

Job Management Partner 1 Version 10

**Job Management Partner 1/Integrated
Management - Manager Quick Reference**

3021-3-304-20(E)

Notices

■ Relevant program products

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

Job Management Partner 1/Integrated Management - View (for Windows)

P-2W2C-6HAL Job Management Partner 1/Integrated Management - View version 10-50

The above product includes the following:

P-CC242C-6HAL Job Management Partner 1/Integrated Management - View version 10-50 (for Windows Server 2003 and Windows XP Professional)

P-CC2A2C-6HAL Job Management Partner 1/Integrated Management - View version 10-50 (for Windows 8.1, Windows 8, Windows Server 2012, Windows 7, Windows Server 2008, and Windows Vista)

Job Management Partner 1/Integrated Management - Manager (for Windows)

P-2W2C-8EAL Job Management Partner 1/Integrated Management - Manager version 10-50

The above product includes the following:

P-CC242C-8EAL Job Management Partner 1/Integrated Management - Manager version 10-50 (for Windows Server 2003)

P-CC2A2C-8EAL Job Management Partner 1/Integrated Management - Manager version 10-50 (for Windows Server 2012 and Windows Server 2008)

Job Management Partner 1/Integrated Management - Manager (for Solaris)

P-9D2C-8EAL Job Management Partner 1/Integrated Management - Manager version 10-50

Job Management Partner 1/Integrated Management - Manager (for AIX)

P-1M2C-8EAL Job Management Partner 1/Integrated Management - Manager version 10-50

Job Management Partner 1/Integrated Management - Manager (for Linux 6.1 (x86) or later, Linux 6.1 (x64) or later, Linux 5.1 (x86) or later, and Linux 5.1 (AMD/Intel 64) or later)

P-812C-8EAL Job Management Partner 1/Integrated Management - Manager version 10-50

■ Trademarks

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 is a trademark of Advanced Micro Devices, Inc.

Itanium is a trademark of Intel Corporation in the United States and other countries.

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 registered trademarks or trademarks of EMC Corporation in the United States and other countries. TELstaff is a registered trademark of Hitachi Solutions.

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.

Windows Vista 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.

The following program product contains some parts whose copyrights are reserved by Oracle Corporation, its subsidiaries, or affiliates: P-9D2C-8EAL.

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

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

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

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

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

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

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

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

This product includes software developed by Andy Clark.

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

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

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



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

HITACHI
Inspire the Next

©Hitachi, Ltd.



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

■ Restrictions

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

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

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

■ Issued

Dec. 2014: 3021-3-304-20(E)

■ Copyright

All Rights Reserved. Copyright (C) 2012, 2014, Hitachi, Ltd.

Summary of amendments

The following table lists changes in this manual (3021-3-304-20(E)) and product changes related to this manual.

Changes	Location
Procedures for installing and setting up JP1/IM and JP1/Base data were added.	1
The description was narrowed down to the procedure for customizing event transfer settings for IM Configuration Management.	2.3
A procedure for monitoring application log file records by using JP1/IM was added.	2.4
A procedure for monitoring Windows event logs by using JP1/IM was added.	2.5
The procedure for changing the severity level of events was changed to use the GUI in place of the definition file.	3.2 , 3.2.1
A procedure for setting up the email notification function to send emails was added.	Appendix A , A.1 , A.2 , A.3
The description of visual monitoring of events to ascertain the extent of impact of a system error was moved from Chapter 1 of this manual.	Appendix B
The description of system monitoring on a business group basis was moved from Chapter 1 of the previous version of this manual.	Appendix C

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

In this version (3021-3-304-20(E)), the table of contents was changed from the previous version (3021-3-304-10(E)). The following shows the correspondence between both versions.

Old (3021-3-304-10(E))	New (3021-3-304-20(E))
--	<i>1. Installing and Setting Up JP1/IM</i>
<i>1. Setting Up a System</i>	<i>2. Setting Up a System</i>
<i>1.4 Centrally monitoring events that are issued in a system</i>	<i>2.3 Customizing events to be monitored</i>
--	<i>2.4 Using event conversion to monitor log files</i>
--	<i>2.5 Using event conversion to monitor Windows event logs</i>
<i>2. Monitoring a System</i>	<i>3. Monitoring a System</i>
<i>3. Detecting Errors</i>	<i>4. Detecting System Errors</i>
<i>4. Troubleshooting Errors</i>	<i>5. Troubleshooting System Errors</i>
--	<i>A. Settings for Using the Email Notification Function (Windows only)</i>
<i>1.5 Visually monitoring events that are issued in a system</i>	<i>B. Visual Monitoring to Ascertain the Extent of Impact of a System Error</i>
<i>1.2 Monitoring business systems on a group basis</i>	<i>C. Monitoring Systems for Each Business Group</i>
--	<i>D. Port Numbers</i>
--	<i>E. List of Services (Windows only)</i>
--	<i>F. Advanced Use</i>
--	<i>G. Reference Material for This Manual</i>

Old (3021-3-304-10(E))	New (3021-3-304-20(E))
--	<i>H. Glossary</i>

Legend:

--: Not applicable to the previous version.

Preface

This manual describes the main way of setting up and operating Job Management Partner 1/Integrated Management - Manager and Job Management Partner 1/Integrated Management - View, based on the system operation cycle. Users who want to learn about Job Management Partner 1/Integrated Management - Manager functions based on the intended use of each function should read this manual first. In this manual, Job Management Partner 1 is abbreviated to *JP1*, and JP1/Integrated Management - Manager and JP1/Integrated Management - View might be generically referred to as *JP1/IM*.

■ What JP1/IM can do

With the growing size and complexity of the systems underpinning an enterprise's business operations, management of system operation is a vital issue. JP1/IM optimizes system operations management by offering integrated management tailored to objectives and integration of operational tasks.

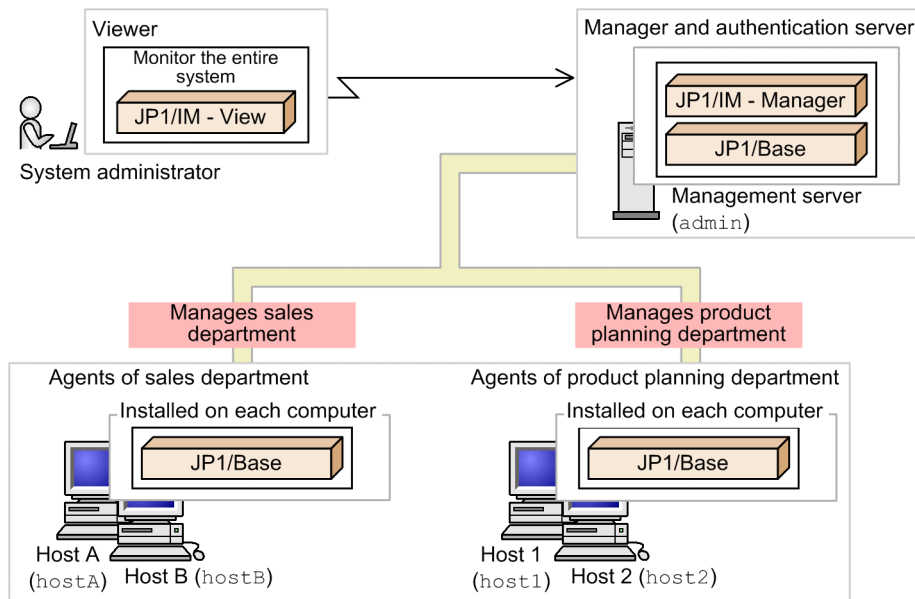
JP1/IM has the following features:

- 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.

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



■ How to read this manual

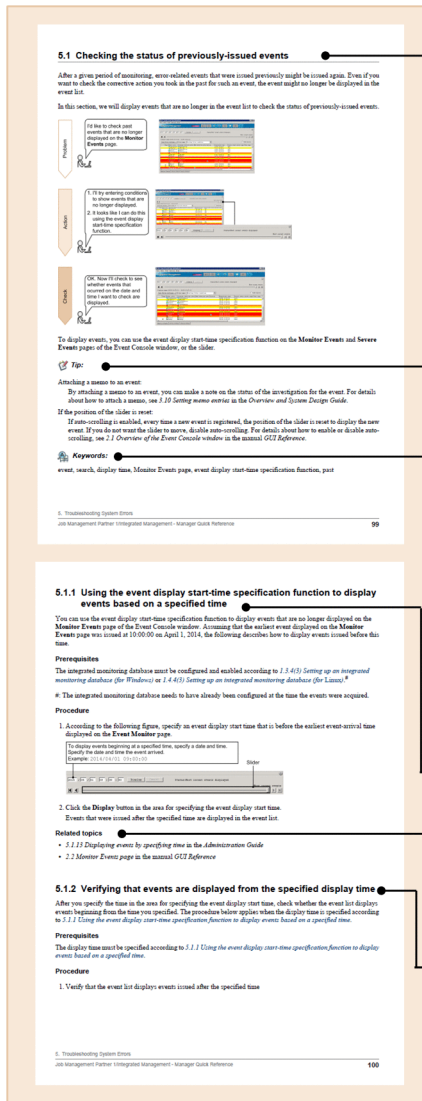
The following environments are required to perform the operations in each window.

Operations on the manager:

Environment in which Windows Server 2008 or Linux 6.1 is used

Operations on the viewer:

Environment in which Windows 7 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.



Tip:

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



Keywords:

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

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:

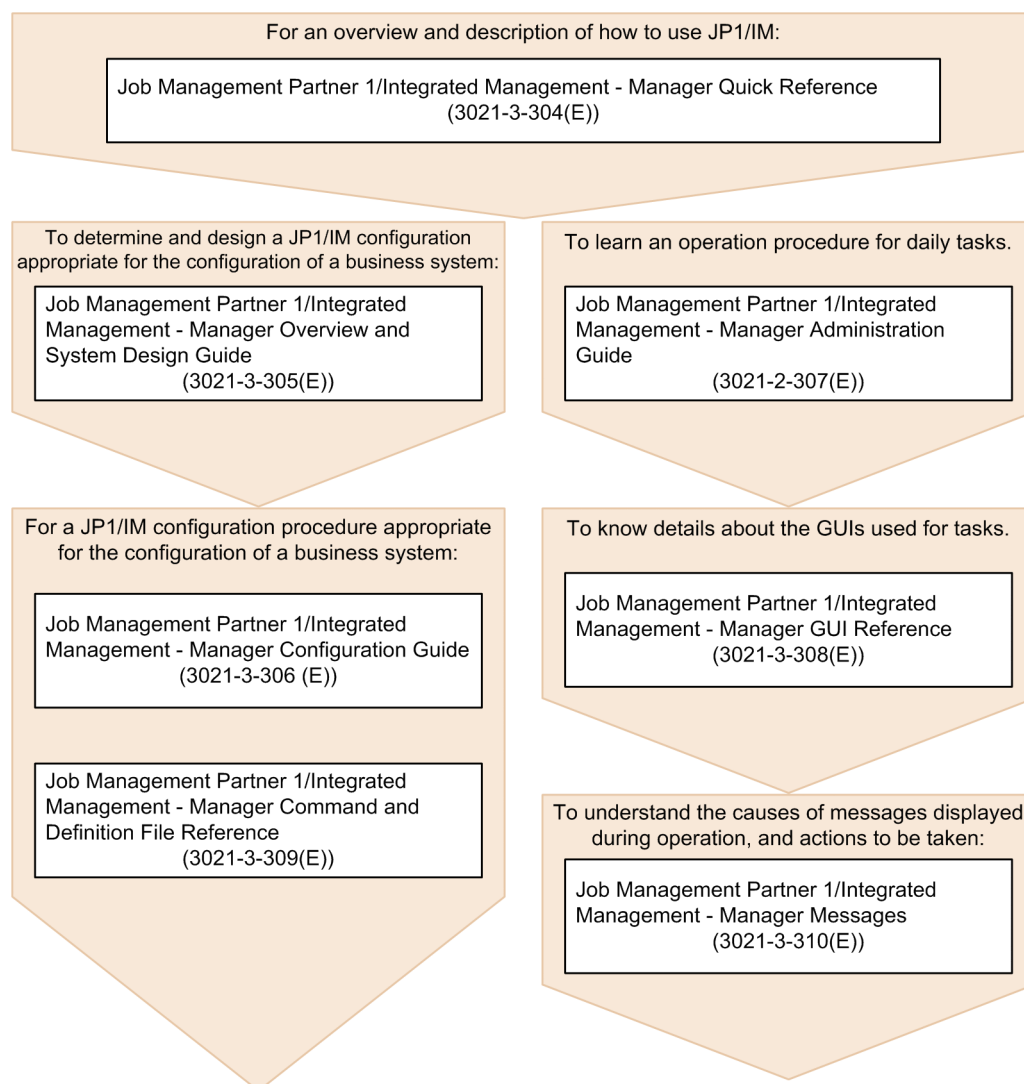
Provides references to sections in related manuals.

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

The windows examples in this manual are accurate as of August 2014. Some windows might differ from the windows of your products due to changes in product specifications.

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:



■ 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 = file-name)</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.

Text formatting	Convention
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 7

1 Installing and Setting Up JP1/IM 16

- 1.1 Preparation before installation 17
- 1.2 Configuration procedures 18
 - 1.2.1 Overview of a basic configuration system 18
 - 1.2.2 Installation and setup procedures 19
 - 1.2.3 Meaning of "Administrator permissions" in descriptions of installation and setup 20
 - 1.2.4 Replacement characters such as "View-path" and "Manager-path" used in procedures 20
- 1.3 Installation and setup (for Windows) 21
 - 1.3.1 Installing the prerequisite product (for Windows) 21
 - 1.3.2 Setting up the prerequisite product (for Windows) 22
 - 1.3.3 Installing JP1/IM (for Windows) 23
 - 1.3.4 Setting up JP1/IM - Manager (for Windows) 25
 - 1.3.5 Setting up JP1/IM - View (Windows only) 27
 - 1.3.6 Starting JP1/IM - Manager (for Windows) 28
- 1.4 Installation and setup (for Linux) 29
 - 1.4.1 Installing the prerequisite product (for Linux) 29
 - 1.4.2 Setting up the prerequisite product (for Linux) 30
 - 1.4.3 Installing JP1/IM (for Linux) 31
 - 1.4.4 Setting up JP1/IM - Manager (for Linux) 32
 - 1.4.5 Starting JP1/IM - Manager (for Linux) 35
- 1.5 Logging in to JP1/IM - Manager from JP1/IM - View 36

2 Setting Up a System 37

- 2.1 Setting up a basic system 38
 - 2.1.1 Procedure for setting up a system by using IM Configuration Management 39
 - 2.1.2 Verifying that the system has been correctly set up by IM Configuration Management 41
- 2.2 Settings for executing commands on monitored hosts from JP1/IM - View 43
 - 2.2.1 Using the user mapping feature to map a JP1 user account to an OS user account 44
 - 2.2.2 Verifying that you can execute a command 46
- 2.3 Customizing events to be monitored 48
 - 2.3.1 Using IM Configuration Management to set a forwarding filter in IM Configuration Management 49
 - 2.3.2 Verifying that the forwarding filter has been correctly set 50
- 2.4 Using event conversion to monitor log files 52

2.4.1	Procedure for starting log file monitoring in JP1/IM	52
2.4.2	Verifying that records can be converted to events by the log file trap	56
2.5	Using event conversion to monitor Windows event logs	58
2.5.1	Monitoring Windows event logs in JP1/IM	58
2.5.2	Verifying that Windows event log data can be converted to events	61
3	Monitoring a System	62
3.1	Filtering the events that are displayed	63
3.1.1	Using the view filter to specify conditions of events to be displayed	63
3.1.2	Verifying that the events that match the view filter conditions are displayed	64
3.2	Changing the severity level of events to better match your operations	65
3.2.1	Using the severity changing function to change the severity level of events	66
3.2.2	Verifying that the severity level was changed	68
3.3	Removing hosts undergoing maintenance from being monitored	70
3.3.1	Using common exclusion conditions in a filter to temporarily stop hosts from being monitored	71
3.3.2	Verifying that events from unmonitored hosts are not displayed	72
3.4	Specifying not to display unnecessary events in the list	74
3.4.1	Using additional common exclusion conditions for a filter to prevent display of unnecessary events	75
3.4.2	Checking whether unnecessary events are displayed	76
3.5	Identifying important events among a large number of issued events	79
3.5.1	Consolidating a large number of events by using the repeated event monitoring suppression function	80
3.5.2	Verifying that a large number of events are consolidated	82
4	Detecting System Errors	84
4.1	Handling multiple events as a single event	85
4.1.1	Settings of the correlation event generation definition file to be created	86
4.1.2	Associating events with correlation events	87
4.1.3	Verifying that the correlation event is generated	88
4.2	Automatically executing a command when a specific event is generated	90
4.2.1	Using the automated action function to execute a command	91
4.2.2	Verifying that a command specified as an automated action was executed	92
4.3	Preventing an action that was already executed once from being executed again during a set period of time	94
4.3.1	Using automated action suppression to prevent an action from being executed	95
4.3.2	Verifying that the same action is not executed repeatedly	96
5	Troubleshooting System Errors	98
5.1	Checking the status of previously-issued events	99
5.1.1	Using the event display start-time specification function to display events based on a specified time	100
5.1.2	Verifying that events are displayed from the specified display time	100
5.2	Searching for events	101

5.2.1	Using the search events function to search for events that match a specified condition	101
5.2.2	Verifying that events were found	102
5.3	Registering corrective action to be used as a guide for known errors	103
5.3.1	Settings in the event guide information file to be created	104
5.3.2	Using the event guide function to register the corrective action to be taken	104
5.3.3	Verifying that the corrective action is registered	105

Appendixes 106

A	Settings for Using the Email Notification Function (Windows only)	107
A.1	Setting up the email notification function (Windows only)	107
A.2	Verifying that the email notification function has been set up correctly (Windows only)	109
A.3	Example definition for an automated action when using the email notification function	110
B	Visual Monitoring to Ascertain the Extent of Impact of a System Error	111
B.1	Procedure for configuring visual monitoring	111
B.2	Verifying that you can monitor the extent of impact of events in map format and tree format	116
C	Monitoring Systems on a Business Group Basis	119
C.1	Procedure for creating business groups	120
C.2	Verifying that the business group settings are specified correctly	125
D	Port Numbers	126
D.1	JP1/IM port numbers	126
D.2	JP1/Base port numbers	126
D.3	Direction of communication through a firewall	127
E	List of Services (Windows only)	129
F	Advanced Use	130
G	Reference Material for this Manual	132
H	Glossary	136

1

Installing and Setting Up JP1/IM

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

1.1 Preparation before installation

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

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 10-50 or later.

- JP1/Base
- JP1/Integrated Management - Manager
- JP1/Integrated Management - View

Configuring the OS environment necessary for installation

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

- Apply the service packs and patches required by JP1/IM to the OS.
- (Linux only) Adjust kernel parameters according to the configuration of JP1/IM.

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 the direction of communication through a firewall, see [D.3 Direction of communication through a firewall](#).

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

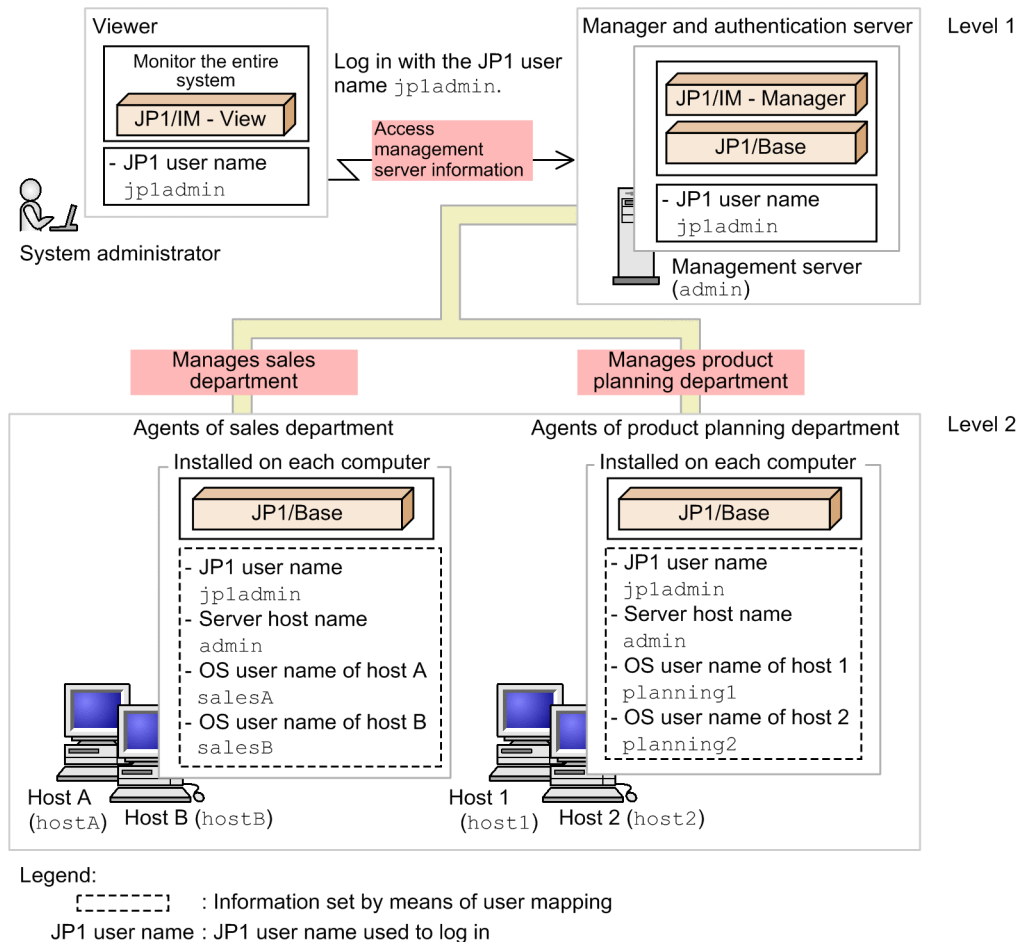
- *1.5 JP1/IM - Manager system configuration* in the *Overview and System Design Guide*
- *1.2.2 Configuring the system environment* in the *Configuration Guide*
- *2.2.2 Configuring the system environment* in the *Configuration Guide*.
- Description of the communication protocols of JP1/Base in the *JP1/Base User's Guide*

1.2 Configuration procedures

This section describes a basic configuration system to let you start monitoring, and the procedures for installing and setting up the required products. In this manual, a system provided by JP1/IM - Manager is called a *system*.

