning Error Critical Alert Emergency Information`	Specifies the conditions of events to be forwarded to the manager. To specify the severity levels of events to be forwarded to the manager, specify the following: `E.SEVERITY IN` *severity-level* ... In this example, events of severity level `Warning`, `Error`, `Critical`, `Alert`, `Emergency`, or `Information` are forwarded to the manager. This specification must be written between `to-upper` and `end-to`.

(2) Creating a forwarding transfer settings file and using IM Configuration Management to set a forwarding filter

In order to customize the event forwarding settings, use IM Configuration Management to set a forwarding filter by editing the forwarding transfer settings file for agents. This manual describes how to set a forwarding filter for events that are forwarded to the management server from host 1 in the basic configuration system. For details about the basic configuration system, see *2.1 Overview of a basic configuration system*.

Prerequisites

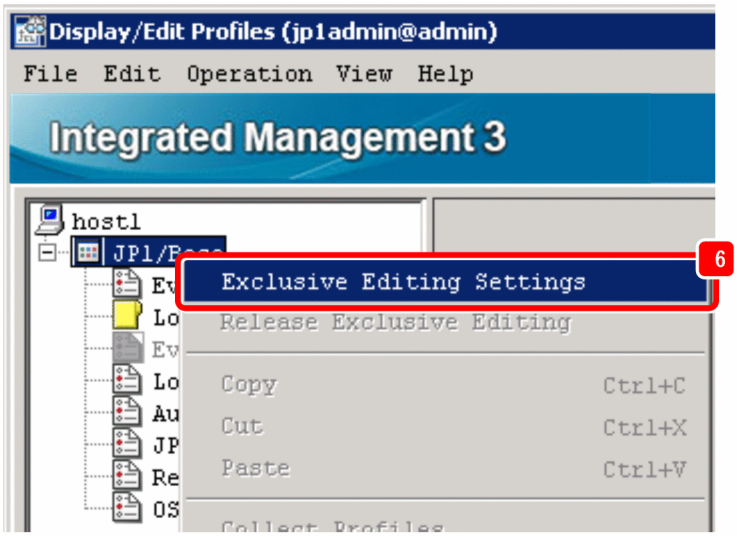
The following conditions must be satisfied:

- The basic configuration system is set up according to *4.1 What is IM Configuration Management?*.
- Host information has been collected.

Procedure

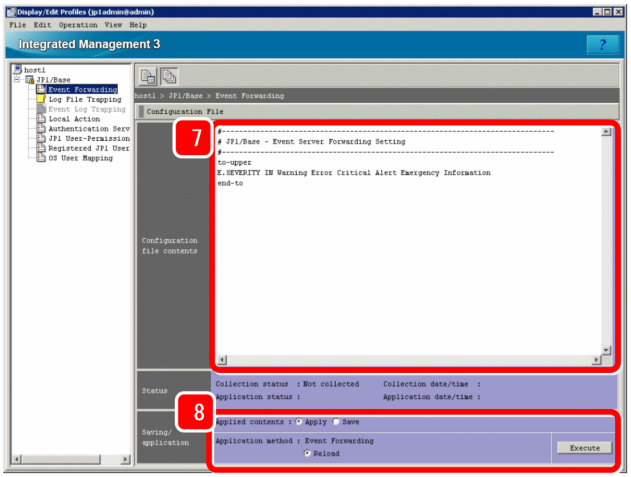
1. From the Windows **Start** menu, select **All Programs**, **JP1_Integrated Management 3 - View**, and then **Configuration Management**. The Login window appears.
2. Enter `jp1admin` for **User name**, `jp1admin` for **Password**, and `admin` for **Host to connect**, and then log in. The IM Configuration Management window appears.
3. Click the **IM Configuration** tab. Then, in the tree area on the **IM Configuration** page, select the agents to which you want to forward events.
4. In the IM Configuration Management, select **View**, and then **Display Profiles**. The Display/Edit Profile window appears.
5. In the tree display area, select **JP1/Base**.

6. In the pop-up menu displayed by right-clicking, select **Exclusive Editing Settings** to obtain exclusive editing rights.
   In the tree display area, the icon for **JP1/Base** is changed from  to  .



7. In the tree display area, select **Event Forwarding**, and then edit the forwarding transfer settings file.
   The following is an entry example:

```
to-upper
E.SEVERITY IN Warning Error Critical Alert Emergency Information
end-to
```



8. After editing the forwarding transfer settings file, confirm that the items in **Saving/application** are set as follows, and then click the **Execute** button:
   - **Applied contents**: **Apply**
   - **Application method**: **Reload**

9. When a dialog box asking you whether you want to apply the settings appears, click the **Yes** button.

Related topics

- *4.1.1 Monitoring from the Central Console* in the *Overview and System Design Guide*
- Descriptions of the forwarding settings file (`forward`) in the *JP1/Base User's Guide*

4.3.2 Verifying that the forwarding filter has been correctly set

On the manager, check the forwarding filter that was set by a JP1 user. For details about setting the forwarding filter, see *4.3.1 (2) Creating a forwarding transfer settings file and using IM Configuration Management to set a forwarding filter*. In this subsection you can check whether an event of severity level `Information` (issued on host 1) is displayed in the event list.

Prerequisites

OS user mapping must be configured according to the procedure in *4.2.1 Configuring user mapping*.

Procedure

1. Set the items in the Command window as described in the table below, and then click the **Execute** button. For details of the procedure, see *4.2.2 Verifying that you can execute a command* .

Item	Setting
Command type	Select **Command of managed host**.
Event information to inherit	Clear the **Inherit event information** check box.
Target host	Enter the following: `host1`
Command	Enter the following: • In Windows: "*Base-path-of-the-execution-host*`\bin\jevsend" -e SEVERITY=Information -m` *information-event*" • In Linux: `/opt/jp1base/bin/jevsend -e SEVERITY=Information -m` *information-event*

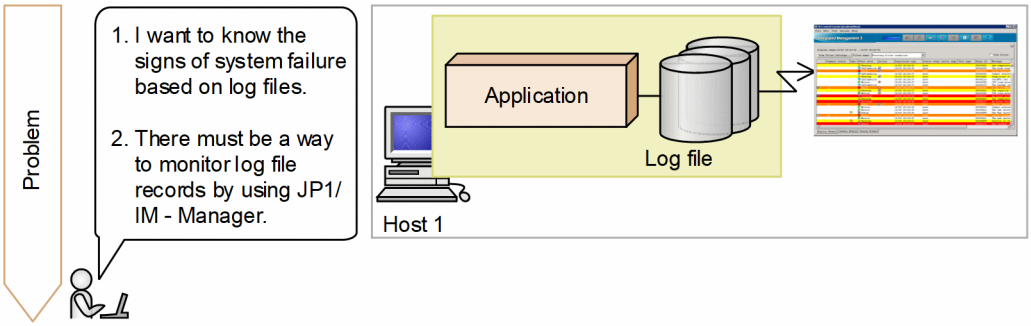
   An event of severity level `Information` is issued on host 1.

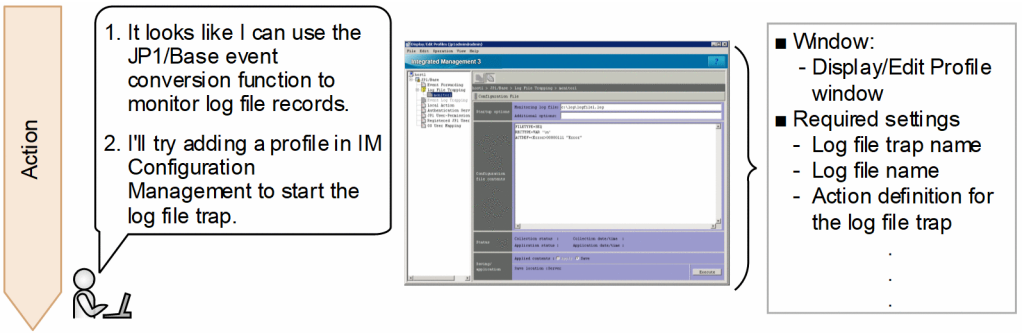
2. Verify that the event of severity level `Information` is displayed in the event list.

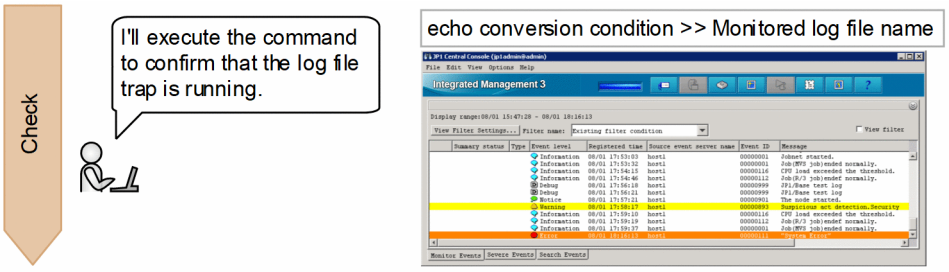
4.4 Using event conversion to monitor log files

By monitoring application log files, you can find the signs of system failure and determine the cause of system failure. To monitor log file records in JP1/IM, you need to configure JP1/Base log file trapping to convert the records to events.

In this section, we will configure JP1/Base log file trapping to allow JP1/IM to monitor log file records.







Keywords:

event, log, monitoring, conversion, application, central console

Tip:

To monitor Windows event logs in JP1/IM:

By converting Windows event logs to JP1 events, you can use JP1/IM to monitor logs output in Windows, such as application error logs. To monitor Windows event logs in JP1/IM, event log trapping is used. Event log trapping is one of the functions provided by JP1/Base, and converts Windows event logs to JP1 events. For details, see the description of conversion of Windows event logs in the *JP1/Base User's Guide*.

4.4.1 What is log file trapping for JP1/Base?

Log file trapping is one of the functions provided by JP1/Base, and converts log file records to events. To monitor Windows event logs in JP1/IM, *log file traps* are used.

To set the log file trapping:

1. Use IM Configuration Management to create a log file trap action-definition file on the host to be monitored.
2. Use IM Configuration Management to start the log file trap on the host to be monitored.

This manual describes an example of setting the log file trap for log files on host 1 in the basic configuration system shown in *2.1 Overview of a basic configuration system*. The target log files have the following format:

- Records are sequentially added from the beginning of the file (sequential file).
- A line of variable-length character string is stored as a record.

Sample log file:

```
--------------------------------------------------
2014/03/07 12:00:00.001 AAAA1111-E "System Error" .....
2014/03/07 12:00:00.002 AAAA1112-I "Information" .....
2014/03/07 12:00:00.003 AAAA1113-I "Warning" .....
:
--------------------------------------------------
```

If you want to set the log file trap for log files of a format other than described in this manual, see the descriptions of event conversion in the *JP1/Base User's Guide*, and check the log file format.

(1) Settings of the the log file trap action-definition file

The following provides the detailed settings of the log file trap action-definition file, which will be created in *4.4.1 (2) Using IM Configuration Management to create log file trap action-definition files on hosts to be monitored*.

Specification details

Specification	Description
`FILETYPE=SEQ` `RECTYPE=VAR '\n'`	Specifies the format of the log file that is the target of the log file trap. In this manual, the target is SEQ sequential files in which a variable-length record is stored per line.
`ACTDEF=<Error>00000111 "System Error"`	Specifies the event conversion condition for records written in the log file. To specify the severity level and event ID of the events converted from records containing a specific character string, specify the following: `ACTDEF=<`*severity-level*`>`*event-ID* `"`*character-string-in-records-to-be-converted*`"`. In this example, records containing the character string `System Error` are converted to events whose severity level is `Error` and event ID is `00000111`.

The following shows an example of a record to be converted to an event, and an example of an event after conversion.

Record to be converted to an event:

```
2014/03/07 12:00:00.001 AAAA1111-E "System Error" .....
```

Event after conversion

- Severity level: `Error`

- Event ID: `00000111`
- Message: `2014/03/07 12:00:00.001 AAAA1111-E "System Error" .....`

(2) Using IM Configuration Management to create log file trap action-definition files on hosts to be monitored

Because JP1 users set log file traps, you need to use IM Configuration Management to create log file trap action-definition files on hosts to be monitored. Perform this procedure on the host to be monitored.

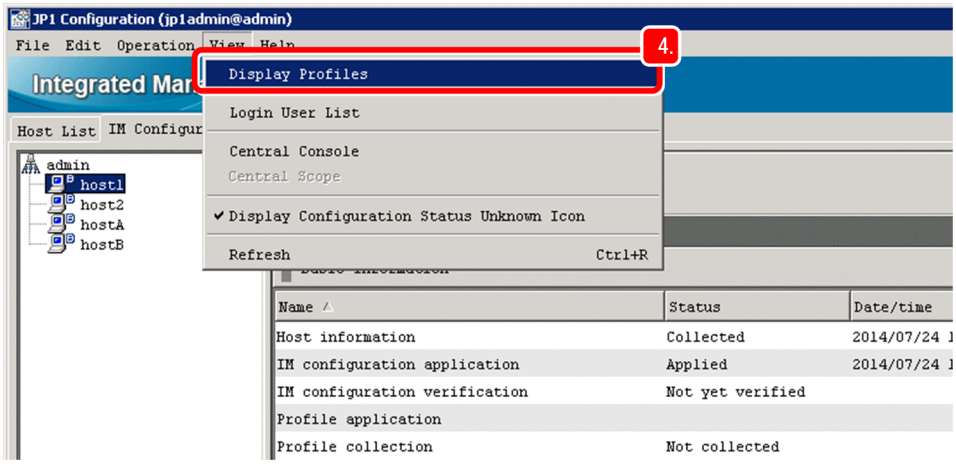
Prerequisites

The following conditions must be satisfied:

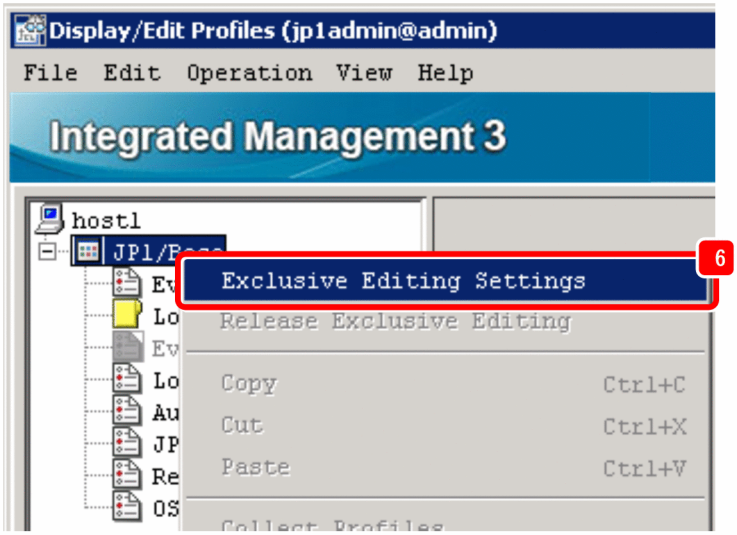
- The basic configuration system is set up according to *4.1 What is IM Configuration Management?*.
- Host information has been collected.
- Log files exist.

Procedure

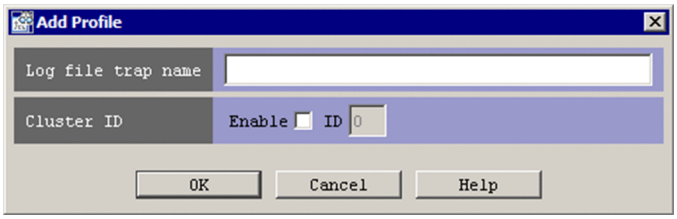
1. From the Windows **Start** menu, select **All Programs**, **JP1_Integrated Management 3 - View**, and then **Configuration Management**. The Login window appears.
2. Enter `jp1admin` for **User name**, `jp1admin` for **Password**, and `admin` for **Host to connect**, and then log in. The IM Configuration Management window appears.
3. Click the **IM Configuration** tab. Then, in the tree area on the **IM Configuration** page, select the hosts on which you want to monitor log files.
4. On the menu bar, select **View**, and then **Display Profiles**. The Display/Edit Profile window appears.



5. In the tree display area, select **JP1/Base**.
6. In the pop-up menu displayed by right-clicking, select **Exclusive Editing Settings** to obtain exclusive editing rights.



7. In the tree display area, select **Log File Trapping**.
8. In the pop-up menu displayed by right-clicking, select **Add Profile** to add a log file trap name.
9. Specify a log file trap name to ensure that the setting values will be unique.



   Enter a unique log file trap name in the text box that appears. To specify a cluster ID, select the **Enable** check box, and then enter the cluster ID. Note that the log file trap is managed by the log file trap name entered here.

