

JP1 Version 12

Integrated Management: Getting Started

3021-3-D50(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 2 - Manager and JP1/Integrated Management 2 - View, see the *Release Notes* for the relevant product.

JP1/Integrated Management 2 - Manager (for Windows):

P-2A2C-8ECL JP1/Integrated Management 2 - Manager 12-00

The above product includes the following:

P-CC2A2C-9MCL JP1/Integrated Management 2 - Manager 12-00 (for Windows Server 2016, Windows Server 2012)

P-CC2A2C-6HCL JP1/Integrated Management 2 - View 12-00 (for Windows Server 2016, Windows 10, Windows 8.1, Windows 8, Windows Server 2012, Windows 7)

JP1/Integrated Management 2 - Manager (for Linux):

P-812C-8ECL JP1/Integrated Management 2 - Manager 12-00

The above product includes the following:

P-CC812C-9MCL JP1/Integrated Management 2 - Manager 12-00 (for Linux 7, Linux 6 (x64), Oracle Linux 7, Oracle Linux 6 (x64), CentOS 7, CentOS 6 (x64))

P-CC9W2C-9MCL JP1/Integrated Management 2 - Manager 12-00 (for SUSE Linux 12)

P-CC2A2C-6HCL JP1/Integrated Management 2 - View 12-00 (for Windows Server 2016, Windows 10, Windows 8.1, Windows 8, Windows Server 2012, Windows 7)

■ Trademarks

HITACHI, JP1 are either trademarks or registered trademarks of Hitachi, Ltd. in Japan and other countries.

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

IBM, AIX are trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide. AMD, AMD Opteron, and combinations thereof, are trademarks of Advanced Micro Devices, Inc.

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

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

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

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

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

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

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

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

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

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

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

This product includes RSA BSAFE(R) Cryptographic software of EMC Corporation.

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

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

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

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

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

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

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

This product includes software developed by Andy Clark.

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

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

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



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

HITACHI
Inspire the Next

Hitachi, Ltd.



■ Restrictions

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

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

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

■ **Issued**

Jan. 2019: 3021-3-D50(E)

■ **Copyright**

Copyright (C) 2019, Hitachi, Ltd.

Copyright (C) 2019, Hitachi Solutions, Ltd.

Summary of amendments

The following table lists changes in this manual (3021-3-D50(E)) and product changes related to this manual.

Changes	Location
The Intelligent Integrated Management Base was added.	<i>1., 2.1, 2.3, 2.4.4, 2.5.4, 2.6, Appendix C, Appendix D, Appendix E</i>
The following terms were added: <ul style="list-style-type: none">• Intelligent Integrated Management Base• integrated operation viewer	<i>Appendix H</i>
The following OSs are no longer supported: <ul style="list-style-type: none">• Windows Server 2008 R2• AIX	--

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 2 - Manager and JP1/Integrated Management 2 - View, based on the system operation cycle. Users who want to learn about JP1/Integrated Management 2 - Manager functions based on the intended use of each function should read this manual first. JP1/Integrated Management 2 - Manager and JP1/Integrated Management 2 - View might be generically referred to as *JP1/IM*.

■ How to read this manual

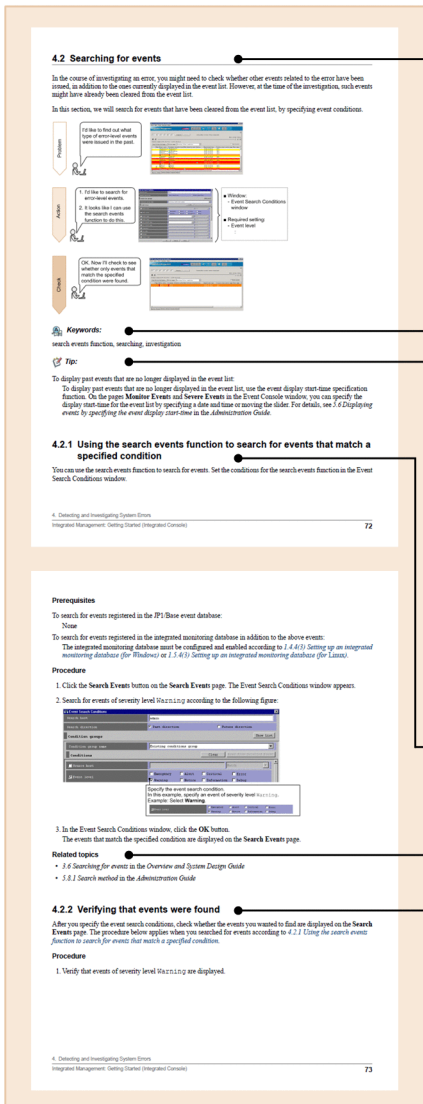
The following environments are required to perform the operations in each window.

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



Overview of tasks
This section provides an overview of the task workflow, in the order of *Problem*, *Action*, and *Check*.

Problem
This area highlights problems one might encounter during monitoring.

Action
Corrective action
This area provides the windows, definition files, and settings required for corrective action.

Check
This area describes the system status checks to perform after taking corrective action.

Keywords:
Provides keywords that are directly and indirectly related to a function. Keywords facilitate easier searching in the manual.

Tip:
Introduces related functions and products. For details, see other JP1/IM - Manager manuals and related product documentation.

Overview of corrective action
This subsection title shows the name of a function needed for corrective action. The descriptions in the subsection cover only the most important aspects of each function.

Related topics:
Provides references to sections in related manuals.

This subsection briefly explains how to check whether settings specified during troubleshooting were correctly applied.

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:

For an overview and description of how to use JP1/IM:

JP1 Version 12 Integrated Management: Getting Started
(3021-3-D50(E))

To determine and design a JP1/IM configuration appropriate for the configuration of a business system:

JP1 Version 12 JP1/Integrated Management
2 - Manager Overview and System Design
Guide
(3021-3-D51(E))

To learn an operation procedure for daily tasks.

JP1 Version 12 JP1/Integrated Management
2 - Manager Administration Guide
(3021-3-D53(E))

For a JP1/IM configuration procedure appropriate for the configuration of a business system:

JP1 Version 12 JP1/Integrated Management
2 - Manager Configuration Guide
(3021-3-D52(E))

To know details about the GUIs used for tasks.

JP1 Version 12 JP1/Integrated Management
2 - Manager GUI Reference
(3021-3-D54(E))

JP1 Version 12 JP1/Integrated Management
2 - Manager Command and Definition File
Reference
(3021-3-D55(E))

To understand the causes of messages displayed during operation, and actions to be taken:

JP1 Version 12 JP1/Integrated Management
2- Manager Messages
(3021-3-D56(E))

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

The following table explains the symbols used in this manual:

Symbol	Convention
	<p>In syntax explanations, a vertical bar separates multiple items, and has the meaning of OR. For example: <code>A B C</code> means A, or B, or C.</p>
{ }	<p>In syntax explanations, curly brackets indicate that only one of the enclosed items is to be selected. For example: <code>{ A B C }</code> means only one of A, or B, or C.</p>
[]	<p>In syntax explanations, square brackets indicate that the enclosed item or items are optional. For example: <code>[A]</code> means that you can specify A or nothing. <code>[B C]</code> means that you can specify B, or C, or nothing.</p>
...	<p>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: <code>A, B, B, . . .</code> means that, after you specify A, B, you can specify B as many times as necessary.</p>

■ 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

Notices 2

Summary of amendments 5

Preface 6

1 Overview 14

1.1 What is explained in this manual 15

1.2 What you can do with JP1/IM 16

2 Installing and Setting Up JP1/IM 19

2.1 Overview of a basic configuration system 20

2.2 Preparation before installation 22

2.2.1 Preparing the products to be installed 22

2.2.2 Prerequisite OSs and OS environment configuration 22

2.2.3 Required amounts of installation memory and disk space 23

2.2.4 Language settings in prerequisite OSs 23

2.2.5 Setting ports used by JP1/IM 23

2.2.6 Setting name resolution 24

2.3 General procedures for installing and setting up JP1/IM 25

2.4 Installation and setup (for Windows) 27

2.4.1 Installing the prerequisite product (for Windows) 27

2.4.2 Setting up the prerequisite product (for Windows) 28

2.4.3 Installing JP1/IM (for Windows) 30

2.4.4 Setting up JP1/IM - Manager (for Windows) 31

2.4.5 Setting up JP1/IM - View (Windows only) 35

2.4.6 Starting JP1/IM - Manager (for Windows) 35

2.5 Installation and setup (for Linux) 37

2.5.1 Installing the prerequisite product (for Linux) 37

2.5.2 Setting up the prerequisite product (for Linux) 38

2.5.3 Installing JP1/IM (for Linux) 39

2.5.4 Setting up JP1/IM - Manager (for Linux) 40

2.5.5 Starting JP1/IM - Manager (for Linux) 44

2.6 Logging in to JP1/IM - Manager from the integrated operation viewer 45

2.7 Logging in to JP1/IM - Manager from JP1/IM - View 46

3 Setting Up Monitoring Targets 47

3.1 What is IM Configuration Management? 48

3.1.1 Registering the hosts into IM Configuration Management 49

3.1.2	Using IM Configuration Management to define the system hierarchy	50
3.1.3	Verifying that the system has been correctly set up by IM Configuration Management	50
3.2	Settings for executing commands on monitored hosts from JP1/IM - View	52
3.2.1	Configuring user mapping	53
3.2.2	Verifying that you can execute a command	55
3.3	Customizing settings for forwarding events from an agent to the manager	57
3.3.1	Using IM Configuration Management to set a forwarding filter	58
3.3.2	Verifying that the forwarding filter has been correctly set	60
3.4	Using event conversion to monitor log files	61
3.4.1	What is log file trapping for JP1/Base?	62
3.4.2	Verifying that records can be converted to events by the log file trap	66
4	Monitoring a System	68
4.1	Monitoring only necessary events	69
4.1.1	Using a view filter to filter events to be displayed	69
4.1.2	Verifying that the events that match the view filter conditions are displayed	70
4.2	Removing hosts undergoing maintenance from the items to be monitored	71
4.2.1	Using common exclusion conditions in a filter to temporarily stop hosts from being monitored	72
4.2.2	Verifying that events from unmonitored hosts are not displayed	73
5	Detecting and Investigating System Errors	76
5.1	Automatically executing a command whenever a specific event is issued	77
5.1.1	Using the automated action function to execute a command whenever an event is issued	78
5.1.2	Verifying that a command specified as an automated action was executed	79
5.2	Searching for events	81
5.2.1	Using the search events function to search for events that match a specified condition	81
5.2.2	Verifying that events were found	82
	Appendixes	83
A	Using the Email Notification Function to Send Emails (Windows Only)	84
A.1	Setting up the email notification function (Windows only)	84
A.2	Verifying that the email notification function has been set up correctly (Windows only)	86
A.3	Example definition for an automated action when using the email notification function (Windows only)	87
B	Using Visual Monitoring to Understand the Extent of the Impact of a System Error	88
B.1	Procedure for configuring visual monitoring	88
B.2	Verifying that you can monitor the extent of impact of events in map format and tree format	93
C	How to Monitor and Manage System Events with the Integrated Operation Viewer	96
C.1	Checking system status	97
D	Port Numbers	99
D.1	JP1/IM port numbers	99
D.2	JP1/Base port numbers	99

D.3	Direction of communication through a firewall	100
E	List of Services (Windows only)	102
F	Advanced Use	103
G	Reference Material for this Manual	105
H	Glossary	108

Index 111

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

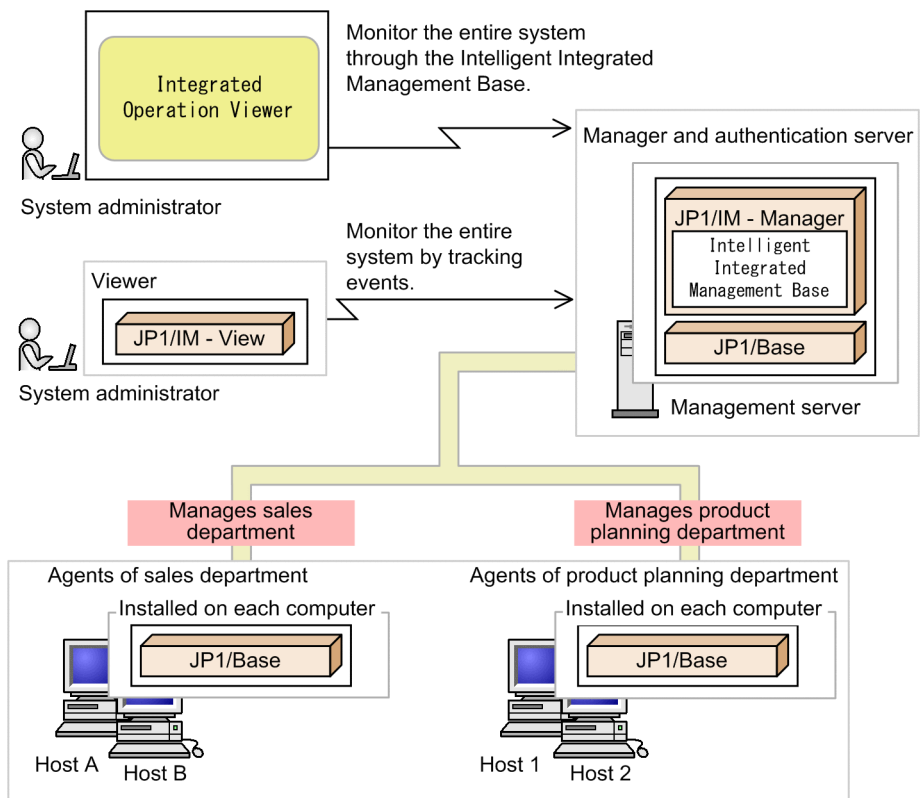
This manual is intended for professionals who want to use JP1/IM to manage and operate open platform systems, and those who are considering introducing JP1/IM. More specifically, it is intended for:

- 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.

The chapters of this manual describe how to install and set up programs, and configure the functions required for intended readers to start system monitoring in a basic configuration. Furthermore, appendixes in this manual explain advanced monitoring functions such as email notifications, visual monitoring, and other functions for efficient use of JP1/IM. This manual also describes how to set up the Intelligent Integrated Management Base and how to monitor and manage events with the integrated operation viewer, which is the viewer for the Intelligent Integrated Management Base.

Operation procedures in this manual assume systems consisting of monitored hosts (agents) and management servers (managers) with JP1/Integrated Management 2- 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:

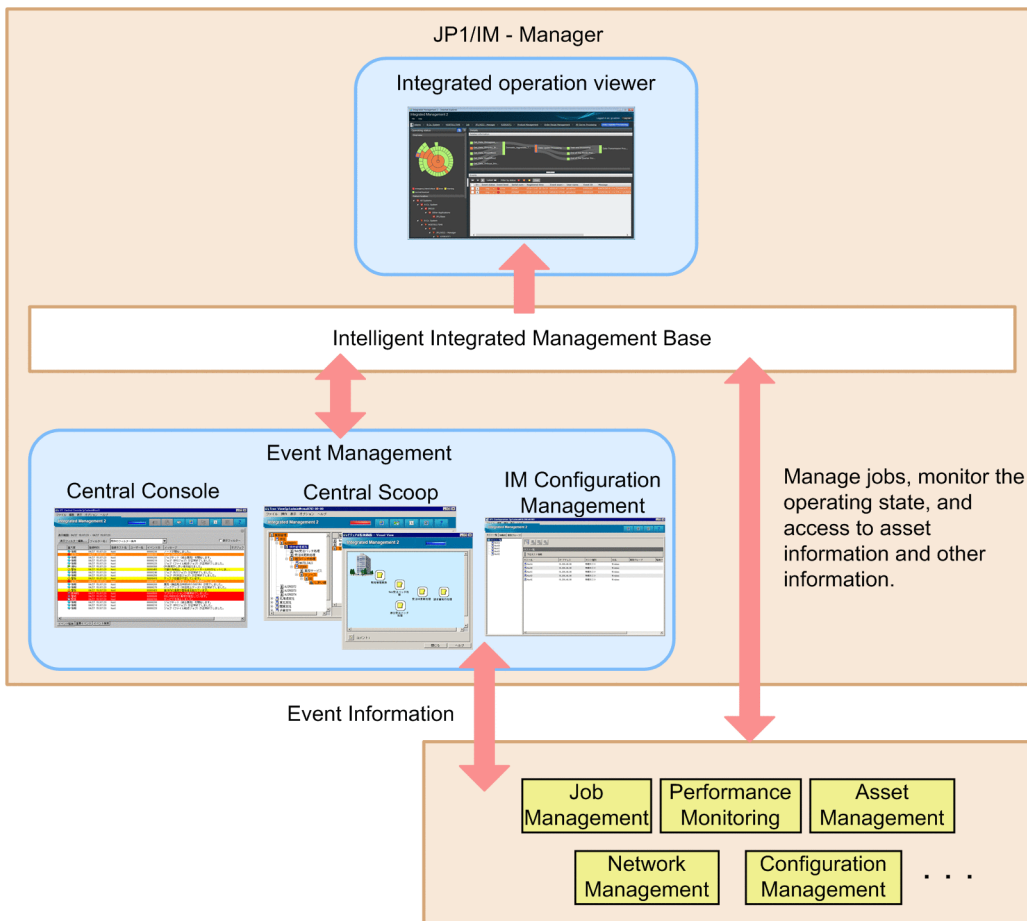
- Providing the viewer (integrated operation viewer) for JP1/IM - Manager (Intelligent Integrated Management Base) to identify relationships between system components
- Integrated management using JP1 events (simply called *events* hereafter) and centralized system monitoring
- Error detection and reporting
- 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

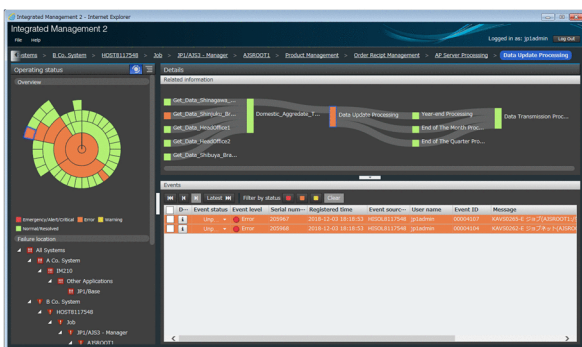


The Intelligent Integrated Management Base of JP1/IM provides the *integrated operation viewer*, which you can use on a Web browser to view relationships between various types of system data including job information and operating information. JP1/IM also provides specific GUI programs for event management that help you monitor and manage status by tracking events issued in the system.