1.2.1 Overview of a basic configuration system

A system consists of *managers* for administering the system, *agents* that are monitored, and *viewers* for monitoring and operating the system. In this manual, a system consisting of the two levels shown in the figure below is defined as a basic configuration system. Each host in the figure has one NIC and only one IP address assigned.



In this example, the system administrator uses the JP1 user name `jpladmin` to log in to a manager called a *management server* (admin), where he or she can use a viewer to monitor the entire system. The management server admin manages events issued by agents of the sales department (hostA and hostB) and agents of the product planning department (host1 and host2).

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*.

To execute commands on monitored hosts, a JP1 user account must be mapped to an OS user account by user mapping. For details about the user mapping procedure, see [2.2 Settings for executing commands on monitored hosts from JP1/IM - View](#).

1.2.2 Installation and setup procedures

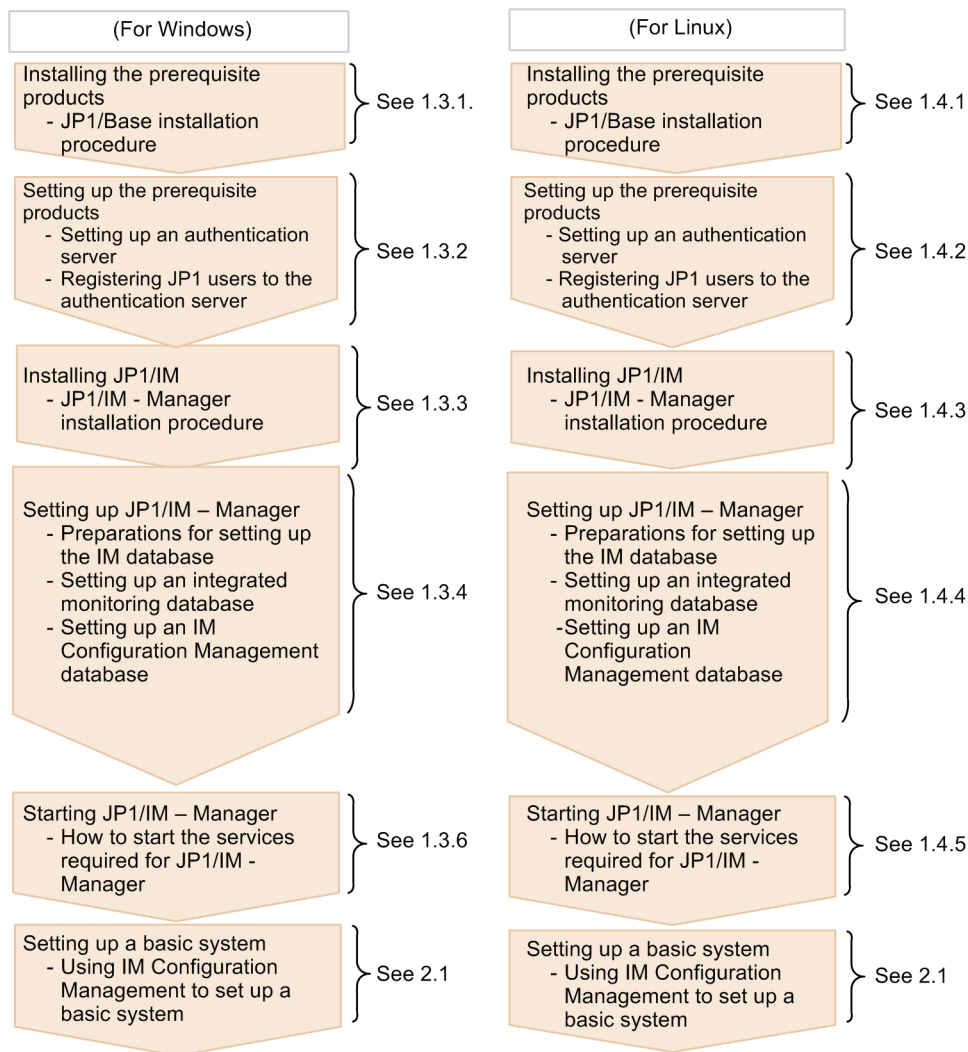
This subsection describes the installation and setup procedures required to configure a basic configuration system.

The procedures for a manager, agent, and viewer are described.

For a manager:

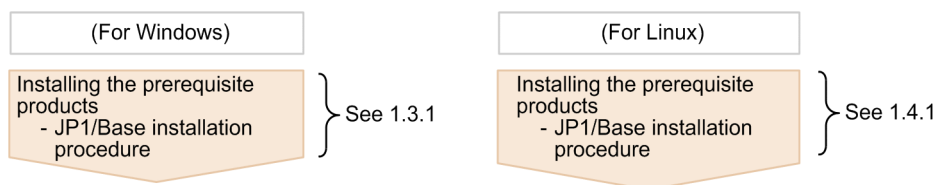
Install the prerequisite products, JP1/Base and JP1/IM - Manager. Set user authentication for JP1/Base to log in to JP1/IM - Manager, and then set up the IM database to use the JP1/IM - Manager functions described in this manual.

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



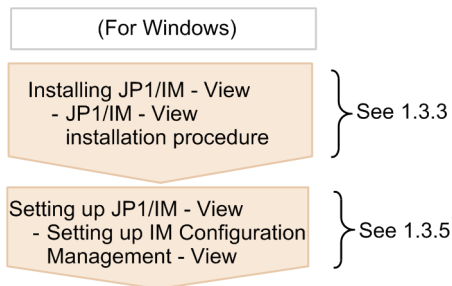
For an agent:

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



For a viewer:

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.



1.2.3 Meaning of "Administrator permissions" in descriptions of installation and setup

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.

1.2.4 Replacement characters such as "View-path" and "Manager-path" used in procedures

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](#).

1.3 Installation and setup (for Windows)

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

1.3.1 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) JP1/Base installation procedure (for Windows)

The following describes how to install JP1/Base in Windows.

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 [2.2.1 Using the user mapping feature to map a JP1 user account to an OS user account](#).

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

1.3.2 Setting up the prerequisite product (for Windows)

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

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

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

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 **Programs, JP1_Base**, and then **Preferences**. The JP1/Base Environment Settings dialog box appears.
2. In the **Order of authentication server** area, click the **Add** button to open the Authentication Server dialog box.
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 the authentication server (for Windows)

The following describes how to register a JP1 user into the authentication server when JP1/Base has been installed in Windows.

Prerequisites

The primary authentication server must be specified.

Procedure

1. From the Windows **Start** menu, select **Programs, JP1_Base**, and then **Preferences**. 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)

If automatic setup processing was performed during installation of JP1/Base, `jpladmin` has already been set for both the JP1 user name and password.

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 (`jpladmin`) 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 if you want to register a JP1 user other than the system administrator, you need to specify the JP1 permission level. For details about the procedure to do this, see [C.1\(2\) Specifying the JP1 resource group names and JP1 permission levels for JP1 users of business groups](#).

1.3.3 Installing JP1/IM (for Windows)

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

(1) JP1/IM - Manager installation procedure (for Windows)

The following describes how to install JP1/IM - Manager in Windows.

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

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 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.

[#]: The default installation folder is *system-drive*: \Program Files (x86)\Hitachi.

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) JP1/IM - View installation procedure (Windows only)

The following describes how to install JP1/IM - View in Windows.

Prerequisites

The following conditions must be satisfied:

- JP1/IM - View supports the OS of the host 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
- 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.

#: The default installation folder is *system-drive*: \Program Files (x86)\HITACHI.

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.

- Program folder

Specify the registration location in the **Start** menu. Note, however, that you cannot specify a program folder when you install JP1/IM - View for Windows 8.1, Windows 8, Windows Server 2012, Windows 7, Windows Server 2008, or Windows Vista.

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

1.3.4 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 [1.3.4\(2\) 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

- [12.1.3 Estimating IM database capacity requirements](#) in the *Overview and System Design Guide*.

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

The following describes preparations required for setting up the IM database in 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

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. 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 an IM database 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.
- 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
```

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/IM-Manager service.

Related topics

- *1.4.2 Setting up the integrated monitoring database 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:

- JP1/IM - View has stopped.
- Sufficient disk space for creating an IM Configuration Management database is allocated.
- 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 [1.3.4\(3\) 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/IM-Manager service.
2. Execute the following `jcfdbsetup` command to create an IM Configuration Management database:
`"manager-path\bin\imdb\jcfdbsetup" -s -q`
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 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*

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

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

(1) Setting up IM Configuration Management - View (Windows only)

The following describes how to register a shortcut used to start IM Configuration Management - View.

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

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

1.3.6 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) How to start the services required for JP1/IM - Manager (for Windows)

Use the following startup procedure if JP1/IM - Manager has been installed in Windows. 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.

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

1.4 Installation and setup (for Linux)

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

1.4.1 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) JP1/Base installation procedure (for Linux)

The following describes how to install JP1/Base in Linux.

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
```

1.4.2 Setting up the prerequisite product (for Linux)

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

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

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

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]
```

Note that the local host name is automatically set as the authentication server name during installation of JP1/Base.

Related topics

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

(2) Registering JP1 users to the authentication server (for Linux)

The following describes how to register a JP1 user into the authentication server when JP1/Base has been installed in Linux.

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/jplbase/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 `jpladmin` 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 (`jpladmin`) 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, set the JP1 permission level. For details about the procedure, see [C.1\(2\) Specifying the JP1 resource group names and JP1 permission levels for JP1 users of business groups](#).

1.4.3 Installing JP1/IM (for Linux)

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

(1) JP1/IM - Manager installation procedure (for Linux)

The following describes how to install JP1/IM - Manager in Linux.

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/jplcons
cp -p jco_start.model jco_start
```

1.4.4 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 [1.4.4\(2\) 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 IMBDDIR=/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 IMBDDIR, 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

- [12.1.3 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 an IM database](#) 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/jplcons/bin/jcodbsetup -f setup-information-file-name -q
```

The IM database service is created at this time.

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

```
/opt/jplcons/bin/jcoimdef -db ON
```

3. Restart the JP1/IM-Manager service.

Related topics

- *2.4.2 Setting up the integrated monitoring database 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 *1.4.4(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/IM-Manager service.

2. Execute the following `jcfdbsetup` command to create an IM Configuration Management database:

```
/opt/jplimm/bin/imdb/jcfdbsetup -s -q
```

3. Execute the following `jcoimdef` command to enable the IM Configuration Management service (`jcfmain`):

```
/opt/jplcons/bin/jcoimdef -cf ON
```

4. Start JP1/IM - Manager.

Related topics

- *2.4.3 Setting up the IM Configuration Management database* 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*

1.4.5 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) How to start the services required for JP1/IM - Manager (for Linux)

The following startup procedure applies when JP1/IM - Manager has been installed in Linux. Execute the JP1/Base automated startup script, and then execute the JP1/IM - Manager automated startup script. 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.

Procedure

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

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

To start system monitoring, you must log in to JP1/IM - Manager from JP1/IM - View. This section describes how to log in to JP1/IM - Manager from JP1/IM - View and display the Event Console window.

Prerequisites

The following conditions must be satisfied:

- JP1/IM - View is installed 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 **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**.
Enter the JP1 user name and password registered on the manager. For **Host to connect**, enter the host name of the manager.
If automatic setup processing was performed during installation of JP1/Base, `jp1admin` has already been set for both the JP1 user name and password.
3. Select the **Central Console** check box.
4. Click the **OK** button.

2

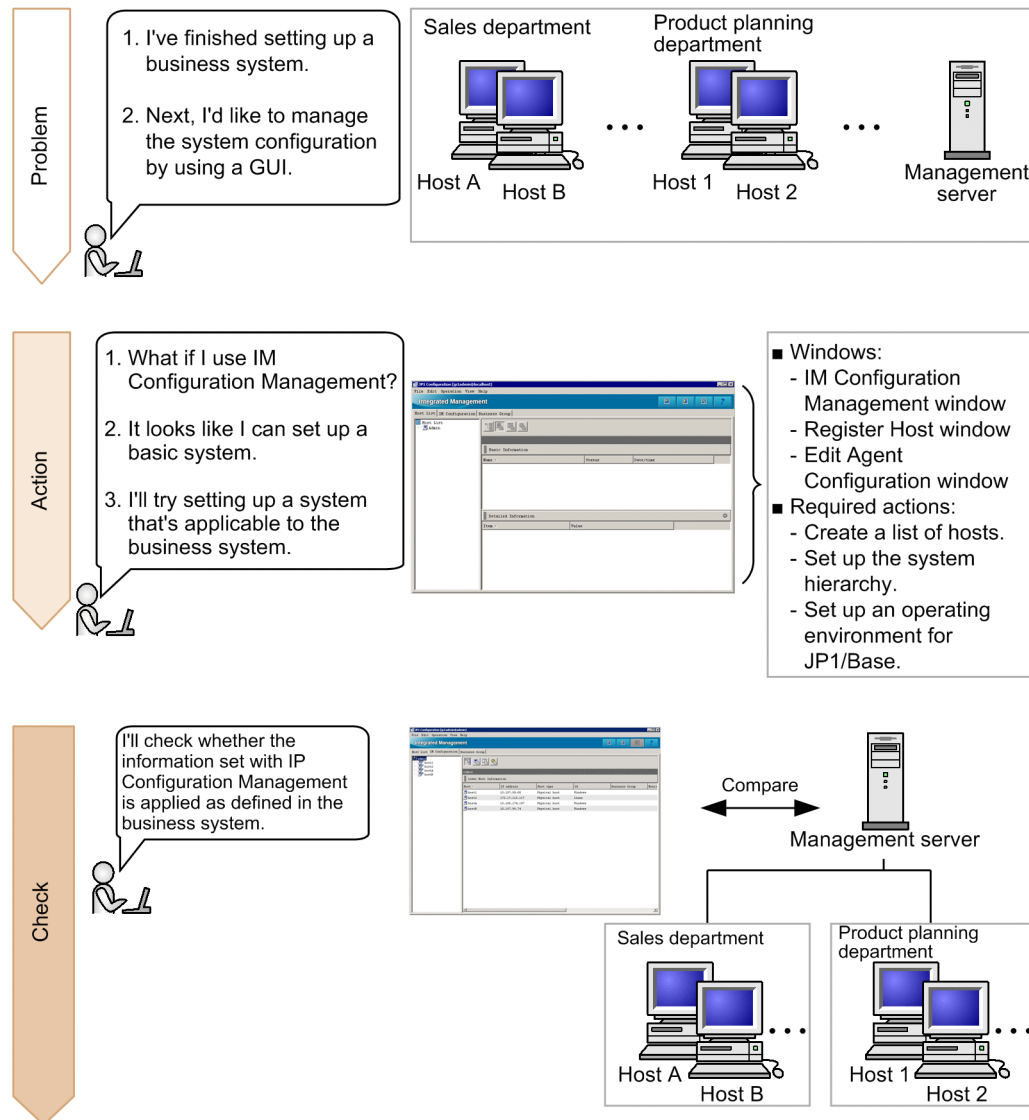
Setting Up a System

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

2.1 Setting up a basic system

To use JP1/IM to centrally manage events issued in a business system, you need to define a system hierarchy (IM configuration) that matches the configuration of the business system. You can use IM Configuration Management to define a system hierarchy.

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



Keywords:

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

2.1.1 Procedure for setting up a system by using IM Configuration Management

To set up a system, you use *IM Configuration Management*, which allows you to centrally manage the hierarchical configuration of hosts in the system. The following describes how to define the basic configuration system shown in [1.2.1 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.

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.

(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. The following describes how to register the hosts into IM Configuration Management.

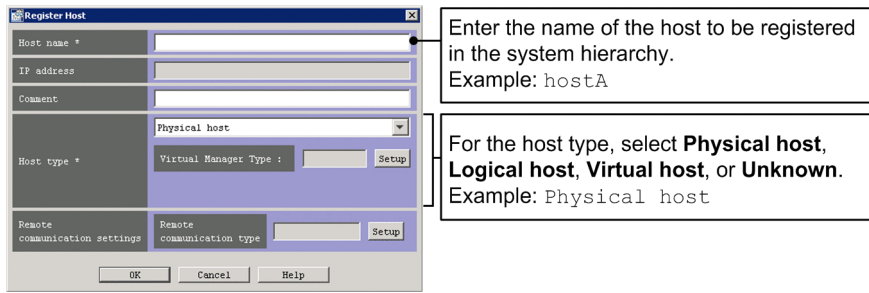
Prerequisites

The following conditions must be satisfied:

- The IM Configuration Management database has been configured and enabled according to [1.3.4\(4\) Setting up an IM Configuration Management database \(for Windows\)](#) or [1.4.4\(4\) 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 [1.2.1 Overview of a basic configuration system](#).
Because `admin` is the local host, it has already been registered. Register hosts A, B, 1, and 2 to IM Configuration Management according to the following figure.



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

Related topics

- *6. System Hierarchy Management Using IM Configuration Management in the Overview and System Design Guide*
- *1.5 Settings for using the functions of IM Configuration Management in the Configuration Guide*
- *1.20.3 Setting up and customizing IM Configuration Management - View in the Configuration Guide*
- *8. Managing the System Hierarchy using IM Configuration Management in the Administration Guide*
- *4. IM Configuration Management Window in the manual GUI Reference*

(2) Using IM Configuration Management to define the system hierarchy

To use JP1/IM to centrally manage events issued in a business system, you need to define the system hierarchy. The following describes how to define the basic configuration system shown in [1.2.1 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

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.

Host	IP address	Host type
host1	10.197.99.68	Physical host
host2	172.17.110.117	Physical host
hostA	10.196.174.197	Physical host

Host	IP address	Host type	OS
hostB	10.197.99.74	Physical host	Windows

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

Related topics

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

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

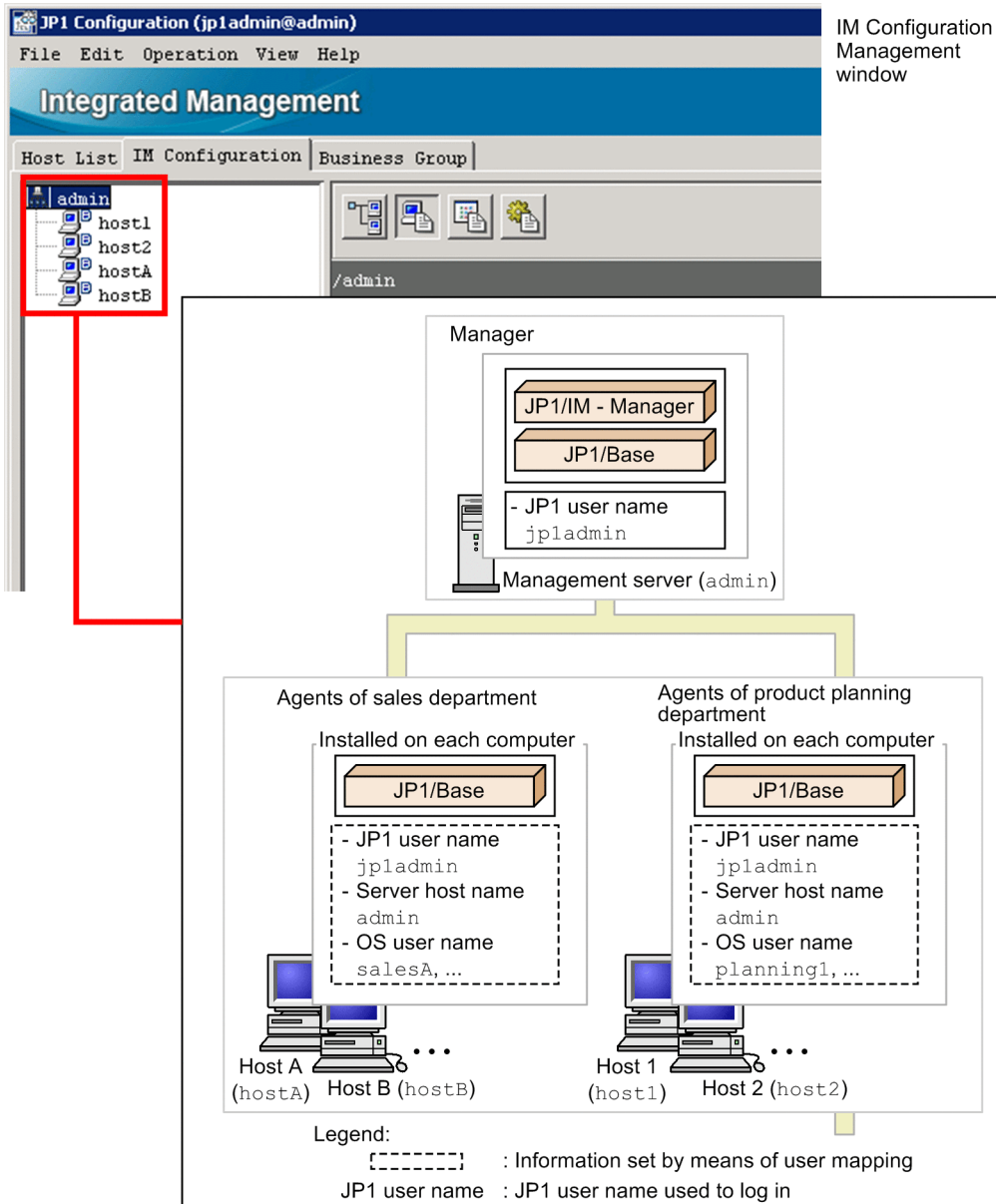
To use JP1/IM to centrally manage events issued in a business system, verify that the system has been set up correctly by IM Configuration Management. The following describes how to verify that the basic configuration system shown in *1.2.1 Overview of a basic configuration system* has been set up.

Prerequisites

The basic configuration system must be set up according to *2.1.1 Procedure for setting up a system by using IM Configuration Management*.

Procedure

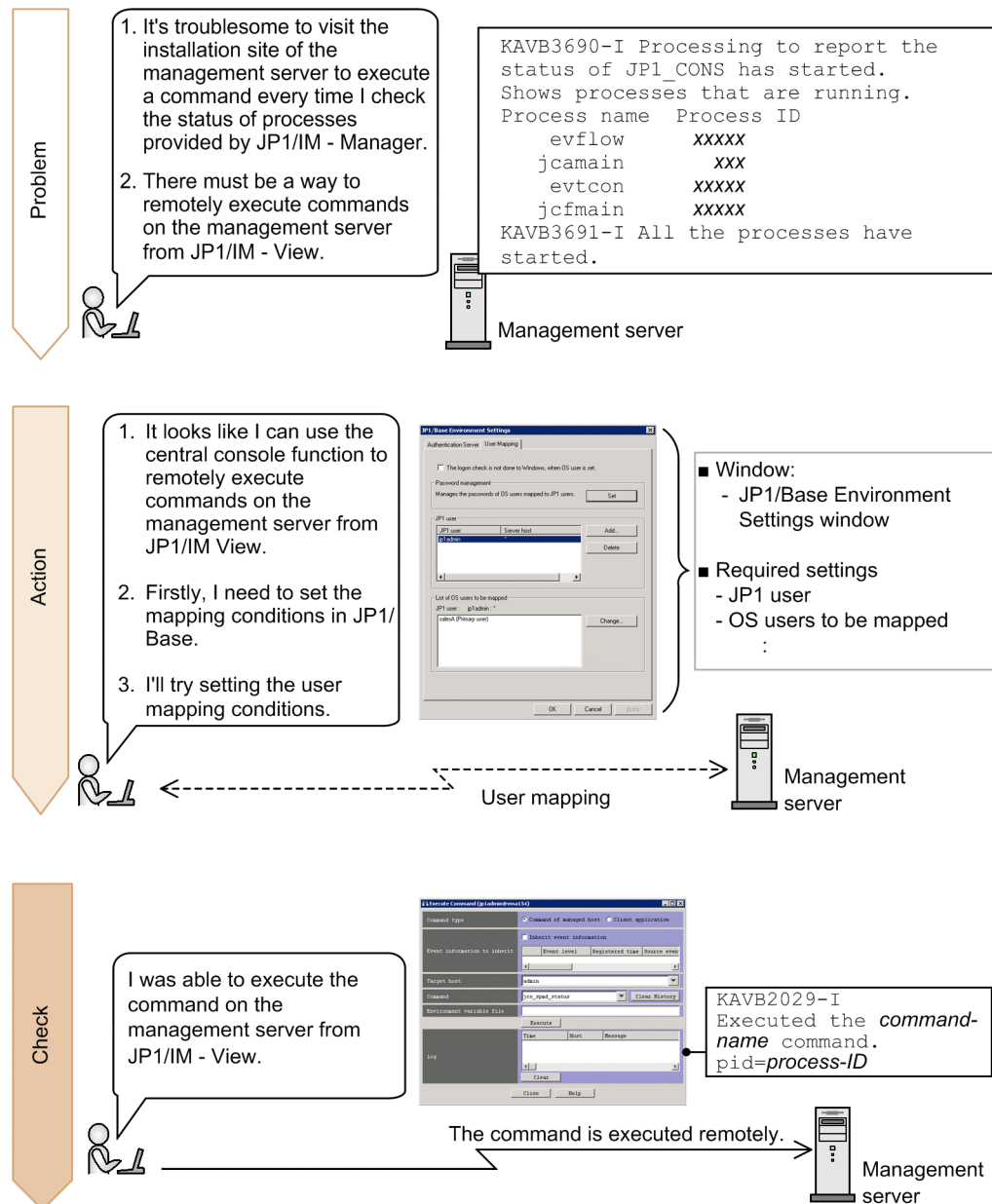
1. In the IM Configuration Management window, select the **IM Configuration** page.
2. Verify that the system hierarchy has been defined as shown in *1.2.1 Overview of a basic configuration system*.



2.2 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.



Note that you can execute commands on the client host (viewer host). This functionality is called *client application execution*, and the commands on the client host are called *client applications*. This functionality can be used without special settings.



Keywords:

user mapping, mapping, command, relationship

2.2.1 Using the user mapping feature to map a JP1 user account to an OS user account

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 [1.2.1 Overview of a basic configuration system](#). You can use the GUI or a command to configure user mapping.

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

The following describes how to use the JP1/Base GUI 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`.

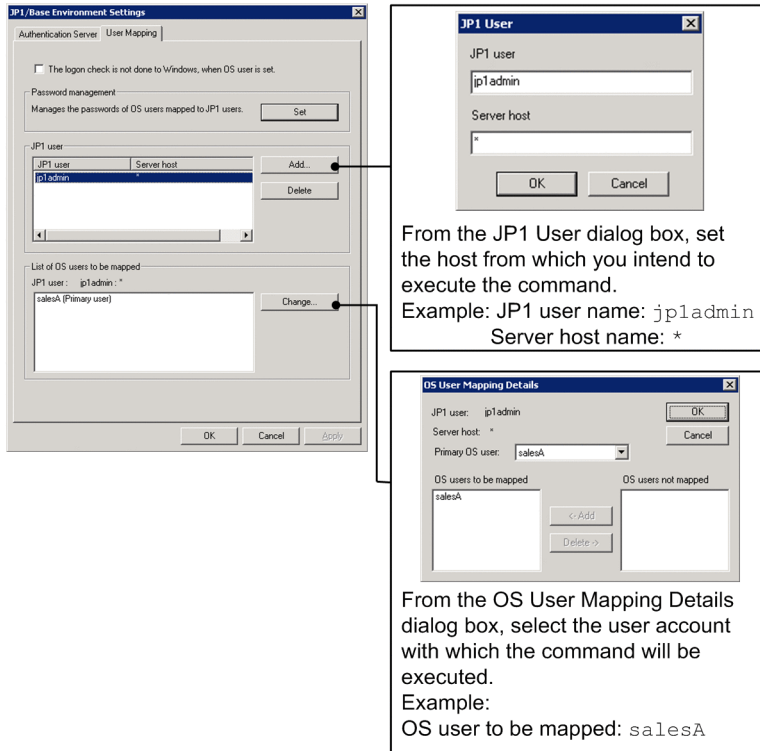
Prerequisites

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 [1.2.1 Overview of a basic configuration system](#).

Procedure

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



Related topics

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

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

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

Prerequisites

The following conditions must be satisfied:

- The OS user to be mapped to the JP1 user has the following user permissions (Windows only):
 - **Log on locally**
 - **Log on as a service**
- The JP1 user who will execute commands from JP1/IM - View is registered in the authentication server.
- The JP1 user who will execute commands from JP1/IM - View has either of the following JP1 permission levels:
 - `JP1_Console_Admin`
 - `JP1_Console_Operator`
- The system is set up according to [1.2.1 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*

2.2.2 Verifying that you can execute a command

The following describes how to check whether you can execute a command from the manager when OS user mapping is configured according to the procedure in section 2.2.1.

Prerequisites

The following conditions must be satisfied:

- OS user mapping is configured according to the procedure in *2.2.1 Using the user mapping feature to map a JP1 user account to an OS user account*.
- 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_spmd_status"" command."
2014/04/02 21:45:06,admin,"KAVB2029-I Executed the ""C:\Program Files
(x86)\Hitachi\JP1Cons\bin\jco_spmd_status"" command. pid=16592"
2014/04/02 21:45:06,admin,KAVB3690-I Processing to report the status of
JP1_CONS has started.
2014/04/02 21:45:06,admin,Shows processes that are running.
2014/04/02 21:45:06,admin,Process name Process ID
2014/04/02 21:45:06,admin, evflow 14256
2014/04/02 21:45:06,admin, jcamain 6292
2014/04/02 21:45:06,admin, evtcon 13308
2014/04/02 21:45:06,admin, jcfmain 13528
2014/04/02 21:45:06,admin,KAVB3691-I All the processes have started.
2014/04/02 21:45:06,admin,"KAVB2013-I Terminated the ""C:\Program Files
(x86)\Hitachi\JP1Cons\bin\jco_spmd_status""command. pid=16592 terminate
code=0 "
```