10. Click the **OK** button.

    The added log file trap name appears in the tree display area. The contents of the log file trap definition file corresponding to the log file trap name appear in the node display area of the Display/Edit Profile window.

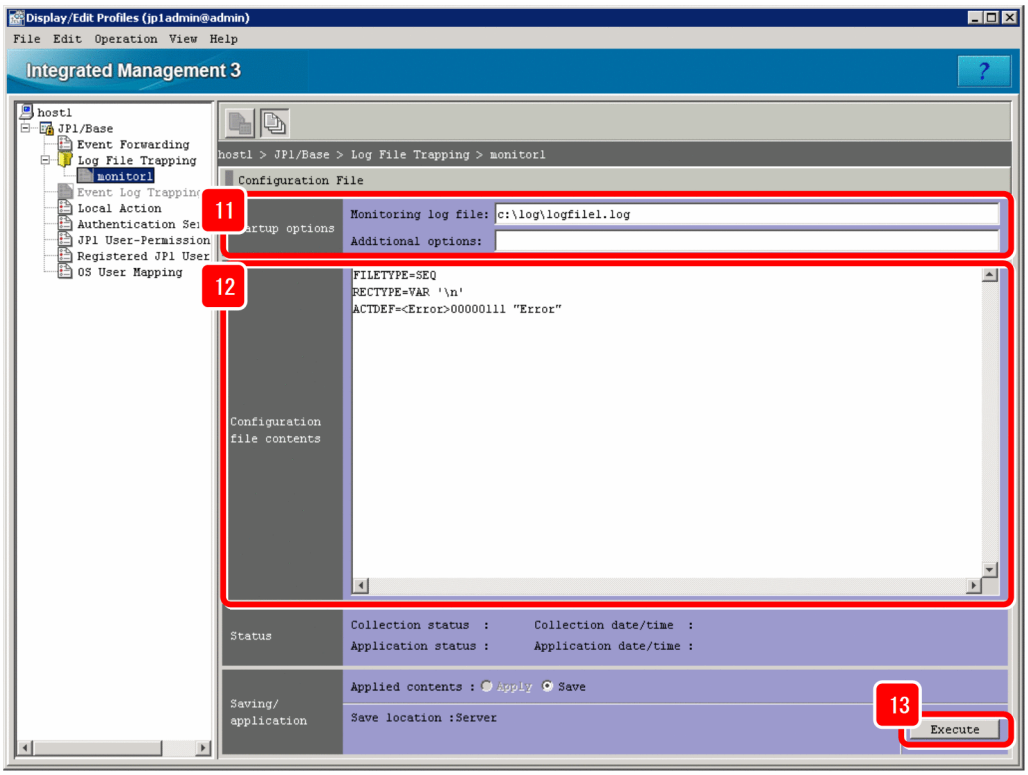
    Note that immediately after the log file trap name is added, nothing is set in the log file trap action-definition file.

11. Specify startup options.

    The following are specification examples:

    - **Monitoring log file**: `c:\log\logfile1.log`
    - **Additional options**: None

    If the host to be added is running on Linux, in **Additional options**, specify the character encoding of the log file that will be the target of the log file trap.



12. Edit the log file trap action-definition file.

    The following is an entry example:

    ```
    FILETYPE=SEQ
    RECTYPE=VAR '\n'
    ACTDEF=<Error>00000111 "System Error"
    ```

13. After editing the startup options and settings, click the **Execute** button.

14. When a dialog box asking you whether you want to apply the settings appears, click the **Yes** button.

    If a KNAN20321-Q message appears in the dialog box, the settings will be applied when IM Configuration Management starts up the log file trap.

Related topics

- *3.5.1 Setting the profiles on hosts in an agent configuration* in the *Configuration Guide*
- *5.1.2 IM Configuration page* in the *GUI Reference*
- *5.9 Display/Edit Profiles window* in the *GUI Reference*
- Descriptions about converting application program log files in the *JP1/Base User's Guide*
- Descriptions of the log file trap action-definition file in the *JP1/Base User's Guide*
- Descriptions of the log-file trap startup definition file in the *JP1/Base User's Guide*

(3) Using IM Configuration Management to start the log file trap on the host to be monitored

Use IM Configuration Management to start log file traps so that JP1 users can monitor application log file records in JP1/IM. Perform this procedure on the host to be monitored.

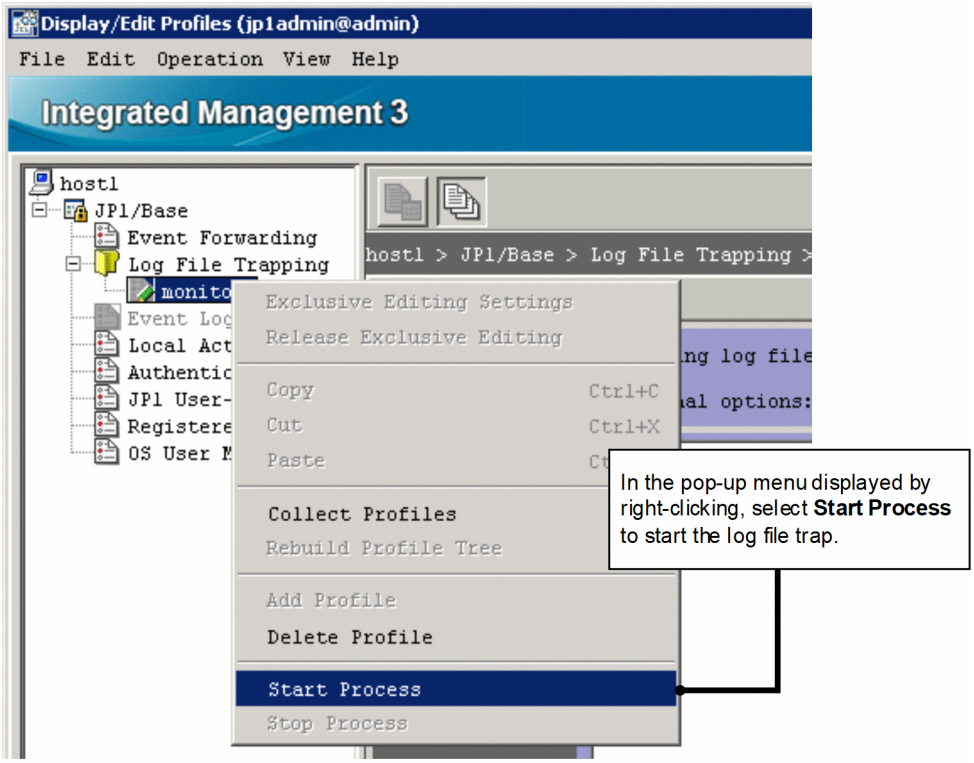
Prerequisites

The following conditions must be satisfied:

- A log file trap action-definition file has been created on the host to be monitored.
- Exclusive editing rights for profiles have been obtained forJP1/Base on the host to be monitored.
- TheJP1/Base LogTrap service is running on the host to be monitored.

Procedure

1. In the tree display area of the Display/Edit Profile window, select the log file trap name for the log file trap you want to start.
2. Start the log file trap by using either of the following methods:
   - On the menu bar, select **Operation**, and then **Start Process**.
   - In the pop-up menu displayed by right-clicking, select **Start Process**.



Related topics

- *3.5.1 Setting the profiles on hosts in an agent configuration* in the *Configuration Guide*
- *5.9 Display/Edit Profiles window* in the *GUI Reference*
- Descriptions of converting application program log files in the *JP1/Base User's Guide*

4.4.2 Verifying that records can be converted to events by the log file trap

After you create a log file trap action-definition file according to *4.4.1 What is log file trapping for JP1/Base?*, you must verify that the log file trap runs normally. To check the operation, output a pseudo record on an agent that is running the log file trap. Before you attempt to start the log file trap, make sure that a pseudo record can be output to the log file.

Prerequisites

Setting of the log file trap must be completed according to *4.4.1 What is log file trapping for JP1/Base?*.

Procedure

1. From the command prompt for the agent (`host1`) on which the log file trap is running, execute the following command:

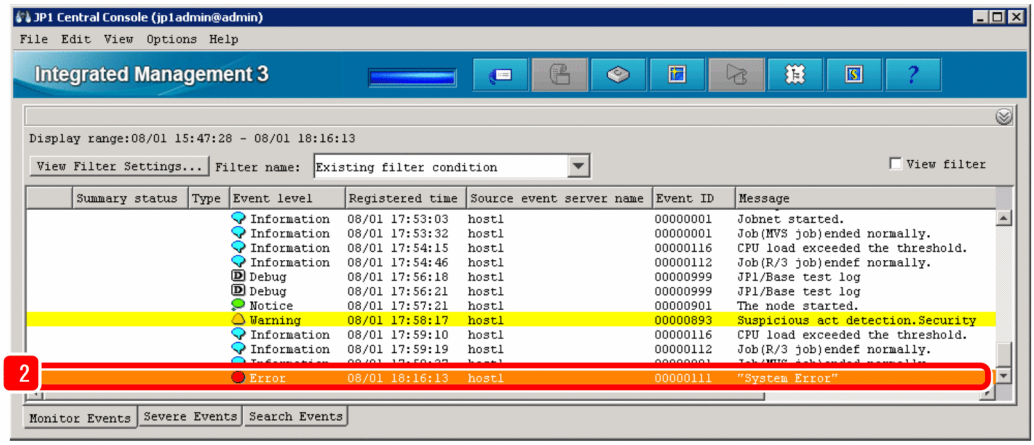
   `echo "System Error">>`*log-file-name*#

   #: In this example, the `echo` command is used to monitor a test file. For the actual operation, monitor a log file output by an application.

   For example, if a log file named `logfile1.log` is stored in `C:\log` in Windows, specify `C:\log\logfile1.log` for *log-file-name*.

2. Verify that the event converted from log data is displayed in the central console.

   In this example, confirm that an event was issued whose severity level was `Error`, source host was `host1`, and message was `System Error`.



Related topics

- *3.1 Overview of the Event Console window* in the *GUI Reference*
- *3.40 Execute Command window* in the *GUI Reference*

5 Monitoring a System

Here, integrated operation viewer monitors the system.

The dashboard allows system-wide monitoring and node-specific monitoring, such as agent.

It also explains how to temporarily narrow down the events displayed in the event list of JP1/IM - View, and to remove the hosts that are being maintained from monitoring.

5.1 Monitoring only necessary events

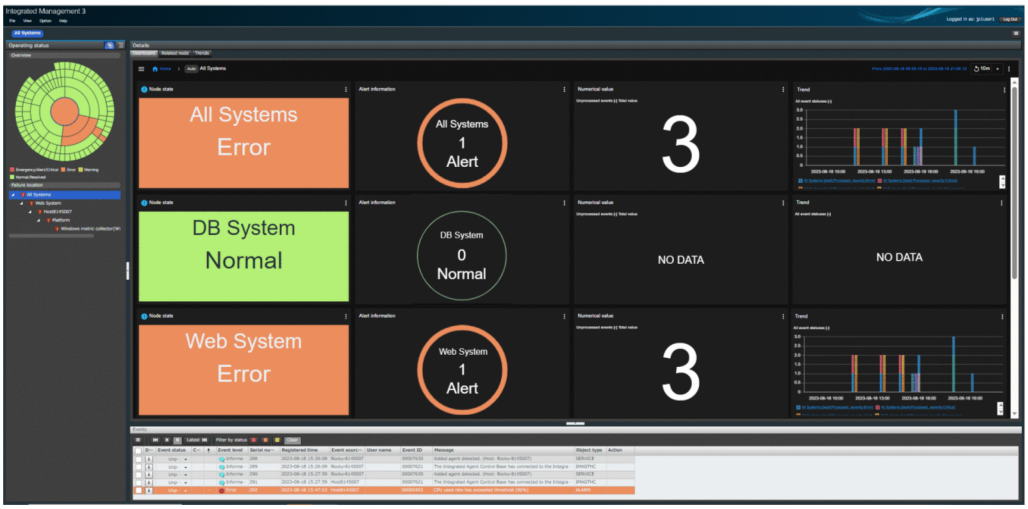
Integrated operation viewer is displayed in a Web browser. For login instructions, see *2.6 Logging in to JP1/IM - Manager from the integrated operation viewer*.

Note that to use integrated operation viewer, Intelligent Integrated Management Base must be set up in JP1/IM - Manager.

When you log in to integrated operation viewer, a system-wide dashboard appears in the upper-right corner, allowing you to view the status of critical events, alert information, the number of unresponsive events, and the response status of the event.

If there is a child system, the status of the child system is also displayed.

Figure 5–1: Sample of integrated operation viewer (1/2)



Select agent in the tree to view the status of critical events, alert information, number of unresponsive events, and response status of events for that agent, and to graphically view trend information for various IT resources-including CPU utilization.

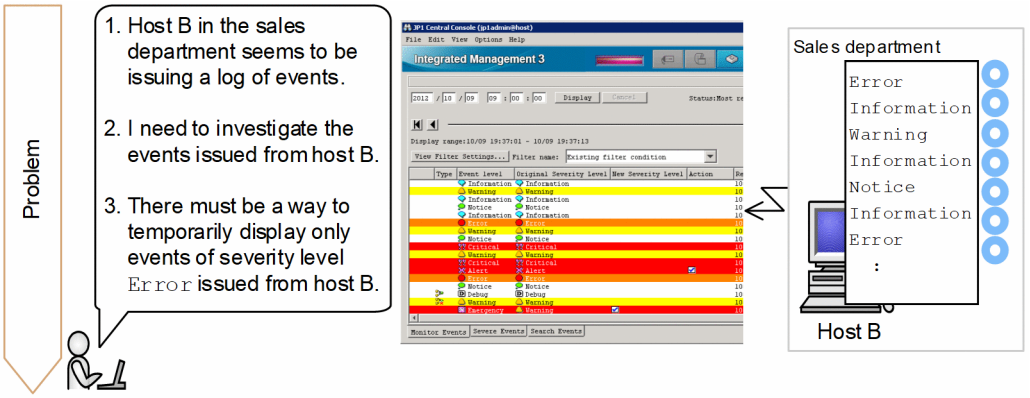
Figure 5–2: Sample of integrated operation viewer (2/2)

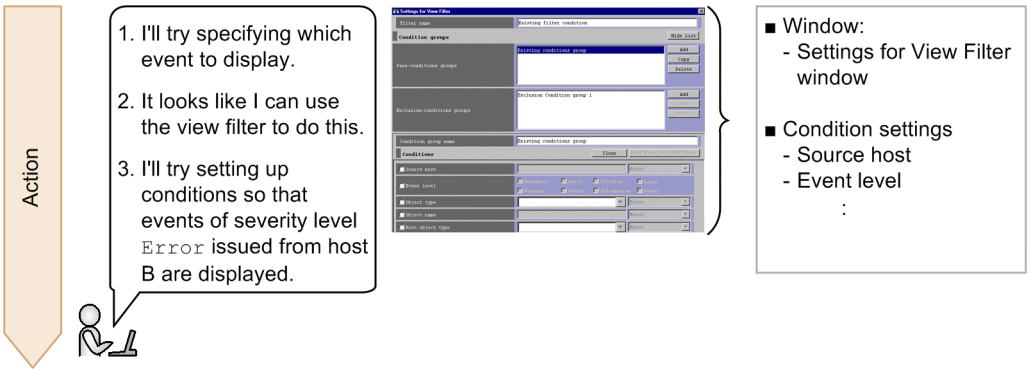
5.2 Monitoring Your System with JP1/IM - View

Explains how to use JP1/IM - View in the viewer to monitor events.

5.2.1 Monitoring only necessary events

When you use JP1/IM - View to monitor events, the events published on the host appear in the event list. When conditions such as host and severity are fixed, you can display only the events that you want to monitor according to those conditions.