The following figures show the major JP1/IM functions.

- Major functions of the Intelligent Integrated Management Base

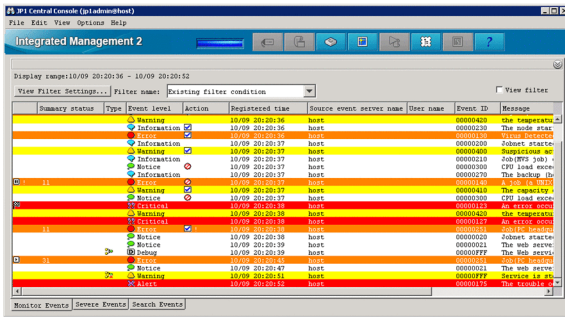
■ Major functions of the Intelligent Integrated Management Base



■ Integrated system monitoring (Integrated Operation Viewer)
Centralizes various events across the system and provides an integrated single view to cover a full operation cycle from detecting problems to identifying affected areas, investing errors, and recovering the system.

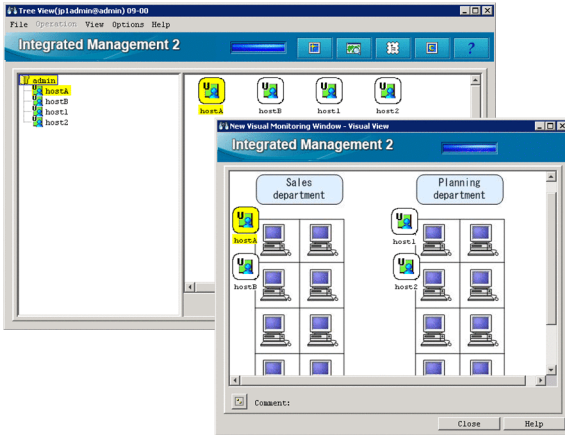
- Major functions of event management

Major functions of event management



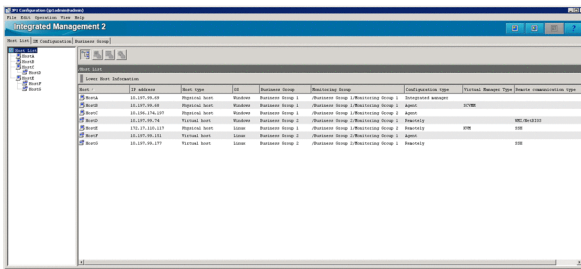
Central monitoring (central console)

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

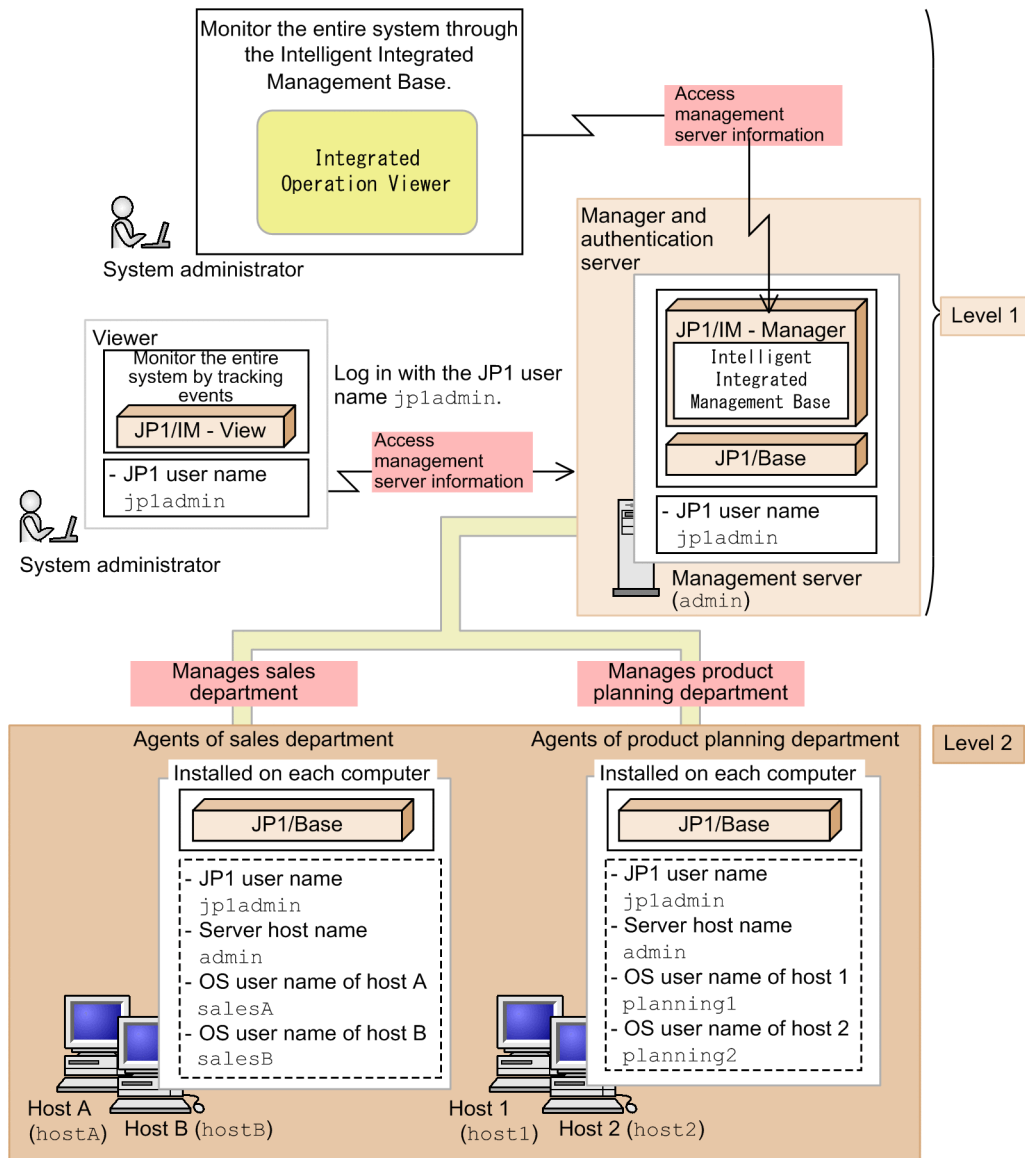
This chapter describes how to install and set up JP1/IM and JP1/Base.

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



Legend:

- : Information set by means of user mapping
- JP1 user name : JP1 user name used to log in

In this example, the system administrator uses a viewer to log in with the JP1 user name `jpladmin`. 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 12-00 or later.

Manager

- JP1/Integrated Management 2 - Manager
- JP1/Base

Agent

In this manual, to monitor agents by using JP1/Base, JP1/Base will be installed on the agents.

- JP1/Base

Viewer

- JP1/Integrated Management 2 - 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:

Manager

- Windows Server 2016, Windows Server 2012
- Linux 7, Linux 6 (x64), Oracle Linux 7, Oracle Linux 6 (x64), CentOS 7, CentOS 6 (x64), SUSE Linux 12

Agent

- Windows Server 2016, Windows 10, Windows 8.1, Windows 8, Windows Server 2012, Windows 7
- HP-UX (IPF)
- Solaris
- AIX
- Linux 7, Linux 6 (x64), Oracle Linux 7, Oracle Linux 6 (x64), CentOS 7, CentOS 6 (x64), SUSE Linux 12

Viewer

- Windows Server 2016, Windows 10, Windows 8.1, Windows 8, Windows Server 2012, Windows 7

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.
- (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, 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	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/Base does not operate normally. Revise the `hosts` file settings.

Related topics

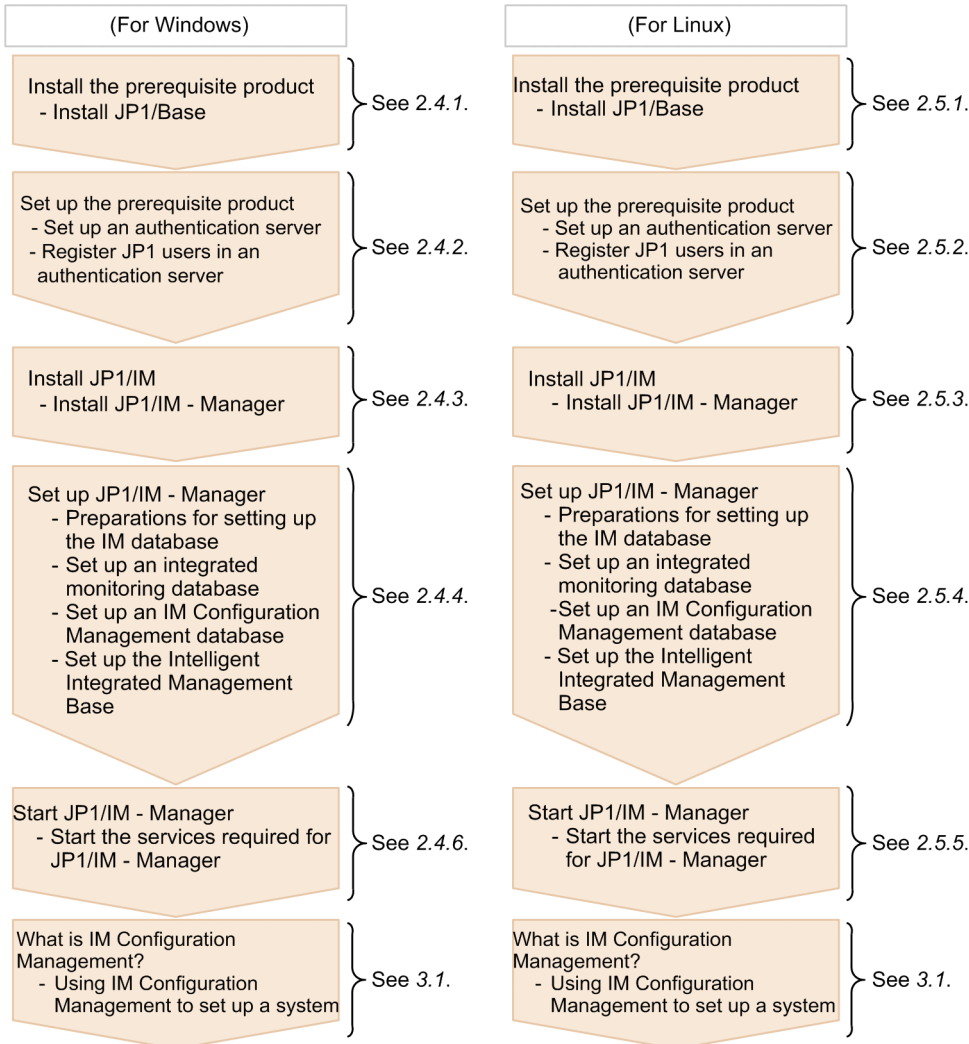
- Description of the communication protocols of JP1/Base in the *JP1/Base User's Guide*

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.



For an agent:

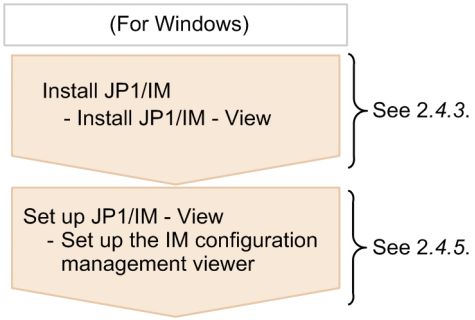
Install JP1/Base to allow the manager to manage events issued by the agent.



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 and the hosts used as agents. This subsection describes the procedure for new installations of JP1/Base.

(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 [3.2.1 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).

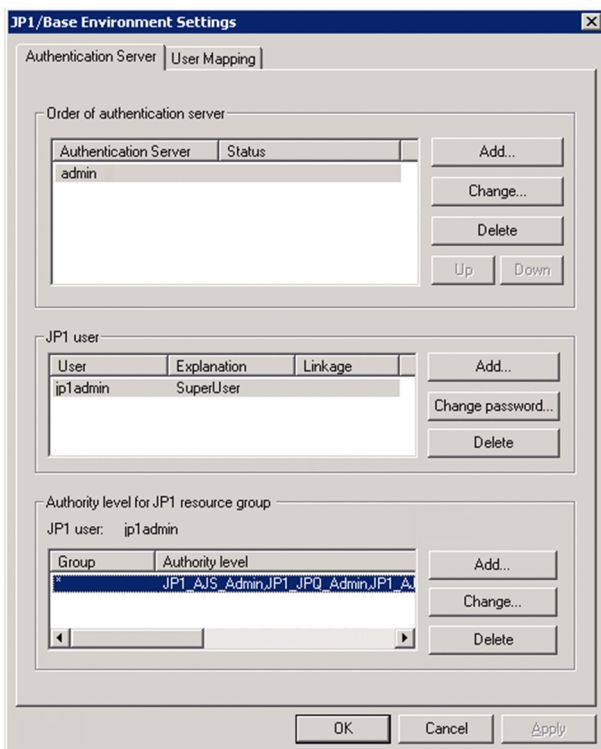
If automatic setup processing was performed during installation of JP1/Base, the local host is set as the authentication server. If automatic setup processing was not performed, and you want to add and set up a host as an authentication server, or you want to set up a different host as an authentication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

- [8.4.1 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	<i>installation-folder</i> \JP1IMM\	Stores JP1/IM - Manager information.
	<i>installation-folder</i> \JP1Cons\	Stores central console information.
	<i>installation-folder</i> \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	<i>installation-folder</i> \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= <i>manager-path</i> \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, <i>manager-path</i> \database is set. To change the value of IMDBDIR, do not specify a network drive (displayed in a list by <code>net use</code> 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= <i>manager-path</i> \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, <i>manager-path</i> \dbms is set. To change the value of IMDBENVDIR, do not specify a network drive (displayed in a list by <code>net use</code> executed from the command prompt) or Windows reserved device file (AUX, CON, NUL, PRN, CLOCK\$, COM[0-9], or LPT[0-9]).

Related topics

- *13.1.3 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 manual *Command and Definition File 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/IM2-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 manual Command and Definition File Reference](#)
- `jcoimdef` in [1. Commands in the manual Command and Definition File 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/IM2-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 manual *Command and Definition File Reference*
- *jcoimdef* in *1. Commands* in the manual *Command and Definition File Reference*

(5) 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.
- The OS user who will execute the `jcoimdef` command has Administrator permissions.