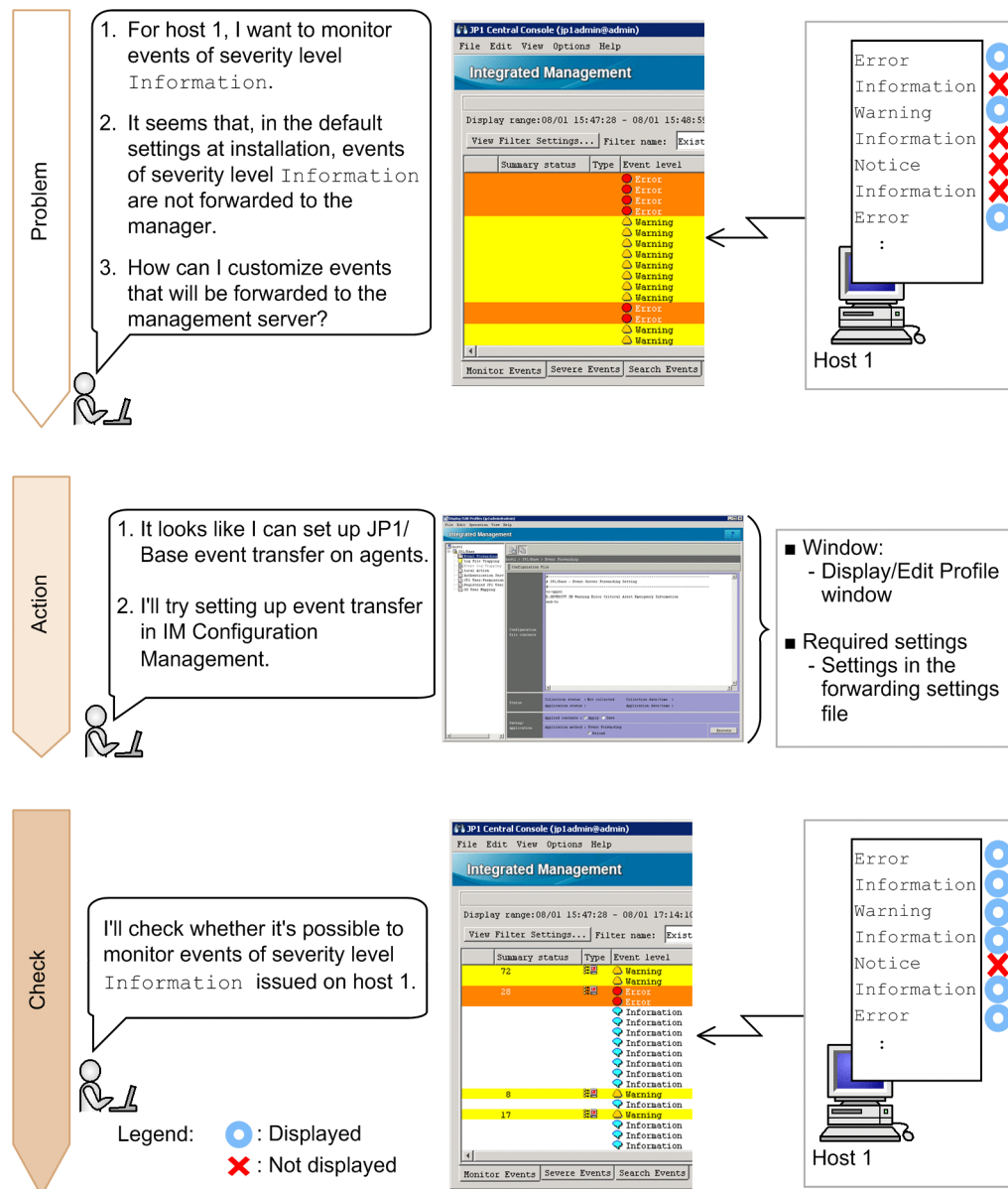
Related topics

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

2.3 Customizing events to be monitored

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

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



Keywords:

event, forwarding, monitoring target, forwarding filter

2.3.1 Using IM Configuration Management to set a forwarding filter in IM Configuration Management

To customize event forwarding settings, you need to use IM Configuration Management to set a *forwarding filter* for agents from which events will be forwarded.

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. This manual describes how to use IM Configuration Management to set a forwarding filter by editing the forwarding transfer settings file for agents.

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

The following provides details about the settings specified in the forwarding settings file that is created in [2.3.1\(2\) 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 that events of severity level Warning, Error, Fatal, Minor, Emergency, or Information are forwarded to the manager. This specification must be written between to-upper and end-to.

(2) 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 [1.2.1 Overview of a basic configuration system](#).

Prerequisites

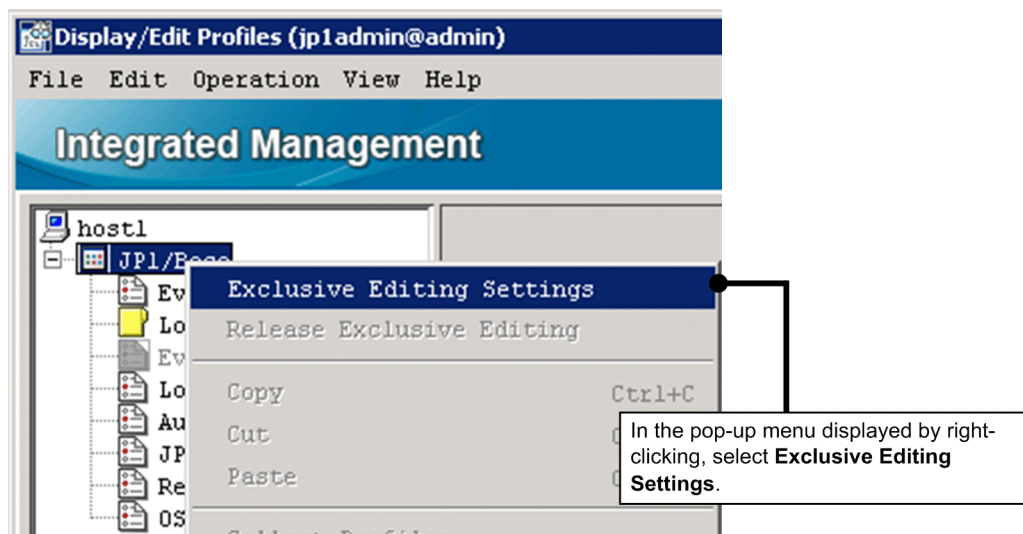
The following conditions must be satisfied:

- The basic configuration system is set up according to [2.1.1 Procedure for setting up a system by using IM Configuration Management](#).
- Host information has been collected.

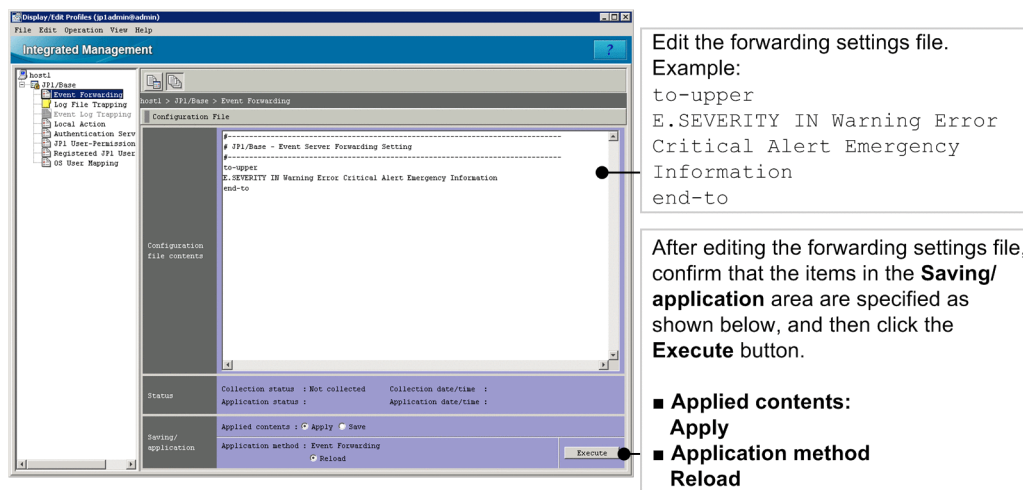
Procedure

1. From the Windows **Start** menu, select **All Programs, JP1_Integrated Management - View**, and then **Configuration Management**. The Login window appears.
2. Enter jpladmin for **User name**, jpladmin 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.



7. In the tree display area, select **Event Forwarding**, and then specify the event forwarding according to the following figure.



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

Related topics

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

2.3.2 Verifying that the forwarding filter has been correctly set

This subsection describes how to verify that the forwarding filter has been correctly set on the manager. For details about setting the forwarding filter, see [2.3.1\(2\) 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 [2.2.1 Using the user mapping feature to map a JPL user account to an OS user account](#).

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 [2.2.2 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: "<i>Base-path</i>\bin\jevsend" -e SEVERITY=Information -m <i>information-event</i>• In Linux: /opt/jplbase/bin/jevsend -e SEVERITY=Information -m <i>information-event</i>

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.

This manual describes an example of setting the log file trap for log files on host 1 in the basic configuration system shown in *1.2.1 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 *JPI/Base User's Guide*, and check the log file format.

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

The following provides details about the settings specified in the log file trap action-definition file. The file is created in *2.4.1(2) Using IM Configuration Management to create a log file trap action-definition file on a host 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 "Error"	Specifies the event conversion condition for records written in the log file, and the severity level and event ID of an event to be issued. In this manual, records containing character string <code>Error</code> are converted to events.

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 a log file trap action-definition file on a host to be monitored

The following describes how to use IM Configuration Management to create a log file trap action-definition file in order to set the log file trap. Perform this procedure on the host to be monitored.

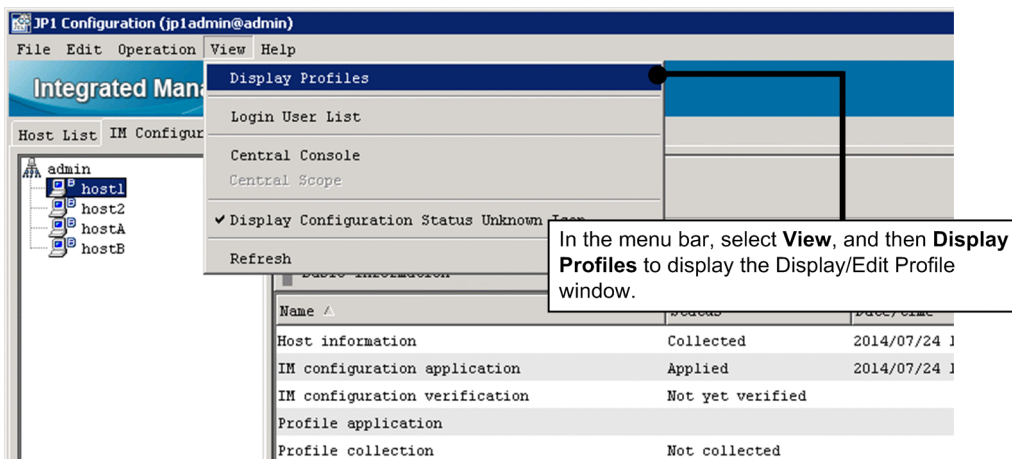
Prerequisites

The following conditions must be satisfied:

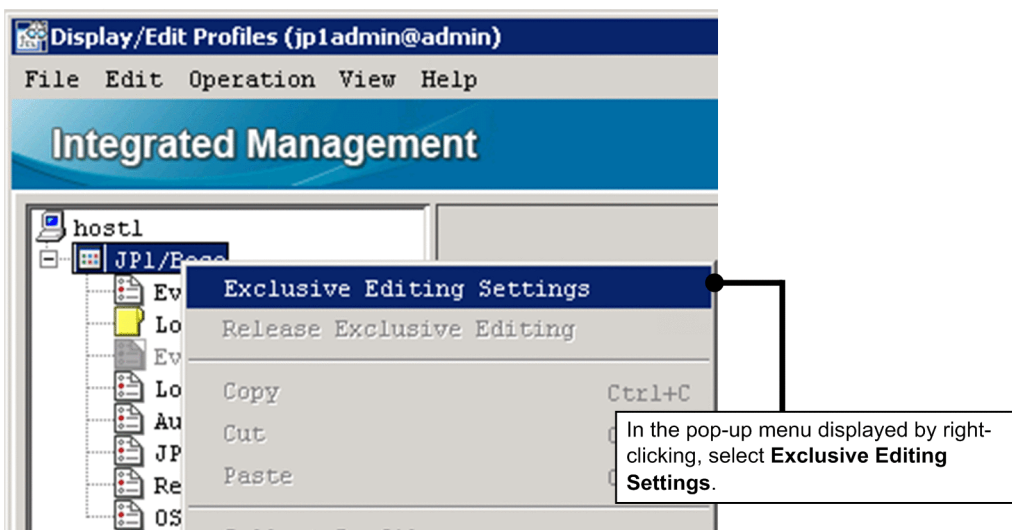
- The basic configuration system is set up according to [2.1.1 Procedure for setting up a system by using IM Configuration Management](#).
- Host information has been collected.