Keywords:

automated action, command, Automatic Action Service, email, notification

(1) Using a view filter to filter events to be displayed

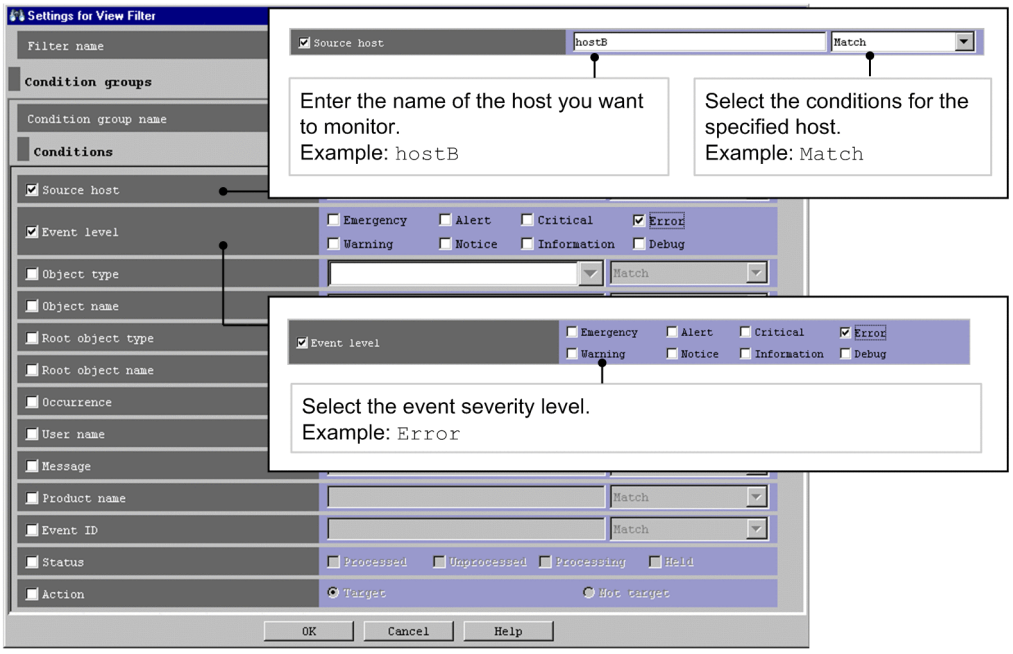
To filter events to be displayed, set up a view filter in the Settings for View Filter window of the central console. In this procedure, you set up the view filter to display events of severity level Error issued from host B.

Prerequisites

None

Procedure

1. In the Monitor Events page of the Event Console window, click View Filter Settings. The Settings for View Filter window appears.



2. When you have finished specifying the settings, click the OK button in the Settings for View Filter window to register the filter conditions.

Related topics

- *5.2.1 Settings for view filters* in the *Configuration Guide*
- *3.28 Settings for View Filter window* in the *GUI Reference*

(2) Verifying that the events that match the view filter conditions are displayed

After you have finished specifying the view filter conditions, check whether the events that match the conditions are displayed.

Prerequisites

A view filter must be set up according to the procedure in 5.2.1(1) Using a view filter to filter events to be displayed.

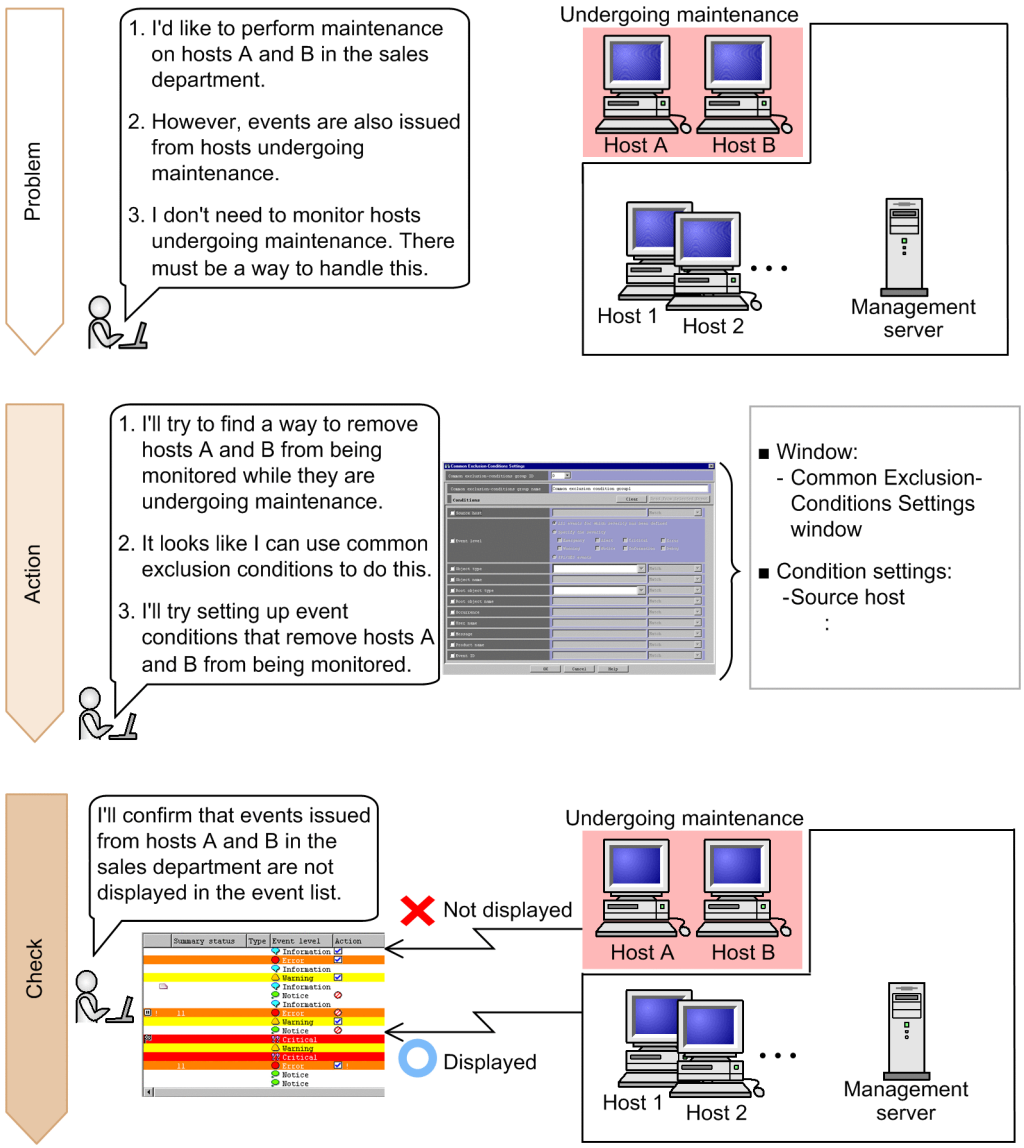
Procedure

1. Select the View filter check box in the Event Console window.
   Verify that the events that match the specified conditions are displayed in the event list.

5.2.2 Removing hosts undergoing maintenance from the items to be monitored

Whenever you restart a server on a host that is undergoing maintenance, a large number of events not needed for system monitoring are issued and displayed in the event list, making it difficult to check necessary events.

To avoid displaying unnecessary events in the event list, in advance remove hosts undergoing maintenance from the items to be monitored. With common exclusion-conditions, you can prevent actions from being executed while you continue monitoring events.



Important

Note:

If you need to perform maintenance on an entire system that includes JP1/IM - Manager, perform the maintenance in the order of higher hosts to lower hosts. If you start maintenance from lower hosts, the events that can be viewed in JP1/IM - View before JP1/IM - Manager stopped might be different from those after JP1/IM - Manager starts.

Keywords:

item, filter, common exclusion-condition, specific, host

Tip:

To remove, from the items to be monitored, the events that are not predefined in common exclusion conditions but become unnecessary while the system is operating:

After system monitoring starts, events that are not predefined in common exclusion conditions but become unnecessary while the system is operating might be issued. Use additional common exclusion conditions in filters to remove, from the items to be monitored, events that become unnecessary while the system is operating. Additional common exclusion conditions are exclusion conditions that are defined by using monitored events while the system is operating. For details, see *4.2.7 (3) Additional common exclusion-conditions* in the *Overview and System Design Guide*, and *6.5.4 Setting an additional common exclusion-condition to exclude a JP1 event from the monitoring target or action execution* in the *Administration Guide*.

(1) Using common exclusion conditions in a filter to temporarily stop hosts from being monitored

To remove hosts undergoing maintenance from the items being monitored, you use common exclusion conditions in a filter. To set common exclusion conditions, you use the Common Exclusion-Condition Settings window of Central Console. You can also use common exclusion conditions to remove action-triggering events from the items being monitored.

Prerequisites

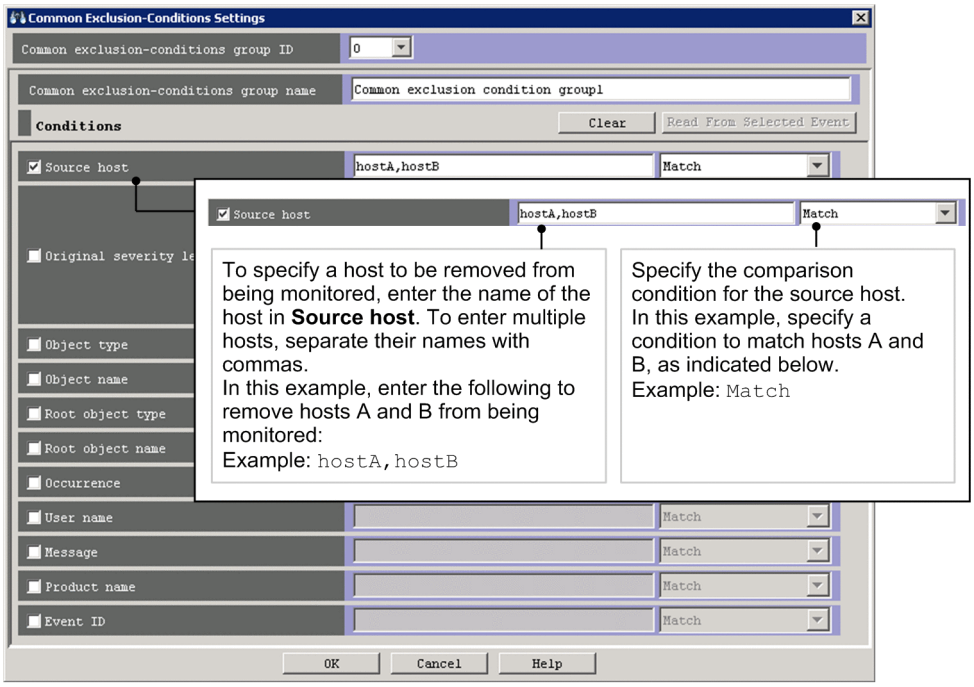
The JP1 user who wants to set common exclusion conditions in a filter must have `JP1_Console_Admin` permissions.

Procedure

1. In the Event Console window, select **Options** and then **System Environment Settings**. In the System Environment Settings window that appears, click the **Editing list** button to display the Event Acquisition Conditions List window.

2. In the Event Acquisition Conditions List, click the **Add** button in the **Common exclusion-conditions groups** area to display the Common Exclusion-Conditions Settings window.

3. Specify common exclusion conditions as described in the following figure:



4. Click the **OK** button in the Common Exclusion-Conditions Settings window.

   The Event Acquisition Conditions List window appears.

5. Click the **OK** button in the Event Acquisition Conditions List window.

   The System Environment Settings window appears.

6. On the **General** page, under **Common exclusion-conditions groups** in the **Event acquisition conditions** area, select the conditions you want to apply in the **Apply** column. Then, click the **Apply** button in the System Environment Settings window.

   The specified conditions are defined.

Related topics

- *4.2.6 Defining filter conditions* in the *Overview and System Design Guide*
- *14.9 Considerations for JP1/IM system-wide maintenance* in the *Overview and System Design Guide*
- *5.2.4 Settings for event acquisition filters* in the *Configuration Guide*
- *3.15 Common Exclusion-Conditions Settings window* in the *GUI Reference*

(2) Verifying that events from unmonitored hosts are not displayed

After you have specified the common exclusion conditions for the filter, make sure that events from the unmonitored hosts are not displayed in the event list. This subsection describes how to verify that events issued on host 1 are displayed in the event list, and that events issued on hosts A and B are not displayed in the event list.

Prerequisites

The following conditions must be satisfied:

- OS user mapping was configured according to *4.2.1 Configuring user mapping*.
- A basic configuration system was set up according to *4.1 What is IM Configuration Management?*.

Procedure

1. In the Event Console window, click the **Execute Command** button. The Execute Command window appears.
2. Set the items in the Execute Command window as described below, and then click the **Execute** button.

Item	Setting
Command type	Select **Command of managed host**.
Event information to inherit	Clear the **Inherit event information** check box.
Target host	Enter the following: `hostA`

Command	Enter the following:
	• In Windows:
	`"`*Base-path*`\bin\jevsend" -e SEVERITY=Warning -m Command executed from host A.`
	• In Linux:
	`/opt/jp1base/bin/jevsend -e SEVERITY=Warning -m Command executed from host A.`

   An event of severity level is `Warning` is issued on host A.

3. Repeat steps 1 and 2. Set the items in the Execute Command window as described below, and then click the **Execute** button.

Item	Setting
Command type	Select **Command of managed host**.
Event information to inherit	Clear the **Inherit event information** check box.
Target host	Enter the following: `hostB`

Command	Enter the following:
	• In Windows:
	`"`*Base-path*`\bin\jevsend" -e SEVERITY=Warning -m Command executed from host B.`
	• In Linux:
	`/opt/jp1base/bin/jevsend -e SEVERITY=Warning -m Command executed from host B.`

   An event of severity level `Warning` is issued on host B.

4. Repeat steps 1 and 2. Set the items in the Execute Command window as described below, and then click the **Execute** button.

Item	Setting
Command type	Select **Command of managed host**.
Event information to inherit	Clear the **Inherit event information** check box.
Target host	Enter the following: `host1`
Command	Enter the following:

Item	Setting
	• In Windows: "*Base-path*\bin\jevsend" -e SEVERITY=Warning -m Command executed from host 1. • In Linux: /opt/jp1base/bin/jevsend -e SEVERITY=Warning -m Command executed from host 1.

An event of severity level `Warning` is issued on host 1.

5. Verify that the event list contains the event issued on host 1, but does not contain the events issued on hosts A and B.

Related topics

- *3.1 Overview of the Event Console window* in the *GUI Reference*
- *3.24.2 Event Attributes page* in the *GUI Reference*
- *3.40 Execute Command window* in the *GUI Reference*

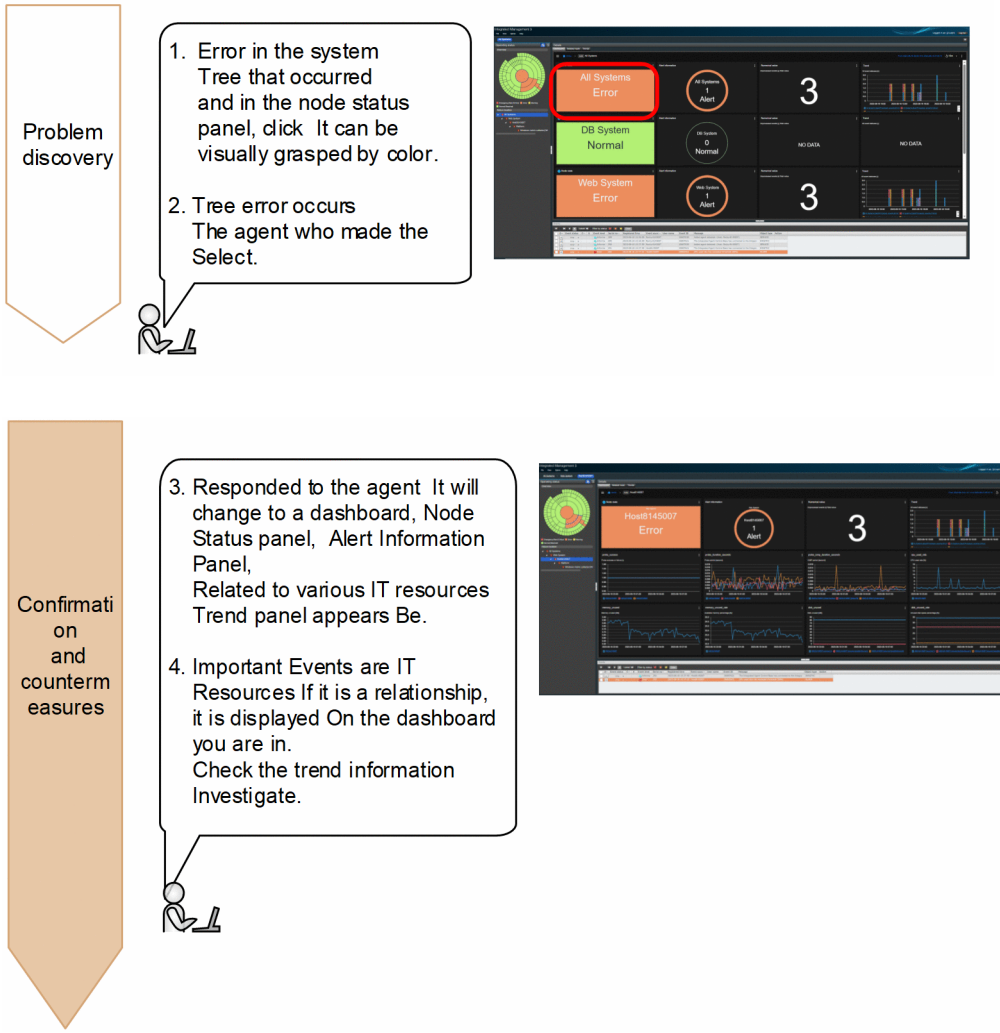
6

Detecting and Investigating System Errors

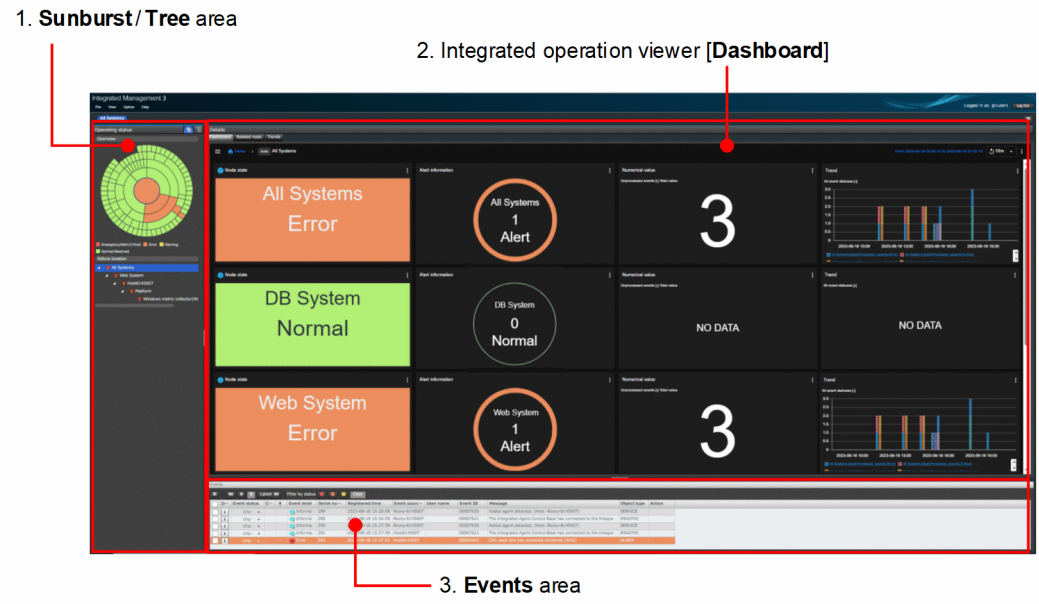
This section explains how to check for fault-related messages and nodes in the integrated operation viewer dashboard, and how to investigate related nodes.