Procedure

1. Stop the JP1/IM2-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. Define the hierarchical structure of the system in the system node definition file (`imdd_systemnode.conf`).
5. 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`).
6. Restart the JP1/IM2 - Manager service.
7. Execute the `jddsetaccessuser` command to configure the users who can access the monitored products when system configuration information is collected.
8. 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`).
9. Execute the `jddcreatetree` command.
10. Define the relationships between IM management nodes in the IM management node link definition file (`imdd_nodeLink_def.conf`).
11. Execute the `jddupdatetree` command.

Related topics

- *1.4.2 Setting up the integrated monitoring database (for Windows) in the Configuration Guide*
- *jcoimdef in 1. Commands in the manual Command and Definition File Reference*
- *jddsetaccessuser in 1. Commands in the manual Command and Definition File Reference*
- *jddcreatetree in 1. Commands in the manual Command and Definition File Reference*
- *jddupdatetree in 1. Commands in the manual Command and Definition File Reference*
- *System node definition file (imdd_systemnode.conf) in 2. Definition Files in the manual Command and Definition File Reference*
- *Category name definition file for IM management nodes (imdd_category_name.conf) in 2. Definition Files in the manual Command and Definition File Reference*
- *Target host definition file for configuration collection (imdd_target_host.conf) in 2. Definition Files in the manual Command and Definition File Reference*
- *IM management node link definition file (imdd_nodeLink_def.conf) in 2. Definition Files in the manual Command and Definition File Reference*

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

This subsection describes how to set up JP1/IM - View.

(1) Setting up the IM configuration management viewer (Windows only)

The following describes how to register a shortcut used to start IM configuration management viewer.

Prerequisites

The following conditions must be specified:

- JP1/IM - View is installed on the viewer.
- The OS user who will execute the `jcovcfsetup` command has Administrator permissions.

Procedure

1. Execute the following `jcovcfsetup` command to register a shortcut to IM configuration management viewer.

```
"view-path\bin\jcovcfsetup" -i
```

The shortcut named **Configuration Management** is added under **JP1_Integrated Management - View** in **All Programs** in the Windows **Start** menu.

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.
- 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/IM2 - Manager DB Server service.
7. Start the JP1/IM2 - Manager service.

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)

Before you start system monitoring with JP1/IM, you need to install JP1/Base on the hosts used as managers and the hosts used as agents. This subsection describes the procedure for new installations of JP1/Base.

(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/jplbase
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 `jbssetusrsv` command has `root` permissions.

Procedure

1. Specify the following `jbssetusrsv` command on the host you want to specify as the authentication server:
`/opt/jplbase/bin/jbssetusrsv 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 `jpladmin` 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

- *8.4.1 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/IM - 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/jplimm/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/jplimm/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 <code>find / -type l</code>).
#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/jplimm/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/jplimm/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 <code>find / -type l</code>).

Related topics

- [13.1.3 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/jplimm/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 manual *Command and Definition File 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/IM-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 manual *Command and Definition File Reference*
- *jcoimdef* in *1. Commands* in the manual *Command and Definition File 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/IM2 - 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 manual *Command and Definition File Reference*
- *jcoimdef* in *1. Commands* in the manual *Command and Definition File Reference*

(5) 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:

- An integrated monitoring database is set up.
- The OS user who will execute the `jcoimdef` command has `root` permissions.

Procedure

1. Stop the JP1/IM2-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. Define the hierarchical structure of the system in the system node definition file (`imdd_systemnode.conf`).
5. 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`).
6. Restart the JP1/IM2 - Manager service.
7. Execute the `jddsetaccessuser` command to configure the users who can access the monitored products when system configuration information is collected.
8. 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`).
9. Execute the `jddcreatetree` command.
10. Define the relationships between IM management nodes in the IM management node link definition file (`imdd_nodeLink_def.conf`).
11. Execute the `jddupdatetree` command.

Related topics

- *2.4.2 Setting up the integrated monitoring database (for UNIX) in the Configuration Guide*
- *jcoimdef in 1. Commands in the manual Command and Definition File Reference*
- *jddsetaccessuser in 1. Commands in the manual Command and Definition File Reference*
- *jddcreatetree in 1. Commands in the manual Command and Definition File Reference*
- *jddupdatetree in 1. Commands in the manual Command and Definition File Reference*
- *System node definition file (imdd_systemnode.conf) in 2. Definition Files in the manual Command and Definition File Reference*
- *Category name definition file for IM management nodes (imdd_category_name.conf) in 2. Definition Files in the manual Command and Definition File Reference*
- *Target host definition file for configuration collection (imdd_target_host.conf) in 2. Definition Files in the manual Command and Definition File Reference*
- *IM management node link definition file (imdd_nodeLink_def.conf) in 2. Definition Files in the manual Command and Definition File 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.

2.6 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.

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

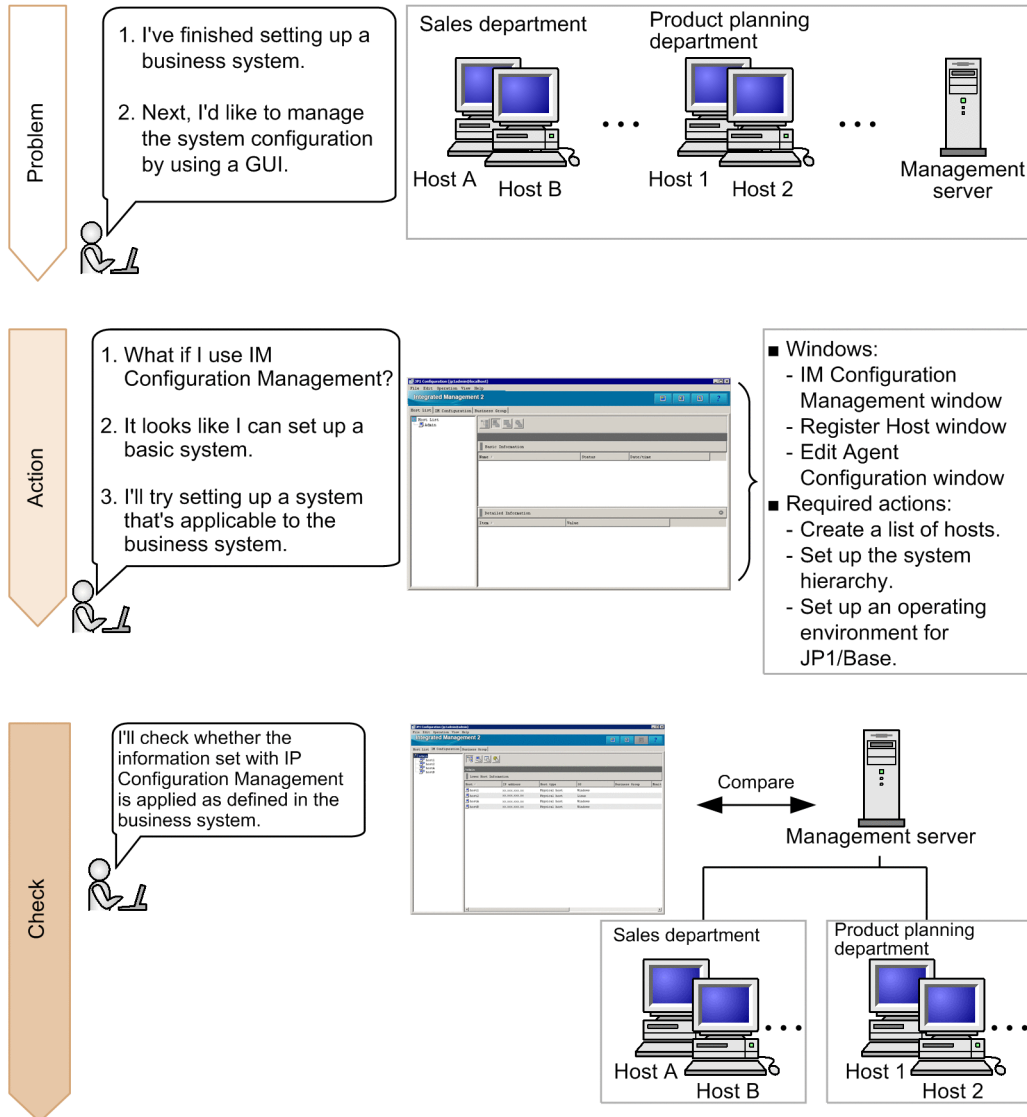
This chapter explains how to define and manage a system configuration, and the preparations that are necessary for monitoring events.

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

3.1 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

3.1.1 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

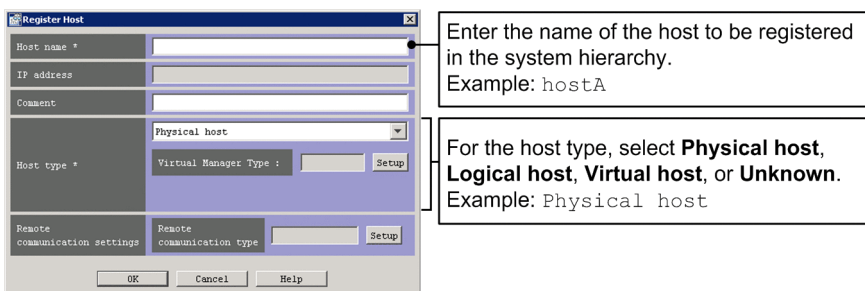
The following conditions must be satisfied:

- 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 - 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.



The screenshot shows the 'Register Host' dialog box with the following fields and callouts:

- Host name ***: A text input field. Callout: "Enter the name of the host to be registered in the system hierarchy. Example: hostA".
- IP address**: A text input field.
- Comment**: A text input field.
- Host type ***: A dropdown menu with 'Physical host' selected. Callout: "For the host type, select **Physical host**, **Logical host**, **Virtual host**, or **Unknown**. Example: Physical host".
- Virtual Manager Type**: A text input field with a 'Setup' button.
- Remote communication settings**: A section containing a 'Remote communication type' text input field and a 'Setup' button.
- Buttons: 'OK', 'Cancel', and 'Help' at the bottom.

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

Related topics

- [7. 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*
- [1.19.3 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 manual *GUI Reference*

3.1.2 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.

IM Configuration Tree

Drag & Drop

Host /	IP address	Host type
host1	XX.XXX.XXX.XX	Physical host
host2	XX.XXX.XXX.XX	Physical host
hostA	XX.XXX.XXX.XX	Physical host

Host /	IP address	Host type	OS
hostB	XX.XXX.XXX.XX	Physical host	Windows

To create a hierarchy such as the one depicted below, drag and drop each host from **Host List** to **IM Configuration Tree**.

```
graph TD; admin[admin] --- host1[host1]; admin --- host2[host2]; admin --- hostA[hostA]; admin --- hostB[hostB];
```

Example: Drag a host from the Sales department and drop it under the management server.

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

- *1.8 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*

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

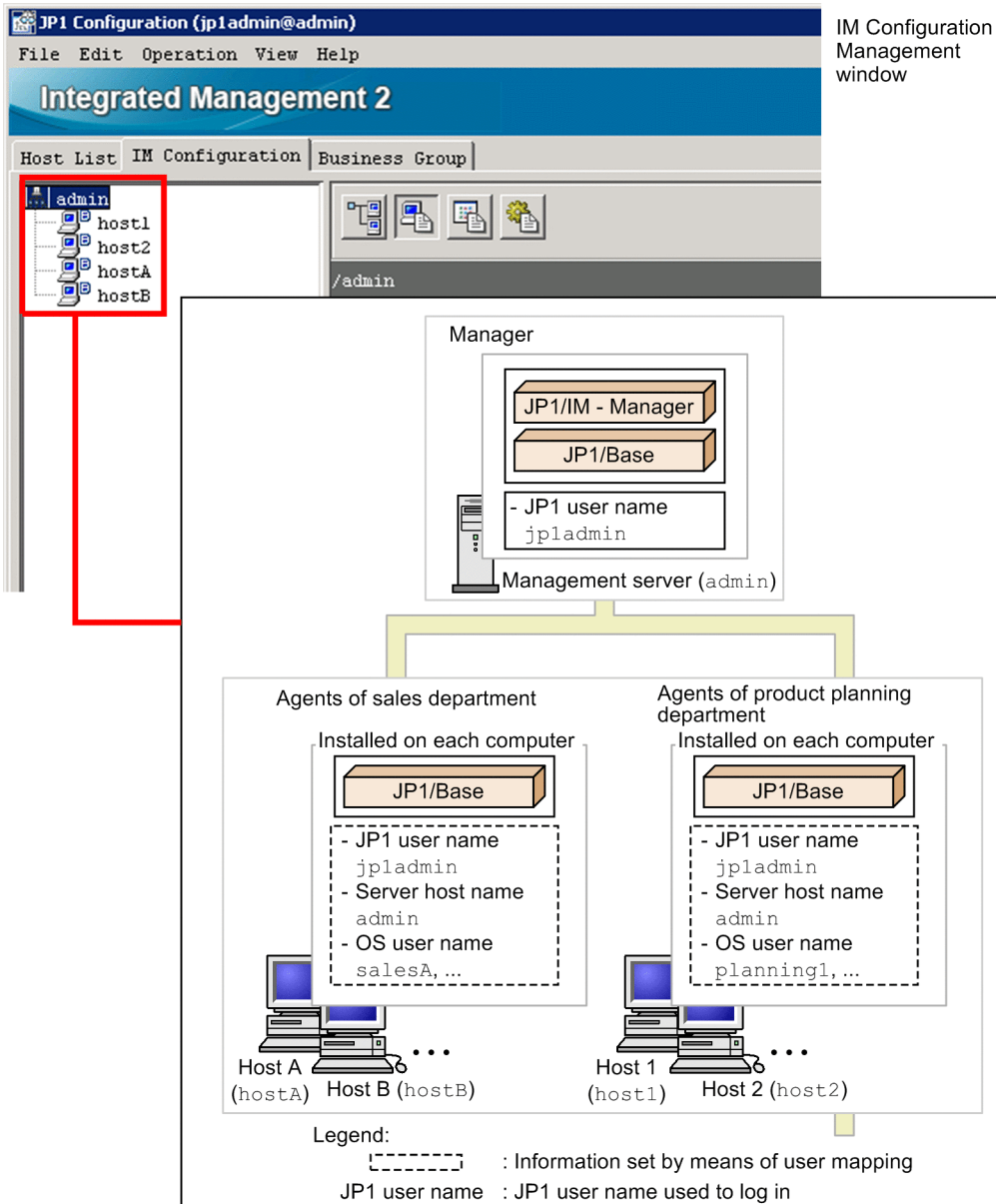
To use JP1/IM to centrally manage events issued in a business system, verify that the system has been set up correctly by IM Configuration Management. The following describes how to verify that the basic configuration system shown in *2.1 Overview of a basic configuration system* has been set up.

Prerequisites

The basic configuration system must be set up according to *3.1 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*.