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 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.

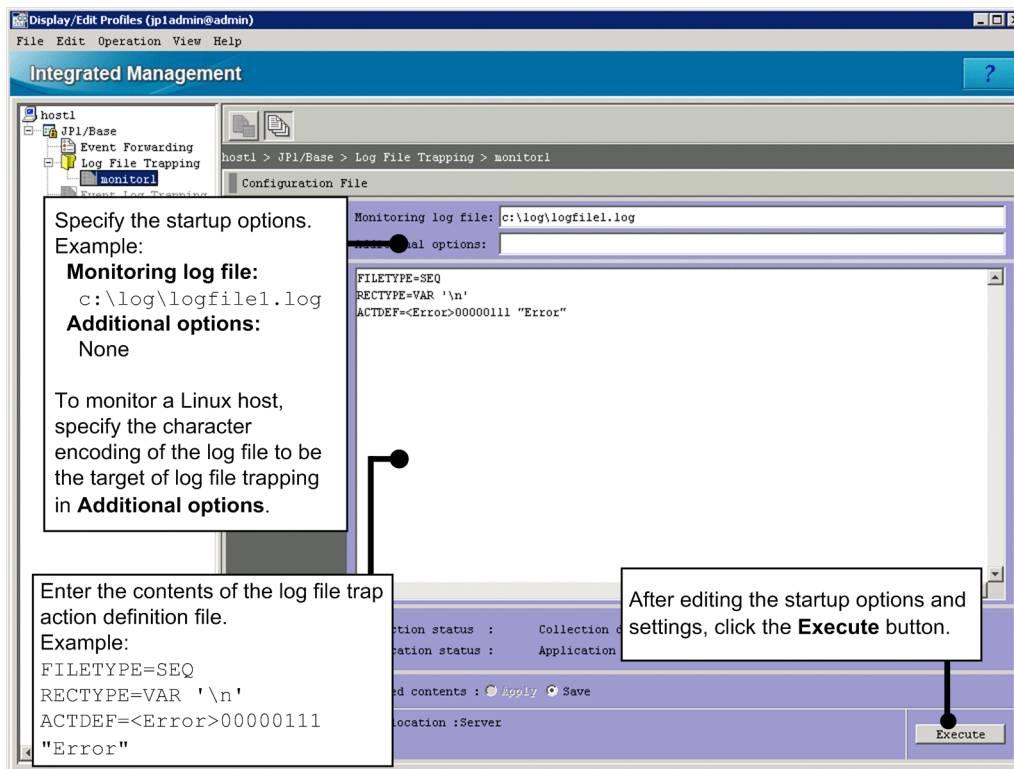
Enter a unique log file trap name in the text box that appears. Note that the log file trap is managed by the log file trap name entered here.

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. Edit the log file trap action-definition file as shown in the following figure.



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

Related topics

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

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

The following describes how to use IM Configuration Management to start the log file trap in order to monitor application log file records with JPI/IM. Perform this procedure on the host to be monitored.

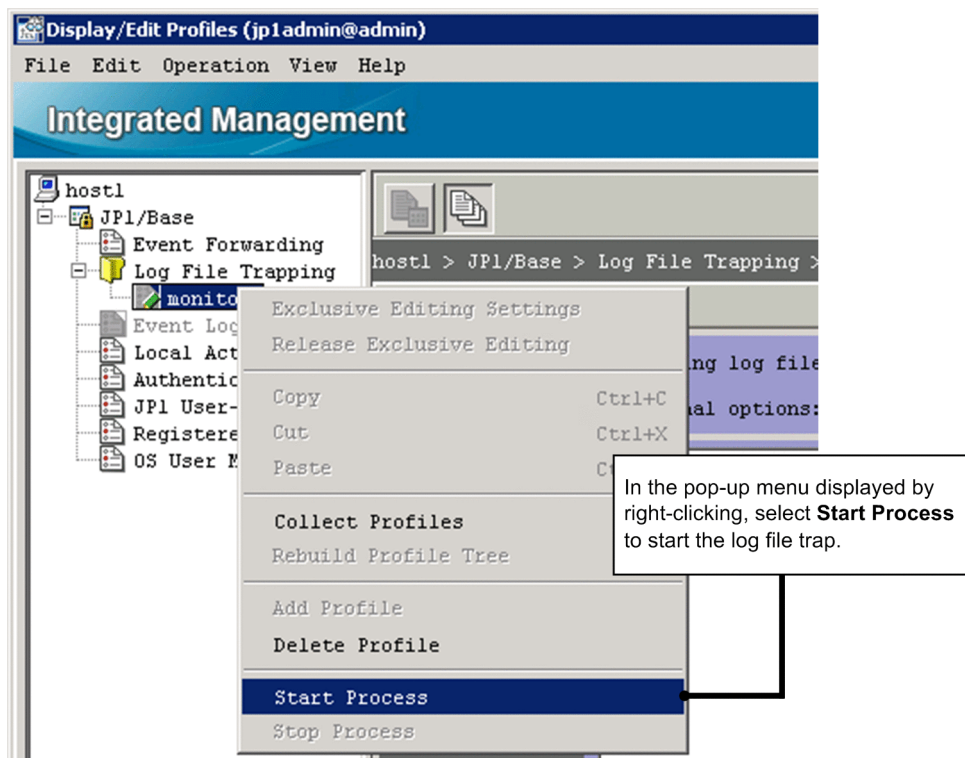
Prerequisites

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 JP1/Base on the host to be monitored.
- The JP1/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*
- [4.9 Display/Edit Profiles window](#) in the manual *GUI Reference*
- Descriptions of converting application program log files in the *JP1/Base User's Guide*

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

After you have created a log file operation definition file, verify that the log file trap is running normally. (For details about how to create the file, see [2.4.1 Procedure for starting log file monitoring in JP1/IM.](#)) This subsection describes how to use a command to output a pseudo record. 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 [2.4.1 Procedure for starting log file monitoring in JPI/IM](#).

Procedure

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

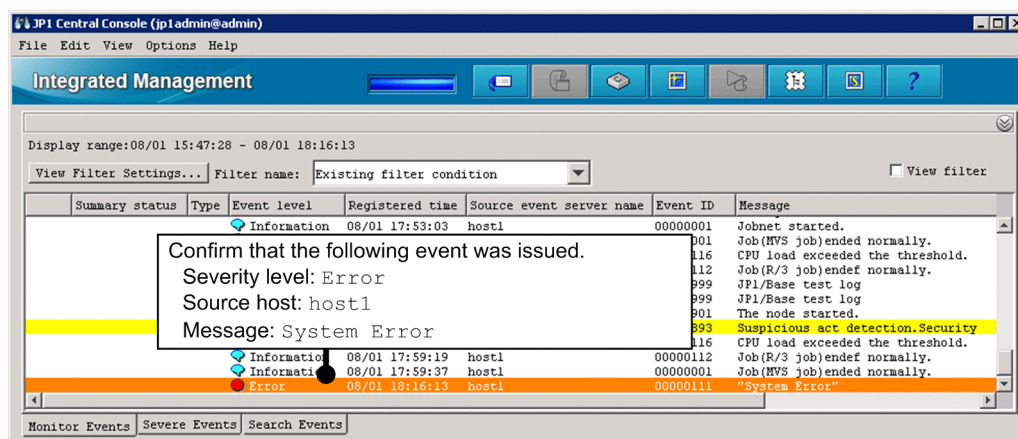
```
echo "System Error">>log-file-name#
```

#: 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

- [2.1 Overview of the Event Console window in the manual GUI Reference](#)
- [2.38 Execute Command window in the manual GUI Reference](#)

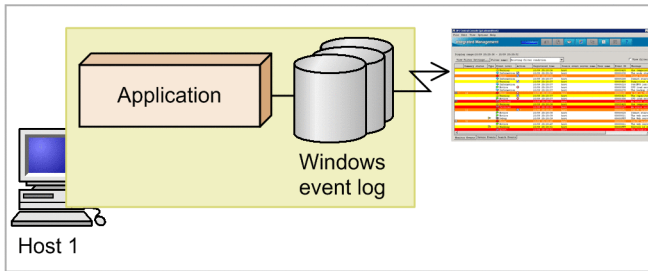
2.5 Using event conversion to monitor Windows event logs

Converting Windows event logs to events handled in JP1 allows JP1/IM to monitor log data output in Windows, such as application error logs. To convert Windows event logs to JP1 events, you need to configure JP1/Base event log trapping.

In this section, we will configure JP1/Base event log trapping to allow JP1/IM to monitor Windows event logs.

Problem

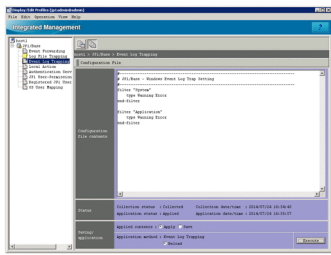
1. An error in an application running in Windows was output to a Windows event log.
2. There must be a way to monitor Windows event logs by using JP1/IM - Manager.



The diagram illustrates the problem: an application on Host 1 writes to a Windows event log. JP1/IM Manager is shown monitoring this log. A person icon is next to the problem statement.

Action

1. It looks like I can use the JP1/Base event conversion function to monitor Windows event logs.
2. I'll try editing a profile in IM Configuration Management to customize the event log trap settings.



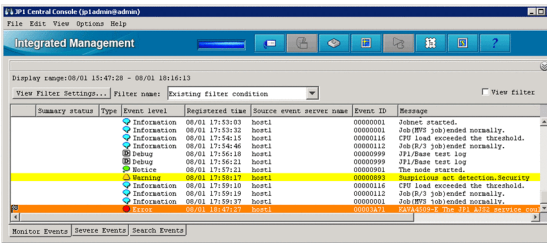
Window:

- Display/Edit Profile window
- Required settings
- Action definition for the event log trap

The screenshot shows the 'Integrated Management' window with the 'Configuration Manager' tab selected. It displays a list of event log traps and their settings. A person icon is next to the action statement.

Check

I'll confirm that the event log trap is running.



The screenshot shows the 'JP1 Central Console' window with the 'Integrated Management' tab selected. It displays a list of event log traps and their status. A person icon is next to the check statement.

Keywords:

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

2.5.1 Monitoring Windows event logs in JP1/IM

To use JP1/IM to monitor Windows event logs, you can use *event log trapping*, which is a JP1/Base function for converting event log data to events handled in JP1.

Event log trapping is enabled when the JP1/Base EventlogTrap service starts in JP1/Base on a host on which you want to monitor Windows event logs.

This manual describes how to customize the event log trap settings for Windows event log data issued on host 1 in the basic configuration system shown in [1.2.1 Overview of a basic configuration system](#).

(1) Settings of the event log trap action-definition file to be created

The following provides details about the settings specified in the the event log trap action-definition file. The file is created in [2.5.1\(2\) Using IM Configuration Management to edit the event log trap action-definition file on the host to be monitored](#).

Specification details

Specification	Description
<code>filter "System"</code> <code>type Warning Error</code> <code>end-filter</code>	Specifies the Windows event log data to be trapped for which <code>System</code> is specified for Log Name . In this manual, log data whose Level is <code>Warning</code> or <code>Error</code> is trapped.
<code>filter "Application"</code> <code>type Warning Error</code> <code>end-filter</code>	Specifies the Windows event log data to be trapped for which <code>Application</code> is specified for Log Name . In this manual, log data whose Level is <code>Warning</code> or <code>Error</code> is trapped.

(2) Using IM Configuration Management to edit the event log trap action-definition file on the host to be monitored

The following describes how to use IM Configuration Management to edit the event log trap action-definition file in order to customize the event log trap settings. Perform this procedure on the host to be monitored.

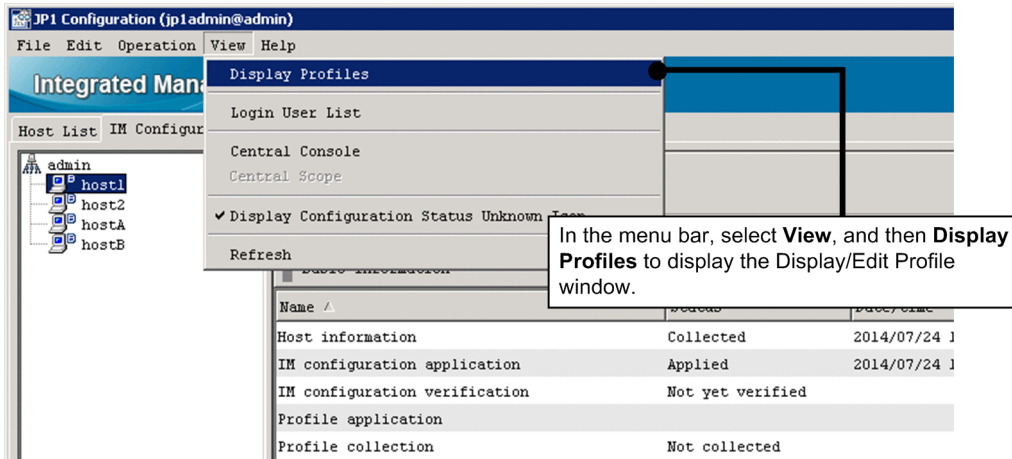
Prerequisites

The following conditions must be satisfied:

- The basic configuration system is set up according to [2.1.1 Procedure for setting up a system by using IM Configuration Management](#).
- The `JP1/Base EventlogTrap` service is running, and host information has been collected.
- The OS of the host to be monitored is Windows.

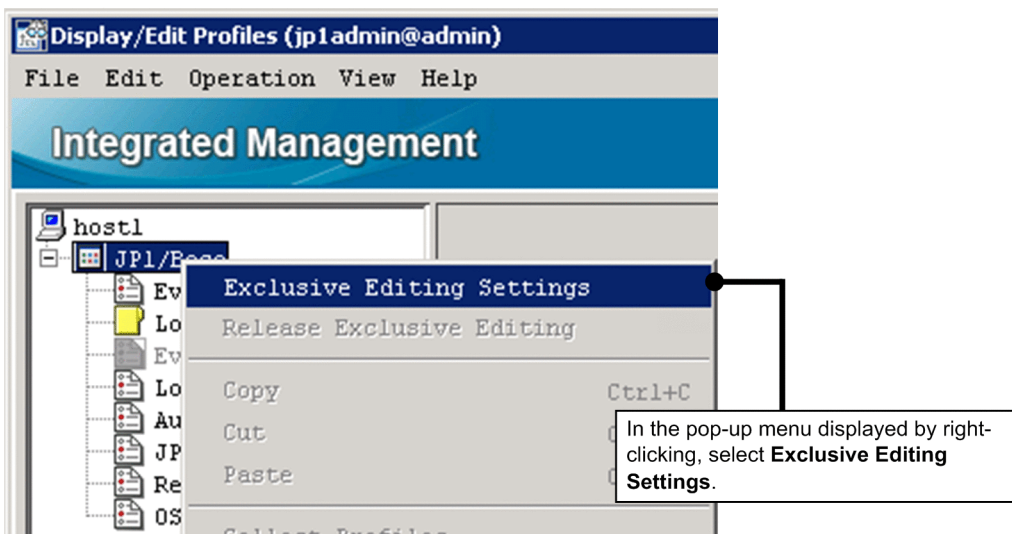
Procedure

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 the Windows event log.
4. On the menu bar, select **View**, and then **Display Profiles**. The Display/Edit Profile window appears.



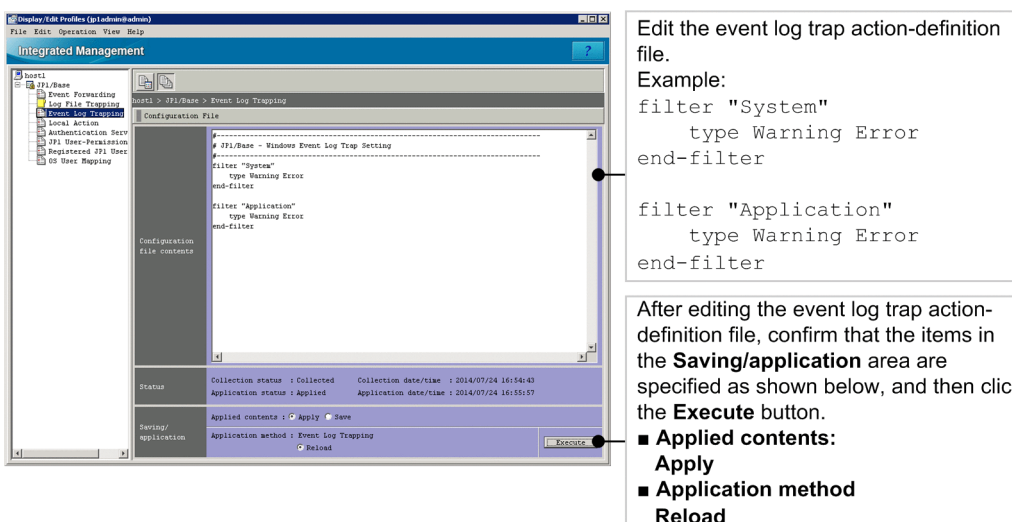
5. In the tree display area, select **JP1/Base**.

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 **Event Log Trapping**.

8. Edit the event log trap action-definition file as shown in the following figure.



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

Related topics

- [3.5.1 Setting the profiles on hosts in an agent configuration](#) in the *Configuration Guide*
- [4.1.2 IM Configuration page](#) in the manual *GUI Reference*
- [4.9 Display/Edit Profiles window](#) in the manual *GUI Reference*
- Descriptions about converting Windows event log data in the *JP1/Base User's Guide*
- Descriptions the event log trap action-definition file (`ntevent.conf`) in the *JP1/Base User's Guide*

2.5.2 Verifying that Windows event log data can be converted to events

After you have edited an event log trap action-definition file, verify that the event log trap is running normally. For details about editing the file, see [2.5.1\(2\) Using IM Configuration Management to edit the event log trap action-definition file on the host to be monitored](#). This subsection describes how to verify that Windows event log data issued on host 1 was converted to a JP1 event.

Prerequisites

The following conditions must be satisfied:

- The JP1/Base EventlogTrap service is running on the host to be monitored.
- Setting of the event log trap has been completed according to [2.5.1\(2\) Using IM Configuration Management to edit the event log trap action-definition file on the host to be monitored](#).

Procedure

1. On the agent (`host1`) on which the event log trap is running, issue Windows event log data that satisfies the following conditions:
 - **Log Name** is `Application`.
 - **Level** is `Error`.

Only information output to Windows event logs after the JP1/Base EventlogTrap started on the host to be monitored can be converted.

2. Verify that the Windows event log data you issued in step 1 is displayed in the event list.

Related topics

- [2.1 Overview of the Event Console window](#) in the manual *GUI Reference*

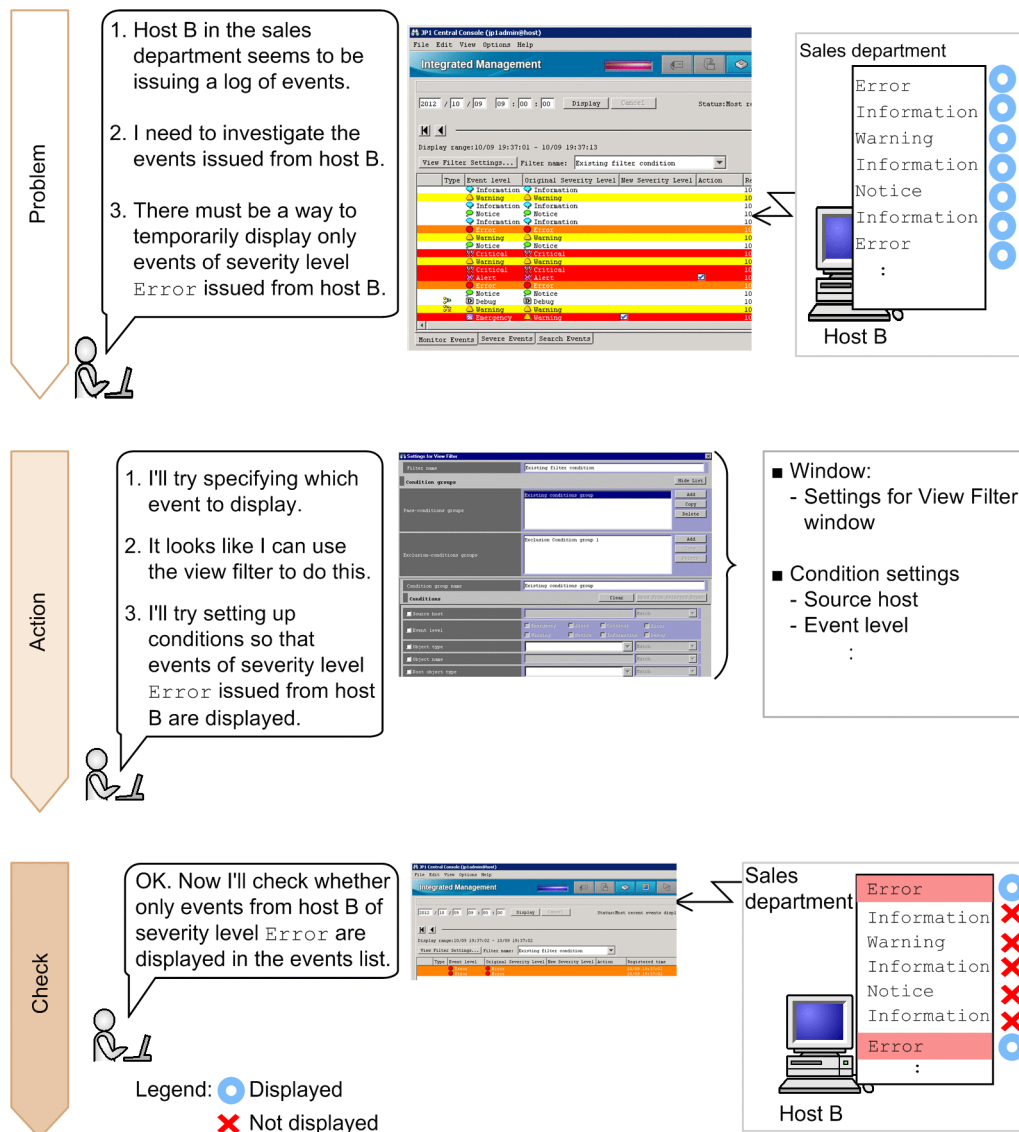
3

Monitoring a System

This chapter explains how to temporarily filter events displayed in the event list, and how to customize the severity of events.