It also describes how to use JP1/IM - View to automatically execute commands to detect system failures, and how to search for error events when investigating system failures.

6.1 About how to monitor and manage system events by integrated operation viewer



When you log in to Intelligent Integrated Management Base in a WWW browser, the following window appears.



No.	Area	Feature Overview
1	Sunburst/Tree	• Displays the status of the nodes throughout the system.
2	Integrated operation viewer [Dashboard]	• Displays the status of the nodes throughout the system. • Displays alert information for the entire system • Displays the number of unhandled events for the entire system. • Displays a graph of the response status of all events throughout the system
3	Events	• Displays a list of events for the entire system

The Node Status pane changes to the status of the failed node based on Intelligent Integrated Management Base's assessment of the system.

The Alert Info pane monitors performance data collected from monitored targets at thresholds and changes colors based on alert ratings. However, you must predefine the threshold settings.

Depending on the number of unhandled events and the number of handled events, you can check the occurrence and response status of critical events.

Related topics

- *2. Definition Files* in the *Command, Definition File and API Reference*

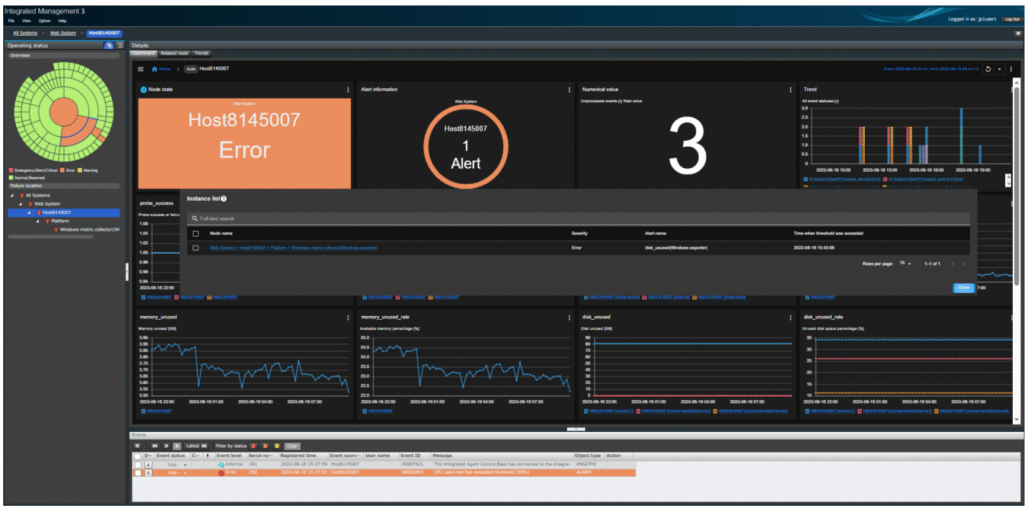
If you select agent in the tree, the dashboard part displays information about agent, for example:

- Agent Node Status Panel
- Alert Info Panel in agent
- Graphing Torrent Information for agent Miscellaneous IT Resources

When alert information is detected on a IT resource, you can view the various IT resource information of the target host graphically on the dashboard, and immediately check the status of the resource spike before and after the time of occurrence.

In addition, if you click ⋮ in the upper right corner of the graph and select "Compare", it can be displayed side by side with the graph of the past (such as one week ago) as shown in the following figure, so it can be used to estimate the cause of the impact when the event occurred.

When an error occurs in the Alert Info panel, clicking the Alert panel displays instance list, and you can check the "Node-name", "Alert-name", and "Threshold Time Exceeded".



When you select an exporter in the instance list, the events that occur in the selected exporter are displayed in the [Event list] part.

Click the Orange button that indicates Error. Events are filtered.

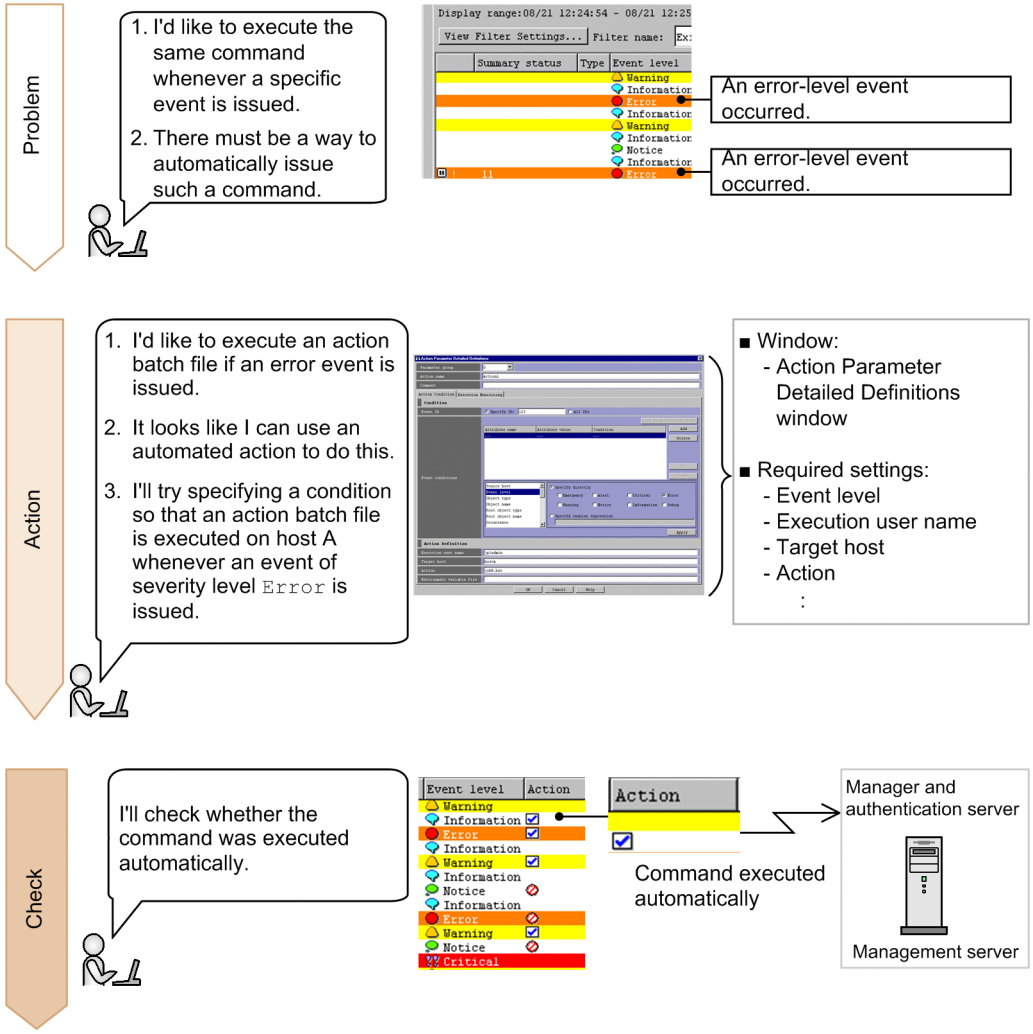
Click the button to see the event details.

Keywords:

GUI, Vision, Events, Sunburst, Tree, Graphics, Monitor Tree, integrated operation viewer, Root JobNet, Visual, Dashboard, Panels

6.2 Automatically executing a command whenever a specific event is issued

When an event is issued, the system administrator might execute one or more commands to handle the event. Executing a particular command every time a specific event occurs is a burden on the system administrator. To reduce the workload, in this section we will specify settings so that a command is automatically executed whenever a specific event is issued.



This manual describes how to execute the batch file `errornotice.bat` to send notification of an error to the system administrator when an event of severity level `Error` is issued. Prepare the batch file in advance, and store it in `C:\jp1im` on the management server for Windows.

In Linux, also use the procedure described below. Make sure that you replace the application's storage location and file name with those for Linux.

Tip:

To avoid re-execution of an action for a certain period of time:

If an event for which an automated action is set is issued many times in a short period of time, the action is automatically executed many times. By using the function for suppressing automated action execution, you can suppress the re-execution of actions for a certain period of time to avoid the execution of unnecessary actions.

For details, see *6.4.4 Suppressing identical actions* in the *Overview and System Design Guide*, and *5.5.4 Setting suppression of automated action execution* in the *Configuration Guide*.

To report the occurrence of a failure by email:

Use the JP1/IM - Manager email notification function to set up the automated action function to send an email when a failure occurs.

For details, see *A.1 (2) Creating an email environment definition file and setting up the email notification function (Windows only)*. In Linux, set up the function to use the `sendmail` command to send emails.

Keywords:

automated action, command, Automatic Action Service, email, notification

6.2.1 Using the automated action function to execute a command whenever an event is issued

You can use the automated action function to automatically execute commands. Set the definitions for automated actions in the Action Parameter Detailed Definitions window. Automated action definitions are the conditions by which automated actions are executed. In automated action definitions, you can also use variables to specify information included in events.

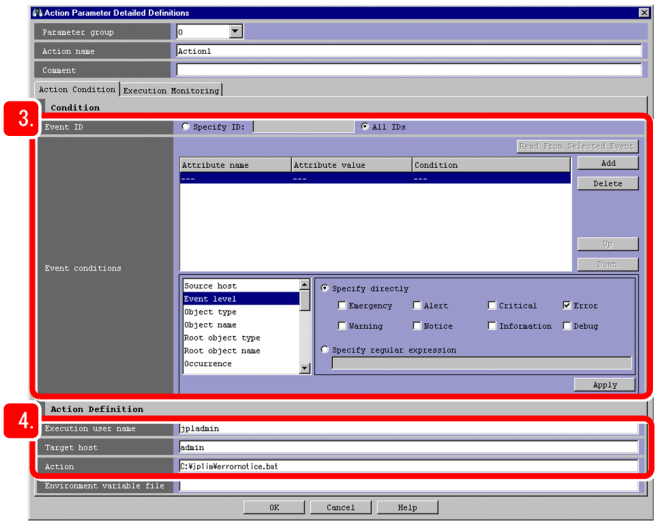
Prerequisites

The following conditions must be satisfied:

- OS user mapping was configured according to the procedure in *4.2.1 Configuring user mapping*.
- A JP1 user who wants to define automated actions must have JP1_Console_Admin permissions.

Procedure

1. In the Event Console window, select **Main Menu**, **Options**, and then **Automated Action Parameter Settings**. The Action Parameter Definitions window appears.
2. In the Action Parameter Definitions window, click the **Add** or **Edit** button. The Action Parameter Detailed Definitions window appears.
3. In **Condition**, specify the settings for **Event ID** and **Event Conditions** to set events that trigger an automated action.
   In this example, specify the following to set events whose severity level is `Error` as trigger events:
   - **Event ID**: Select **All IDs**.
   - List box: Select **Event level**.
   - **Specify directly**: Select the **Error** check box.



4. In **Action Definition**, specify an automated action to be executed when an event specified in **Condition** occurs.
   In this example, enter the items as follows:
   - **Execution user name**: `jp1admin`
     Enter the JP1 user name of the system administrator who will execute the action.
   - **Target host**: `admin`
     Enter the host name of the management server on which the action is to be executed.
   - **Action**: `C:\jp1im\errornotice.bat`
     Enter the name of the batch file that is stored on the management server and sends notification of an error to the system administrator.
5. In the Action Parameter Detailed Definitions window, click the **OK** button. The Action Parameter Definitions window appears.
6. In the Action Parameter Definitions window, click the **Apply** button.
   The specified settings are updated.

Related topics

- *3.33.1 Action Parameter Detailed Definitions window* in the *GUI Reference*

6.2.2 Verifying that a command specified as an automated action was executed

After you have finished specifying the automated action, check whether the command was executed according to your specifications. This subsection describes how to verify that the automated action for executing the batch file `errornotice.bat` to send an error notification to the management server (a Windows machine) is executed when an event whose severity level is `Error` is issued.

Prerequisites

OS user mapping must be configured according to the procedure in *4.2.1 Configuring user mapping*.

Procedure

1. In the Event Console window, click the **Execute Command** button. The Execute Command window appears.
2. Set the items in the Execute Command window as described below, and then click the **Execute** button.

Item	Setting
Command type	Select **Command of managed host**.
Event information to inherit	Clear the **Inherit event information** check box.
Target host	Enter the following: `hostA`

Command	Enter the following:
	• In Windows:
	`"`*Base-path*`\bin\jevsend" -e SEVERITY=Error`
	• In Linux:
	`/opt/jp1base/bin/jevsend -e SEVERITY=Error`

   An event of severity level `Error` is issued on host A.

   In the **Action** column in the event list, an executed action icon (☑) is displayed for the event that triggered the automated action.
3. In the Event Console window, select the event issued in step 2. To display the Action Log window, select **View**, and then select **Action Log**.
4. In the Action Log window, confirm that **Ended** is displayed in the **Status** column for the action shown in the **Log** list.