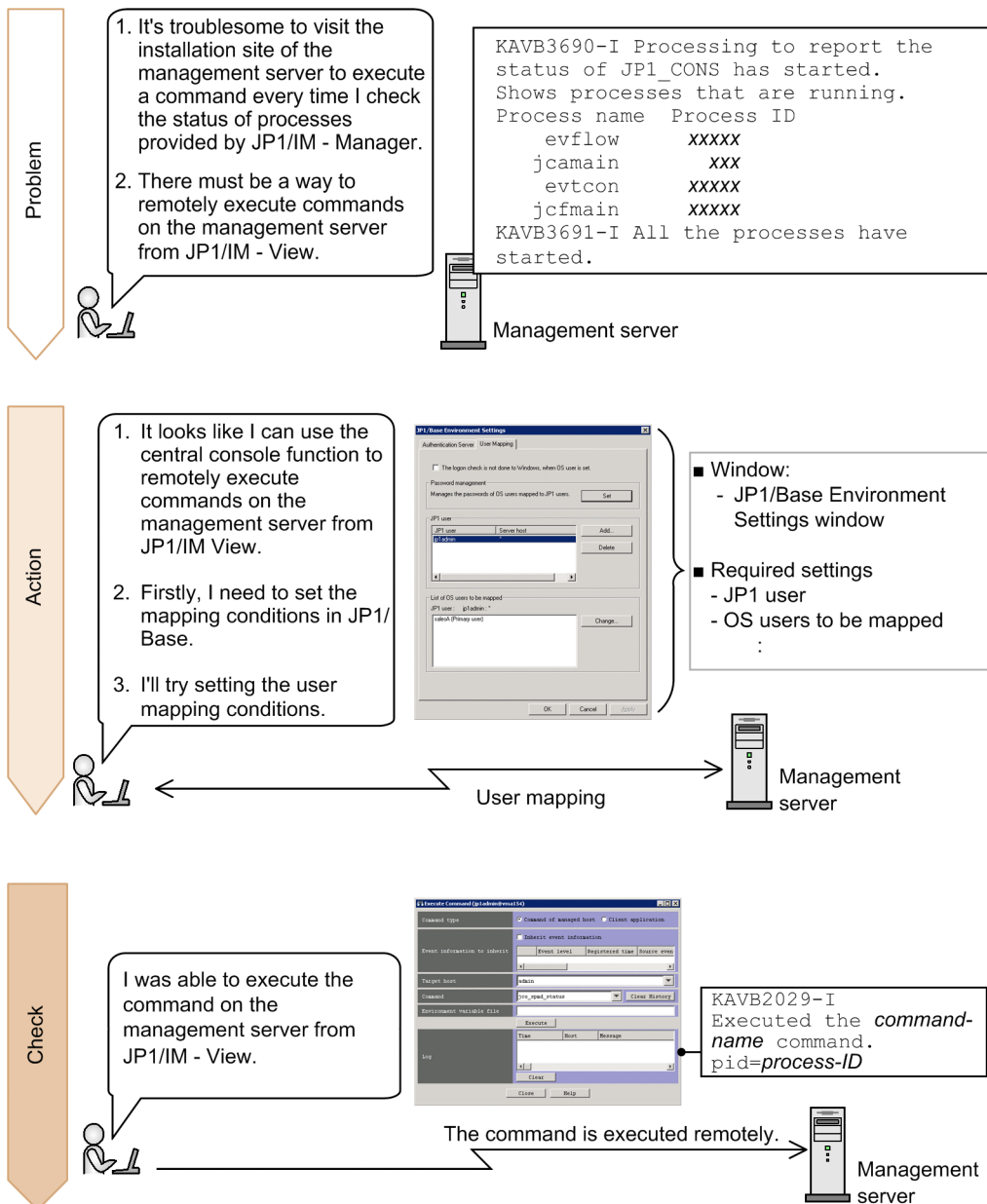


3.2 Settings for executing commands on monitored hosts from JP1/IM - View

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

3.2.1 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`.

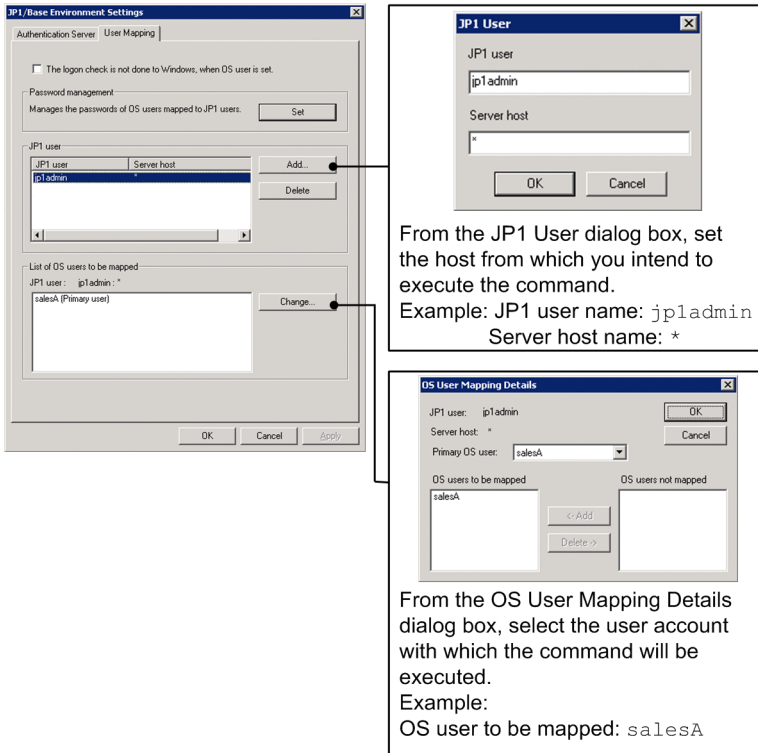
Prerequisites

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

- *8.4 Core functionality provided by JPI/Base in the Overview and System Design Guide*
- Descriptions of how to configure user mapping in the *JPI/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 `jpladmin` 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 jpladmin -sha -o salesA`
- In Linux:
`/opt/jplbase/bin/jbssetumap -u jpladmin -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*

3.2.2 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 [3.2.1 Configuring user mapping](#).
- The OS user who will execute the `jco_spmc_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_spmc_status` command as follows to check whether the command can be executed:
 - In Windows:
`"Console-path\bin\jco_spmc_status"`
 - In Linux:
`/opt/jplcons/bin/jco_spmc_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_spmc_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 manual *Command and Definition File Reference*

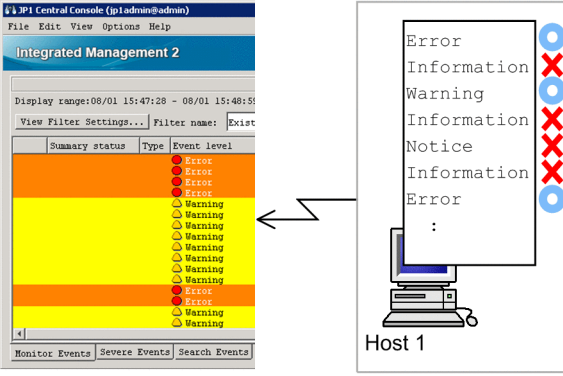
3.3 Customizing settings for forwarding events from an agent to the manager

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.

Problem

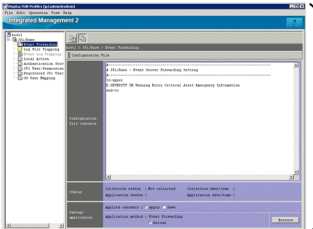
1. For host 1, I want to monitor events of severity level Information.
2. It seems that, in the default settings at installation, events of severity level Information are not forwarded to the manager.
3. How can I customize events that will be forwarded to the management server?



Host 1

Action

1. It looks like I can set up JP1/Base event transfer on agents.
2. I'll try setting up event transfer in IM Configuration Management.

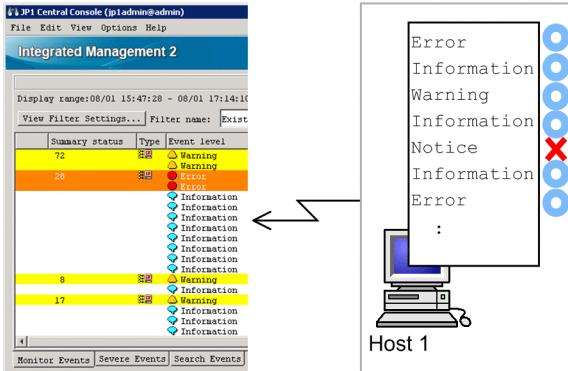


- Window: - Display/Edit Profile window
- Required settings - Settings in the forwarding settings file

Check

I'll check whether it's possible to monitor events of severity level Information issued on host 1.

Legend: ● : Displayed ✗ : Not displayed



Host 1

Keywords:

event, forwarding, monitoring target, forwarding filter

3.3.1 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 [3.3.1 \(2\) 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 <i>severity-level</i> ... 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

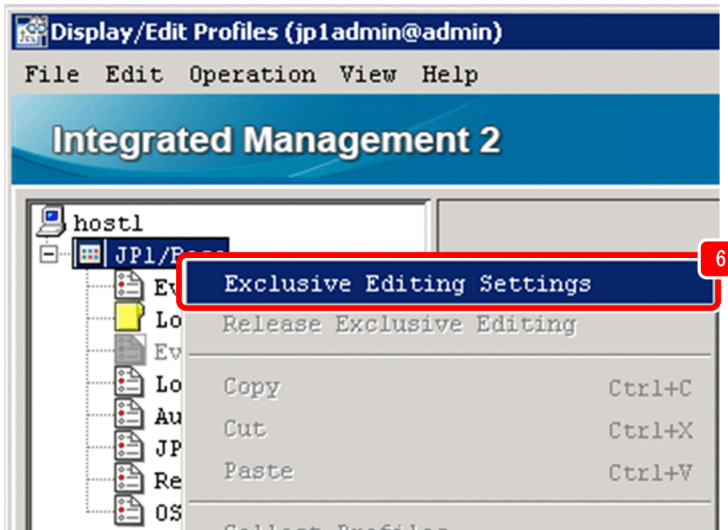
The following conditions must be satisfied:

- The basic configuration system is set up according to [3.1 What is IM Configuration Management?](#).
- Host information has been collected.

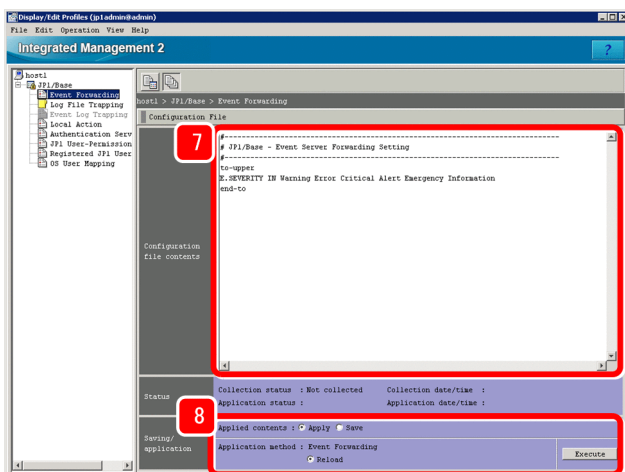
Procedure

1. From the Windows **Start** menu, select **All Programs, JP1_Integrated Management - 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 **JPI/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 *JPI/Base User's Guide*

3.3.2 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 [3.3.1 \(2\) 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 [3.2.1 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 [3.2.2 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: <ul style="list-style-type: none">• In Windows: <code>"Base-path-of-the-execution-host\bin\jvsend" -e SEVERITY=Information -m information-event</code>• In Linux: <code>/opt/jplbase/bin/jvsend -e SEVERITY=Information -m information-event</code>

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.

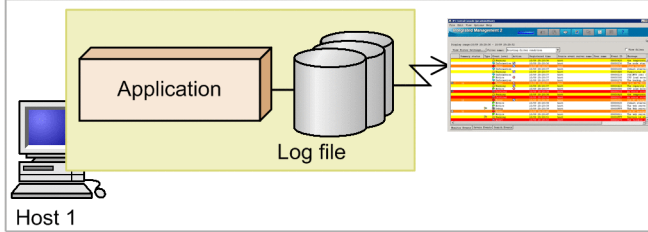
3.4 Using event conversion to monitor log files

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.

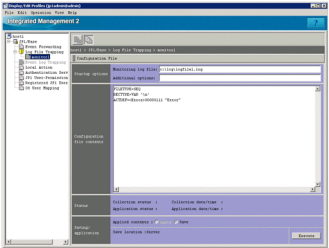
Problem

1. I want to know the signs of system failure based on log files.
2. There must be a way to monitor log file records by using JP1/IM - Manager.



Action

1. It looks like I can use the JP1/Base event conversion function to monitor log file records.
2. I'll try adding a profile in IM Configuration Management to start the log file trap.

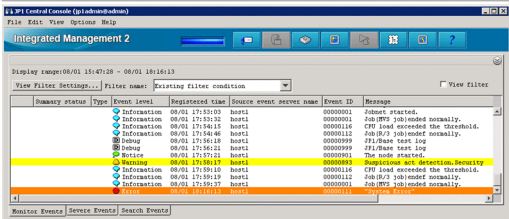


- Window:
 - Display/Edit Profile window
- Required settings
 - Log file trap name
 - Log file name
 - Action definition for the log file trap

Check

I'll execute the command to confirm that the log file trap is running.

```
echo conversion condition >> Monitored log file name
```



Priority	Status	Type	Event Level	Registered Time	Source Event	Server Name	Event ID	Message
Information				08/01 17:53:00	host1		0000001	Agent started.
Information				08/01 17:53:00	host1		0000001	Job CPU job ended normally.
Information				08/01 17:54:15	host1		0000116	CPU load exceeded the threshold.
Information				08/01 17:54:46	host1		0000112	Job CPU job ended normally.
Debug				08/01 17:54:18	host1		0000099	J1/Share test log
Debug				08/01 17:54:21	host1		0000099	J2/Share test log
Warning				08/01 17:55:11	host1		0000091	The node reached.
Warning				08/01 17:56:13	host1		0000091	Supervisor not detected. Security
Information				08/01 17:55:19	host1		0000116	CPU load exceeded the threshold.
Information				08/01 17:55:19	host1		0000112	Job CPU job ended normally.
Information				08/01 17:55:20	host1		0000001	Job CPU job ended normally.
Error				08/01 17:55:17	host1		0000111	System Error.

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*.

3.4.1 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 [3.4.1 \(2\) 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.

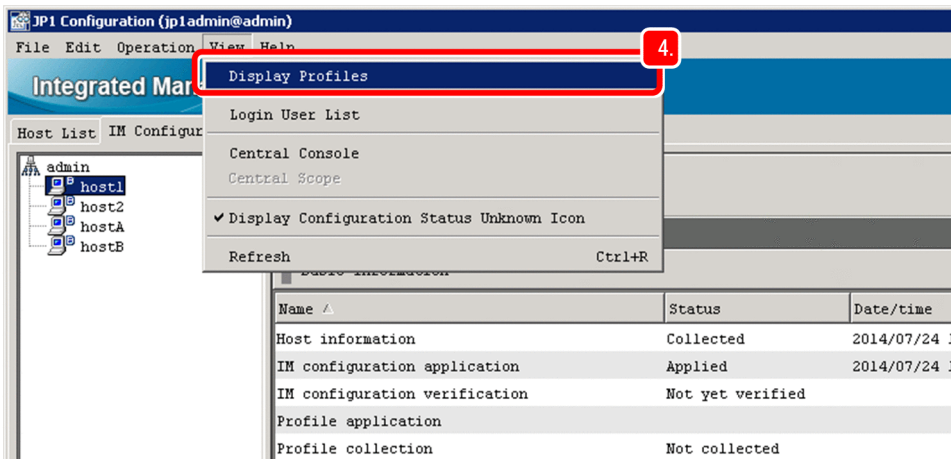
Prerequisites

The following conditions must be satisfied:

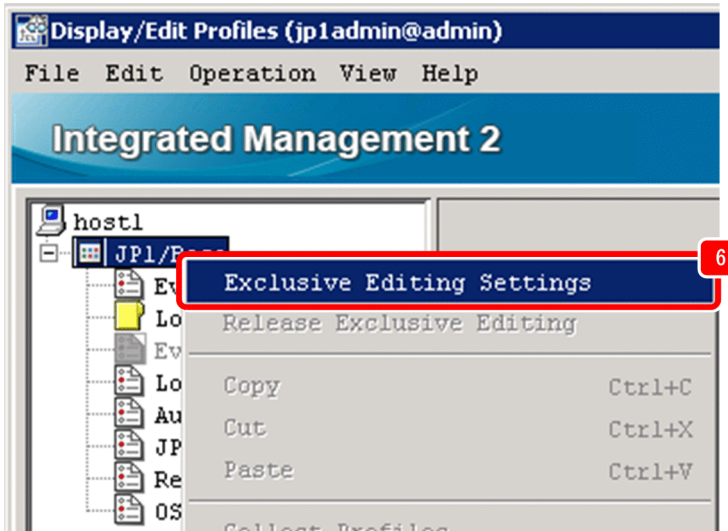
- The basic configuration system is set up according to *3.1 What is IM Configuration Management?*.
- Host information has been collected.
- Log files exist.

Procedure

1. From the Windows **Start** menu, select **All Programs, JP1_Integrated Management - 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.



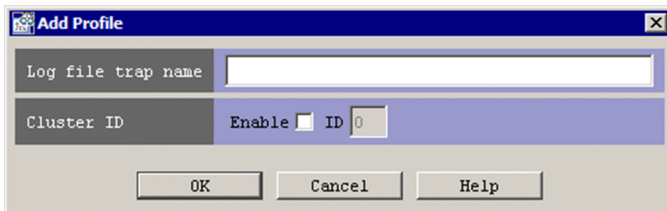
5. In the tree display area, select **JP1/Base**.
6. In the pop-up menu displayed by right-clicking, select **Exclusive Editing Settings** to obtain exclusive editing rights.



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.