3.1 Filtering the events that are displayed

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.



This manual describes how to specify the settings to display events of severity level **Error** issued on host B.

Keywords:

display, event, specific, filtering, view filter

3.1.1 Using the view filter to specify conditions of events to be displayed

The following describes how to set up the view filter by using the Settings for View Filter window of the central console to filter the events that are displayed. 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.

Settings for View Filter

Filter name

Condition groups

Condition group name

Conditions

☒ Source host

☒ Event level

☐ Object type

☐ Object name

☐ Root object type

☐ Root object name

☐ Occurrence

☐ User name

☐ Message

☐ Product name

☐ Event ID

☐ Status

☐ Action

Source host: hostB Match

Event level: Error

Emergency Alert Critical Error

Warning Notice Information Debug

OK Cancel Help

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

- [4.2.1 Settings for view filters](#) in the *Configuration Guide*
- [2.26 Settings for View Filter window](#) in the manual *GUI Reference*

3.1.2 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

The view filter must be set up according to the procedure in [3.1.1 Using the view filter to specify conditions of events to be displayed](#).

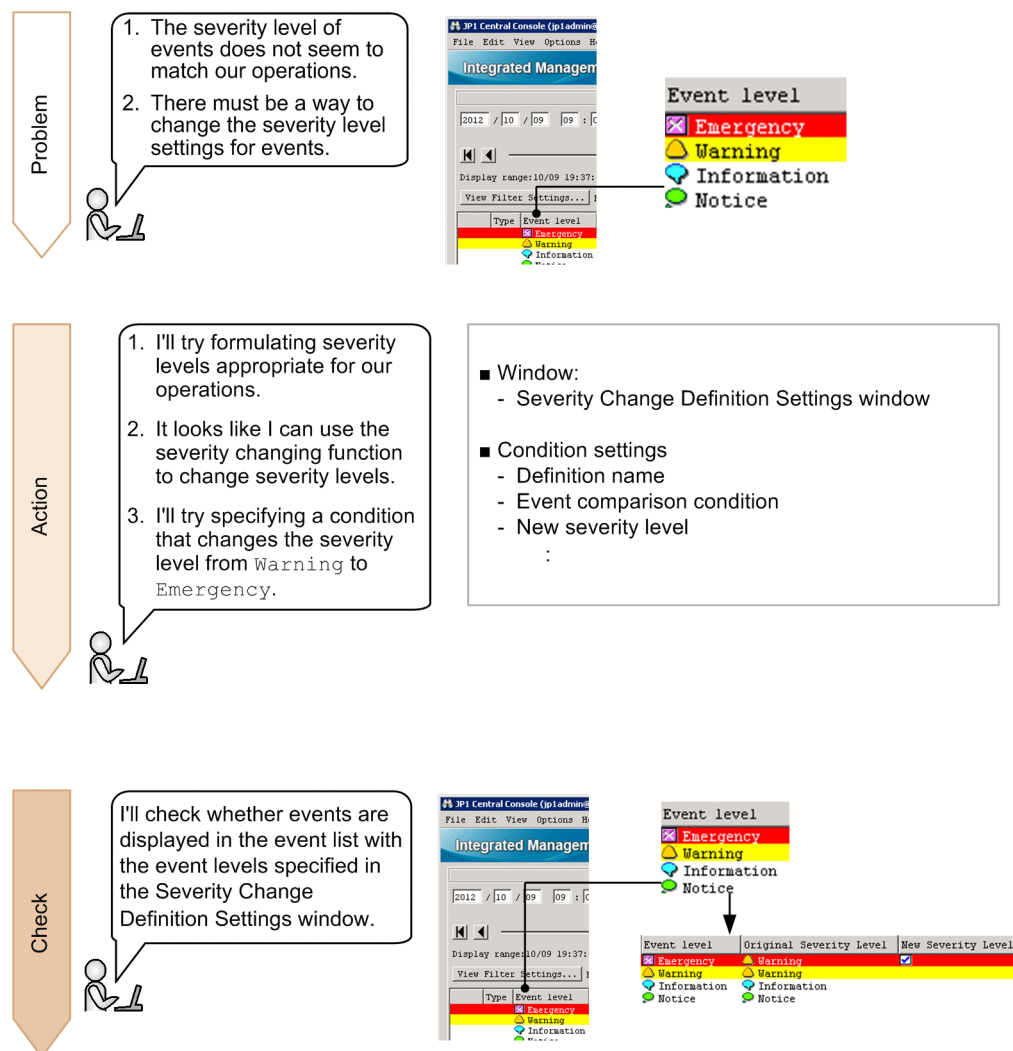
Procedure

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.

3.2 Changing the severity level of events to better match your operations

The severity levels of events forwarded to JP1/IM - Manager are preset according to the event type. However, depending on the status of the issuing host or the operating state of the system, the preset severity levels might not match the severity of an event.

In this section, we will change the severity level of events to better match your operations so that you can monitor events with severity levels that are consistent with your system operations.



This manual describes how to change the severity level to Emergency for events of severity level Warning issued on host A.

Keywords:

severity level, change, monitoring, definition, severity changing function

3.2.1 Using the severity changing function to change the severity level of events

You use the severity changing function to change the severity level of events to better match your operations. The following describes how to use the Severity Change Definition Settings window to change the severity level to Emergency for events of severity level Warning.

Prerequisites

The following conditions must be satisfied:

- The integrated monitoring database is configured and enabled according to [1.3.4\(3\) Setting up an integrated monitoring database \(for Windows\)](#) or [1.4.4\(3\) Setting up an integrated monitoring database \(for Linux\)](#).
- The JP1 user who will change the severity level has JP1_Console_Admin permissions.
- The OS user who will execute the `jcoimdef` command has Administrator or `root` permissions.

Procedure

1. Execute the following `jcoimdef` command to change the settings to enable the event severity changing function:

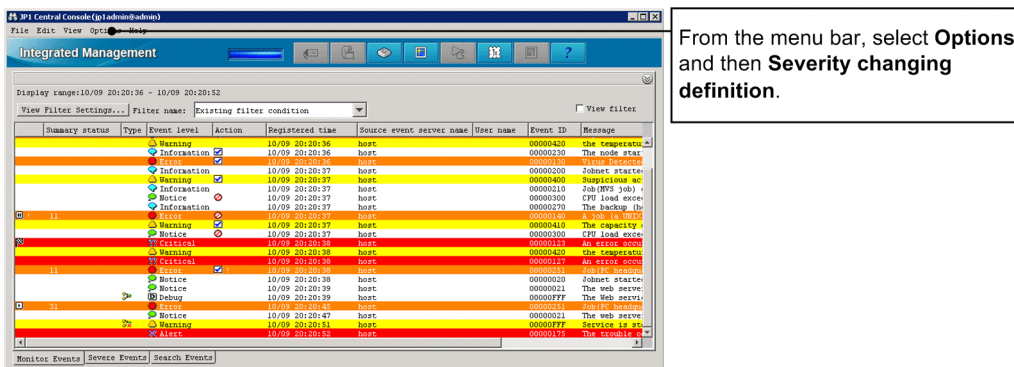
- In Windows:
`"Console-path\bin\jcoimdef" -chsev ON`
- In Linux:
`/opt/jp1cons/bin/jcoimdef -chsev ON`

2. Restart JP1/IM - Manager.

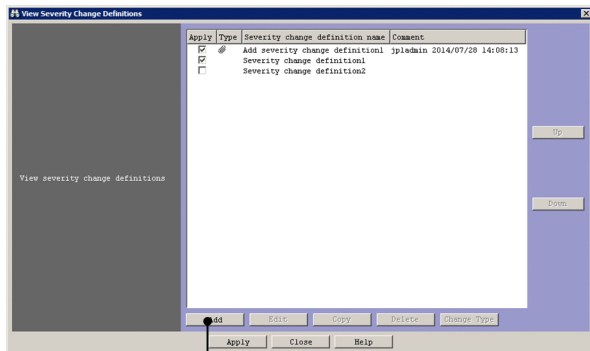
3. From the Windows **Start** menu, select **All Programs, JP1_Integrated Management - View**, and then **Integrated View**. The Login window appears.

4. Enter `jp1admin` for **User name**, `jp1admin` for **Password**, and `admin` for **Host to connect**, and then log in. The Event Console window appears.

5. In the Event Console window, select **Options**, and then **Severity changing definition**. The View Severity Change Definitions window appears.

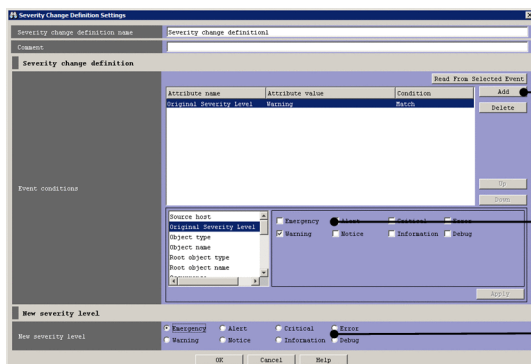


6. In the View Severity Change Definitions window, click the **Add** button to display the Severity Change Definition Settings window.



Click the **Add** button to display the Severity Change Definition Settings window.

- Specify the condition for events whose severity level is to be changed, select the severity level for **New severity level**, and then click **OK**.

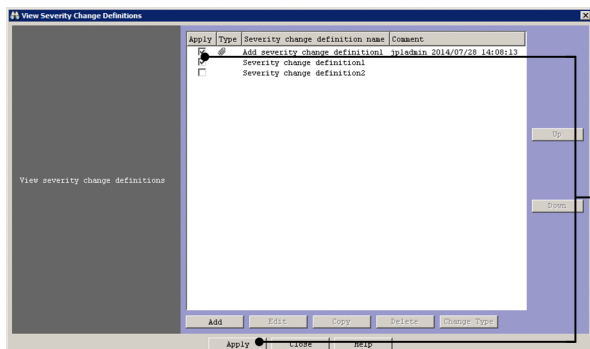


Click the **Add** button to add event condition items.

Specify the event condition as follows:
Original severity level: Specify **Warning** and **Match**.

For **New severity level**, select **Emergency**.

- In the View Severity Change Definitions window, select the **Apply** check box for the severity change definition added in step 7.



Select the **Apply** check box to enable the definition, and then click the **Apply** button.

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

Related topics

- 11.1.8 Considerations for changing JPI event levels in the Overview and System Design Guide
- 4.11 Setting the severity changing function in the Configuration Guide
- 2.20 View Severity Change Definitions window in the manual GUI Reference
- 2.21 Severity Change Definition Settings window (Add Severity Change Definition Settings window) in the manual GUI Reference

3.2.2 Verifying that the severity level was changed

After you have finished specifying the conditions for the severity changing function, verify that the events with the new severity level are displayed in the event list. The following describes how to verify that an event whose severity level changed to Emergency is displayed in the event list.

Prerequisites

The following conditions must be satisfied:

- The following items are specified as event list items in the Preferences window, which is displayed by selecting **Main Menu, Options, and then Preferences**:
 - **Event level**
 - **Original severity level**
 - **New severity level**
- OS user mapping was configured according to the procedure in [2.2.1 Using the user mapping feature to map a JPI user account to an OS user account](#).

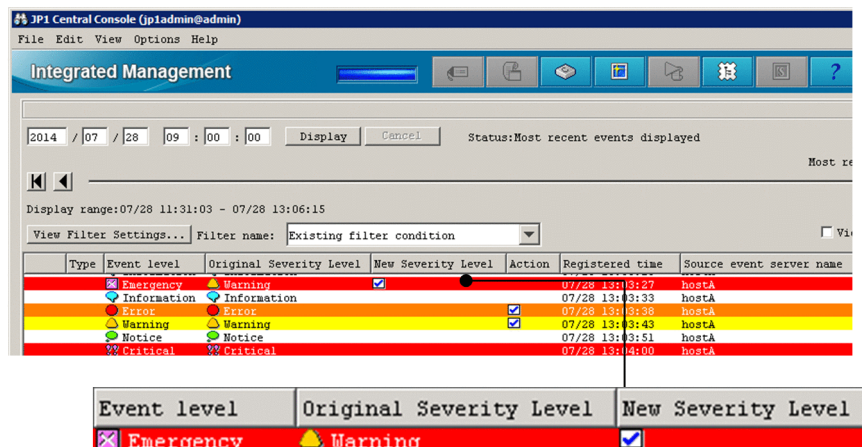
Procedure

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: "Base-path\bin\jvsend" -e SEVERITY=Warning • In Linux: /opt/jplbase/bin/jvsend -e SEVERITY=Warning

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

3. Check the severity level of the event according to the following figure:



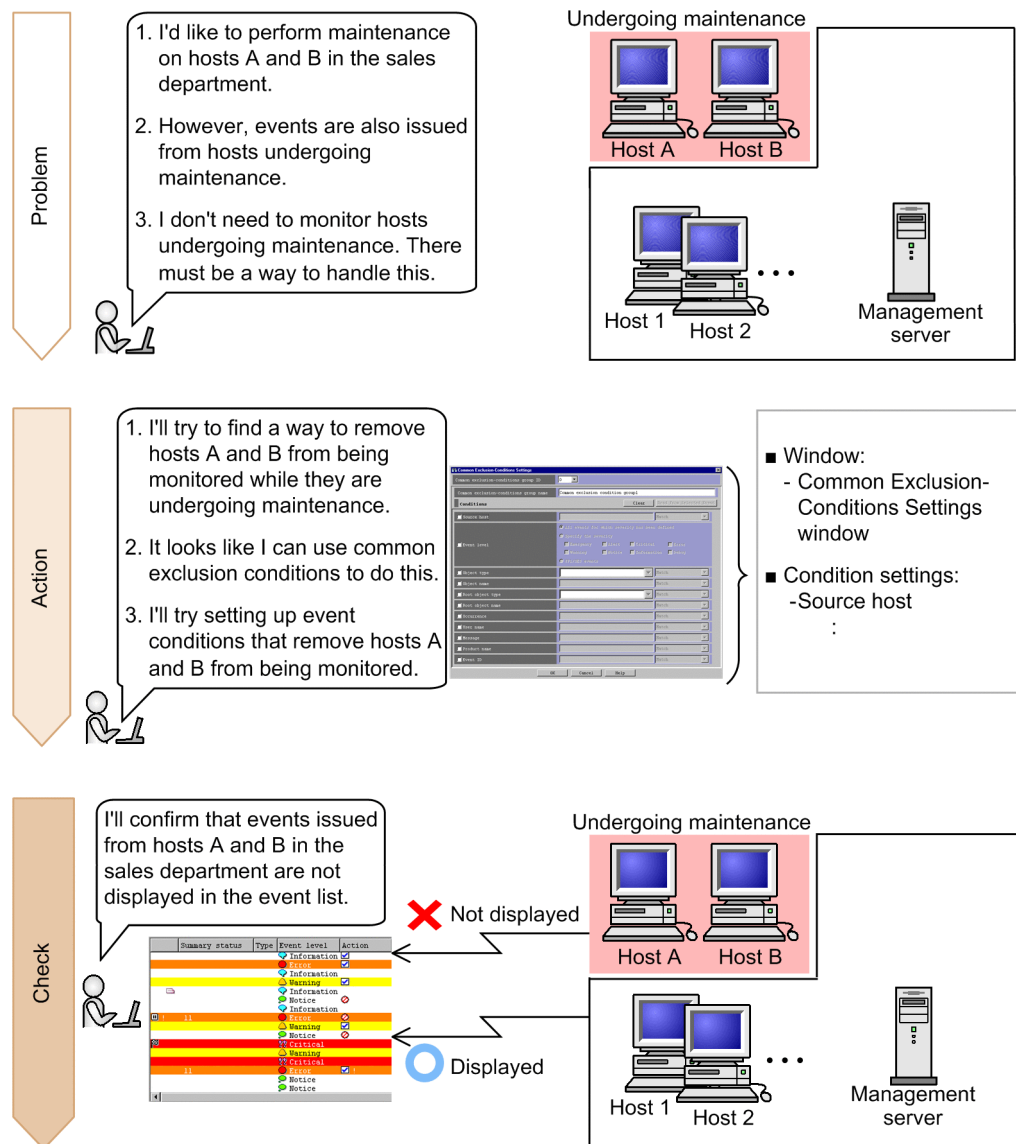
Related topics

- *2.1 Overview of the Event Console window in the manual GUI Reference*
- *2.38 Execute Command window in the manual GUI Reference*
- *2.22 Preferences window in the manual GUI Reference*

3.3 Removing hosts undergoing maintenance from being 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.

In this section, we will stop a couple of hosts that are undergoing maintenance from being monitored so that these unnecessary events are not displayed.



We will specify settings to remove events issued on hosts A and B from being monitored while these hosts are undergoing maintenance.

Important note

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

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

To remove hosts undergoing maintenance from 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 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.

- Click the **OK** button in the Event Acquisition Conditions List window.
The System Environment Settings window appears.
- 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

- 3.2.6 *Defining filter conditions* in the *Overview and System Design Guide*
- 12.10 *Considerations for JPI/IM system-wide maintenance* in the *Overview and System Design Guide*
- 4.2.4 *Settings for event acquisition filters* in the *Configuration Guide*
- 2.15 *Common Exclusion-Conditions Settings window* in the manual *GUI Reference*

3.3.2 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 the procedure in [2.2.1 Using the user mapping feature to map a JPI user account to an OS user account](#).
- A basic configuration system is set up according to [2.1.1 Procedure for setting up a system by using IM Configuration Management](#).

Procedure

- In the Event Console window, click the **Execute Command** button. The Execute Command window appears.
- 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 Command executed from host A. In Linux: /opt/jplbase/bin/jevsend -e SEVERITY=Warning -m Command executed from host A.

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

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

Item	Setting
Command type	Select Command of managed host .
Event information to inherit	Clear the Inherit event information check box.
Target host	Enter the following: hostB
Command	Enter the following: <ul style="list-style-type: none">• In Windows: "<i>Base-path</i>\bin\jevsend" -e SEVERITY=Warning -m Command executed from host B.• In Linux: /opt/jplbase/bin/jevsend -e SEVERITY=Warning -m Command executed from host B.

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

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

Item	Setting
Command type	Select Command of managed host .
Event information to inherit	Clear the Inherit event information check box.
Target host	Enter the following: host1
Command	Enter the following: <ul style="list-style-type: none">• In Windows: "<i>Base-path</i>\bin\jevsend" -e SEVERITY=Warning -m Command executed from host 1.• In Linux: /opt/jplbase/bin/jevsend -e SEVERITY=Warning -m Command executed from host 1.