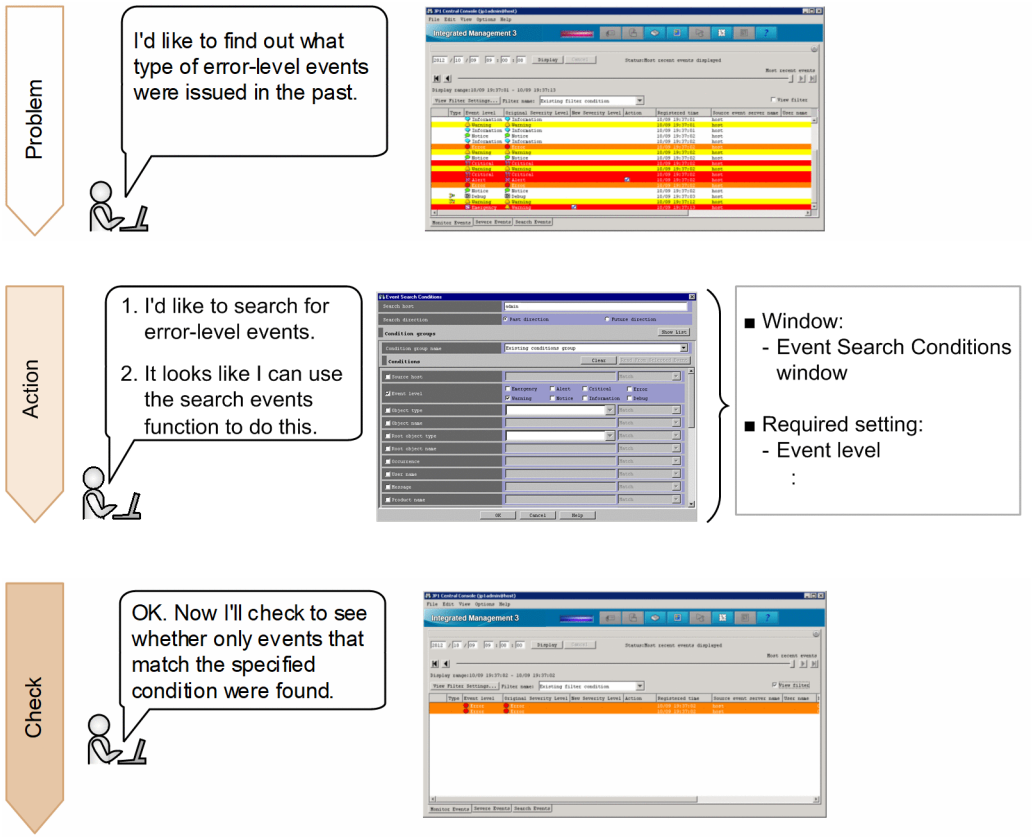
Related topics

- *3.1 Overview of the Event Console window* in the *GUI Reference*
- *3.36 Action Log window* in the *GUI Reference*
- *3.40 Execute Command window* in the *GUI Reference*

6.3 How to search for events in JP1/IM - View

To investigate a fault, in addition to the events listed in the event list, you must check the events to see if any events related to the fault have been issued. However, the event may have already been cleared from the event list during the failure investigation phase.

Let's search for events that have been cleared from the event list by specifying event conditions.



Keywords:

search events function, searching, investigation

Tip:

To display past events that are no longer displayed in the event list:

To display past events that are no longer displayed in the event list, use the event display start-time specification function. On the pages **Monitor Events** and **Severe Events** in the Event Console window, you can specify the display start-time for the event list by specifying a date and time or moving the slider. For details, see *6.6 Displaying an event by specifying an event display start-time* in the *Administration Guide*.

6.3.1 Using the search events function to search for events that match a specified condition

You can use the search events function to search for events. Set the conditions for the search events function in the Event Search Conditions window.

Prerequisites

To search for events registered in the JP1/Base event database:

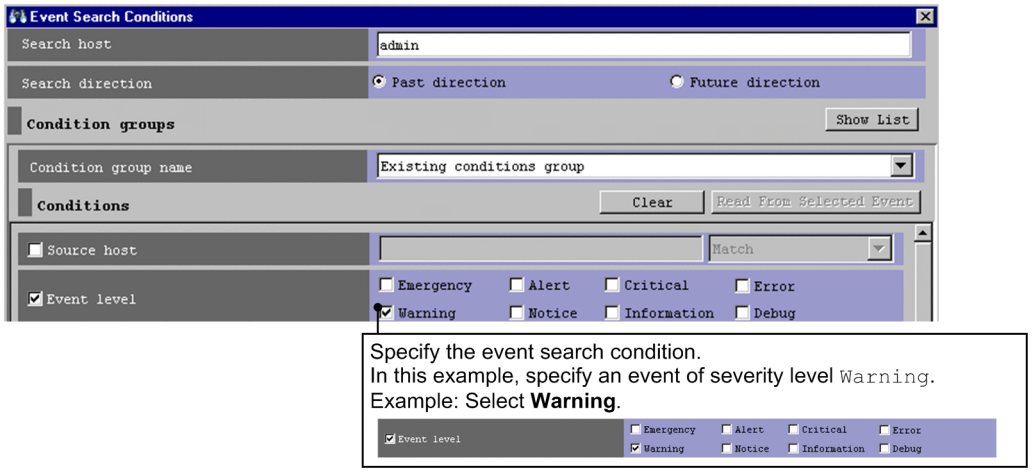
None

To search for events registered in the integrated monitoring database in addition to the above events:

The integrated monitoring database must be configured and enabled according to *2.4.4(3) Setting up an integrated monitoring database (for Windows)* or *2.5.4(3) Setting up an integrated monitoring database (for Linux)*.

Procedure

1. Click the **Search Events** button on the **Search Events** page. The Event Search Conditions window appears.
2. Search for events of severity level `Warning` according to the following figure:



3. In the Event Search Conditions window, click the **OK** button.

   The events that match the specified condition are displayed on the **Search Events** page.

Related topics

- *4.6 Searching for events* in the *Overview and System Design Guide*
- *6.8.1 Search method* in the *Administration Guide*

6.3.2 Verifying that events were found

After you specify the event search conditions, check whether the events you wanted to find are displayed on the **Search Events** page. The procedure below applies when you searched for events according to *6.3.1 Using the search events function to search for events that match a specified condition*.

Procedure

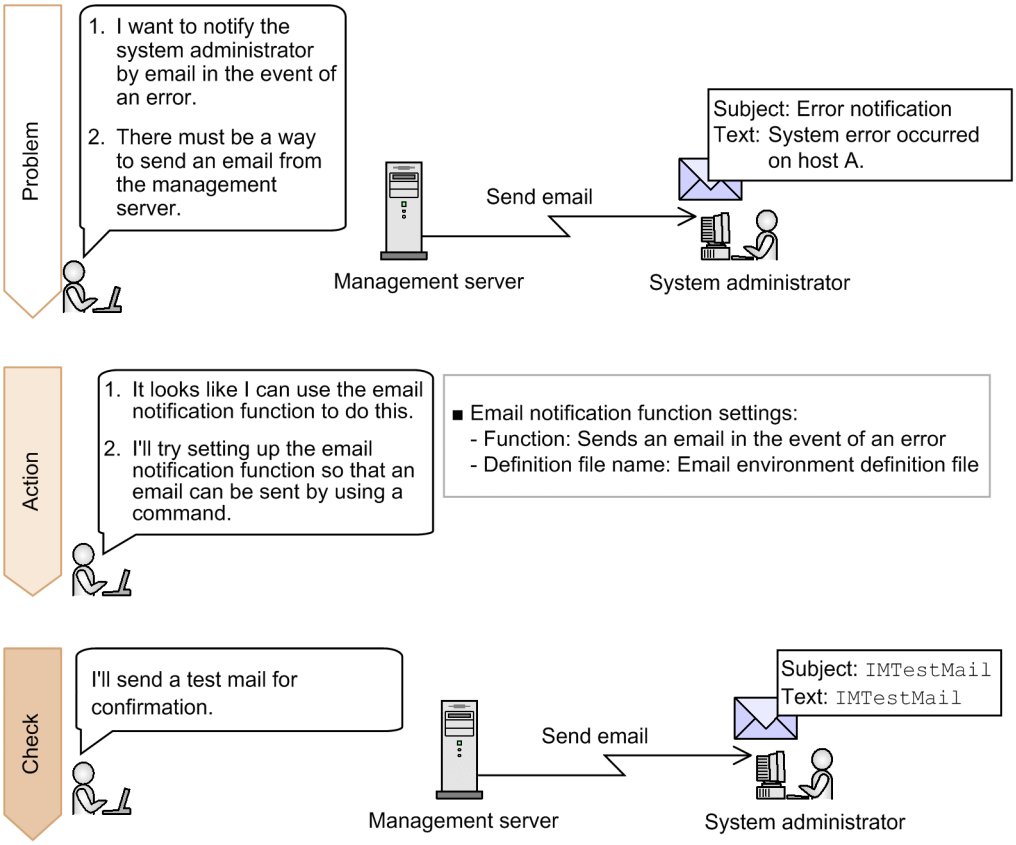
1. Verify that events of severity level `Warning` are displayed.

Appendixes

A. Using the Email Notification Function to Send Emails (Windows Only)

If you want to send emails by using only JP1/IM - Manager, use the JP1/IM - Manager email notification function. To use this function, you need to set up an email environment definition file.

In this appendix, we will set up an email environment definition file for JP1/IM - Manager so that you can send emails.



A.1 Setting up the email notification function (Windows only)

The email notification function provided by JP1/IM - Manager uses the JP1/IM - Manager `jimmail` command to send emails. This manual describes how to specify the settings for using the email notification function to send emails.

(1) Settings of the email environment definition file to be created

The following provides the detailed settings of the email environment definition file that will be created in *A.1 (2) Creating an email environment definition file and setting up the email notification function (Windows only)*.

Specification details for the email environment definition file

Specification	Target setting	Description
`From=jp1_xxx@yyy.jp`	Source email address	Specifies the source email address in the range of 1 to 256 bytes. Specify only one address. You can use the following characters: • Alphanumeric characters (0-9 and a-z) • At mark (`@`)

Specification	Target setting	Description
		• Period (.) • Hyphen (-) • Underscore (_)
`SmtpServer=`*host-name-or-IP-address-of-the-SMTP-server*	Host name or IP address of the SMTP server	Specifies the host name or IP address of the SMTP server that is connected for sending email. IP addresses are supported only for IPv4. You can specify only one SMTP server.
`AuthMethod=SMTP`	Authentication method when sending an email	Specifies the authentication method used on the mail server when sending an email. `NONE`: No authentication • `POP`: POP before SMTP authentication • `SMTP`: SMTP-AUTH authentication (LOGIN/PLAIN) The default is `NONE`.
`AuthUser=`*authentication-account-name*	Authentication account name used for POP before SMTP authentication or SMTP-AUTH authentication	Specifies the authentication account name used for POP before SMTP authentication or SMTP-AUTH authentication. You can use a string of 1 to 255 bytes. The default is a null character (`""`).

(2) Creating an email environment definition file and setting up the email notification function (Windows only)

To customize the settings of the email notification function, you need to set up the email environment definition file. This manual describes how to specify the settings required for connecting the mail server by using SMTP-AUTH authentication.

Prerequisites

The following conditions must be satisfied:

- A mail server that supports SMTP-AUTH authentication is provided in advance.
- The mail server has an IPv4 IP address.
- The OS user who will execute the `jimmailpasswd` command has Administrator permissions.

Procedure

1. Use a text editor to open the email environment definition file.
   Console-path`\conf\mail\jimmail.conf`
2. In the email environment definition file, specify the following items:
   - From
     `From=jp1_xxx@yyy.jp`
   - SmtpServer
     `SmtpServer=`*host-name-or-IP-address-of-the-SMTP-server*
   - AuthMethod
     `AuthMethod=SMTP`
   - AuthUser
     `AuthUser=`*authentication-account-name*
3. Execute the following `jimmailpasswd` command to set the authentication password:

"*Console-path*\bin\jimmailpasswd" -p *authentication-password*

4. Set up the communication environment.
   - Name resolution for the mail server host
     Set up the `jp1hosts`, `jp1hosts2`, and `hosts` files and DNS so that the SMTP server name and POP3 server name can be resolved.
   - Firewall settings
     Set up a firewall to allow SMTP/POP3 communication between the `jimmail` command and the mail server.

Related Topics

- *Email environment definition file (jimmail.conf)* in *2. Definition Files* in the *Command, Definition File and API Reference*
- *jimmail (Windows only)* in *1. Commands* in the *Command, Definition File and API Reference*
- *jimmailpasswd (Windows only)* in *1. Commands* in the *Command, Definition File and API Reference*
- *3.1 Registering hosts* in the *Configuration Guide*
- *9.3.1 Basic information about firewalls* in the *Configuration Guide*

A.2 Verifying that the email notification function has been set up correctly (Windows only)

This appendix describes how to verify that, after you set up an email environment definition file according to *A.1 (2) Creating an email environment definition file and setting up the email notification function (Windows only)*, the receiver received an email that was sent from JP1/IM - Manager by executing the `jimmail` command.

Prerequisites

The following conditions must be satisfied:

- The email notification function has been set up according to *A.1 (2) Creating an email environment definition file and setting up the email notification function (Windows only)*.
- The email receiving terminal is able to receive the email address specified for the destination in the `jimmail` command.
- The OS user who will execute the `jimmail` command has Administrator permissions.

Procedure

1. Execute the `jimmail` command.
   In the following example, the command sends an email to `user@hitachi.com`:
   "*Console-path*\bin\jimmail" -to user@hitachi.com -s IMTestMail -b IMTestMail
2. Confirm that the email arrived at the address specified for the destination.
   Confirm that the email addressed to `userA@hitachi.com` arrived at the receiving terminal.

A.3 Example definition for an automated action when using the email notification function (Windows only)

When you define an automated action, you can specify the `jimmail` command as the action to be executed so that an email will be sent based on the attribute values of an event that triggers the automated action. Below is an example definition when the `jimmail` command is specified as the action to be executed. For details about how to define an automated action, see *6.2.1 Using the automated action function to execute a command whenever an event is issued*.

Example definition of an automated action when specifying the `jimmail` command as the action to be executed

Item to be set	Description
Event ID	**All IDs are selected**.
Event conditions	The event level matches Error.
Execution user name	`jp1admin`
Target host	`admin`
Action	`jimmail.exe -to user@hitachi.com -s "[Event level:$EVSEV] Error notification" -b "An error occurred on a monitored host.\n---\nSerial number=$EVSEQNO\nEvent issue date=$EVDATE $EVTIME\nEvent ID=$EVIDBASE\nError level=$EVSEV\nProduct name=$EV"PRODUCT_NAME"\nMessage=$EVMSG\n---\nFrom:IM-M host($ACTHOST)"`

The following shows an example email that is sent when the automated action is specified as described above:

Item	Description
Source (From)	`jp1_xxx@yyy.jp`
Destination (To)	`user@hitachi.com`
Email subject	`[Event level:Error]Error notification`

Email text	`An error occurred on a monitored host.`
	`---`
	`Serial number=1234567`
	`Event issue date=2014/01/01 10:00:00`
	`Event ID=000A`
	`Error level=Error`
	`Product name=/HITACHI/XXXXX/JP1`
	`nMessage=System error occurred on a monitored host`
	`---`
	`From:IM-M host(admin)`

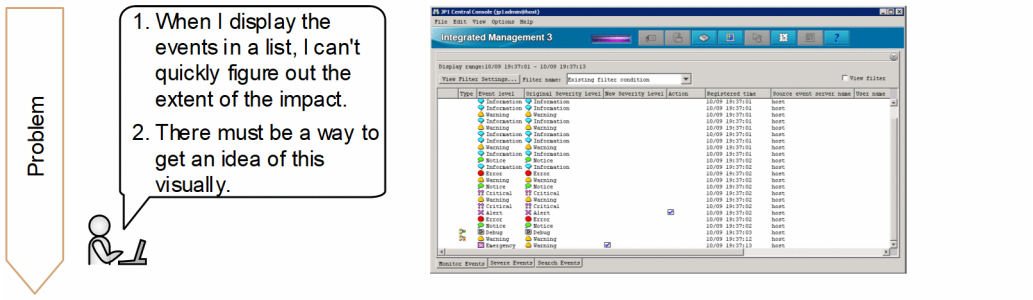
When you define an automated action, consider the specified event conditions and suppression of automated actions to prevent a heavy load on the system due to execution of a large number of automated actions.

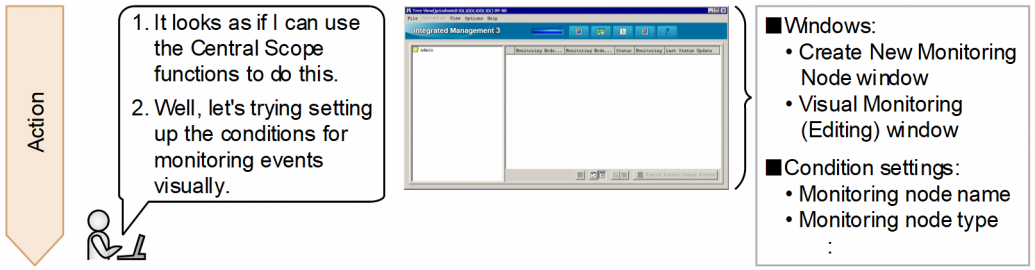
Related Topics

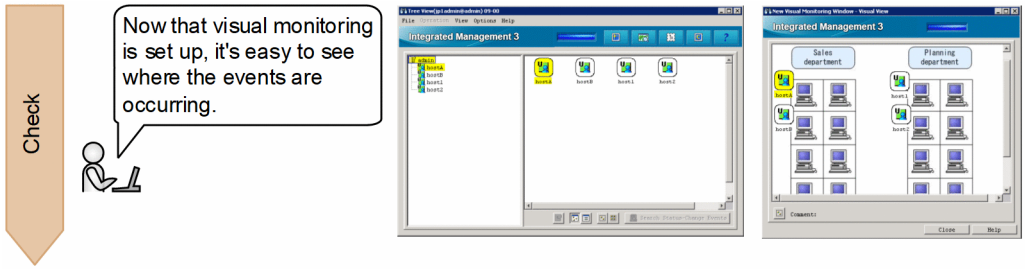
- *4.19.5 Inheriting event information when a command is executed* in the *Overview and System Design Guide*

B. Using Visual Monitoring to Understand the Extent of the Impact of a System Error

You can display the hierarchy and location of the monitored hosts for a visual indication of the extent to which an event issued in the system impacts the hosts. In this section, we will visually monitor a system to understand the extent of an event's impact.