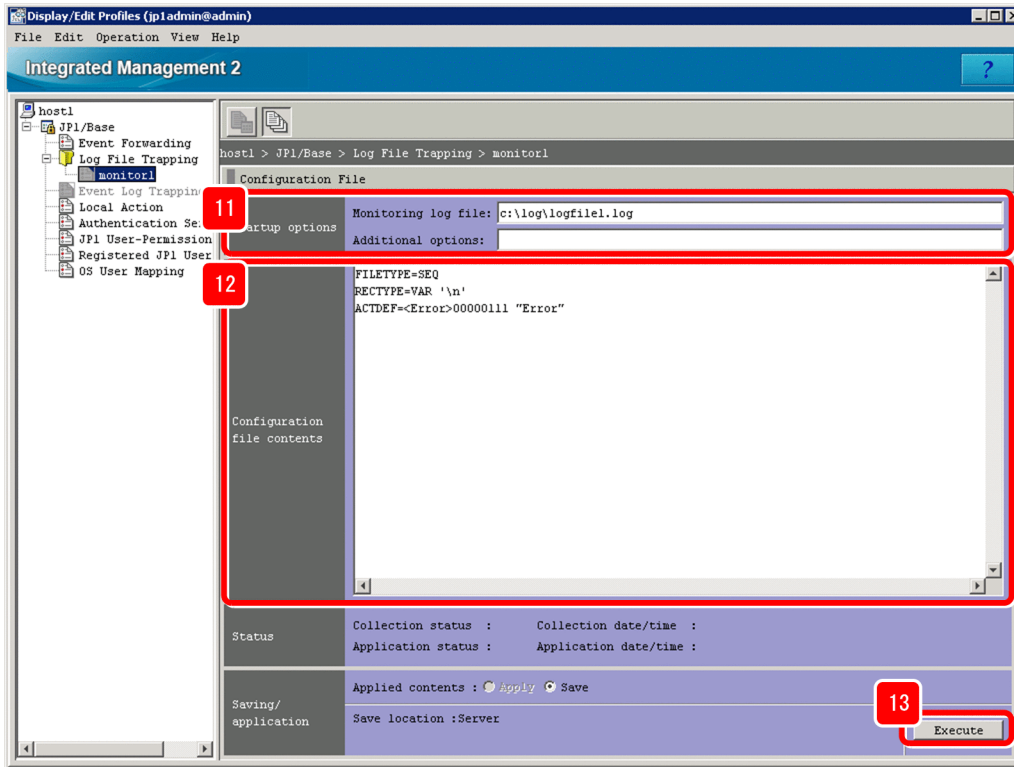
Note that immediately after the log file trap name is added, nothing is set in the log file trap action-definition file.

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 manual GUI Reference](#)
- [5.9 Display/Edit Profiles window in the manual 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.

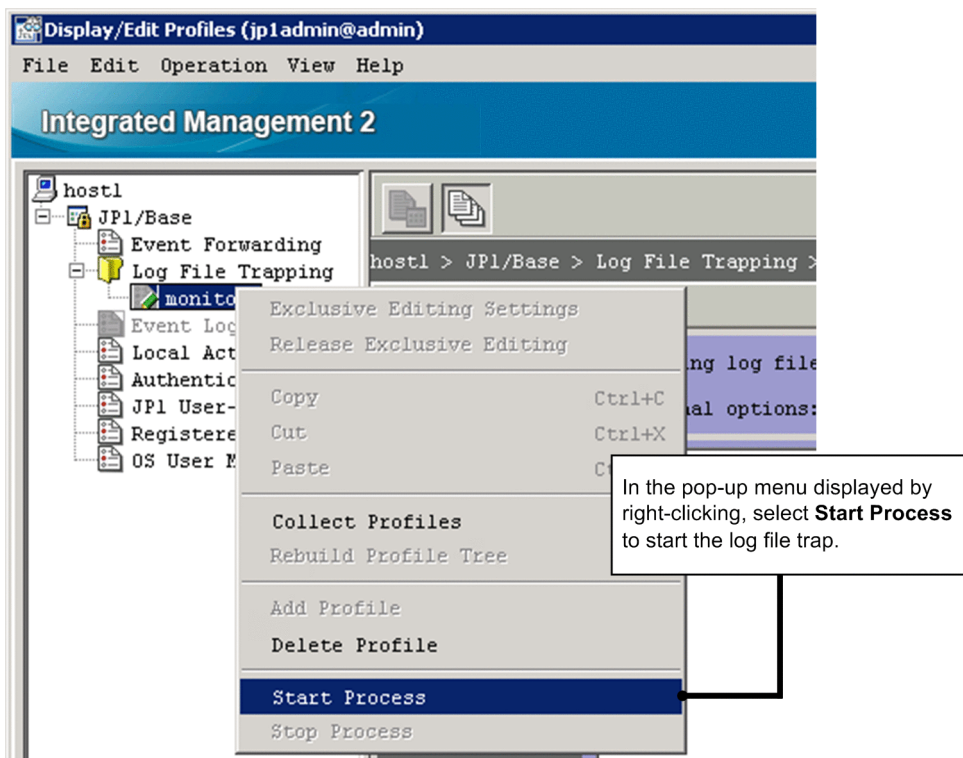
Prerequisites

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 for JPI/Base on the host to be monitored.
- The JPI/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 manual *GUI Reference*
- Descriptions of converting application program log files in the *JPI/Base User's Guide*

3.4.2 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 [3.4.1 What is log file trapping for JPI/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 [3.4.1 What is log file trapping for JPI/Base?](#).

Procedure

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

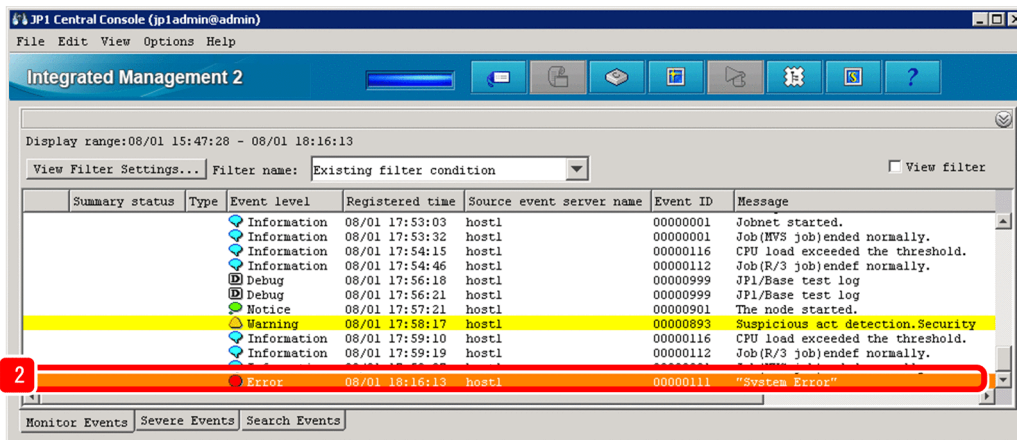
```
echo "System Error">>log-file-name#
```

#: 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 manual GUI Reference](#)
- [3.40 Execute Command window in the manual GUI Reference](#)

4

Monitoring a System

This chapter describes how to temporarily filter events to be displayed in the event list of a viewer and how to remove hosts undergoing maintenance from the items to be monitored.

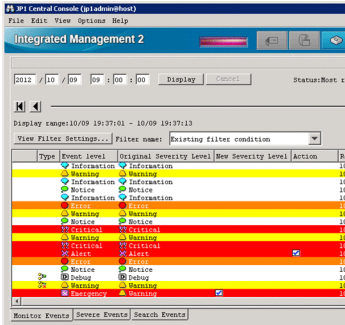
This chapter assumes that the system is monitored by using JP1/IM - View.

4.1 Monitoring only necessary events

When you use a viewer to monitor events, events issued on hosts are displayed in the event list. If conditions such as for the host and severity level were established, you can display only the events you want to monitor according to the conditions that are set. In this section, we will specify conditions to temporarily filter the events to be displayed.

Problem

1. Host B in the sales department seems to be issuing a log of events.
2. I need to investigate the events issued from host B.
3. There must be a way to temporarily display only events of severity level `Error` issued from host B.



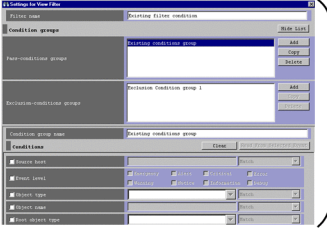
Sales department

- Error
- Information
- Warning
- Information
- Notice
- Information
- Error
- :

Host B

Action

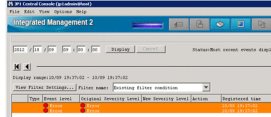
1. I'll try specifying which event to display.
2. It looks like I can use the view filter to do this.
3. I'll try setting up conditions so that events of severity level `Error` issued from host B are displayed.



- Window:
 - Settings for View Filter window
- Condition settings
 - Source host
 - Event level
 - :

Check

OK. Now I'll check whether only events from host B of severity level `Error` are displayed in the events list.



Sales department

- Error
- Information
- Warning
- Information
- Notice
- Information
- Error
- :

Host B

Legend: ● Displayed
✗ Not displayed

Keywords:

display, event, specific, filtering, view filter

4.1.1 Using a view filter to filter events to be displayed

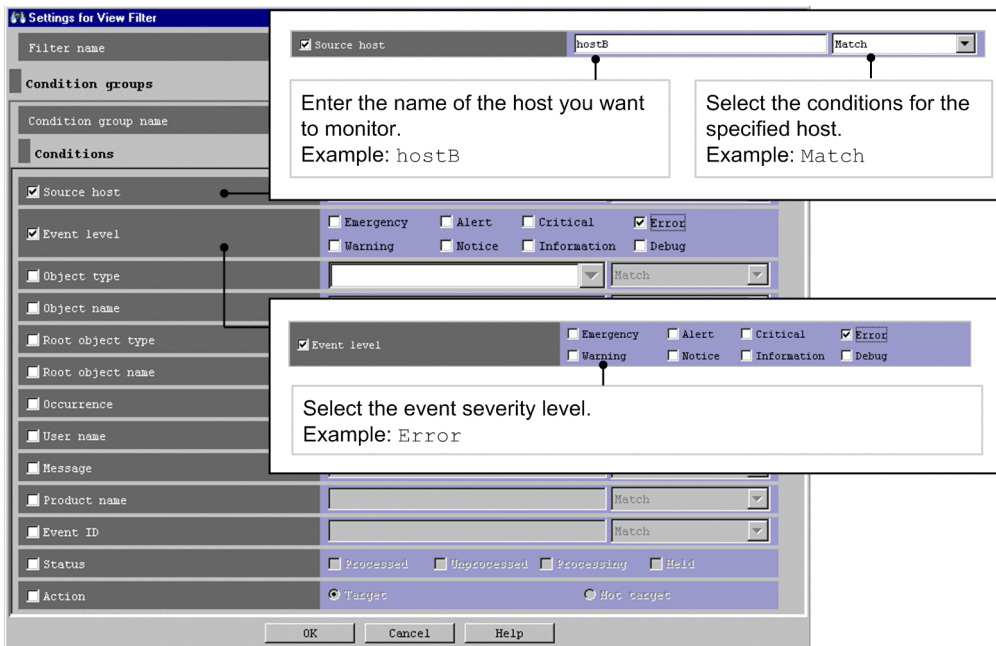
To filter events to be displayed, set up a view filter in the Settings for View Filter window of the central console. In this procedure, you set up the view filter to display events of severity level `Error` issued from host B.

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 manual GUI Reference](#)

4.1.2 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 [4.1.1 Using a view filter to filter events to be displayed](#).

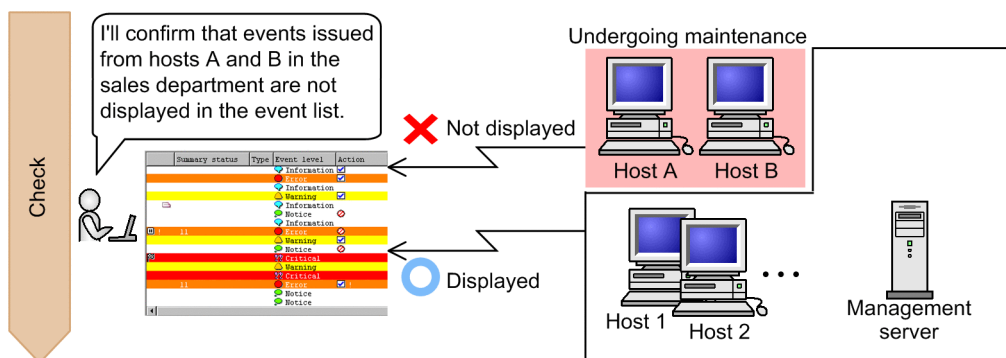
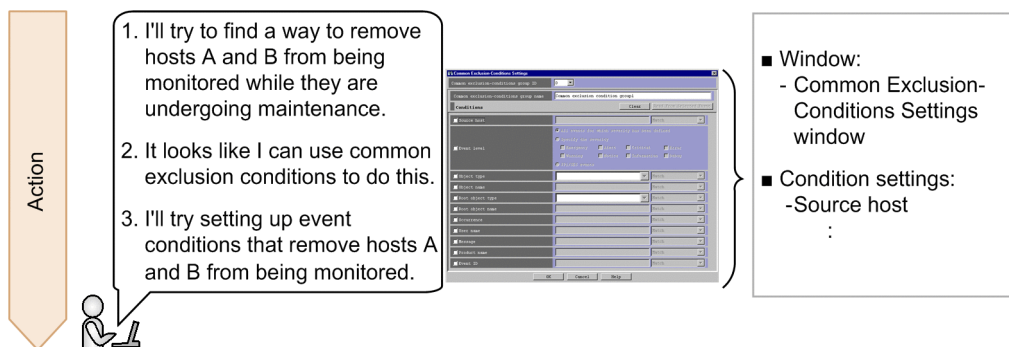
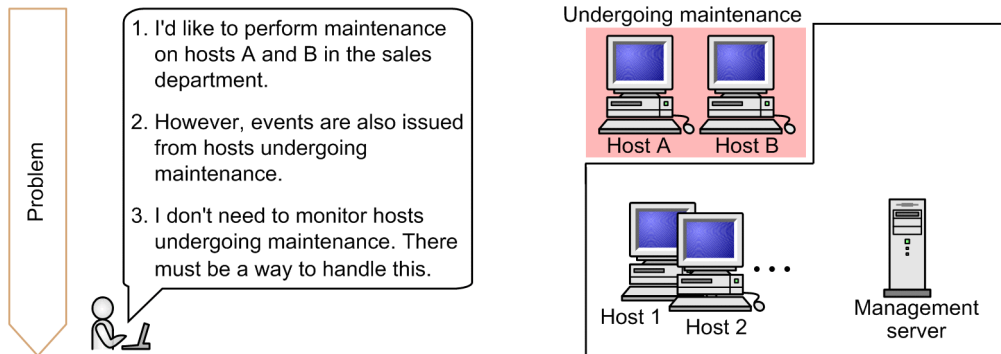
Procedure

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.

4.2 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*.

4.2.1 Using common exclusion conditions in a filter to temporarily stop hosts from being monitored

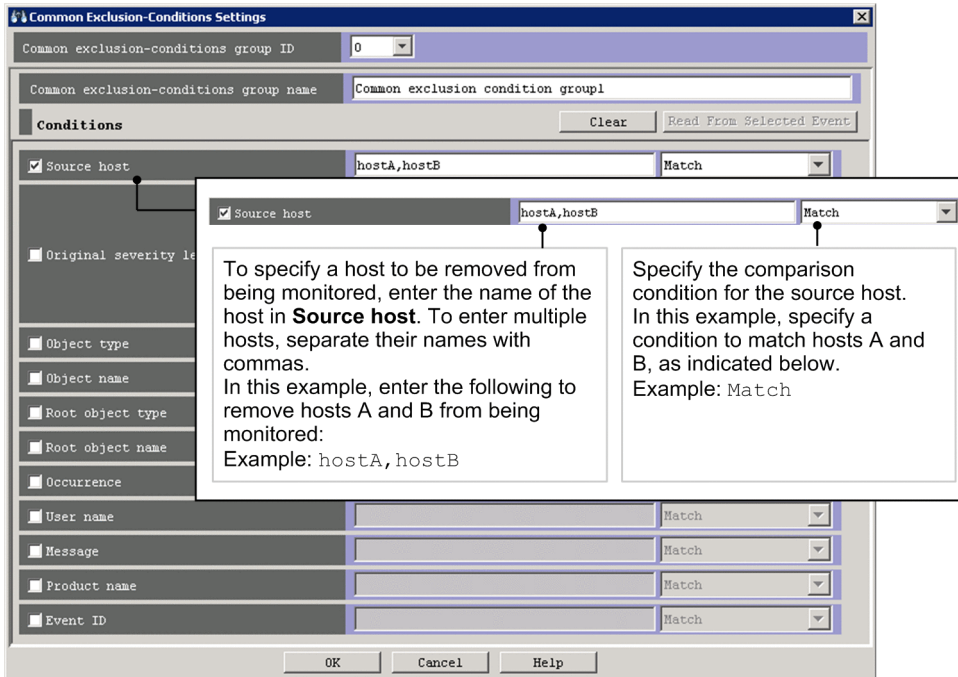
To remove hosts undergoing maintenance from the items being monitored, you use common exclusion conditions in a filter. To set common exclusion conditions, you use the Common Exclusion-Condition Settings window of Central Console. You can also use common exclusion conditions to remove action-triggering 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*
- [13.10 Considerations for JPI/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 manual *GUI Reference*.