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

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

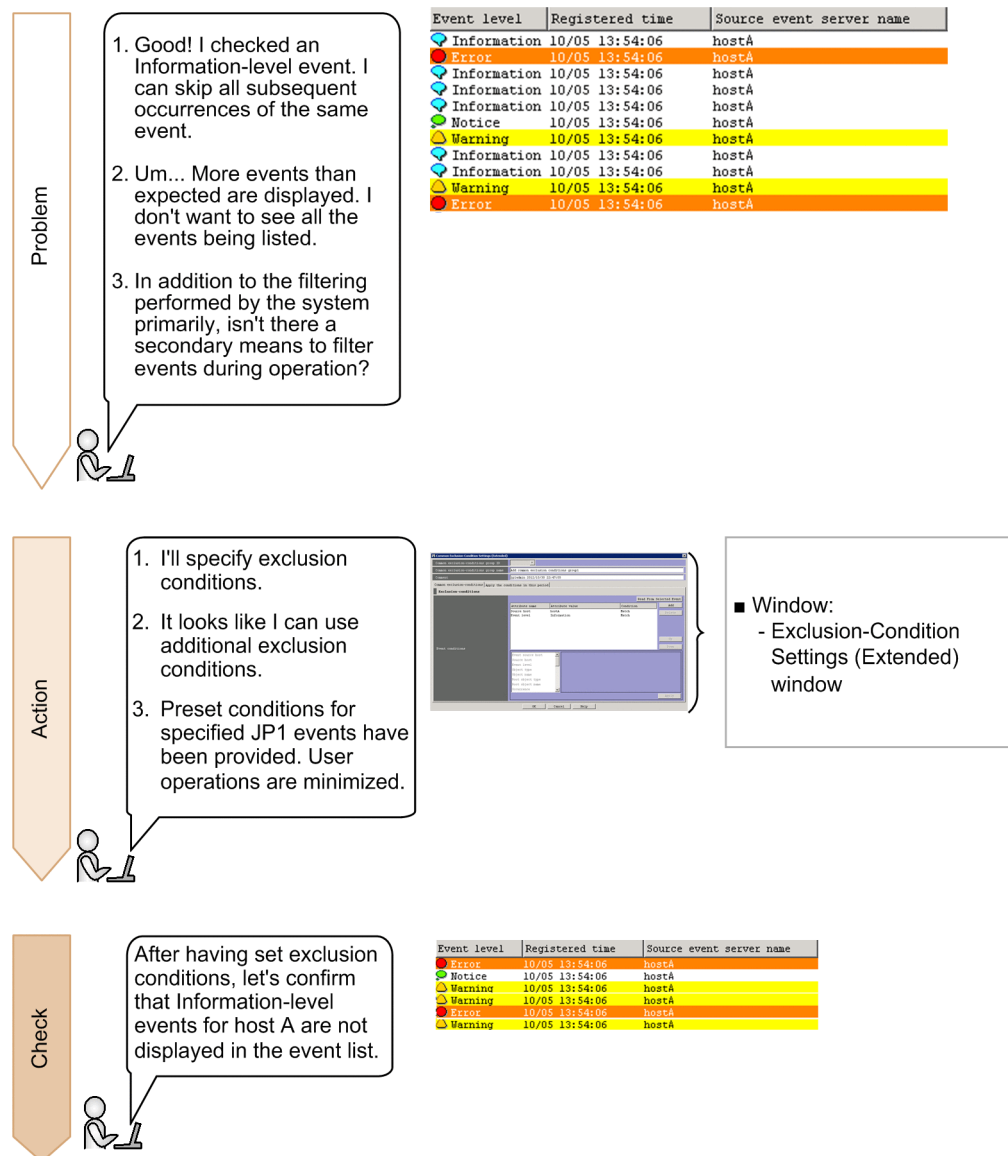
Related topics

- *2.1 Overview of the Event Console window in the manual GUI Reference*
- *2.22.2 Event Attributes page in the manual GUI Reference*
- *2.38 Execute Command window in the manual GUI Reference*

3.4 Specifying not to display unnecessary events in the list

After system monitoring has started filtering events based on the predefined common exclusion conditions, you might feel some events that were acquired are no longer necessary.

Let's remove such events from being monitored so that they are no longer displayed in the event list during operation.



This manual describes how to select an event of severity level *Information*, issued on host A, in the event list of the Event Console window to prevent unnecessary events from being displayed.

Keywords:

filter, additional common exclusion-condition, during operation, extended

3.4.1 Using additional common exclusion conditions for a filter to prevent display of unnecessary events

To remove unnecessary events from being monitored, you use additional common exclusion conditions for a filter. These conditions can be used only when extended mode is set for common exclusion conditions. To set additional common exclusion conditions, use the Common Exclusion-Condition Settings (Extended) window of the central console. The following explains how to set an additional common exclusion condition to prevent unnecessary events from being displayed in the list during operation.

Prerequisites

The following conditions must be satisfied:

- The JP1 user who wants to set additional common exclusion condition for a filter has JP1_Console_Admin permissions.
- The OS user who will execute the jbssetcnf and jcochcefmode commands has Administrator or root permissions.

Procedure

1. Stop JP1/IM - Manager.
2. Create a definition file for extending regular expressions that can be used for JP1/Base. You can specify any file name.

Specify as follows in the definition file:

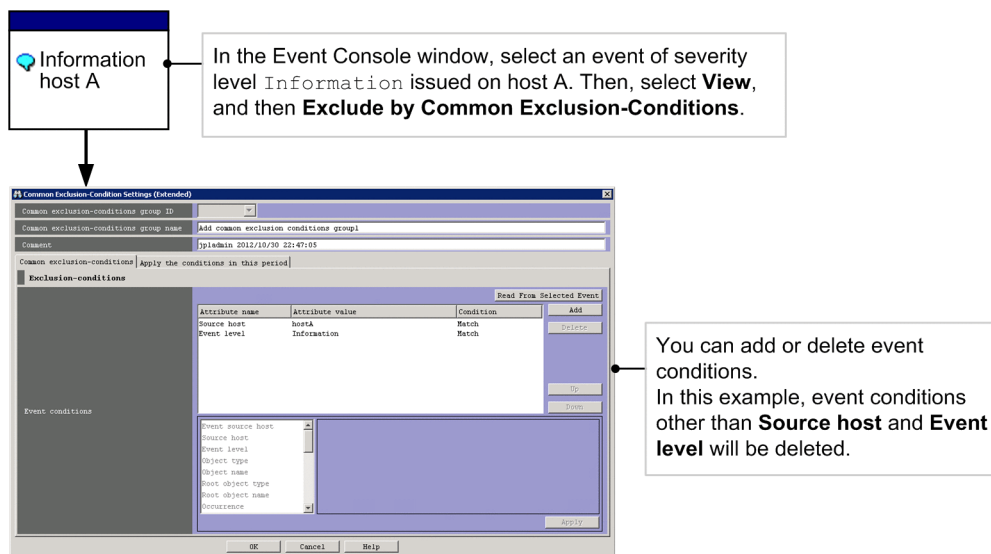
```
-----  
[JP1_DEFAULT\JP1BASE\  
"REGEXP"="EXTENDED"  
-----
```

3. Execute the following jbssetcnf command to apply the settings to JP1/Base common definition information:

- In Windows:
`"Base-path\bin\jbssetcnf" definition-file-name`
- In Linux:
`/opt/jp1base/bin/jbssetcnf definition-file-name`

4. Restart JP1/Base.
5. Execute the following jcochcefmode command to change the operating mode for the common exclusion conditions:
 - In Windows:
`"Console-path\bin\jcochcefmode" -m extended`
 - In Linux:
`/opt/jp1cons/bin/jcochcefmode -m extended`
6. Start JP1/IM - Manager.
7. From the Windows **Start** menu, select **All Programs, JP1_Integrated Management - View**, and then **Integrated View**. The Login window appears.

8. Enter `jp1admin` for **User name**, `jp1admin` for **Password**, and `admin` for **Host to connect**, and then log in. The Event Console window appears.
 9. In the Event Console window, verify that an unnecessary event of severity level `Information` issued on host `A` is displayed in the event list.
 10. In the event list of the Event Console window, select an event that you think is unnecessary. Then, from the **View** menu, select **Exclude by Common Exclusion-Conditions** to display the Common Exclusion-Condition Settings (Extended) window.
- Note that this window is not displayed unless the selected event satisfies either of the following conditions:
- The event is registered in the event database on the agent host.
 - The event is registered in the event database or the integrated monitoring database on the manager to which JP1/IM - View has logged in.
11. Specify the settings as described in the following figure to prevent the unnecessary event from being displayed.



12. In the Common Exclusion-Condition Settings (Extended) window, click the **OK** button.
A message that asks you whether you want to apply the settings appears.
13. Click the **Yes** button.
An event indicating that additional common exclusion conditions have just been set is issued.

Related topics

- [3.2.6\(1\)\(c\) Additional common exclusion-conditions in the Overview and System Design Guide](#)
- [5.1.14 Excluding JP1 events from monitoring by setting additional common exclusion-conditions in the Administration Guide](#)
- [2.16 Common Exclusion-Condition Settings \(Extended\) window in the manual GUI Reference](#)
- The description of how to extend regular expressions to be used in the *JP1/Base User's Guide*

3.4.2 Checking whether unnecessary events are displayed

After you have set additional common exclusion conditions for a filter, check whether any events that you excluded from monitoring are displayed in the event list. The following describes how to verify that an event of severity level

Information issued on host A is not displayed in the event list. The following also describes how to verify that 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 [2.2.1 Using the user mapping feature to map a JPI user account to an OS user account](#).

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=Information -m Command executed from host A.</code>• In Linux: <code>/opt/jplbase/bin/jevsend -e SEVERITY=Information -m Command executed from host A.</code>

An event of severity level Information is issued on host A.

3. Verify that the event of severity level Information issued on host A is not displayed in the event list.
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: host1
Command	Enter the following: <ul style="list-style-type: none">• In Windows: <code>"Base-path\bin\jevsend" -e SEVERITY=Information -m Command executed from host 1.</code>• In Linux: <code>/opt/jplbase/bin/jevsend -e SEVERITY=Information -m Command executed from host 1.</code>

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

5. Verify that the event of severity level Information issued on host 1 is displayed in the event list.

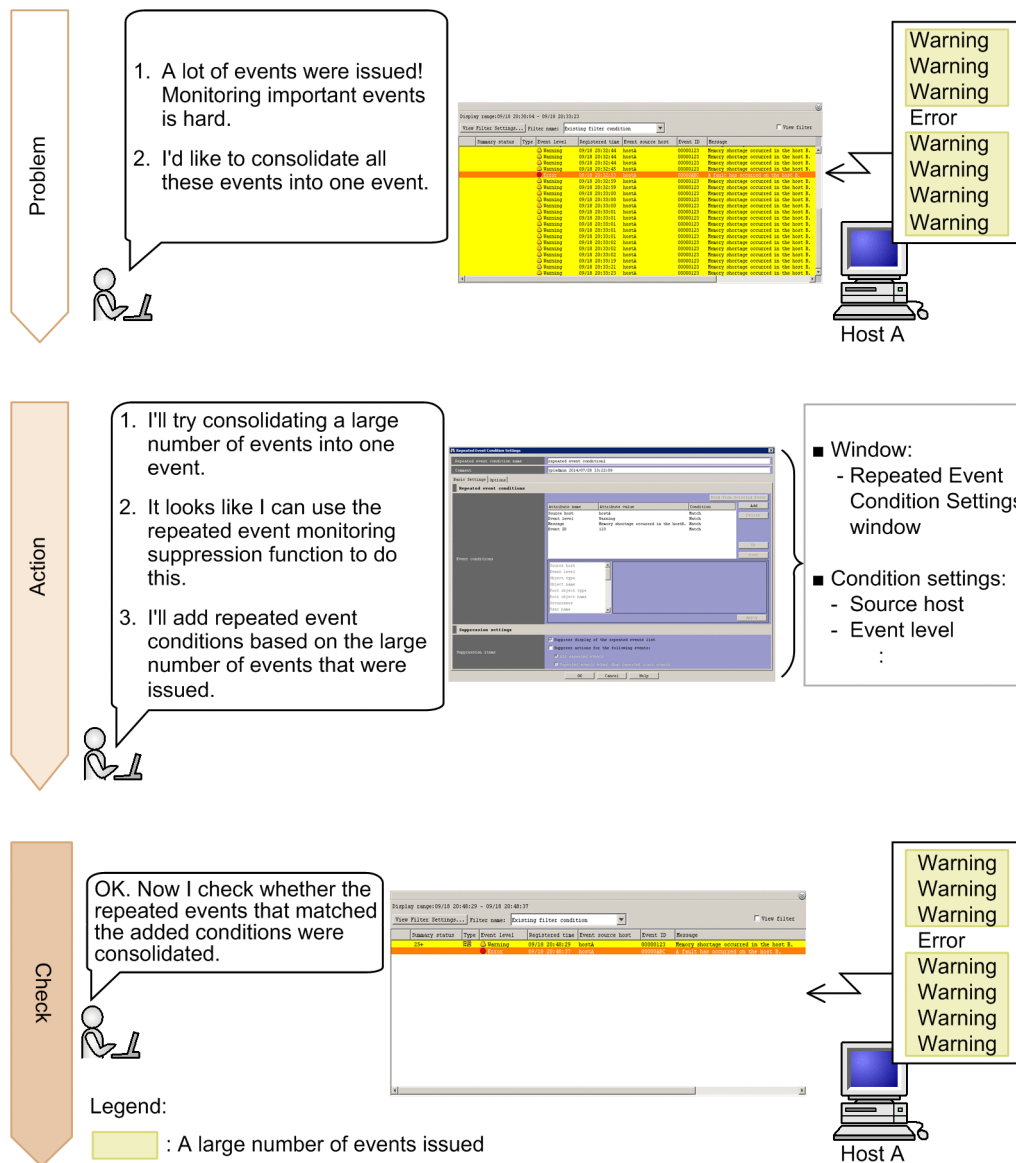
Related topics

- *2.1 Overview of the Event Console window in the manual GUI Reference*
- *2.38 Execute Command window in the manual GUI Reference*

3.5 Identifying important events among a large number of issued events

While the system is being monitored, a large number of events might be issued in a short period of time. In this case, important events buried in many other events might be overlooked.

In this section, we will consolidate a large number of events into one event so that important events are not overlooked.



This manual describes how to use the Repeated Event Condition Settings window to specify that repeatedly-issued events that match the following conditions are immediately displayed as one consolidated event:

- Source host: Host A
- Severity level: Warning
- Message: A memory shortage occurred on host B
- Event ID: 123



Tip:

To prevent automated actions from being executed when a large number of events are issued:

If you do not want to execute automated actions when a large number of events specified in the automated action definition are issued, you can use the Repeated Event Condition Settings window to suppress automated actions. For details about the Repeated Event Condition Settings window, see *2.17 Repeated Event Condition Settings window* in the manual *GUI Reference*.



Keywords:

event, consolidation, event list, filter, a large number of

3.5.1 Consolidating a large number of events by using the repeated event monitoring suppression function

When a large number of events are issued, an event that matches the conditions specified by the user is called a *repeated event*. You can use the repeated event monitoring suppression function to consolidate repeated events into one event. You can set up this function in the Repeated Event Condition Settings window of the central console.

Prerequisites

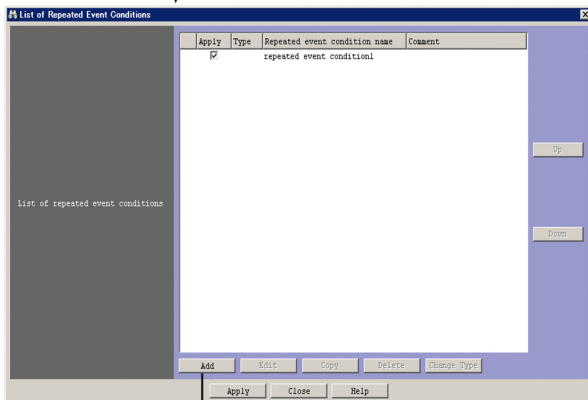
The following conditions must be satisfied:

- The integrated monitoring database was configured and enabled according to *1.3.4(3) Setting up an integrated monitoring database (for Windows)* or *1.4.4(3) Setting up an integrated monitoring database (for Linux)*.
- The JP1 user who wants to suppress repeated events has JP1_Console_Admin permissions.
- The user who will execute the `jcoimdef` command has Administrator or root permissions.

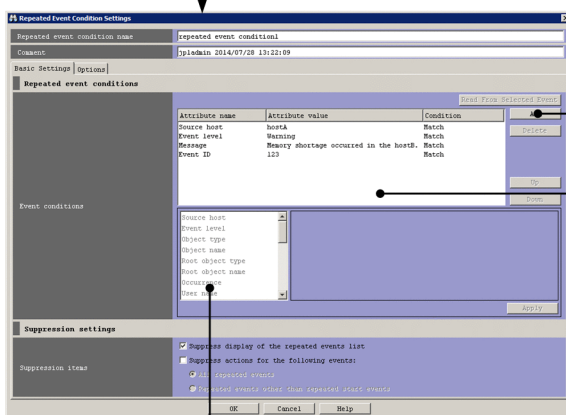
Procedure

1. Execute the following `jcoimdef` command to enable the repeated event monitoring suppression function:
 - In Windows:
`"Console-path\bin\jcoimdef" -storm ON`
 - In Linux:
`/opt/jplcons/bin/jcoimdef -storm ON`
2. Restart JP1/IM - Manager and JP1/IM - View.
3. From the Windows **Start** menu, select **All Programs, JP1_Integrated Management - View**, and then **Integrated View**. The Login window appears.
4. Enter `jpladmin` for **User name**, `jpladmin` for **Password**, and `admin` for **Host to connect**, and then log in. The Event Console window appears.
5. Select **Main Menu, Options**, and then **Repeated Event Condition Settings**. In the List of Repeated Event Conditions that opens, click the **Add** button to display the Repeated Event Condition Settings window.
6. Specify the repeated event conditions according to the following figure:

Select **Main Menu**, **Options**, and then **Repeated Event Condition Settings**. The List of Repeated Event Conditions window opens.



Click the **Add** button to open the Repeated Event Condition Settings window.



Click the **Add** button to add event condition items. Click the **Delete** button to delete the items.

Specify the event condition as follows:

- **Source host:** Specify `hostA` and `Match`.
- **Event level:** Specify `Warning` and `Match`.
- **Message:** Specify `A memory shortage occurred on host B.` and `Match`.
- **Event ID:** Specify `123` and `Match`.

From this list (attribute name list), select the attribute of the condition you added by using the **Add** button.

- In the Repeated Event Condition Settings window, click the **OK** button.
- In the List of Repeated Event Conditions window, select the **Apply** check box for the repeated event condition added in step 7.
- In the List of Repeated Event Conditions window, click the **Apply** button.
- When a dialog box asking you whether you want to apply the settings appears, click the **Yes** button.

Related topics

- *3.4 Suppressing display of repeated events in the Overview and System Design Guide*
- *5.1.6 Suppressing monitoring of large numbers of events by setting repeated event conditions in the Administration Guide*
- *2.17 Repeated Event Condition Settings window in the manual GUI Reference*
- *1. jcoimdef in the manual Command and Definition File Reference*

3.5.2 Verifying that a large number of events are consolidated

After you have specified the repeated event conditions, verify that the repeated events were consolidated as you intended. The following describes how to execute the verification command.

Prerequisites

OS user mapping must be configured according to the procedure in [2.2.1 Using the user mapping feature to map a JPI user account to an OS user account](#).

Procedure

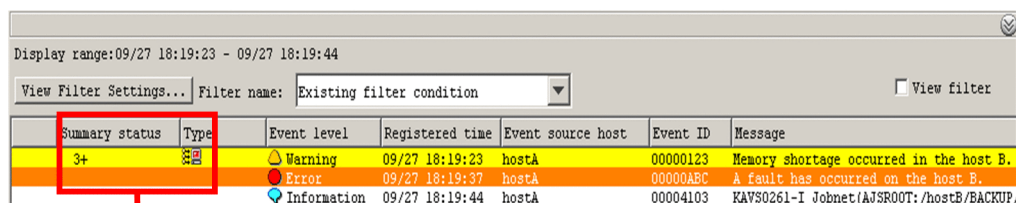
1. In the Event Console window, click the **Execute Command** button. The Execute Command window appears.
2. Set the items in the Execute Command window as described below, and then click the **Execute** button.





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" -i 123 -e SEVERITY=Warning -m A memory shortage occurred on host B</code>• In Linux: <code>/opt/jplbase/bin/jevsend -i 123 -e SEVERITY=Warning -m A memory shortage occurred on host B</code>


An event with severity level Warning, event ID 123, and the message A memory shortage occurred on host B is issued on host A.

3. Execute the command above two or three times to repeatedly issue the event with severity level Warning, event ID 123, and the message A memory shortage occurred on host B on host A.
Make sure that steps 2 and 3 terminate within the time specified for **End monitoring period**, for which the default value is 300 seconds.
4. In the event list in the Event Console window, verify that the events issued in steps 2 and 3 were consolidated into one event.

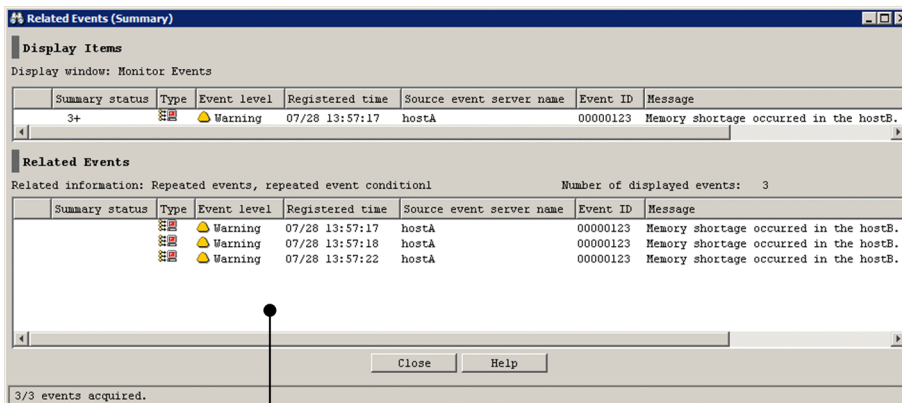
The number of consolidated events is indicated in the **Summary Status** column in the event list. An icon indicating that repeated events are consolidated is displayed in the **Type** column.