Keywords:

GUI, visual, event, tree, graphics, monitoring tree, central scope, object-oriented, visual

B.1 Procedure for configuring visual monitoring

To visually monitor the system, you can use a *central scope*, which captures events issued in the system based on a logical perspective.

Use the following procedure to configure the central scope:

1. Set up the central scope.
2. Configure the central scope to enable visual monitoring in a tree format.
3. Set the attributes of monitoring nodes
4. Configure the central scope to enable visual monitoring in a map format.

This manual describes how to configure the central scope to monitor the basic configuration system *2.1 Overview of a basic configuration system*. This manual also describes how to specify that the status of the monitoring node changes when an event of severity level `Warning` is received from host A. The following separately describes the configuration procedure for tree format and map format.

(1) Setting up the central scope

When JP1/IM - Manager is installed, the central scope function is disabled. Therefore, you must use the `jcoimdef` command to enable the central scope service. Perform this operation on managers.

Prerequisites

The OS user who will execute the `jcsdbsetup`, `jcoimdef`, and `jco_spmd_status` commands has Administrator or `root` permissions.

Procedure

1. Stop the JP1/IM3 - Manager service.
2. Execute the following `jcsdbsetup` command to create a central scope database:
   - In Windows:
     "*Scope-path*\bin\jcsdbsetup"
   - In Linux:
     /opt/jp1scope/bin/jcsdbsetup
3. Execute the following `jcoimdef` command to enable the central scope service (`jcsmain`):
   - In Windows:
     "*Console-path*\bin\jcoimdef" -s ON
   - In Linux:
     /opt/jp1cons/bin/jcoimdef -s ON
4. Start the JP1/IM3 - Manager service.
5. Execute the following `jco_spmd_status` command to make sure that the central scope service is running:
   - In Windows:
     "*Console-path*\bin\jco_spmd_status"
   - In Linux:
     /opt/jp1cons/bin/jco_spmd_status

   Make sure that `jcsmain` is displayed as a running process.

Related topics

- *jcoimdef* in *1. Commands* in the *Command, Definition File and API Reference*
- *jcsdbsetup* in *1. Commands* in the *Command, Definition File and API Reference*

(2) Configuring the central scope to enable visual monitoring in a tree format

To visually monitor the system hierarchy, add monitoring nodes in the Monitoring Tree window of the central scope.

Prerequisites

A JP1 user must satisfy the following conditions in order to perform the operation:

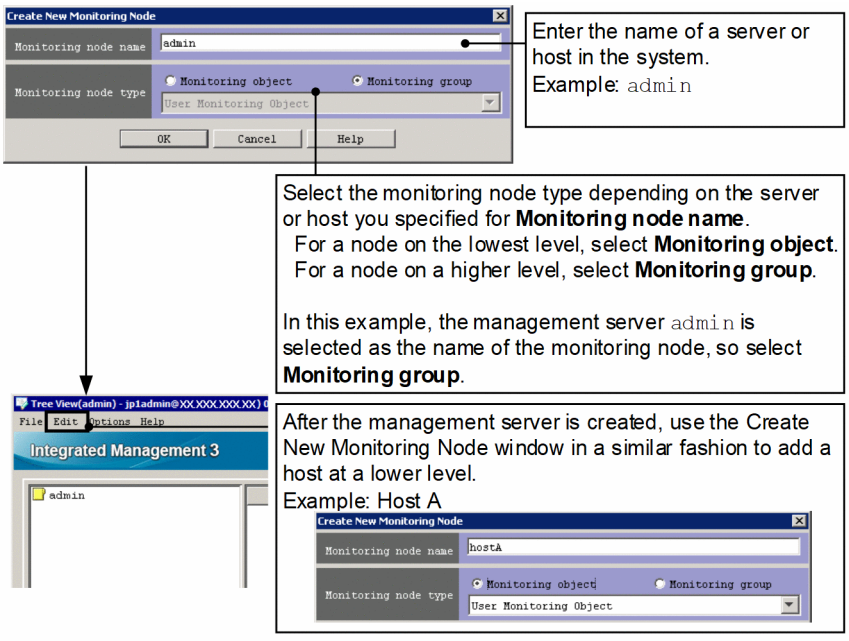
- JP1 permission level `JP1_Console_Admin` has been assigned.
- JP1 resource group `JP1_Console` has been assigned.

Procedure

1. From the Windows **Start** menu, select **All Programs**, **JP1_Integrated Management - View**, and then **Edit Monitoring Tree**. The Monitoring Tree (Editing) window appears.
   After logging in to the central scope, you can also display the Monitoring Tree (Editing) window from the Monitoring Tree window.

2. In the Monitoring Tree (Editing) window, select **Edit**, and then **Create New Monitoring Node**. The Create New Monitoring Node window appears.

3. Add the monitoring nodes according to the following figure.



4. In the Monitoring Tree (Editing) window, select **File**, and then **Update Server Tree** to apply the edited tree data to the Monitoring Tree window.
   When the Login window appears, enter the JP1 user name and password registered on the authentication server.

Related topics

- *6.3.1 Opening the Monitoring Tree (Editing) window* in the *Configuration Guide*
- *6.3.3 Generating a monitoring tree automatically* in the *Configuration Guide*
- *4.1 Logging in to JP1/IM - Manager* in the *Administration Guide*
- *1.2 Login window* in the *GUI Reference*
- *4.1 Overview of the Monitoring Tree window* in the *GUI Reference*
- *4.15 Monitoring Tree (Editing) window* in the *GUI Reference*

(3) Setting the attributes of monitoring nodes

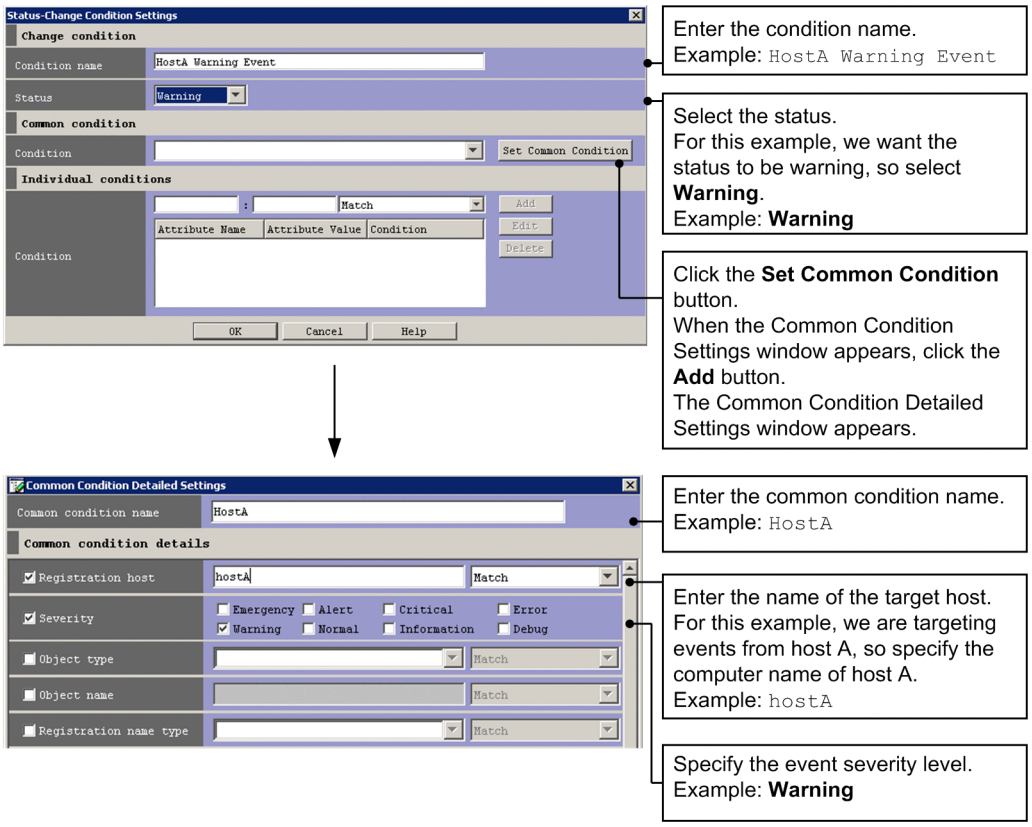
By setting the attributes of monitoring nodes, you can change the icon used by a monitoring node or change the status of a monitoring node when an event is received. The following describes how to set the monitoring node attributes for host A shown in *2.1 Overview of a basic configuration system*.

Prerequisites

Monitoring nodes must be displayed in the Monitoring Tree window.

Procedure

1. In the Monitoring Tree window, select host A.
2. In the pop-up menu displayed by right-clicking, select **Properties** to open the Properties window.
3. Select the **Status-Change Condition** list box, and then click the **Add** button. The Status-Change Condition Settings window appears.
4. Specify the necessary settings in the Status-Change Condition Settings window and the Common Condition Detailed Settings window according to the following figure.



5. In the Common Condition Detailed Settings window, click the **OK** button.
6. In the Common Condition Settings window, click the **Close** button.
7. In the Status-Change Condition Settings list box, from the **Condition** pull-down list under **Common condition**, select the common condition name you added in step 4.
8. In the Status-Change Condition Settings window, click the **OK** button.
9. In the Properties window, click the **Apply** button.

Related topics

- *4.9 Properties window* in the *GUI Reference*
- *4.12 Status-Change Condition Settings window* in the *GUI Reference*
- *4.13 Common Condition Settings window* in the *GUI Reference*
- *4.14 Common Condition Detailed Settings window* in the *GUI Reference*

(4) Configuring the central scope to enable visual monitoring in a map format

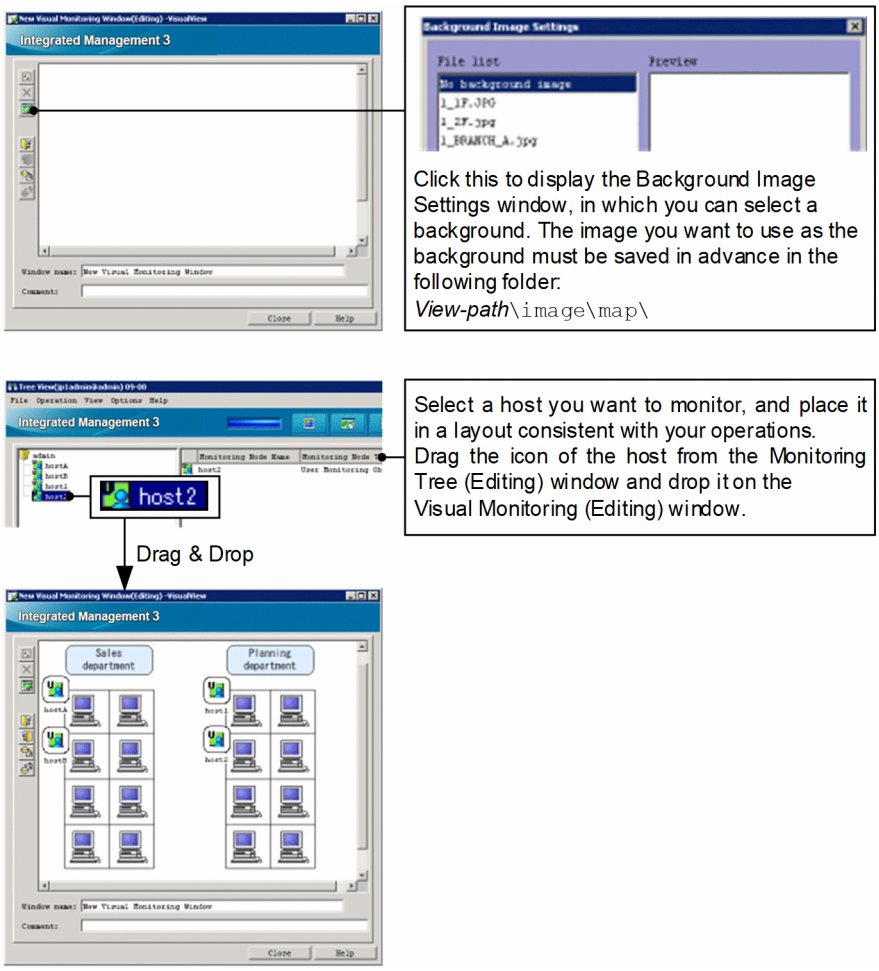
To display hosts in a map format, you first create a Visual Monitoring window. The following describes how to create the Visual Monitoring window from the Visual Monitoring (Editing) window.

Prerequisites

Monitoring nodes must be displayed in the Monitoring Tree window.

Procedure

1. From the Windows **Start** menu, select **All Programs**, **JP1_Integrated Management - View**, and then **Edit Monitoring Tree**. The Edit View window appears.
2. In the Monitoring Tree (Editing) window, from the menu bar, select **Acquire Tree from Server** to apply the settings in the Monitoring Tree window to the Monitoring Tree (Editing) window.
3. In the Monitoring Tree (Editing) window, from the menu bar, select **Edit**, and then **Create New Visual Monitoring Window**. The Visual Monitoring (Editing) window appears.
4. Create a Visual Monitoring window according to the following figure.



5. Click the (Update the Visual Monitoring) button to apply the settings of the Visual Monitoring window to the manager.
   When the Login window appears, enter the JP1 user name and password registered on the authentication server.

Related topics

- *4.4 Visual Monitoring (Editing) window* in the *GUI Reference*
- *4.5 Visual Monitoring window* in the *GUI Reference*
- *6.4.1 Opening an edit window for the Visual Monitoring window* in the *Configuration Guide*
- *6.4.3 Customizing a Visual Monitoring window* in the *Configuration Guide*

B.2 Verifying that you can monitor the extent of impact of events in map format and tree format

In the Monitoring Tree window and the Visual Monitoring window, check the extent of the impact of events. The following describes how to issue events on host A shown in *2.1 Overview of a basic configuration system*.

Prerequisites

OS user mapping must be completed according to *4.2.1 Configuring user mapping*.

Procedure

1. In the Event Console window, click the **Execute Command** button. The Execute Command window appears.

2. Follow the procedure in *4.2.2 Verifying that you can execute a command* to set the items in the Execute Command window as described below, and then click the **Execute** button.

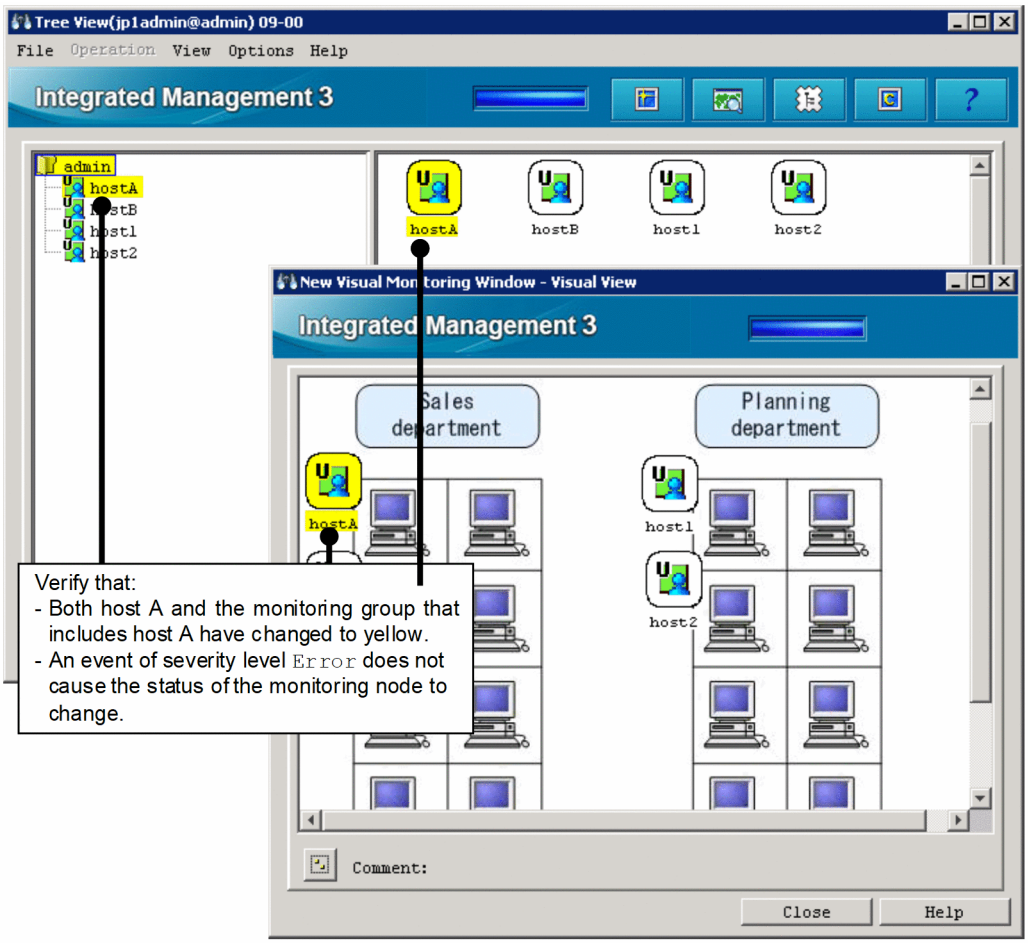
Item	Setting
Command type	Select **Command of managed host**.
Event information to inherit	Clear the **Inherit event information** check box.
Target host	Enter the following: `hostA`

Command	Enter the following:
	• In Windows:
	`"`*Base-path*`\bin\jevsend" -e SEVERITY=Warning -m Warning Event Issued`
	• In Linux:
	`/opt/jp1base/bin/jevsend -e SEVERITY=Warning -m Warning Event Issued`

   An event of severity level `Warning` is issued on host A.