4.2.2 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 [3.2.1 Configuring user mapping](#).
- A basic configuration system was set up according to [3.1 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: <ul style="list-style-type: none">• In Windows: <code>"Base-path\bin\jevsend" -e SEVERITY=Warning -m Command executed from host A.</code>• In Linux: <code>/opt/jplbase/bin/jevsend -e SEVERITY=Warning -m Command executed from host A.</code>

An event of severity level `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: <ul style="list-style-type: none">• In Windows: <code>"Base-path\bin\jevsend" -e SEVERITY=Warning -m Command executed from host B.</code>• In Linux: <code>/opt/jplbase/bin/jevsend -e SEVERITY=Warning -m Command executed from host B.</code>

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
	<ul style="list-style-type: none"> <li data-bbox="432 174 1458 271">• In Windows: <code>"Base-path\bin\jvsend" -e SEVERITY=Warning -m Command executed from host 1.</code> <li data-bbox="432 277 1458 374">• In Linux: <code>/opt/jplbase/bin/jvsend -e SEVERITY=Warning -m Command executed from host 1.</code>

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 manual *GUI Reference*
- [3.24.2 Event Attributes page](#) in the manual *GUI Reference*
- [3.40 Execute Command window](#) in the manual *GUI Reference*

5

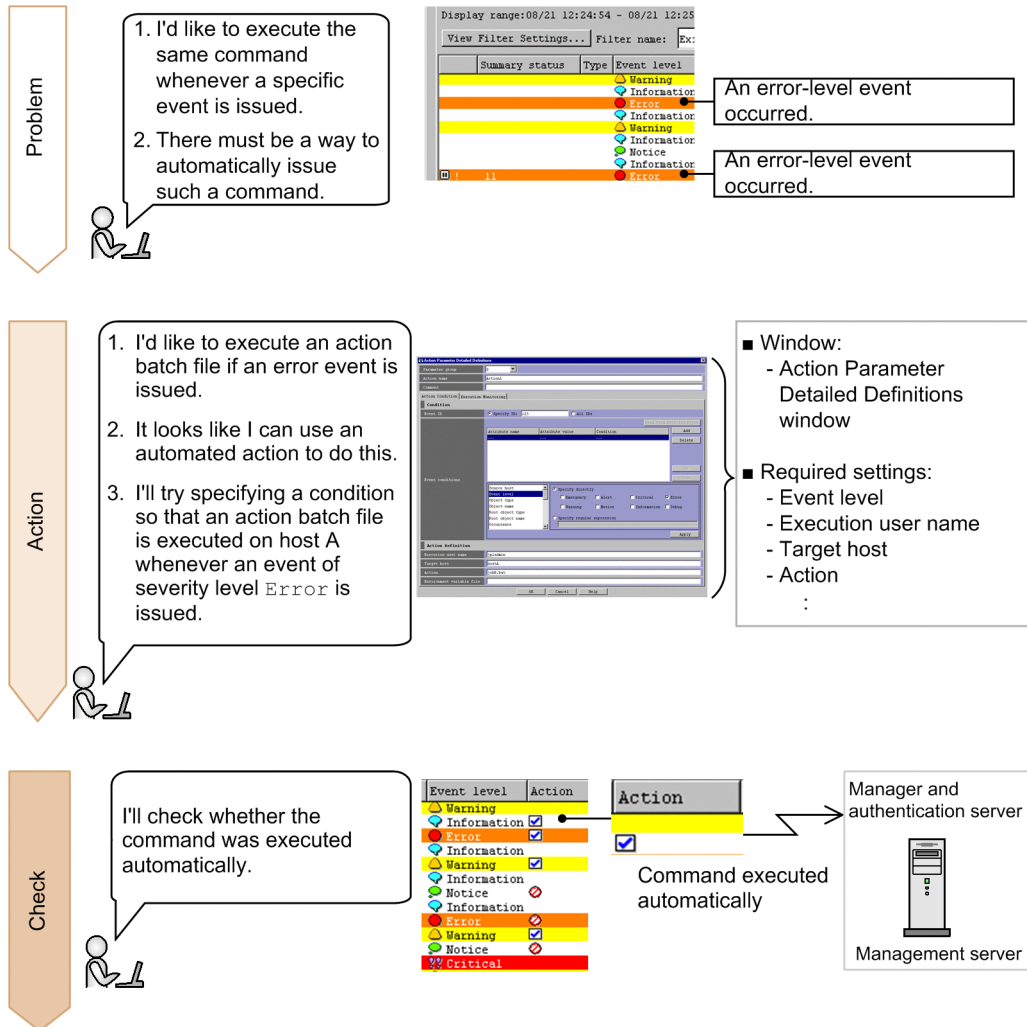
Detecting and Investigating System Errors

This chapter explains how to automatically execute commands based on the kind of system error that is detected, and how to search error events to investigate a system error.

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

5.1 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:\jplim` 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

5.1.1 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.

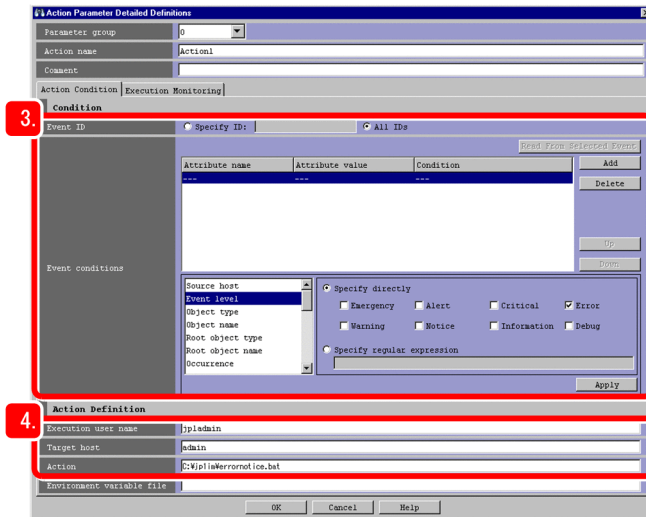
Prerequisites

The following conditions must be satisfied:

- OS user mapping was configured according to the procedure in [3.2.1 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:** jpladmin
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:\jplim\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 manual *GUI Reference*

5.1.2 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 [3.2.1 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: <ul style="list-style-type: none">• In Windows: <code>"Base-path\bin\jevsend" -e SEVERITY=Error</code>• In Linux: <code>/opt/jplbase/bin/jevsend -e SEVERITY=Error</code>

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 manual *GUI Reference*
- [3.36 Action Log window](#) in the manual *GUI Reference*
- [3.40 Execute Command window](#) in the manual *GUI Reference*

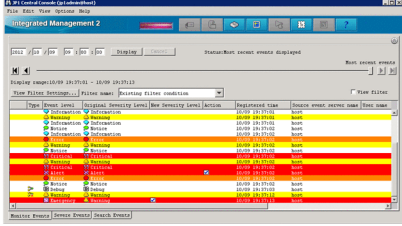
5.2 Searching for events

In the course of investigating an error, you might need to check whether other events related to the error have been issued, in addition to the ones currently displayed in the event list. However, at the time of the investigation, such events might have already been cleared from the event list.

In this section, we will search for events that have been cleared from the event list, by specifying event conditions.

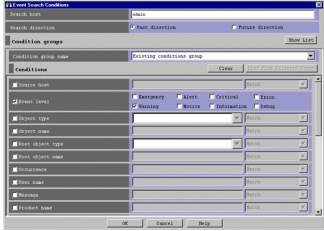
Problem

I'd like to find out what type of error-level events were issued in the past.



Action

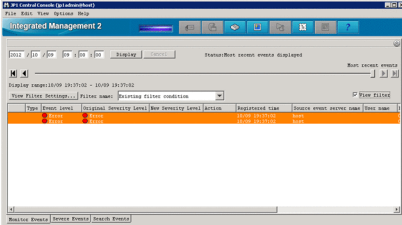
1. I'd like to search for error-level events.
2. It looks like I can use the search events function to do this.



- Window:
 - Event Search Conditions window
- Required setting:
 - Event level

Check

OK. Now I'll check to see whether only events that match the specified condition were found.



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*.

5.2.1 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:

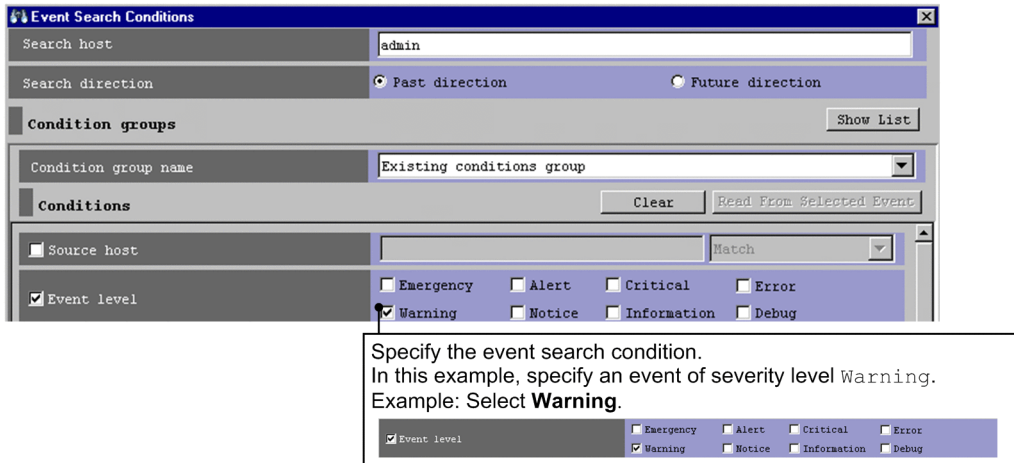
None

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](#)

5.2.2 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 [5.2.1 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.

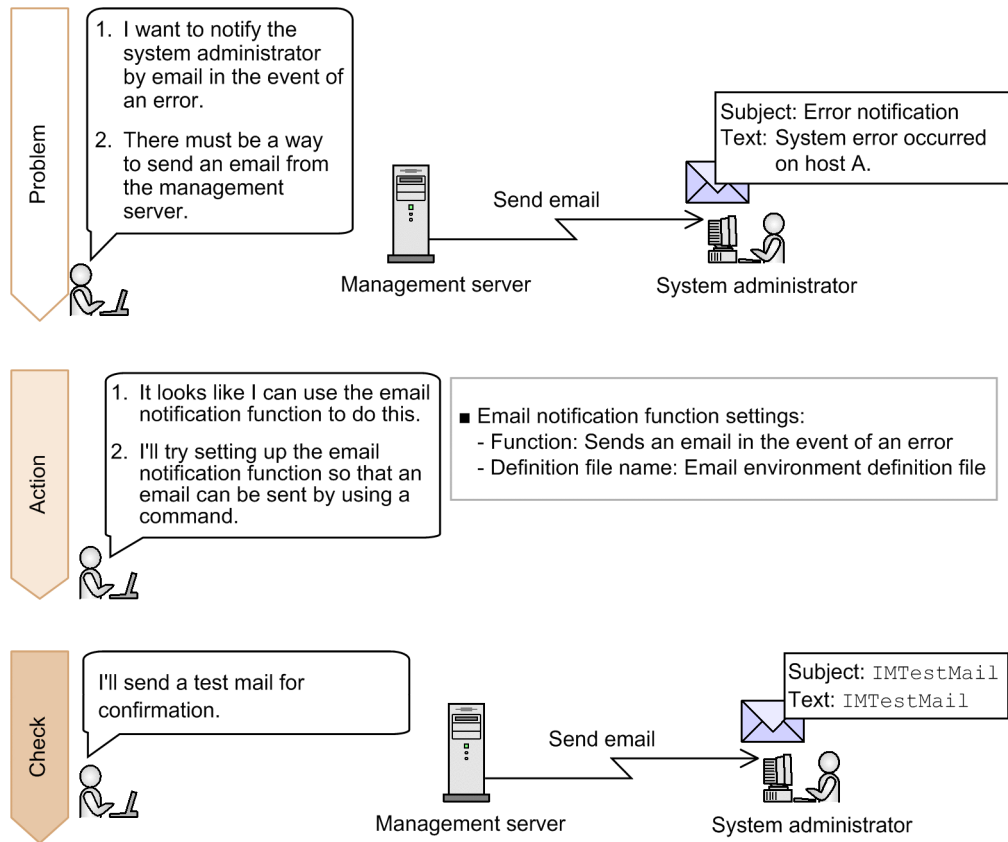


Appendixes

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: <ul style="list-style-type: none"> Alphanumeric characters (0-9 and a-z) At mark (@)

Specification	Target setting	Description
		<ul style="list-style-type: none"> • Period (.) • Hyphen (-) • Underscore (_)
<code>SmtPServer=host-name-or-IP-address-of-the-SMTP-server</code>	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.
<code>AuthMethod=SMTP</code>	Authentication method when sending an email	<p>Specifies the authentication method used on the mail server when sending an email. NONE: No authentication</p> <ul style="list-style-type: none"> • POP: POP before SMTP authentication • SMTP: SMTP-AUTH authentication (LOGIN/PLAIN) <p>The default is NONE.</p>
<code>AuthUser=authentication-account-name</code>	Authentication account name used for POP before SMTP authentication or SMTP-AUTH authentication	<p>Specifies the authentication account name used for POP before SMTP authentication or SMTP-AUTH authentication.</p> <p>You can use a string of 1 to 255 bytes.</p> <p>The default is a null character ("").</p>

(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 `jplhosts`, `jplhosts2`, 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 manual Command and Definition File Reference*
- *jimmail (Windows only) in 1. Commands in the manual Command and Definition File Reference*
- *jimmailpasswd (Windows only) in 1. Commands in the manual Command and Definition File 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 [5.1.1 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	<code>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) "</code>

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

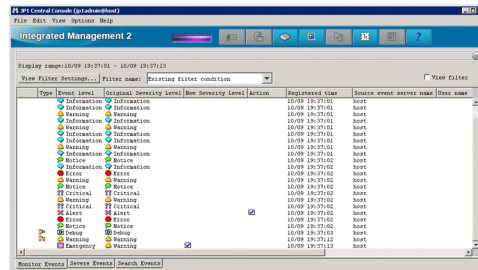
- [4.19.5 Inheriting event information when a command is executed](#) in the *Overview and System Design Guide*

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.

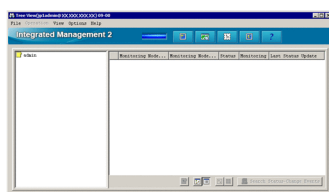
Problem

1. When I display the events in a list, I can't quickly figure out the extent of the impact.
2. There must be a way to get an idea of this visually.



Action

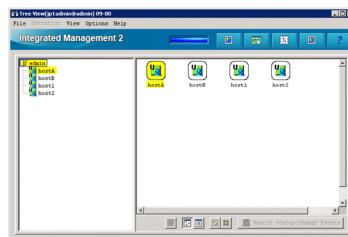
1. It looks as if I can use the Central Scope functions to do this.
2. Well, let's try setting up the conditions for monitoring events visually.



- Windows:
 - Create New Monitoring Node window
 - Visual Monitoring (Editing) window
- Condition settings:
 - Monitoring node name
 - Monitoring node type
 -

Check

Now that visual monitoring is set up, it's easy to see where the events are occurring.



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/IM2 - 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/IM2 - 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 manual *Command and Definition File Reference*
- `jcsdbsetup` in *1. Commands* in the manual *Command and Definition File 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.

Enter the name of a server or host in the system.
Example: admin

Select the monitoring node type depending on the server or host you specified for **Monitoring node name**.
For a node on the lowest level, select **Monitoring object**.
For a node on a higher level, select **Monitoring group**.