Display range: 09/27 18:19:23 - 09/27 18:19:44							
View Filter Settings...		Filter name: Existing filter condition		View filter			
Summary status	Type	Event level	Registered time	Event source host	Event ID	Message	
3+		 Warning	09/27 18:19:23	hostA	00000123	Memory shortage occurred in the host B.	
		 Error	09/27 18:19:37	hostA	00000ABC	A fault has occurred on the host B.	
		 Information	09/27 18:19:44	hostA	00004103	KAVS0261-I Jobnet(AJ5R00T:/hostB/BACKUP,	

The total number of consolidated events is indicated in the **Summary status** column.
The icon  indicating that the repeated events are consolidated is displayed in the **Type** column.

5. Select and then right-click an event that is being consolidated. In the pop-up menu that appears, select **Display Related Event List** to open the Related Events (Summary) window.
6. In this window, verify that the list under **Related Events** only shows the events that were issued on host A with severity level Warning, event ID 123, and the message A memory shortage occurred on host B.



A list of consolidated repeated events is displayed.

Related topics

- *2.1 Overview of the Event Console window in the manual GUI Reference*
- *2.38 Execute Command window in the manual GUI Reference*

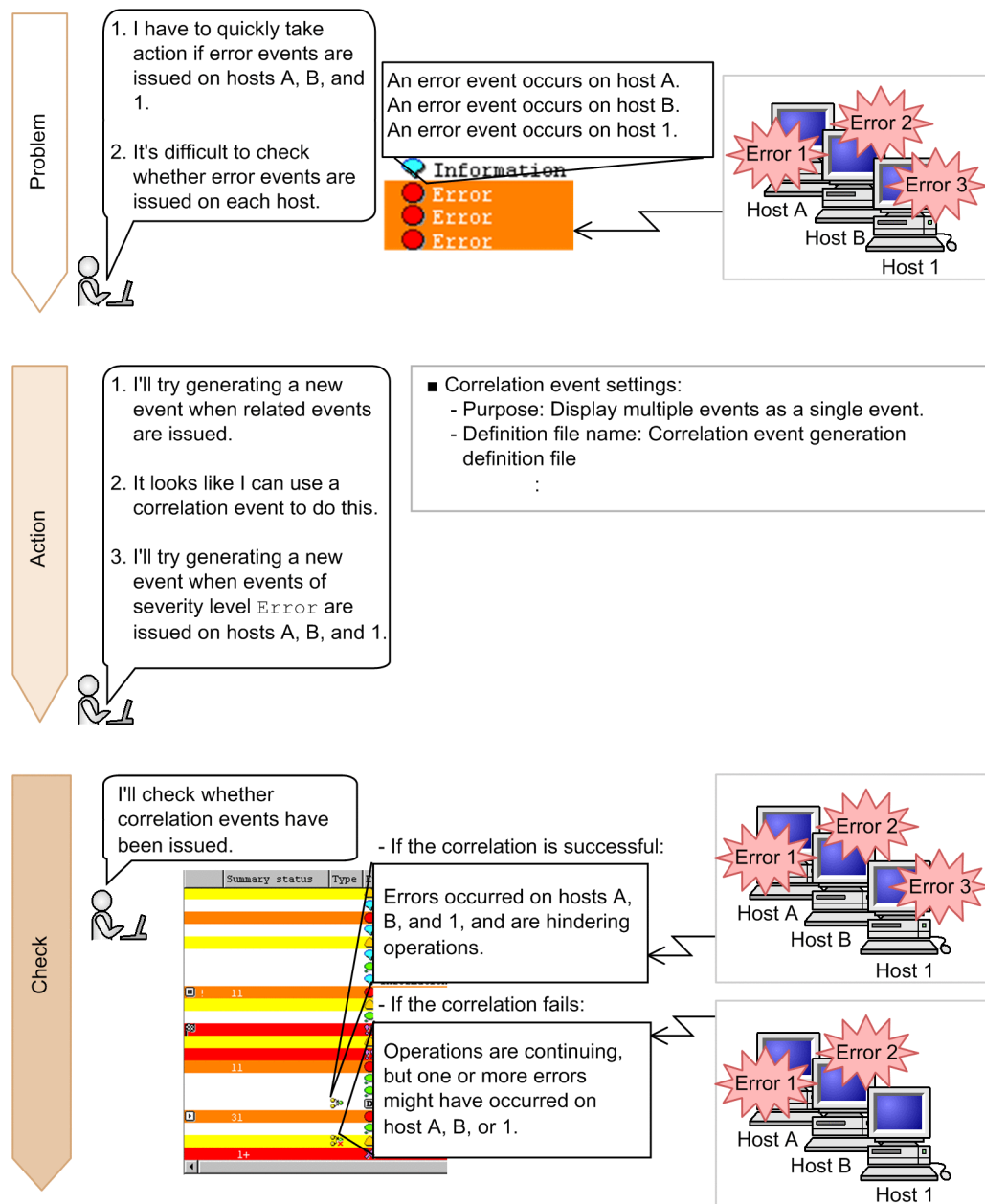
4

Detecting System Errors

This chapter explains how to display multiple events as a single event, and how to automatically execute commands based on the kind of system error that is detected.

4.1 Handling multiple events as a single event

Events that are issued are tied to certain occurrences, such as a system starting, or an error being generated. Depending on the sequence and combination in which such related events are issued, you might have to quickly take action appropriate for these events. To help identify important events that need to be dealt with quickly, you can treat multiple events as a single issue.



This manual describes how to specify settings to generate the following events when a correlation is successful or fails.

When the correlation is successful:

- Condition for a succeeded correlation:
Events of severity level `Error` are issued on hosts A, B, and 1 within 60 seconds.
- Event that is generated:
An event of severity level `Warning` with message `Errors occurred on hosts A, B, and 1, which are hindering operations`

When the correlation fails:

- Condition for a failed correlation:
The condition for a successful correlation does not exist.
- Event that is generated:
An event of severity level `Information` with message `Operations are continuing, but one or more errors might have occurred on host A, B, and/or 1`



Keywords:

correlation event, a large number of, consolidation, summary, event, succeeded, failed, generate, do not generate

4.1.1 Settings of the correlation event generation definition file to be created

The following provides details about the settings specified in the correlation event generation definition file that is created in [4.1.2 Associating events with correlation events](#).

Specification details

Specification	Description
<code>CON=E.SEVERITY==Error,B.SOURCESERVER==hostA</code> <code>CON=E.SEVERITY==Error,B.SOURCESERVER==hostB</code> <code>CON=E.SEVERITY==Error,B.SOURCESERVER==host1</code>	<p>Specifies the event conditions used in specifying a correlation event generation condition.</p> <p>Specify as follows to set error-level events issued on host A as a condition:</p> <ul style="list-style-type: none">• Set the severity level to match <code>Error</code>: <code>E.SEVERITY==Error</code>• Set the event-issuing host to match host A: <code>E.SOURCESERVER==hostA</code> <p>In a similar way, specify error-level events issued on hosts B and host 1 as conditions.</p>
<code>TYPE=combination</code>	<p>Specifies the type of correlation event generation condition that is defined. Specify as follows to set the combination of host A, host B, and host 1 as a condition:</p> <ul style="list-style-type: none">• <code>TYPE=combination</code>
<code>SUCCESS_EVENT=E.SEVERITY:Warning,B.MESSAGE:</code> <code>"Errors occurred on hosts A, B, and 1, which are hindering operations."</code>	<p>Specifies the correlation event that is generated if the correlation event generation condition is successful.</p> <p>Specify as follows to generate an event of severity level <code>Warning</code> with message <code>Errors occurred on hosts A, B, and 1, which are hindering operations</code>.</p> <ul style="list-style-type: none">• Specify the severity level <code>Warning</code>: <code>E.SEVERITY:Warning</code>• Specify the message to be displayed: <code>B.MESSAGE:Errors occurred on hosts A, B, and 1, which are hindering operations.</code>

Specification	Description
<pre>FAIL_EVENT=E.SEVERITY:Information,B.MESSAGE: "Operations are continuing, but one or more errors might have occurred on host A, B, and/or 1."</pre>	<p>Specifies the correlation event that is generated if the correlation event generation condition fails.</p> <p>Specify as follows to generate an event of severity level Information with message Operations are continuing, but one or more errors might have occurred on host A, B, and/or 1.</p> <ul style="list-style-type: none"> • Specify the severity level Information: E.SEVERITY:Information • Specify the message to be displayed: B.MESSAGE:Operations are continuing, but one or more errors might have occurred on host A, B, and/or 1.

4.1.2 Associating events with correlation events

To handle multiple events as a single error, you use correlation events. You can set correlation events in the correlation event generation definition file.

Prerequisites

The OS user who will execute the `jcoimdef` and `jcoegschange` commands must have Administrator or root permissions.

Procedure

1. Execute the following `jcoimdef` command to enable the correlation event generation function:
 - In Windows:

```
"Console-path\bin\jcoimdef" -egs ON
```
 - In Linux:

```
/opt/jplcons/bin/jcoimdef -egs ON
```
2. Using a text editor, open a correlation event generation definition file (example: `teigil.conf`), which is in the following location:
 - In Windows: Any folder
 - In Linux: Any directory

Use `.conf` as the extension of the correlation event generation definition file. In the file name, you can use alphanumeric characters and underscores (`_`).

3. Enter the following specifications:

```
-----
VERSION=2
[error_gradation]
CON=E.SEVERITY==Error,B.SOURCESERVER==hostA
CON=E.SEVERITY==Error,B.SOURCESERVER==hostB
```

```
CON=E.SEVERITY==Error,B.SOURCESERVER==host1
TYPE=combination
SUCCESS_EVENT=E.SEVERITY:Warning,B.MESSAGE:"Errors occurred on hosts A, B,
and 1, which are hindering operations."
FAIL_EVENT=E.SEVERITY:Information,B.MESSAGE:"Operations are continuing, but
one or more errors might have occurred on host A, B, and/or 1."
-----
```

4. Save the information specified in `teigil.conf`.

5. Execute the `jcoegschange` command on the manager to apply the settings of the correlation event generation definition file.

- In Windows:

```
"Console-path\bin\jcoegschange" -f correlation-event-generation-definition-file-name
```

- In Linux:

```
/opt/jplcons/bin/jcoegschange -f correlation-event-generation-definition-file-name
```

Specify the name of the correlation event generation definition file in relative or absolute path format. For example, if `teigil.conf` is stored in `C:\jplim` in Windows, specify `C:\jplim\teigil.conf` as the absolute path name of the correlation event generation definition file.

6. Restart JP1/IM - Manager.

The correlation event generation function is enabled when JP1/IM - Manager restarts.

Related topics

- *3.3 Issue of correlation events in the Overview and System Design Guide*
- *4.6 Setting correlation event generation in the Configuration Guide*
- *5.1.10 Displaying and handling correlation events in the Administration Guide*
- *1. jcoegschange in the manual Command and Definition File Reference*
- *Correlation event generation definition file in 2. Definition Files in the manual Command and Definition File Reference*

4.1.3 Verifying that the correlation event is generated

After you have finished specifying the correlation event conditions, verify that the correlation event is generated according to your specifications. The following describes how to generate a correlated event and then check the icon displayed for **Type**.

Prerequisites

Type must be set as an item displayed in the event list in the Preferences window, which is displayed by selecting **Main Menu**, **Options**, and then **Preferences**.

Procedure

1. Execute the following `jevsend` command on host A to issue an error event:


- In Windows:

```
"Base-path\bin\jevsend" -e SEVERITY=Error
```

- In Linux:
`/opt/jplbase/bin/jevsend -e SEVERITY=Error`


In a similar way, execute the `jevsend` command on hosts B and I to issue error events.

If error events are issued on hosts A, B, and I within 60 seconds, a correlation event is generated, and then either of the following icons appears in the **Type** column of the event list.

Type	Description
	This correlation event is generated if a correlation event generation condition exists.

2. Execute the following `jevsend` command on host A to issue an error event, and then wait 60 seconds.

Because an error event is not issued on any host other than host A within 60 seconds, a correlation event is generated, and then either of the following icons appears in the **Type** column of the event list.

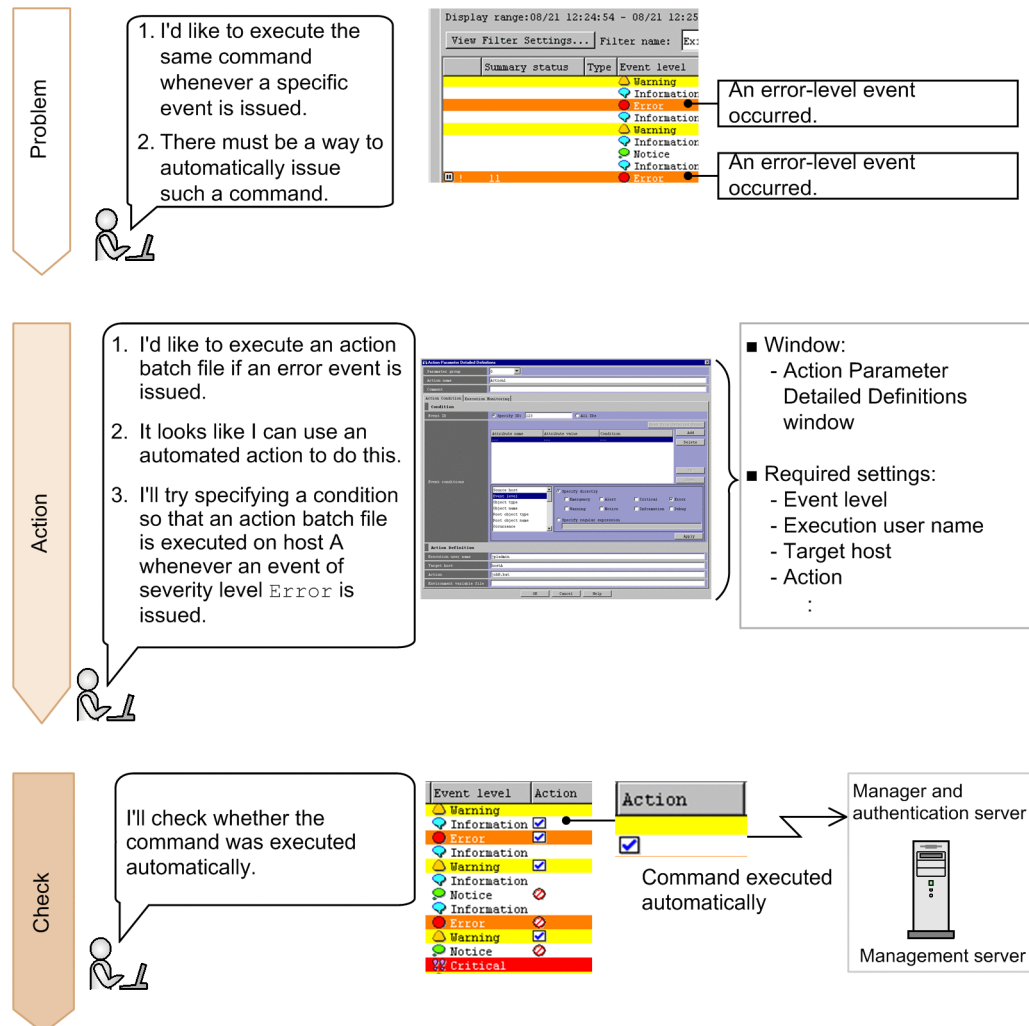
Type	Description
	This correlation event is generated if a correlation event generation condition does not exist.

Related topics

- *5.1.10 Displaying and handling correlation events in the Administration Guide*
- *2.22 Preferences window in the manual GUI Reference*

4.2 Automatically executing a command when a specific event is generated

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 specify that the error action batch file (`errortaisaku.bat`) in `C:\jplim` is executed on the management server (Windows computer) when an event of severity level **Error** is issued. Prepare the error action batch file in advance.

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 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\(2\) 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

4.2.1 Using the automated action function to execute a command

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

A JP1 user who wants to define automated actions must have JP1_Console_Admin permissions.

Procedure

1. 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. Define the automated actions according to the following figure:

Condition: Specify the condition of events for which an automated action is executed.
In this example, specify the condition as shown below to set events of severity level **Error** as the condition:

Source host: Specify directly
☐ Emergency ☐ Alert ☐ Critical ☒ Error
☐ Warning ☐ Notice ☐ Information ☐ Debug
☐ Specify regular expression

Action definition: Specify the automated action that is executed when an event specified in **Condition** occurs.
In this example, enter the following settings:

- **Execution user name:** Set the system administrator as the executing user.
Example: jpladmin
- **Target host:** Perform the action on the management server.
Example: admin
- **Action:** Execute the error action batch file (errortaisaku.bat) stored in C:\jplim.
Example: C:\jplim\errortaisaku.bat

4. In the Action Parameter Detailed Definitions window, click the **OK** button. The Action Parameter Definitions window appears.

5. In the Action Parameter Definitions window, click the **Apply** button.
The specified settings are updated.

Related topics

- [2.31.1 Action Parameter Detailed Definitions window](#) in the manual *GUI Reference*

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

After you have finished specifying the automated action, check whether the command was executed according to your specifications. The following describes how to verify that an automated action that executes the action batch file (`errortaisaku.bat`) on the management server (Windows computer) is triggered when an event of severity level `Error` is issued.

Prerequisites


OS user mapping must be configured according to the procedure in [2.2.1 Using the user mapping feature to map a JPI user account to an OS user account](#).

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: "Base-path\bin\jevsend" -e SEVERITY=Error• In Linux: /opt/jplbase/bin/jevsend -e SEVERITY=Error

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

In the **Action** column in the event list, an executed action icon () is displayed for the event that triggered the automated action.

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

Related topics

- [2.1 Overview of the Event Console window](#) in the manual *GUI Reference*
- [2.34 Action Log window](#) in the manual *GUI Reference*

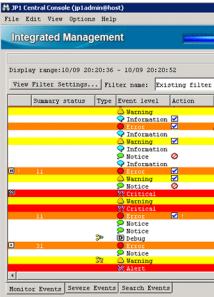
- 2.38 *Execute Command* window in the manual *GUI Reference*

4.3 Preventing an action that was already executed once from being executed again during a set period of time

An automated action that is triggered by an event is executed automatically, thereby reducing the system administrator's workload. However, if a large number of events that trigger the automated action are issued within a short period of time, the action is executed repeatedly. To prevent actions from being executed unnecessarily, you can prevent an action that has already been executed once from being executed again during a set period of time.

Problem

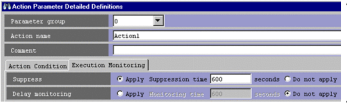
1. If I set up an error action batch file to be executed, it will be executed each time the same event occurs.
2. The error action batch file needs to be executed only once. There has to be a way to deal with this.



The action is executed every time the same event occurs.

Action

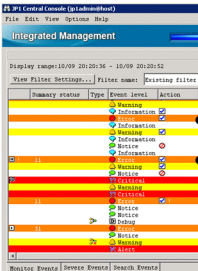
1. I'll try preventing an automated action from being executed repeatedly.
2. It looks like I can use automated action suppression to do this.
3. I'll try specifying conditions so that once the error action batch file is executed, it will not be executed again for 10 minutes.



- Window:
 - Action Parameter Detailed Definitions window
- Required settings:
 - Suppress
 - :

Check

I'll confirm that automated action suppression prevents an error action batch file already executed from being executed again for a specified period.



Executed

Execution of error action batch file

Execution of error action batch file

Not executed

This manual describes how to specify the system so that the automated action specified in [4.2.1 Using the automated action function to execute a command](#) is not executed for 10 minutes (600 seconds).



Tip:

To prevent automated actions defined for events that match repeated event conditions from being executed:

You can use the Repeated Event Condition Settings window to prevent automated actions defined for events that match repeated event conditions from being executed. For details about the Repeated Event Condition Settings window, see *2.17 Repeated Event Condition Settings window* in the manual *GUI Reference*.



Keywords:

automated action, generate, a large number of, time, suppression

4.3.1 Using automated action suppression to prevent an action from being executed

You can use automated action suppression to prevent an action that was already executed from being executed again for a set period of time. Set up automated action suppression in the Action Parameter Detailed Definitions window.

Prerequisites

The following conditions must be satisfied:

- An automated action has been defined according to the procedure in *4.2.1 Using the automated action function to execute a command*.
- A JP1 user who wants to define the automated action has JP1_Console_Admin permissions.

Procedure

1. In the Action Parameter Definitions window, in **Action parameters**, select the automated action specified in *4.2.1 Using the automated action function to execute a command*, and then click the **Edit** button. The Action Parameter Detailed Definitions window appears.
2. In the Action Parameter Detailed Definitions window, select the **Execution Monitoring** tab, and then specify the settings as shown below:

To suppress an automated action, specify a suppression time (in seconds).
For this example, enter the following setting to specify a suppression time of 10 minutes (600 seconds):
Example: 600

Suppress ☒ Apply Suppression time 600 seconds ☐ Do not apply

3. In the Action Parameter Detailed Definitions window, click the **OK** button to display the Action Parameter Definitions window.
4. In the Action Parameter Definitions window, click the **Apply** button.
The specified settings are updated.

Related topics

- *5.4.4 Suppressing identical actions* in the *Overview and System Design Guide*

- 4.5.4 *Setting suppression of automated action execution* in the *Configuration Guide*
- 2.31.1 *Action Parameter Detailed Definitions* window in the manual *GUI Reference*

4.3.2 Verifying that the same action is not executed repeatedly

After you have finished setting up suppression of automated actions, use the procedure below to make sure that the same action is not executed repeatedly.

Prerequisites

OS user mapping has been configured according to the procedure in [2.2.1 Using the user mapping feature to map a JPI user account to an OS user account](#).