3. Check the Monitoring Tree window and Visual Monitoring window.

   Among the monitoring nodes, the status of the monitoring node on which the error occurred, and the monitoring group that includes that monitoring node, automatically change to the error status.



For this example, verify that host A and the monitoring group that includes host A change to yellow when an event of severity level `Warning` is issued.

4. Repeat step 2. Set the items in the Execute Command window as described below, and then click the **Execute** button.

Item	Setting
Command type	Select **Command of managed host**.
Event information to inherit	Clear the **Inherit event information** check box.
Target host	Enter the following: `hostA`
Command	Enter the following: • In Windows: "*Base-path*\bin\jevsend" -e SEVERITY=Error -m Error Event Issued • In Linux: /opt/jp1base/bin/jevsend -e SEVERITY=Error -m Error Event Issued

An event of severity level `Error` is issued on host A.

5. Check the Monitoring Tree window and Visual Monitoring window.

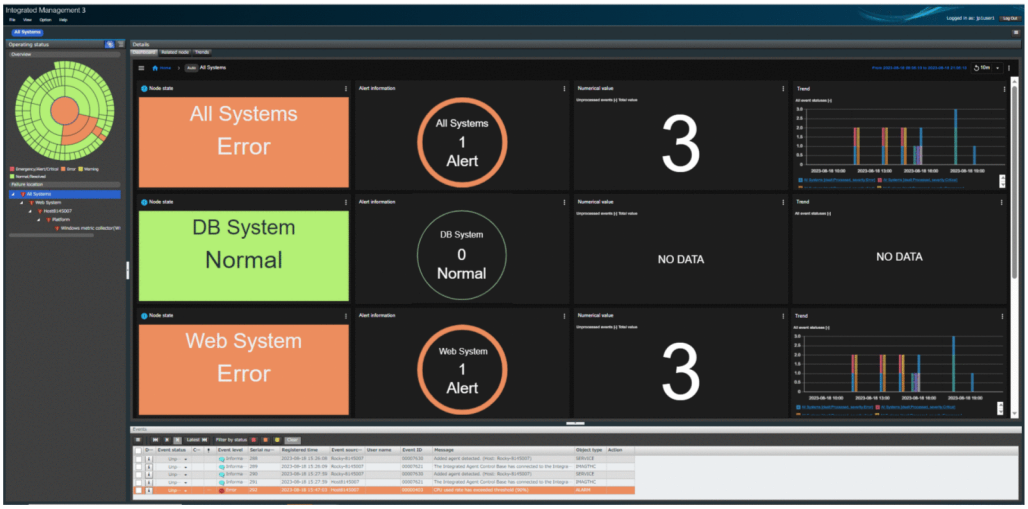
For this example, verify that the status of host A or the monitoring group that includes host A does not change when an event of severity level `Error` is issued.

Related topics

- *3.1 Overview of the Event Console window* in the *GUI Reference*
- *3.40 Execute Command window* in the *GUI Reference*

C. Visualizing IT Health

When you log in to Intelligent Integrated Management Base in a WWW browser, the following window appears.

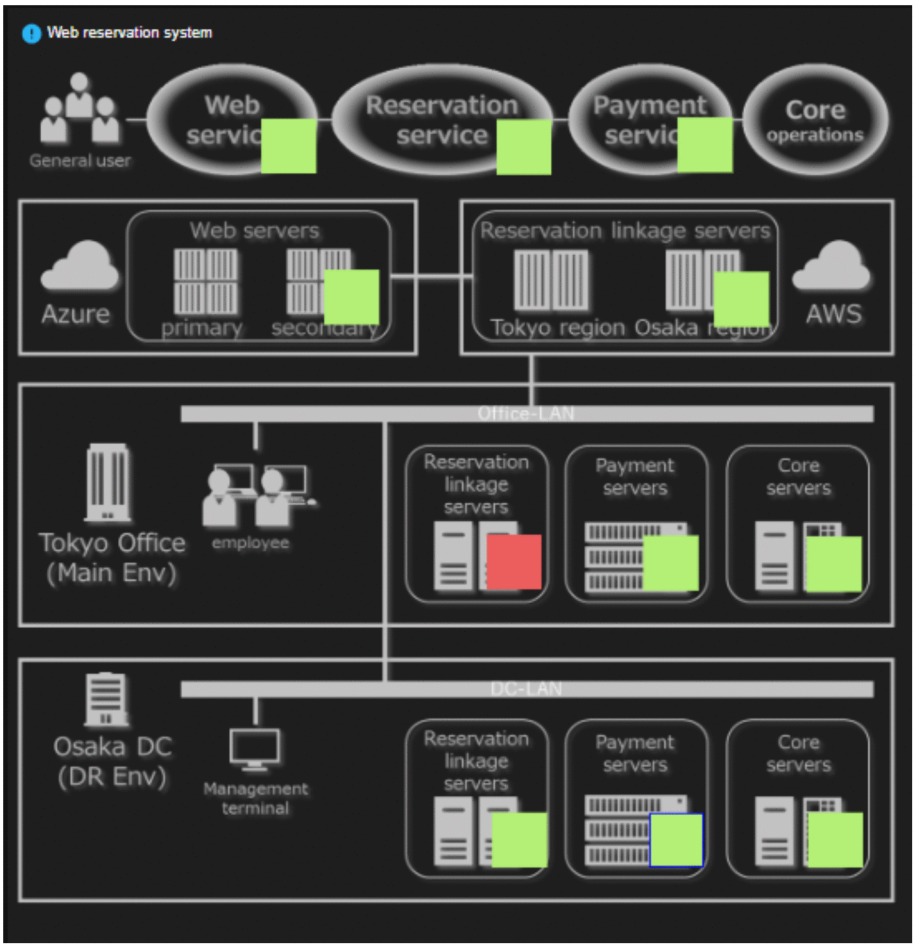


Integrated operation viewer [Dashboard] allows you to create several original dashboards that are tailored to your needs, apart from the system-generated dashboards.

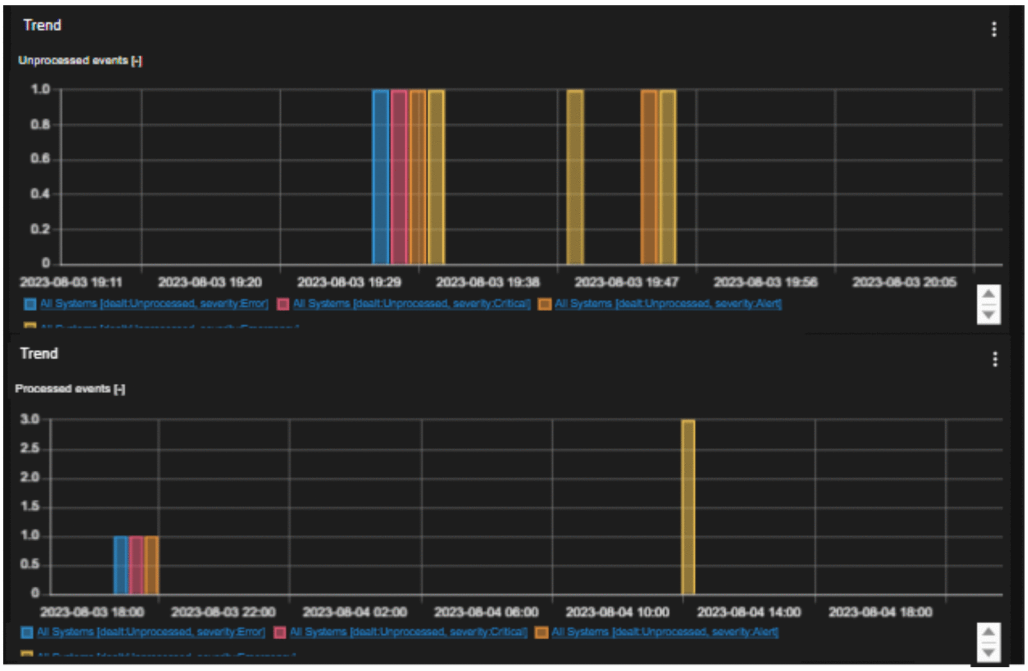
See: *2. Integrated Operation Viewer Window* in the *GUI Reference*.

For example, a system that realizes Web reservation services is not limited to Web related systems, but is linked with related systems such as payment systems and mission-critical business systems to realize services. Therefore, to check the health of Web reservation service, you need to monitor several systems together. In Node state map pane of the dashboard, you can specify a background image and view the nodes on the background image.

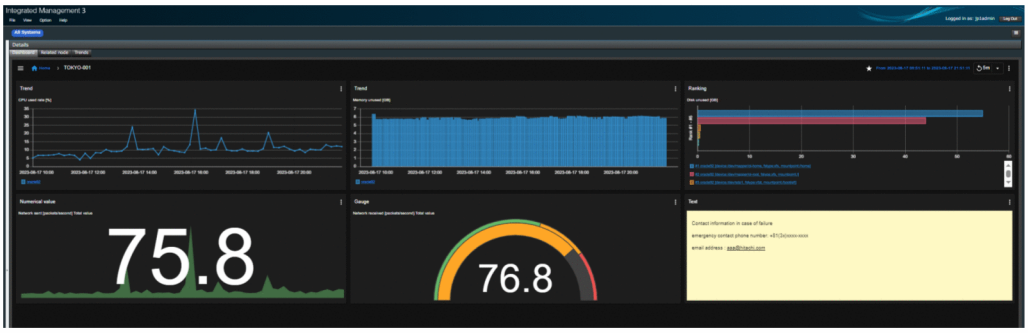
In the following example, you can see the state of a node with a small green or red square.



Transitions of "Unhandled events" and "Number of handled events" of critical events can also be graphed by node. This allows you to grasp the occurrence and response status by time-of-day or monthly time-of-day and can be used to assess the health of IT and improve planning.



You can also create a dashboard that selects only trend information you are interested in in among the various nodes, if you have more than one system. Trend information can be visualized and displayed in line charts, bar charts, gauges, numbers, and ranking formats.



By displaying the free disk space for one month, you can monitor predictable capacity shortage in the future.

Integrated operation viewer [Dashboard] can also display only the Dashboard window without displaying the tree or event list immediately after logging in.

D. Port Numbers

This appendix describes the port numbers used by JP1/IM and JP1/Base and related to the systems described in this manual. The protocol is TCP/IP. The port numbers are set when the product is installed.

D.1 JP1/IM port numbers

The table below lists the JP1/IM port numbers related to the systems described in this manual. In addition to these port numbers, port numbers 1025 to 65535/tcp which are automatically assigned by the OS are used at the time of communication. Note, however, that the range of assigned port numbers might differ depending on the OS.

List of JP1/IM port numbers related to the systems described in this manual

Service name	Port number	IM-V	IM-M	Description
`jp1imevtcon`	20115/tcp	Y	Y	Used to connect to JP1/IM - Manager (event console service) from JP1/IM - View
`jp1imcmda`	20238/tcp	Y	--	Used to execute commands from JP1/IM - View
`jp1imcss`	20305/tcp	Y	Y	Used to connect to JP1/IM - Manager (central scope service) from JP1/IM - View
`JP1/IM3-Manager DB Server`	20700/tcp	--	N	Used for internal processing by JP1/IM - Manager (IM database)
`jp1imcf`	20702/tcp	Y	Y	Used to connect to JP1/IM - Manager (IM Configuration Management service) from JP1/IM - View
`jp1imfcs`	20701/tcp	--	Y	Used for internal processing by JP1/IM - Manager (event base service)
`jp1imegs`	20383/tcp	--	Y	Used for internal processing by JP1/IM - Manager (Event Generation Service)
`jddmain`	20703/tcp	--	--	Used to connect to JP1/IM - Manager (Intelligent Integrated Management Base service) from a Web client (a Web browser or a client to issue REST APIs)

Legend:

IM-V: JP1/IM - View

IM-M: JP1/IM - Manager

Y: Registered in the `services` file at installation

N: Cannot be registered in the `services` file

--: Not registered in the `services` file at installation (No need to set)

D.2 JP1/Base port numbers

The table below lists the JP1/Base port numbers related to the systems described in this manual. In addition to these port numbers, port numbers 1025 to 65535/tcp which are automatically assigned by the OS are used at the time of communication. Note, however, that the range of port numbers assigned might depend on the OS.

List of JP1/Base port numbers related to the systems described in this manual

Service name	Port numbers	Description
`jp1imevt`	20098/tcp	Used to forward events to other hosts

Service name	Port numbers	Description
jp1imevtapi	20099/tcp	Used by all products that register and acquire events, and functions for issuing and acquiring events
jp1imrt	20237/tcp	Used by IM Configuration Management
jp1imcmda	20238/tcp	Used to execute commands
jp1imcmdc	20239/tcp	Used to execute commands
jp1bsuser	20240/tcp	Used by user authentication servers
jp1bsplugin	20306/tcp	Used to collect and distribute definition information for JP1/IM
jp1bscom	20600/tcp	Used for communication between IM Configuration Management and service management control

D.3 Direction of communication through a firewall

The table below describes the direction in which hosts communicate through a firewall. JP1/IM and JP1/Base support both packet filtering and NAT (static mode).

Direction of communication through a firewall

Service name	Port number	Direction of communication
jp1imevt	20098/tcp	JP1/Base that transfers events -> JP1/Base that receives events
jp1imevtapi	20099/tcp	A program (such as JP1/IM - Manager) that acquires events -> JP1/Base
jp1imevtcon	20115/tcp	JP1/IM - View -> JP1/IM - Manager (central console)
jp1imrt	20237/tcp	JP1/IM - Manager -> JP1/Base
jp1imcmda	20238/tcp	JP1/IM - View -> JP1/IM - Manager (central console) JP1/IM - Manager (central console) -> JP1/Base[#1]
jp1imcmdc	20239/tcp	JP1/Base on a host with JP1/IM - Manager installed <- -> JP1/Base on a host that executes commands
jp1bsuser	20240/tcp	JP1/IM - Manager -> JP1/Base
jp1imcss	20305/tcp	JP1/IM - View -> JP1/IM - Manager (central console)
jp1bsplugin	20306/tcp	Higher-level program using services such as JP1/IM - Manager -> JP1/Base
jp1imegs	20383/tcp	Firewall setup is unnecessary because all communication takes place on the machine on which JP1/IM - Manager is installed.
jp1bscom	20600/tcp	JP1/IM - Manager <- -> JP1/Base on another host
JP1/IM3-Manager DB Server	20700/tcp	JP1/IM - Manager -> JP1/IM-Manager DB Server
jp1imfcs	20701/tcp	Firewall setup is unnecessary because all communication takes place on the machine on which JP1/IM - Manager is installed.
jp1imcf	20702/tcp	JP1/IM - View -> JP1/IM - Manager (IM Configuration Management)
jddmain	20703/tcp	Web client (Web browser or client to issue REST APIs) -> JP1/IM - Manager (Intelligent Integrated Management Base)
jimmail	25/tcp[#2]	JP1/IM - Manager -> Mail server (SMTP) (without authentication)

Service name	Port number	Direction of communication
	587/tcp[#2]	JP1/IM - Manager -> Mail server (SMTP) (for SMTP-AUTH authentication)
	110/tcp[#2]	JP1/IM - Manager -> Mail server (POP3) (for POP before SMTP authentication)

Legend:

->: Direction of the connection when the connection is established

#1: JP1/Base on a manager

#2: The port number at the connection destination might change depending on the port used by the connection destination server.