In this example, the management server `admin` is selected as the name of the monitoring node, so select **Monitoring group**.

After the management server is created, use the Create New Monitoring Node window in a similar fashion to add a host at a lower level.
Example: Host A

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 manual GUI Reference](#)
- [4.1 Overview of the Monitoring Tree window in the manual GUI Reference](#)
- [4.15 Monitoring Tree \(Editing\) window in the manual GUI Reference](#)

(3) Setting the attributes of monitoring nodes

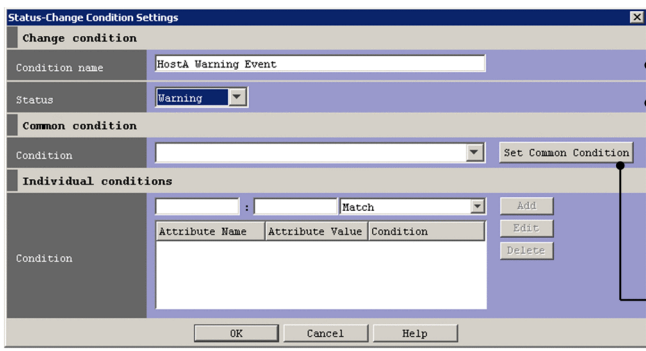
By setting the attributes of monitoring nodes, you can change the icon used by a monitoring node or change the status of a monitoring node when an event is received. The following describes how to set the monitoring node attributes for host A shown in *2.1 Overview of a basic configuration system*.

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.

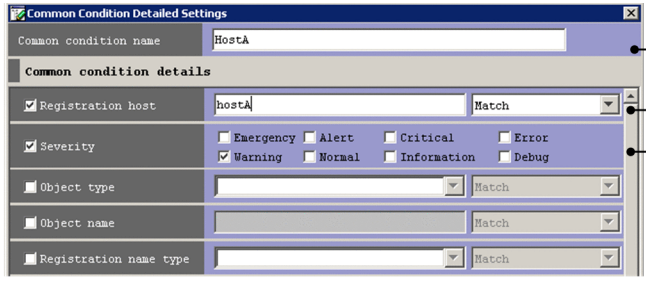


The screenshot shows the 'Status-Change Condition Settings' dialog box. The 'Change condition' section has 'HostA Warning Event' in the 'Condition name' field and 'Warning' selected in the 'Status' dropdown. The 'Common condition' section has a dropdown menu and a 'Set Common Condition' button. The 'Individual conditions' section contains a table with columns 'Attribute Name', 'Attribute Value', and 'Condition', and buttons for 'Add', 'Edit', and 'Delete'. The 'OK', 'Cancel', and 'Help' buttons are at the bottom.

Enter the condition name.
Example: HostA Warning Event

Select the status.
For this example, we want the status to be warning, so select **Warning**.
Example: **Warning**

Click the **Set Common Condition** button.
When the Common Condition Settings window appears, click the **Add** button.
The Common Condition Detailed Settings window appears.



The screenshot shows the 'Common Condition Detailed Settings' dialog box. The 'Common condition name' field contains 'HostA'. The 'Common condition details' section has several fields: 'Registration host' (hostA), 'Severity' (Warning selected), 'Object type', 'Object name', and 'Registration name type', each with a 'Match' dropdown. The 'OK' button is at the bottom.

Enter the common condition name.
Example: HostA

Enter the name of the target host.
For this example, we are targeting events from host A, so specify the computer name of host A.
Example: hostA

Specify the event severity level.
Example: **Warning**

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

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

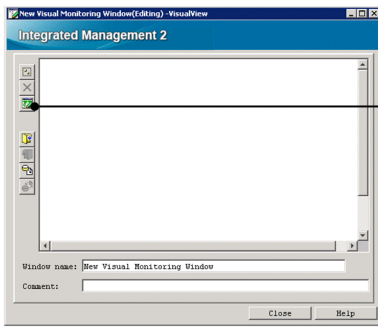
To display hosts in a map format, you first create a Visual Monitoring window. The following describes how to create the Visual Monitoring window from the Visual Monitoring (Editing) window.

Prerequisites

Monitoring nodes must be displayed in the Monitoring Tree window.

Procedure

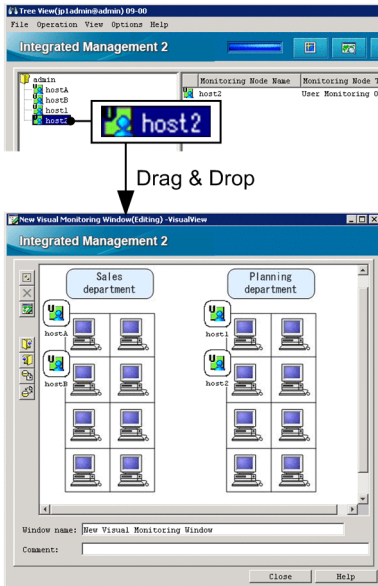
1. From the Windows **Start** menu, select **All Programs, JP1_Integrated Management - View**, and then **Edit Monitoring Tree**. The Edit View window appears.
2. In the Monitoring Tree (Editing) window, from the menu bar, select **Acquire Tree from Server** to apply the settings in the Monitoring Tree 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.




Background Image Settings

File list	Preview
No background image	
1_1F.JPG	
1_2F.jpg	
1_BRANCH_A.jpg	

Click this to display the Background Image Settings window, in which you can select a background. The image you want to use as the background must be saved in advance in the following folder:
View-path\image\map\



Select a host you want to monitor, and place it in a layout consistent with your operations. Drag the icon of the host from the Monitoring Tree (Editing) window and drop it on the Visual Monitoring (Editing) window.

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 manual *GUI Reference*
- 4.5 Visual Monitoring window in the manual *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 [3.2.1 Configuring user mapping](#).

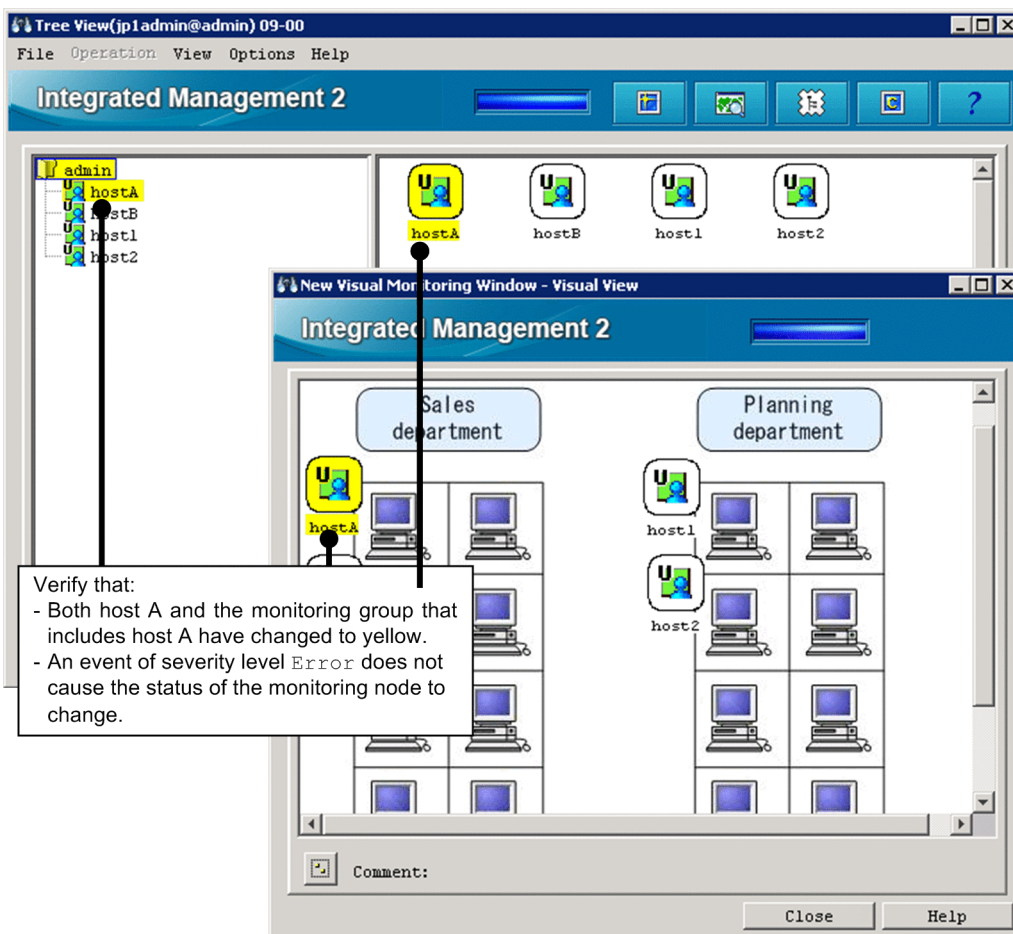
Procedure

1. In the Event Console window, click the **Execute Command** button. The Execute Command window appears.
2. Follow the procedure in [3.2.2 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: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none">• In Windows: "<i>Base-path</i>\bin\jevsend" -e SEVERITY=Error -m Error Event Issued• In Linux: /opt/jplbase/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

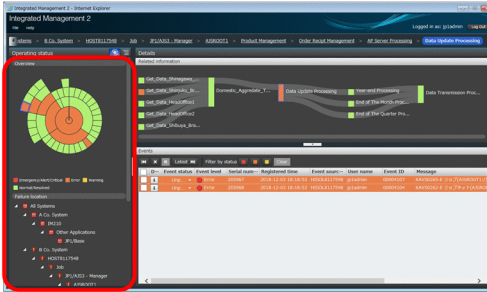
- *3.1 Overview of the Event Console window* in the manual *GUI Reference*
- *3.40 Execute Command window* in the manual *GUI Reference*

C. How to Monitor and Manage System Events with the Integrated Operation Viewer

The integrated operation viewer allows you to visually review the hierarchical structure of the monitored hosts as well as the statuses and the affected areas of events occurring in the monitored hosts, in a centralized window.

Problem

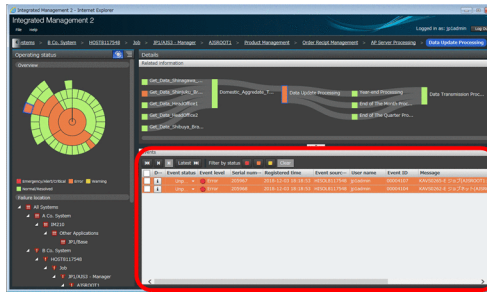
1. You can visually grasp system status by colors of components.



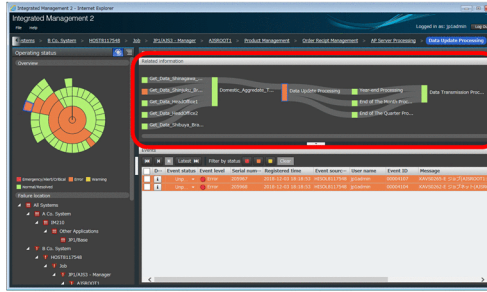
Action / Check

2. You can check whether events occur on the components in the same window.

3. You can filter events by just selecting a color. No filter setting is needed.



4. You can easily determine the affected area by checking the relationships between root jobnets



The integrated operation viewer is displayed in a Web browser. For details about how to log in, see [2.6 Logging in to JP1/IM - Manager from the integrated operation viewer](#).

The Intelligent Integrated Management Base must be set up in JP1/IM - Manager before you can use the integrated operation viewer.

Keywords:

GUI, visual, event, sunburst, tree, graphic, monitoring tree, integrated operation viewer, root jobnet, visual

C.1 Checking system status

The integrated operation viewer allows you to check system status.

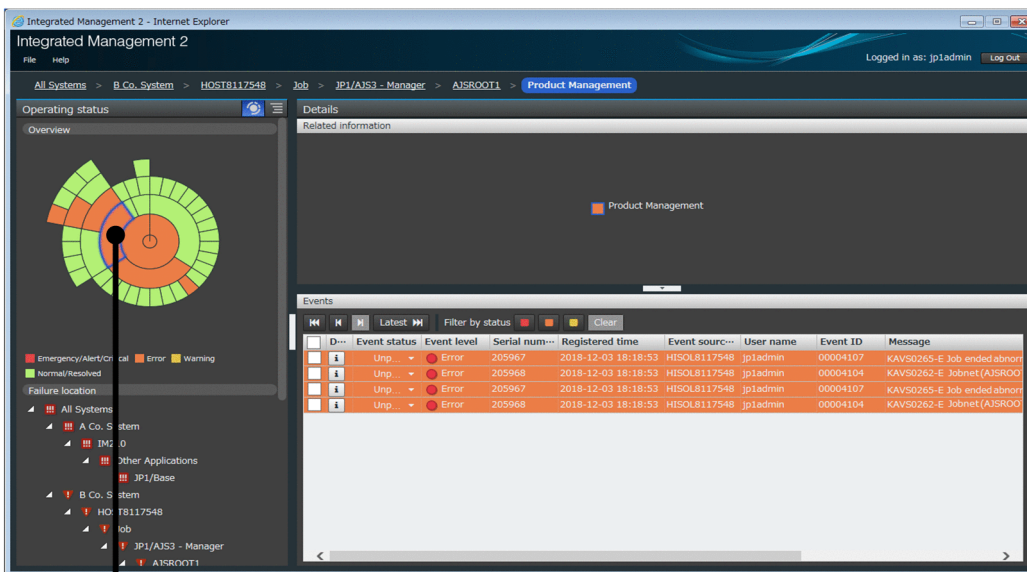
This section describes how to check the failures occurring in the managed system.

Prerequisites

The OS user mapping must be configured according to the procedure in [3.2.1 Configuring user mapping](#).

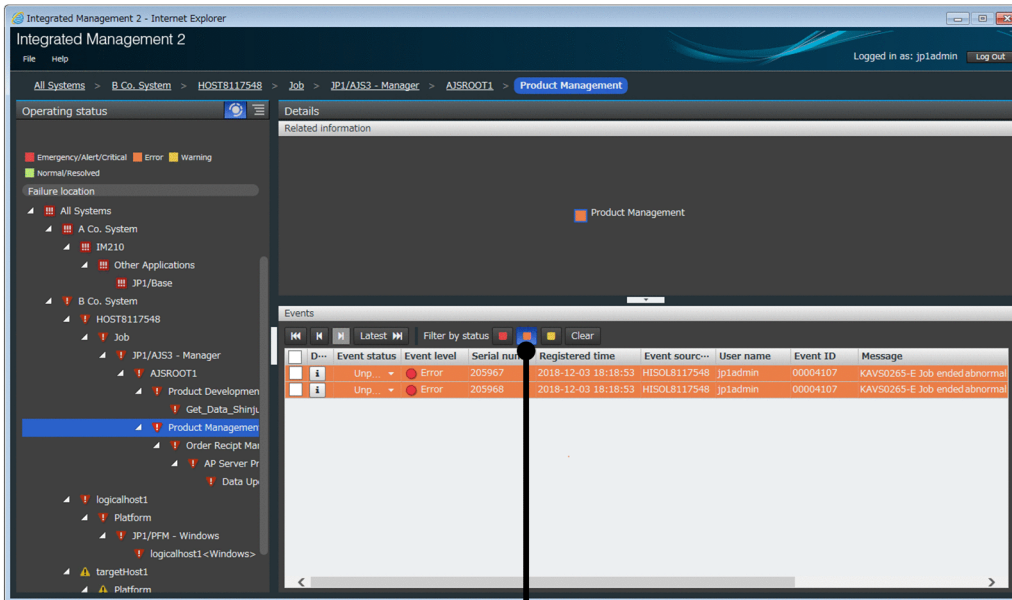
Procedure


1. Display the integrated operation viewer in a Web browser.
2. In the sunburst chart or **Failure location**, select a component where a failure has occurred. Here, select `Product Management`.
3. In this example, the color of the groups to which `Product Management` belongs is changed to indicate failure statuses.



Verify that:
- **Product Management** and the groups including **Product Management** is orange.

4. Events occurring on `Product Management` appear in the **Events** area.
5. Click the orange button indicating **Error**. The events are filtered.



6. Click the  button to see the details of the event.

Related topics

- *2. Integrated Operation Viewer Window* in the manual *GUI Reference*

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
jplimevtcon	20115/tcp	Y	Y	Used to connect to JP1/IM - Manager (event console service) from JP1/IM - View
jplimcmda	20238/tcp	Y	--	Used to execute commands from JP1/IM - View
jplimcss	20305/tcp	Y	Y	Used to connect to JP1/IM - Manager (central scope service) from JP1/IM - View
JP1/IM2-Manager DB Server	20700/tcp	--	N	Used for internal processing by JP1/IM - Manager (IM database)
jplimcf	20702/tcp	Y	Y	Used to connect to JP1/IM - Manager (IM Configuration Management service) from JP1/IM - View
jplimfcs	20701/tcp	--	Y	Used for internal processing by JP1/IM - Manager (event base service)
jplimegs	20383/tcp	--	Y	Used for internal processing by JP1/IM - Manager (Event Generation Service)
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
jplimevt	20098/tcp	Used to forward events to other hosts

Service name	Port numbers	Description
jplimevtapi	20099/tcp	Used by all products that register and acquire events, and functions for issuing and acquiring events
jplimrt	20237/tcp	Used by IM Configuration Management
jplimcmda	20238/tcp	Used to execute commands
jplimcmdc	20239/tcp	Used to execute commands
jplbsuser	20240/tcp	Used by user authentication servers
jplbsplugin	20306/tcp	Used to collect and distribute definition information for JP1/IM
jplbscom	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
jplimevt	20098/tcp	JP1/Base that transfers events -> JP1/Base that receives events
jplimevtapi	20099/tcp	A program (such as JP1/IM - Manager) that acquires events -> JP1/Base
jplimevtcon	20115/tcp	JP1/IM - View -> JP1/IM - Manager (central console)
jplimrt	20237/tcp	JP1/IM - Manager -> JP1/Base
jplimcmda	20238/tcp	JP1/IM - View -> JP1/IM - Manager (central console) JP1/IM - Manager (central console) -> JP1/Base ^{#1}
jplimcmdc	20239/tcp	JP1/Base on a host with JP1/IM - Manager installed <- -> JP1/Base on a host that executes commands
jplbsuser	20240/tcp	JP1/IM - Manager -> JP1/Base
jplimcss	20305/tcp	JP1/IM - View -> JP1/IM - Manager (central console)
jplbsplugin	20306/tcp	Higher-level program using services such as JP1/IM - Manager -> JP1/Base
jplimegs	20383/tcp	Firewall setup is unnecessary because all communication takes place on the machine on which JP1/IM - Manager is installed.
jplbscom	20600/tcp	JP1/IM - Manager <- -> JP1/Base on another host
JP1/IM2-Manager DB Server	20700/tcp	JP1/IM - Manager -> JP1/IM-Manager DB Server
jplimfcs	20701/tcp	Firewall setup is unnecessary because all communication takes place on the machine on which JP1/IM - Manager is installed.
jplimcf	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/IM2-Manager	JP1_Console	Manual	JP1/IM - Manager (Intelligent Integrated Management Base, central console, central scope, and IM Configuration Management) service for physical hosts
JP1/IM2-Manager DB Server	HiRDBEmbeddedEdition_JM0	Manual	IM database service for physical hosts

[#]: The default startup type at 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.	<ul style="list-style-type: none"> • <i>4.2 Filtering of JP1 events</i> in the <i>Overview and System Design Guide</i> • <i>12.1.3 Considerations for filtering JP1 events</i> in the <i>Overview and System Design Guide</i> • <i>5.2 Setting JP1 event filtering</i> in the <i>Configuration Guide</i>
Correlation event	When a related event is issued, a new event can be issued.	<ul style="list-style-type: none"> • <i>4.3 Issue of correlation events</i> in the <i>Overview and System Design Guide</i> • <i>12.1.4 Considerations for issuing correlation events</i> in the <i>Overview and System Design Guide</i> • <i>5.6 Settings for generating correlation events</i> in the <i>Configuration Guide</i> • <i>6.4.2 Checking detailed information about a correlation event and changing the response status</i> in the <i>Administration Guide</i>
Repeated event monitoring suppression	A large number of events can be consolidated into one event to avoid overlooking important events.	<ul style="list-style-type: none"> • <i>4.4 Suppressing display of repeated events</i> in the <i>Overview and System Design Guide</i> • <i>12.1.5 Considerations for suppressing the monitoring of repeated events and a large number of events</i> in the <i>Overview and System Design Guide</i> • <i>5.3 Setting monitoring of repeated events to be prevented</i> in the <i>Configuration Guide</i> • <i>6.10 Taking actions for the generation of a large number of events</i> in the <i>Administration Guide</i>
Suppressing forwarding of a large number of events	You can prevent a large number of events issued on an agent from being forwarded to the manager.	<ul style="list-style-type: none"> • <i>4.5.9 Suppressing the forwarding of a large number of events</i> in the <i>Overview and System Design Guide</i> • <i>12.1.7 Considerations for suppressing the forwarding of a large number of events</i> in the <i>Overview and System Design Guide</i> • <i>6.10 Taking actions for the generation of a large number of events</i> in the <i>Administration Guide</i>
Severity changing function	Users can freely change the severity of events depending on system operations.	<ul style="list-style-type: none"> • <i>4.7 Changing the event level (severity) of JP1 events</i> in the <i>Overview and System Design Guide</i> • <i>12.1.8 Considerations for changing JP1 event levels</i> in the <i>Overview and System Design Guide</i> • <i>5.13 Setting the severity changing function</i> in the <i>Configuration Guide</i> • <i>6.9.4 Changing the severity level of JP1 events</i> in the <i>Administration Guide</i>
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.	<ul style="list-style-type: none"> • <i>4.8 Changing the message display format</i> in the <i>Overview and System Design Guide</i> • <i>12.1.9 Considerations for changing display messages for JP1 events</i> in the <i>Overview and System Design Guide</i> • <i>5.14 Setting the display message change function</i> in the <i>Configuration Guide</i> • <i>6.9.5 Changing the message displayed for a JP1 event</i> in the <i>Administration Guide</i>

Function	Overview	Related topics
Event guide function	Guide information for investigating and resolving events that occur during system monitoring can be displayed.	<ul style="list-style-type: none"> • <i>4.10 Event guide function</i> in the <i>Overview and System Design Guide</i> • <i>12.1.10 Considerations for setting event guide information</i> in the <i>Overview and System Design Guide</i> • <i>5.8 Editing event guide information</i> in the <i>Configuration Guide</i>
Remote monitoring [#]	You can monitor log files on monitored hosts without JP1/Base installed.	<ul style="list-style-type: none"> • <i>7.2.8 Selection of agent configuration or remote monitoring configuration</i> in the <i>Overview and System Design Guide</i> • <i>7.6 Managing remotely monitored hosts</i> in the <i>Overview and System Design Guide</i> • <i>12.5.2 Managing the remote monitoring configuration</i> in the <i>Overview and System Design Guide</i> • <i>1.17 Specifying settings for monitoring logs on remotely monitored hosts (for Windows)</i> in the <i>Configuration Guide</i> • <i>2.16 Specifying settings for monitoring logs on remotely monitored hosts (for UNIX)</i> in the <i>Configuration Guide</i>
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.	<ul style="list-style-type: none"> • <i>7.3 Virtualization configuration management</i> in the <i>Overview and System Design Guide</i> • <i>3.3 Setting a virtualization system configuration</i> in the <i>Configuration Guide</i>
Business group	Operations and information that users are allowed can be restricted by group.	<ul style="list-style-type: none"> • <i>7.4 Managing business groups</i> in the <i>Overview and System Design Guide</i> • <i>12.5.4 Considerations for business groups</i> in the <i>Overview and System Design Guide</i> • <i>3.4 Setting business groups</i> in the <i>Configuration Guide</i> • <i>5.19 Setting reference and operation restrictions on business groups</i> in the <i>Configuration Guide</i> • <i>9.4 Managing business groups</i> in the <i>Administration Guide</i>
Linkage with other JP1 products	JP1/IM can be linked with products such as JP1/Service Support and JP1/Navigation Platform to monitor systems.	<ul style="list-style-type: none"> • <i>9. Linking with Other Products</i> in the <i>Overview and System Design Guide</i> • <i>10. Settings for Linking to Other JP1 Products</i> in the <i>Configuration Guide</i>
Support of cluster environment	Using JP1/IM in a cluster system allows system monitoring to continue if a server failure occurs.	<ul style="list-style-type: none"> • <i>13.3.8 Configuration for operation in a cluster system</i> in the <i>Overview and System Design Guide</i> • <i>7. Operation and Environment Configuration in a Cluster System (for Windows)</i> in the <i>Configuration Guide</i> • <i>8. Operation and Environment Configuration in a Cluster System (for UNIX)</i> in the <i>Configuration Guide</i>

[#]: 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 7	Microsoft(R) Windows(R) 7 Enterprise
	Microsoft(R) Windows(R) 7 Professional
	Microsoft(R) Windows(R) 7 Ultimate
Windows 8	Windows(R) 8 Enterprise
	Windows(R) 8 Pro
Windows 8.1	Windows(R) 8.1 Enterprise
	Windows(R) 8.1 Pro
Windows 10	Windows(R) 10 Enterprise 32-bit
	Windows(R) 10 Enterprise 64-bit
	Windows(R) 10 Home 32-bit
	Windows(R) 10 Home 64-bit
	Windows(R) 10 Pro 32-bit
	Windows(R) 10 Pro 64-bit
Windows Server 2012	Microsoft(R) Windows Server(R) 2012 Datacenter
	Microsoft(R) Windows Server(R) 2012 Standard
	Microsoft(R) Windows Server(R) 2012 R2 Datacenter
	Microsoft(R) Windows Server(R) 2012 R2 Standard
Windows Server 2016	Microsoft(R) Windows Server(R) 2016 Datacenter
	Microsoft(R) Windows Server(R) 2016 Standard

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

Abbreviations for manual titles

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

Abbreviations	Full name
Overview and System Design Guide	<i>JPI Version 12/Integrated Management 2 - Manager Overview and System Design Guide</i>
Configuration Guide	<i>JPI Version 12/Integrated Management 2 - Manager Configuration Guide</i>
Administration Guide	<i>JPI Version 12/Integrated Management 2 - Manager Administration Guide</i>
GUI Reference	<i>JPI Version 12/Integrated Management 2 - Manager GUI Reference</i>

Abbreviations	Full name
Command and Definition File Reference	<i>JP1 Version 12/Integrated Management 2 - Manager Command and Definition File Reference</i>
Messages	<i>JP1 Version 12/Integrated Management 2 - Manager Messages</i>
JP1/Base User's Guide User's Guide	<i>JP1 Version 12/Base User's Guide</i>

Conventions: Abbreviations for product names

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

Abbreviation	Full name	
AIX	AIX 7.1	
	AIX 7.2	
HP-UX (IPF)	HP-UX 11i V3 (IPF)	
JP1/IM	JP1/IM - Manager	JP1/Integrated Management 2 - Manager
	JP1/IM - View	JP1/Integrated Management 2 - View
Linux	CentOS 6 (x64)	CentOS 6 (x64)
	CentOS 7	CentOS 7
	Linux 6 (x64)	Red Hat Enterprise Linux (R) Server 6 (64-bit x86_64)
	Linux 7	Red Hat Enterprise Linux (R) Server 7
	Oracle Linux 6 (x64)	Oracle Linux (R) Operating System 6 (x64)
	Oracle Linux 7	Oracle Linux (R) Operating System 7
	SUSE Linux 12	SUSE Linux (R) Enterprise Server 12
Solaris	Solaris 10 (SPARC)	
	Solaris 11 (SPARC)	

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

Acronym	Meaning
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	<i>View-path</i>	<i>system-drive</i> : \Program Files\Hitachi\JP1CoView
	JP1/Base	<i>Base-path</i>	<i>system-drive</i> : \Program Files\Hitachi\JP1Base
x64	JP1/IM - View	<i>View-path</i>	<i>system-drive</i> : \Program Files (x86)\Hitachi\JP1CoView
	JP1/IM - Manager	<i>Manager-path</i>	<i>system-drive</i> : \Program Files (x86)\Hitachi\JP1IMM
		<i>Console-path</i>	<i>system-drive</i> : \Program Files (x86)\Hitachi\JP1Cons
		<i>Scope-path</i>	<i>system-drive</i> : \Program Files (x86)\Hitachi\JP1Scope
JP1/Base	<i>Base-path</i>	<i>system-drive</i> : \Program Files (x86)\Hitachi\JP1Base	

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

H. Glossary

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

In JP1/IM, a host managed by a manager, or a program managed by a manager program. JP1/Base acts as the agent program in a JP1/IM system, receiving processing requests from JP1/IM - View and JP1/IM - Manager, and performing tasks such as managing JP1 events and executing commands.

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.

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

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

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

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 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

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 - 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

manager

A program whose role is to manage other programs or a host whose role is to manage other hosts in the JP1/IM system

In the JP1/IM system, JP1/IM - Manager serves as the manager program, and manages the agent program JP1/Base.

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

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

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

A

advanced use 103
agents 20
automated action 77
automated action when using email notification function (Windows only), example definition 87
automatically executing command whenever specific event is issued 77

B

basic configuration system, overview 20
business group 104

C

central console 53
central scope 88
common exclusion conditions 72
common exclusion conditions in filter to temporarily stop hosts from being monitored 72
configuring user mapping 53
configuring visual monitoring, procedure 88
conventions
 fonts and symbols 9
 version numbers 9
correlation event 103

D

display message change function 103

E

email notification function, setting up (Windows only) 84
email notification function, using to send emails (Windows only) 84
Event Console window 46
event guide function 104
event receiver filter 103
Event Search Conditions window 82

F

firewall, direction of communication through 100
font conventions 9
customizing settings for forwarding events from agent to manager, customizing settings for 57

G

general procedures for installing and setting up JP1/IM 25
glossary 108

H

How to Monitor and Manage System Events with the Integrated Operation Viewer 96

I

IM configuration 109
IM Configuration Management 48
IM Configuration Management, overview 48
IM Configuration Management database 31, 40
IM database 25
installation and setup (for Linux) 37
installation and setup (for Windows) 27
installation memory and disk space, required amounts of 23
installing and setting up JP1/IM 19
installing and setting up JP1/IM, general procedures 25
installing JP1/IM (for Linux) 39
installing JP1/IM (for Windows) 30
installing prerequisite product (for Linux) 37
installing prerequisite product (for Windows) 27
integrated monitoring database 31, 40
Intelligent Integrated Management Base 16

J

JP1/Base 22
JP1/Base port numbers 99
JP1/IM - Manager 20
JP1/IM port numbers 99
JP1/IM - View 30
JP1events 16

L

language settings in prerequisite OSs 23
log file trapping for JP1/Base, overview 62
logging in to JP1/IM - Manager from JP1/IM - View 46
Logging in to JP1/IM - Manager from the integrated operation viewer 45

M

managers 20
monitoring only necessary events 69
monitoring systems 68

N

name resolution, setting 24

O

overview of basic configuration system 20

P

port numbers 99
ports used by JP1/IM, setting 23
preparation before installation 22
preparing products to be installed 22
prerequisite OSs and OS environment configuration 22

R

reference material for this manual 105
registering hosts into IM Configuration Management 49
removing hosts undergoing maintenance from items to be monitored 71
repeated event monitoring suppression 103

S

search events function, using to search for events that match specified condition 81
searching for events 81
services (Windows only), list 102
settings for executing commands on monitored hosts from JP1/IM - View 52
setting up JP1/IM - Manager (for Linux) 40
setting up JP1/IM - Manager (for Windows) 31
setting up JP1/IM - View (Windows only) 35
setting up monitoring targets 47
setting up prerequisite product (for Linux) 38
setting up prerequisite product (for Windows) 28
severe events filter 103
severity changing function 103
severity level 57
starting JP1/IM - Manager (for Linux) 44
starting JP1/IM - Manager (for Windows) 35
symbol conventions 9
system errors, detecting and investigating 76

U

using automated action function to execute command whenever event is issued 78
using event conversion to monitor log files 61
using IM Configuration Management to define system hierarchy 50
using IM Configuration Management to set forwarding filter 58
using view filter to filter events to be displayed 69

V

verifying that command specified as automated action was executed 79
verifying that email notification function has been set up correctly (Windows only) 86
verifying that events from unmonitored hosts are not displayed 73
verifying that events that match view filter conditions are displayed 70
verifying that events were found 82
verifying that forwarding filter has been correctly set 60
verifying that records can be converted to events by log file trap 66
verifying that system has been correctly set up by IM Configuration Management 50
verifying that you can execute command 55
verifying that you can monitor extent of impact of events in map format and tree format 93
version number conventions 9
viewer 20
view filter 69
visual monitoring, procedure for configuring 88
visual monitoring, using to understand extent of impact of system error 88

 **Hitachi, Ltd.**

6-6, Marunouchi 1-chome, Chiyoda-ku, Tokyo, 100-8280 Japan