To use any of the port numbers listed above to establish a connection, you must specify that the firewall allows the traffic on the *service-name* port to pass through. You must also specify that ANY can pass through the firewall in response to the session established for the port number for *service-name*. The response must be ANY because the OS performs automatic numbering.

When a connection is established, the port number in the table is used by the side being connected (the side the arrow points at). The connecting side uses an available port number assigned by the OS. The range of port numbers that can be used depends on the OS.

When you install JP1/IM and JP1/Base on a firewall server machine, communications within that machine might also be subject to the firewall restrictions. In this case, set up the firewall so that services can use the port numbers in the table even for communications within the firewall server machine.

Related topics

- *9.3 Operating in a firewall environment* in the *Configuration Guide*

E. List of Services (Windows only)

This appendix describes the Windows versions of JP1/Base and JP1/IM - Manager services related to the systems described in this manual.

List of JP1/Base services related to the systems described in this manual

Display name	Service name	Startup type#	Description
JP1/Base	JP1_Base	Manual	Used for user management and process management
JP1/Base Event	JP1_Base_Event	Manual	Used for managing events and sending and receiving events with other hosts
JP1/Base EventlogTrap	JP1_Base_EventlogTrap	Manual	Used for using event log trapping
JP1/Base LogTrap	JP1_Base_LogTrap	Manual	Used for using log file trapping

#: The default startup type at installation

List of JP1/IM - Manager services related to the systems described in this manual

Display name	Service name	Startup type#	Description
JP1/IM3-Manager	JP1_Console	Manual	JP1/IM - Manager (Intelligent Integrated Management Base, central console, central scope, and IM Configuration Management) service for physical hosts
JP1/IM3-Manager DB Server	HiRDBEmbeddedEdition_JM0	Manual	IM database service for physical hosts

#: The default startup type at installation

Service-list for system-related JP1/IM - Agent described in this manual

Display name	Service Name	Startup type#	Description
JP1/IM3-Agent	jpc_imagent	Automatic	Communication relay service between the Integration Manager host and integrated agent host
JP1/IM3-Agent proxy	jpc_imagentproxy	Automatic	Communication relay service between the Integration Manager host and integrated agent host
JP1/IM3-Agent action	jpc_imagentaction	Automatic	Integrated agent automatic action service

#: The startup type described here is the setting at the time of installation.

F. Advanced Use

This appendix outlines the functions for more efficient use of JP1/IM. For details, see the manuals of the JP1/IM series products.

Functions for advanced use of JP1/IM

Function	Overview	Related topics
Event receiver filter and severe events filter	Filters not described in this manual can also be configured in JP1/IM.	• *4.2 Filtering of JP1 events* in the *Overview and System Design Guide* • *13.1.3 Considerations for filtering JP1 events* in the *Overview and System Design Guide* • *5.2 Setting JP1 event filtering* in the *Configuration Guide*
Correlation event	When a related event is issued, a new event can be issued.	• *4.3 Issue of correlation events* in the *Overview and System Design Guide* • *13.1.4 Considerations for issuing correlation events* in the *Overview and System Design Guide* • *5.6 Settings for generating correlation events* in the *Configuration Guide* • *6.4.2 Checking detailed information about a correlation event and changing the response status* in the *Administration Guide*
Repeated event monitoring suppression	A large number of events can be consolidated into one event to avoid overlooking important events.	• *4.4 Suppressing display of repeated events* in the *Overview and System Design Guide* • *13.1.5 Considerations for suppressing the monitoring of repeated events and a large number of events* in the *Overview and System Design Guide* • *5.3 Setting monitoring of repeated events to be prevented* in the *Configuration Guide* • *6.10 Taking actions for the generation of a large number of events* in the *Administration Guide*
Suppressing forwarding of a large number of events	You can prevent a large number of events (JP1/Base) issued on an agent from being forwarded to the manager.	• *4.5.9 Suppressing the forwarding of a large number of events* in the *Overview and System Design Guide* • *13.1.7 Considerations for suppressing the forwarding of a large number of events* in the *Overview and System Design Guide* • *6.10 Taking actions for the generation of a large number of events* in the *Administration Guide*
Severity changing function	Users can freely change the severity of events depending on system operations.	• *4.7 Changing the event level (severity) of JP1 events* in the *Overview and System Design Guide* • *13.1.8 Considerations for changing JP1 event levels* in the *Overview and System Design Guide* • *5.13 Setting the severity changing function* in the *Configuration Guide* • *6.9.4 Changing the severity level of JP1 events* in the *Administration Guide*
Display message change function	Messages are converted into the specified format before they are displayed in JP1/IM - View so that users can recognize the messages more easily.	• *4.8 Changing the message display format* in the *Overview and System Design Guide* • *13.1.9 Considerations for changing display messages for JP1 events* in the *Overview and System Design Guide* • *5.14 Setting the display message change function* in the *Configuration Guide* • *6.9.5 Changing the message displayed for a JP1 event* in the *Administration Guide*
Event guide function	Guide information for investigating and resolving events that occur during system monitoring can be displayed.	• *4.10 Event guide function* in the *Overview and System Design Guide* • *13.1.10 Considerations for setting event guide information* in the *Overview and System Design Guide* • *5.8 Editing event guide information* in the *Configuration Guide*
Remote monitoring[#]	You can monitor log files on monitored hosts without JP1/Base and JP1/IM - Agent installed.	• *8.2.8 Selection of agent configuration or remote monitoring configuration* in the *Overview and System Design Guide* • *8.6 Managing remotely monitored hosts* in the *Overview and System Design Guide* • *13.5.2 Managing the remote monitoring configuration* in the *Overview and System Design Guide*

Function	Overview	Related topics
		• *1.18 Specifying settings for monitoring logs on remotely monitored hosts (for Windows)* in the *Configuration Guide* • *2.17 Specifying settings for monitoring logs on remotely monitored hosts (for UNIX)* in the *Configuration Guide*
System monitoring in virtualization configurations	You can use a program such as virtualization environment management software to acquire information about a virtual machine and display the configuration in a tree format.	• *8.3 Virtualization configuration management* in the *Overview and System Design Guide* • *3.3 Setting a virtualization system configuration* in the *Configuration Guide*
Business group	Operations and information that users are allowed can be restricted by group.	• *8.4 Managing business groups* in the *Overview and System Design Guide* • *13.5.4 Considerations for business groups* in the *Overview and System Design Guide* • *3.4 Setting business groups* in the *Configuration Guide* • *5.19 Setting reference and operation restrictions on business groups* in the *Configuration Guide* • *9.4 Managing business groups* in the *Administration Guide*
Linkage with other JP1 products	JP1/IM can be linked with products such as JP1/Service Support and JP1/Navigation Platform to monitor systems.	• *10. Linking with Other Products* in the *Overview and System Design Guide* • *10. Settings for Linking to Other JP1 Products* in the *Configuration Guide*
Support of cluster environment	Using JP1/IM in a cluster system allows system monitoring to continue if a server failure occurs.	• *14.3.7 Configuration for operation in a cluster system* in the *Overview and System Design Guide* • *7. Operation and Environment Configuration in a Cluster System (for Windows)* in the *Configuration Guide* • *8. Operation and Environment Configuration in a Cluster System (for UNIX)* in the *Configuration Guide*

#: In remote monitoring, log monitoring might stop or log data might no longer be acquired as events due to a communication failure related to specification restrictions. If the system cannot tolerate such situations, install JP1/Base and use it for monitoring rather than configuring remote monitoring in JP1/IM.

G. Reference Material for this Manual

This appendix provides reference material for readers of this manual, including abbreviations for Microsoft product names and manual titles.

Abbreviations for Microsoft product names

This manual uses the following abbreviations for Microsoft product names:

Abbreviation	Full name
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 sometimes used generically, referring to Windows Server 2025, Windows 11, Windows Server 2022, Windows Server 2019, Windows Server 2016, and Windows 10.

Abbreviations for manual titles

This manual uses the following abbreviations for manual titles in *Related topics*:

Abbreviations	Full name
Overview and System Design Guide	*JP1 Version 13/Integrated Management 3 - Manager Overview and System Design Guide*
Configuration Guide	*JP1 Version 13/Integrated Management 3 - Manager Configuration Guide*
Administration Guide	*JP1 Version 13/Integrated Management 3 - Manager Administration Guide*
GUI Reference	*JP1 Version 13/Integrated Management 3 - Manager GUI Reference*
Command, Definition File and API Reference	*JP1 Version 13/Integrated Management 3 - Manager Command, Definition File and API Reference*
Messages	*JP1 Version 13/Integrated Management 3 - Manager Messages*
JP1/Base User's Guide User's Guide	*JP1 Version 13/Base User's Guide*

Conventions: Abbreviations for product names

This manual uses the following abbreviations for Hitachi and non-Hitachi products:

Abbreviation		Full name
JP1/IM	JP1/IM - Agent	JP1/Integrated Management 3 - Agent
	JP1/IM - Manager	JP1/Integrated Management 3 - Manager
	JP1/IM - View	JP1/Integrated Management 3 - View
Linux	Amazon Linux 2023	Amazon Linux(R) 2023
	Linux 7	Red Hat(R) Enterprise Linux (R) Server 7
	Linux 8	Red Hat(R) Enterprise Linux (R) Server 8
	Linux 9	Red Hat(R) Enterprise Linux (R) Server 9
	Oracle Linux 7	Oracle Linux (R) Operating System 7
	Oracle Linux 8	Oracle Linux (R) Operating System 8
	Oracle Linux 9	Oracle Linux (R) Operating System 9
	SUSE Linux 12	SUSE Linux (R) Enterprise Server 12
	SUSE Linux 15	SUSE Linux (R) Enterprise Server 15

Conventions: Acronyms

This manual uses the following acronyms:

Acronym	Meaning
DNS	Domain Name System
GUI	Graphical User Interface
HTTP	HyperText Transfer Protocol
IP	Internet Protocol
LAN	Local Area Network
NIC	Network Interface Card
TCP/IP	Transmission Control Protocol/Internet Protocol
UNC	Universal Naming Convention
URL	Uniform Resource Locator
WWW	World Wide Web

Installation folders for JP1/IM and JP1/Base (for Windows)

The table below lists the installation folders for JP1/IM and JP1/Base. The locations represented by *system-drive*`:\Program Files` and *system-drive*`:\Program Files (x86)` are determined by an OS environment variable when the product is installed. Therefore, the actual installation folder might differ depending on the environment.

OS environment	Product name	Installation folder	Default installation folder#
x86	JP1/IM - View	*View-path*	*system-drive*`:\Program Files\Hitachi\JP1CoView`
	JP1/IM - Agent	*Agent-path*	*system-drive*`:\Program Files\Hitachi\jp1ima`

OS environment	Product name	Installation folder	Default installation folder#
	JP1/Base	*Base-path*	*system-drive*:\Program Files\Hitachi\JP1Base
x64	JP1/IM - View	*View-path*	*system-drive*:\Program Files (x86)\Hitachi\JP1CoView
	JP1/IM - Agent	*Agent-path*	*system-drive*:\Program Files (x86)\Hitachi\jp1ima
	JP1/IM - Manager	*Manager-path*	*system-drive*:\Program Files (x86)\Hitachi\JP1IMM
		Console-path	*system-drive*:\Program Files (x86)\Hitachi\JP1Cons
		Scope-path	*system-drive*:\Program Files (x86)\Hitachi\JP1Scope
	JP1/Base	*Base-path*	*system-drive*:\Program Files (x86)\Hitachi\JP1Base

#: Represents the installation folder when the product is installed in the default location.

H. Glossary

A

action-excluded event

An event that is excluded from automated-action execution by a common exclusion-condition where the exclusion target is set to the action

agent

A host that is managed by a manager in a JP1/IM. Alternatively, a program managed by a manager program. In JP1/IM, JP1/IM - Agent and JP1/Base act as agent programs. They receive requests from JP1/IM - View and JP1/IM - Manager to manage JP1 events, execute commands, and so on.

automated action

A function that automatically executes a command as an action when a specific JP1 event is received

In an automated action definition, you can specify conditions for executing the action and the command to be executed as the action.

B

business group

A unit of monitored hosts grouped by using JP1/IM - IM Configuration Management based on a certain purpose, such as units of systems used for individual businesses or the scope of monitoring targets for individual system administrators

C

central console

A program that enables integrated system management by centrally managing events in the system based on JP1 events

central scope

A program that enables objective-oriented system monitoring via a graphical user interface matched to the objectives of the system administrator

common exclusion-conditions

Conditions that form part of an event acquisition filter and consist of a group of conditions for filtering out JP1 events monitored by JP1/IM and excluding JP1 events from automated-action execution

correlation event

A JP1 event issued by correlation processing

E

event acquisition filter

A filter for setting detailed conditions about the JP1 events to be acquired by JP1/IM - Manager for display in the Event Console window

Event Console window

A JP1/IM - View window that shows the JP1 events received by the central console, in chronological order

event guide function

A function that displays guide information in the JP1/IM central console for investigating and resolving JP1 events that occur during system monitoring. The event guide function displays guidance targeted to a specific JP1 event.

event receiver filter

A filter for setting conditions, for individual JP1 users, about the JP1 events that can be viewed in the Event Console window

I

IM Configuration

A system hierarchy managed by IM Configuration Management

IM Configuration Management

A function that centrally manages the system hierarchy managed by JP1/IM (IM configuration) and the settings of the hosts that compose the system from IM Configuration Management - View

IM Configuration Management database

A database used by JP1/IM - Manager when implementing IM Configuration Management

IM database

A database provided by JP1/IM - Manager. IM database is a generic term for the IM Configuration Management database and the integrated monitoring database.

Integrated agent

Agent using JP1/IM - Agent.

It consists of "JP1/IM agent control base" and "add-on program" running on integrated agent host.

Intelligent Integrated Management Database

This database is used to store various types of information used in the Intelligent Integrated Management Base.

integrated monitoring database

A database that JP1/IM - Manager uses for the Intelligent Integrated Management Base and the central console

integrated operation viewer

A viewer that provides user interface to access the Intelligent Integrated Management Base

Intelligent Integrated Management Base

A base provided by JP1/IM to enable an integrated way to manage and collate various types of data and knowledge and share the information

Intelligent Integrated Management Database

This is a database for storing various pieces of data used by Intelligent Integrated Management Base. Refers to PostgreSQL and extensions that are embedded in a JP1/IM - Manager.

J

JP1 event

Information for managing events occurring in the system within the JP1 framework. In this manual, JP1 events are abbreviated as *events*.

JP1 events are managed by the JP1/Base event service. Events generated in the system are recorded in a database as JP1 events.

JP1/Base

A program that provides the core functionality of JP1/IM.

JP1/Base carries out processing such as the sending and receiving of events, user management, and startup control. It also serves as the agent in a JP1/IM system.

JP1/Base is a prerequisite program for JP1/IM - Manager.

JP1/IM - Agent

A agent that enables you to monitor systems in your on-premises and cloud environments and collects performance data from managed hosts and sends it to JP1/IM - Manager.

JP1/IM - Manager

A program that enables integrated system management by providing centralized monitoring and operation across all system resources. JP1/IM - Manager consists of three components: the central console, the central scope, and IM Configuration Management.

JP1/IM - View

A GUI program that provides viewer functionality for realizing integrated system management in JP1/IM

M

manager

A program whose role is to manage other programs on the system through JP1/IM. Or a host whose role is to manage other hosts on the system.

In JP1/IM, JP1/IM - Manager manages agent programs JP1/IM - Agent and JP1/Base as a manager program.

R

repeated event
: A JP1 event that matches a condition specified by the user

repeated-event monitoring suppression
: Functionality that prevents a large number of repeated events from being displayed in the event list of the Event Console window and that prevents a large number of actions corresponding to repeated events from being executed

S

severe events filter
: A filter that defines the severe events to be displayed in the Severe Events page of the Event Console window

severity changing function
: A function that lets users freely change the severity level of a JP1 event

severity level
: One of the attributes of a JP1 event, indicating the severity of an event that occurred in the system

V

viewer
: A GUI program that provides purpose-built windows for integrated system management in JP1/IM. *Viewer* may also refer to the host running the GUI program

  Note that the Intelligent Integrated Management Base is accessed through the integrated operation viewer, instead of the GUI programs.

view filter
: A filter that sets conditions about the JP1 events to be displayed in the Event Console window

Index

Hitachi, Ltd.
6-6, Marunouchi 1-chome, Chiyoda-ku, Tokyo, 100–8280 Japan