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: "Base-path\bin\jevsend" -e SEVERITY=Error • In Linux: /opt/jplbase/bin/jevsend -e SEVERITY=Error


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

3. Repeat step 2.




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

4. Wait 10 minutes, and then repeat step 2.

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

If the automated action is suppressed, the icon () indicating that the automated action has been suppressed is displayed in the **Action** column in the event list.

5. Verify that the following is displayed in the **Action column** in the event list.

- The first time the command is executed:
The icon () indicating an executed action is displayed.
- The second time the command is executed:
The icon () indicating that the automated action has been suppressed is displayed.
- The third time the command is executed:
The icon () indicating an executed action is displayed because the ten minutes specified as the suppression time have elapsed.

Related topics

- *2.1 Overview of the Event Console window in the manual GUI Reference*
- *2.38 Execute Command window in the manual GUI Reference*

5

Troubleshooting System Errors

This chapter explains how to display previously-issued events to investigate a system error, and how to register and display the corrective action to take for an error.

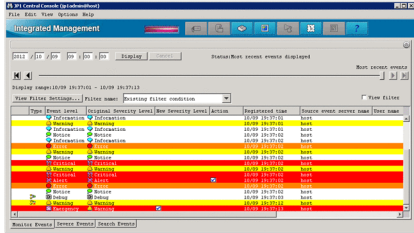
5.1 Checking the status of previously-issued events

After a given period of monitoring, error-related events that were issued previously might be issued again. Even if you want to check the corrective action you took in the past for such an event, the event might no longer be displayed in the event list.

In this section, we will display events that are no longer in the event list to check the status of previously-issued events.

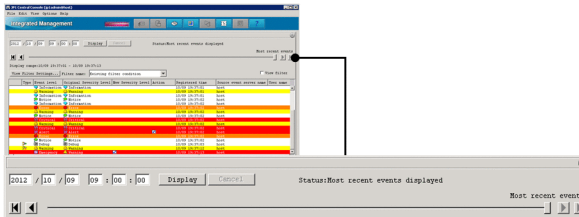
Problem

I'd like to check past events that are no longer displayed on the **Monitor Events** page.



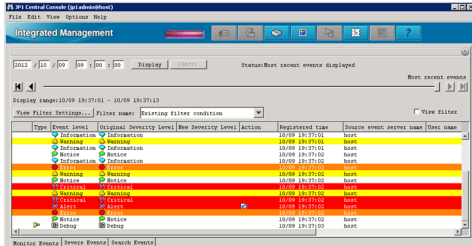
Action

1. I'll try entering conditions to show events that are no longer displayed.
2. It looks like I can do this using the event display start-time specification function.



Check

OK. Now I'll check to see whether events that occurred on the date and time I want to check are displayed.



To display events, you can use the event display start-time specification function on the **Monitor Events** and **Severe Events** pages of the Event Console window, or the slider.



Tip:

Attaching a memo to an event:

By attaching a memo to an event, you can make a note on the status of the investigation for the event. For details about how to attach a memo, see *3.10 Setting memo entries* in the *Overview and System Design Guide*.

If the position of the slider is reset:

If auto-scrolling is enabled, every time a new event is registered, the position of the slider is reset to display the new event. If you do not want the slider to move, disable auto-scrolling. For details about how to enable or disable auto-scrolling, see *2.1 Overview of the Event Console window* in the manual *GUI Reference*.



Keywords:

event, search, display time, Monitor Events page, event display start-time specification function, past

5.1.1 Using the event display start-time specification function to display events based on a specified time

You can use the event display start-time specification function to display events that are no longer displayed on the **Monitor Events** page of the Event Console window. Assuming that the earliest event displayed on the **Monitor Events** page was issued at 10:00:00 on April 1, 2014, the following describes how to display events issued before this time.

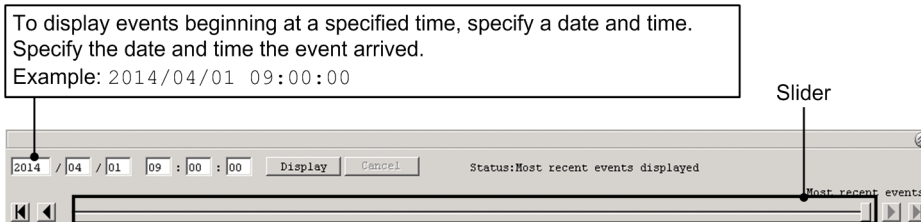
Prerequisites

The integrated monitoring database must be configured and enabled according to [1.3.4\(3\) Setting up an integrated monitoring database \(for Windows\)](#) or [1.4.4\(3\) Setting up an integrated monitoring database \(for Linux\)](#).[#]

#: The integrated monitoring database needs to have already been configured at the time the events were acquired.

Procedure

1. According to the following figure, specify an event display start time that is before the earliest event-arrival time displayed on the **Event Monitor** page.



2. Click the **Display** button in the area for specifying the event display start time. Events that were issued after the specified time are displayed in the event list.

Related topics

- [5.1.13 Displaying events by specifying time in the Administration Guide](#)
- [2.2 Monitor Events page in the manual GUI Reference](#)

5.1.2 Verifying that events are displayed from the specified display time

After you specify the time in the area for specifying the event display start time, check whether the event list displays events beginning from the time you specified. The procedure below applies when the display time is specified according to [5.1.1 Using the event display start-time specification function to display events based on a specified time](#).

Prerequisites

The display time must be specified according to [5.1.1 Using the event display start-time specification function to display events based on a specified time](#).

Procedure

1. Verify that the event list displays events issued after the specified time

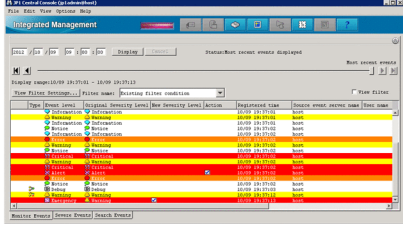
5.2 Searching for events

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

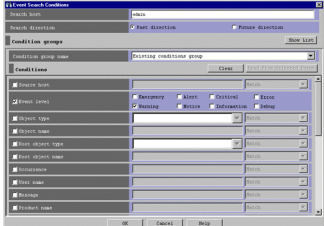
I'd like to find out what type of error-level events were issued in the past.



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.

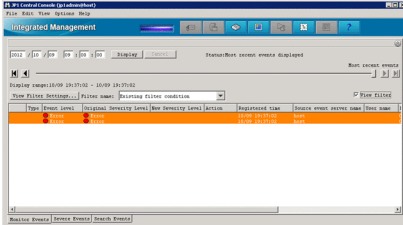


■ Window:
- Event Search Conditions window

■ 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

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 [1.3.4\(3\) Setting up an integrated monitoring database \(for Windows\)](#) or [1.4.4\(3\) 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:

The screenshot shows the 'Event Search Conditions' dialog box. The 'Search host' field contains 'admin'. The 'Search direction' has 'Past direction' selected. Under 'Condition groups', 'Existing conditions group' is selected. In the 'Conditions' section, 'Source host' is set to 'Match'. Under 'Event level', 'Warning' is selected, while 'Emergency', 'Alert', 'Critical', 'Error', 'Notice', 'Information', and 'Debug' are not. A callout box points to the 'Warning' checkbox with the text: 'Specify the event search condition. In this example, specify an event of severity level Warning. Example: Select **Warning**.'

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

- *3.6 Searching for events in the Overview and System Design Guide*
- *5.5.1 Search method in the Administration Guide*

5.2.2 Verifying that events were found

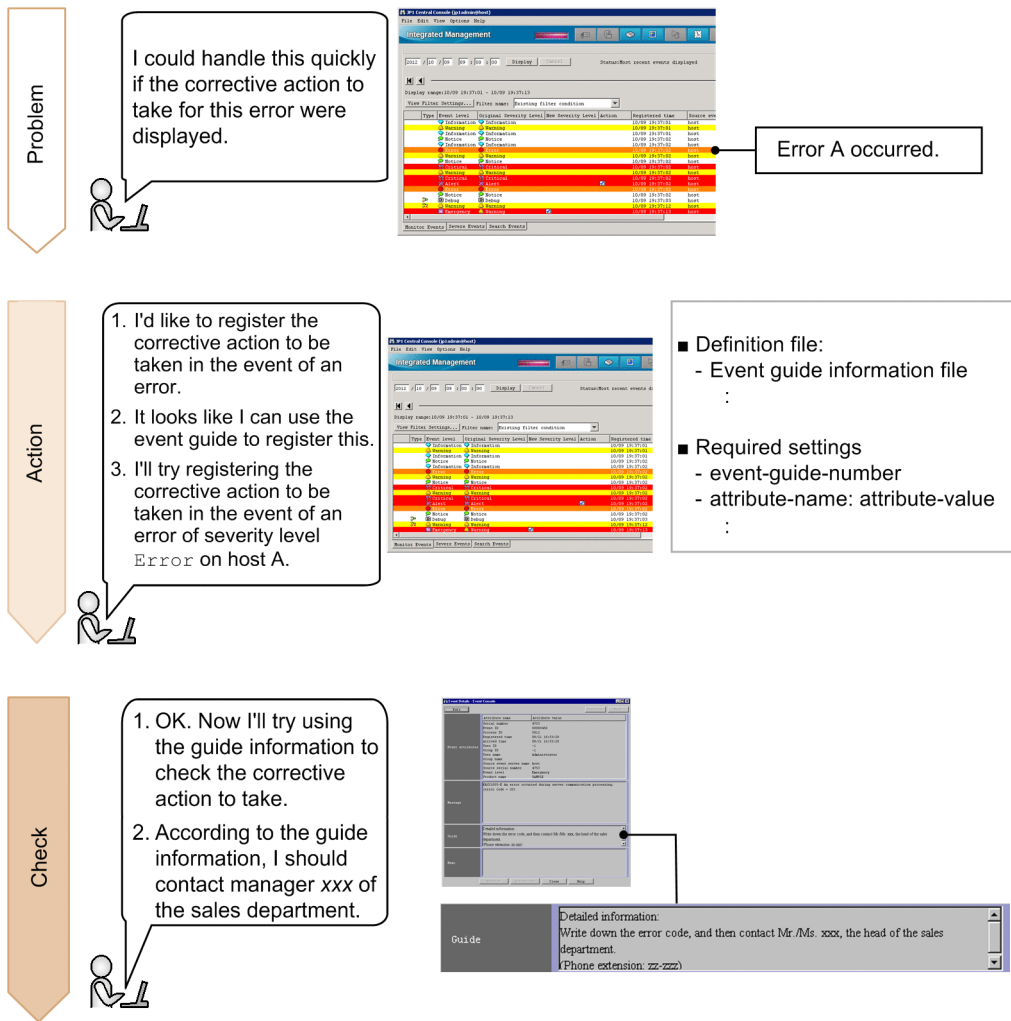
After you specify the event search conditions, check whether the events you wanted to find are displayed on the **Search Events** page. The procedure below applies when you searched for events according to *5.2.1 Using the search events function to search for events that match a specified condition*.

Procedure

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

5.3 Registering corrective action to be used as a guide for known errors

It is very difficult for the system administrator to be sure that the most appropriate action is taken in every single error case. However, by registering corrective actions for errors, if the same error occurs again, the corrective action can be displayed, allowing the system administrator to keep better track of appropriate actions.



Tips:

To clarify the corrective actions:

If JP1/Integrated Management - Navigation Platform is linked, the flow of a job can be displayed as a flowchart. A step-by-step guide for the procedure required in the flowchart can also be displayed. By visualizing the flow of the job and the operation procedure, you can identify the corrective actions to be taken.

To start an application that is linked to an event:

Select an event, and then, in a separate window, start the application that has been linked to the displayed event. For details about how to set up this link, see *4.14 Setting monitor startup for linked products* in the *Configuration Guide*.

To identify the corrective actions to be taken:

If JP1/Integrated Management - Service Support is linked, the person in charge of troubleshooting and the deadline and priority of the job can be specified in advance for each event. You can visualize the process required to solve a problem, and identify who must do what, and by when.

For details, see the *Job Management Partner 1/Integrated Management - Service Support Configuration and Administration Guide*.



Keywords:

corrective action, event, event guide, error, event guide information

5.3.1 Settings in the event guide information file to be created

The following provides details about the settings specified in the event guide information file that is created in [5.3.2 Using the event guide function to register the corrective action to be taken](#).

Specification details

Specification	Description
EV_COMP=E.SEVERITY>Error EV_COMP=B.SOURCESERVER:hostA	Specifies conditions for comparing events: Specify the conditions as follows: <ul style="list-style-type: none">Set the severity level to Error: EV_COMP=E.SEVERITY>ErrorSet the event-issuing host to host A: EV_COMP=B.SOURCESERVER:hostA
EV_GUIDE=Detailed Information\nWrite down the error code, and then contact Mr./Ms. xxx, the head of the sales department\nPhone extension:zz-zzz	Specifies the message to be displayed in the event guide.

5.3.2 Using the event guide function to register the corrective action to be taken

You can use the event guide function to register (for later display) the corrective action to be taken for events. To use the event guide function, you create an event guide information file named `jco_guide.txt`.

Prerequisites

None

Procedure

1. Edit the event guide information file so that the action to be taken is displayed if an event of severity level `Error` is issued on host A in the sales department.

Enter the following specifications in `jco_guide.txt`:

```
-----  
DESC_VERSION=1  
[EV_GUIDE_1]  
#Contact Information in Case of Error on Host A  
EV_COMP=E.SEVERITY>Error  
EV_COMP=B.SOURCESERVER:hostA
```

```
EV_GUIDE=Detailed Information\nWrite down the error code, and then contact  
Mr./Ms. xxx, the head of the sales department\nPhone extension:zz-zzz  
[END]
```

2. Save the event guide information file in the following location:

- Windows:
 "**Console-path**\conf\guide\"
- Linux:
 /etc/opt/jplcons/conf/guide/

3. Restart JP1/IM - Manager to register the defined settings.

4. Restart JP1/IM - View.

Related topics

- [4.8.1 How to edit event guide information in the Configuration Guide](#)
- [Event guide information file \(jco_guide.txt\) in 2. Definition Files in the manual Command and Definition File Reference](#)

5.3.3 Verifying that the corrective action is registered

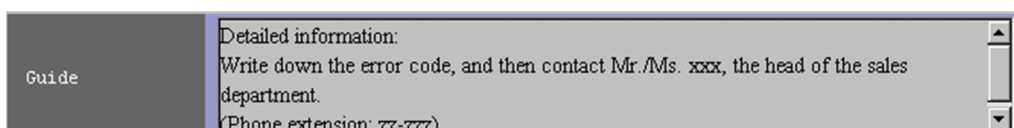
The following describes how to verify that the corrective action is registered for the event after you have set the event guide information by using the event guide function.

Prerequisites

The event guide function must be set up according to [5.3.2 Using the event guide function to register the corrective action to be taken](#).

Procedure

1. Execute the following `jevsend` command on host A to issue an error-level event:
 - Windows:
 "**Base-path**\bin\jevsend" -e SEVERITY=Error
 - Linux:
 /opt/jplbase/bin/jevsend -e SEVERITY=Error
2. Select the issued event in the event list and, in the Event Console window, select **View**, and then **Event Details**. Event guide information for the selected event is displayed in the Event Details window.
3. For this example, verify that the following is displayed:



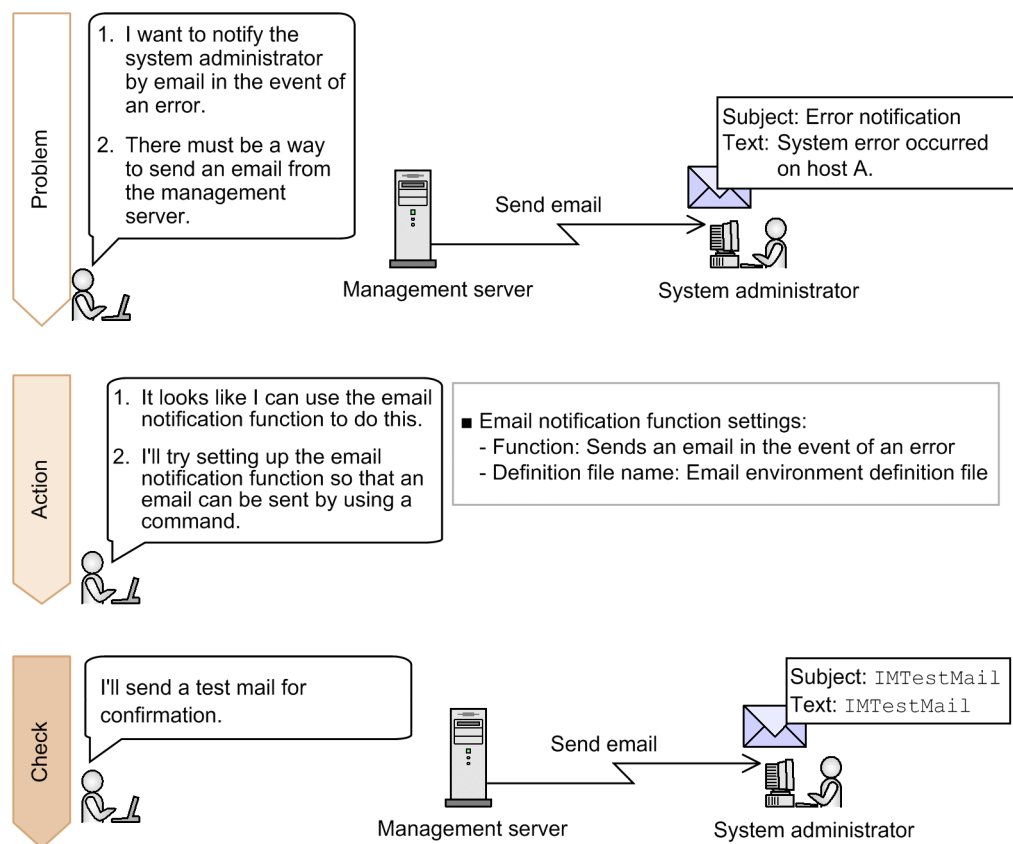


Appendixes

A. Settings for Using the Email Notification Function (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 details about the settings specified in the email environment definition file that is created in [A.1\(2\) 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 (_)
SmtServer=host-name-or-IP-address-of-the-SMTP-server	Host name or IP address of the SMTP server	Specifies the host name or IP address of the SMTP server that is connected for sending email. IP addresses are supported only for IPv4. You can specify only one SMTP server.
AuthMethod=SMTP	Authentication method when sending an email	Specifies the authentication method used on the mail server when sending an email. NONE: No authentication <ul style="list-style-type: none"> • POP: POP before SMTP authentication • SMTP: SMTP-AUTH authentication (LOGIN/PLAIN) The default is NONE.
AuthUser=authentication-account-name	Authentication account name used for POP before SMTP authentication or SMTP-AUTH authentication	Specifies the authentication account name used for POP before SMTP authentication or SMTP-AUTH authentication. You can use a string of 1 to 255 bytes. The default is a null character ("").

(2) 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
- SmtServer
SmtServer=**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 **new-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**
- *7.3.1 Basic information about firewalls in the *Configuration Guide**

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

This subsection describes how to verify that the email notification function has been set up correctly. In this subsection, you can check whether a sent email has arrived at the destination by executing the `jimmail` command from JP1/IM - Manager. Note that you must first set up the environment definition file according to [A.1\(2\) Setting up the email notification function \(Windows only\)](#).

Prerequisites

The following conditions must be satisfied:

- The email notification function has been set up according to [A.1\(2\) 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

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 [4.2.1 Using the automated action function to execute a command](#).

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	jpladmin
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)	jpl_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

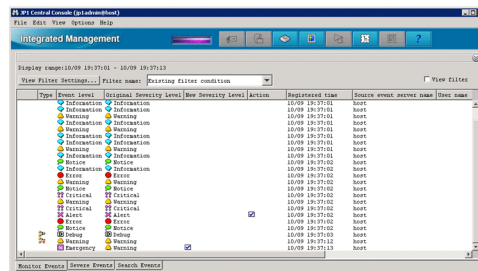
- [3.16.5 Inheriting event information when a command is executed](#) in the *Overview and System Design Guide*

B. Visual Monitoring to Ascertain the Extent of 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.

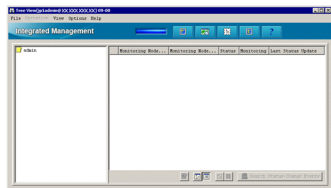
Problem

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

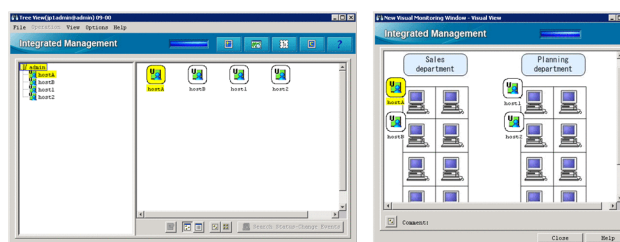
1. It looks as if I can use the Central Scope functions to do this.
2. Well, let's try setting up the conditions for monitoring events visually.



- 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 [1.2.1 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. The following describes how to set up the central scope to enable its function. Perform this operation on managers.

Prerequisites

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

Procedure

1. Stop the JP1/IM - 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/IM-Manager service.
5. Execute the following `jco_spmc_status` command to make sure that the central scope service is running:
 - In Windows:
`"Console-path\bin\jco_spmc_status"`
 - In Linux:
`/opt/jp1cons/bin/jco_spmc_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. The following describes how to do this.

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.

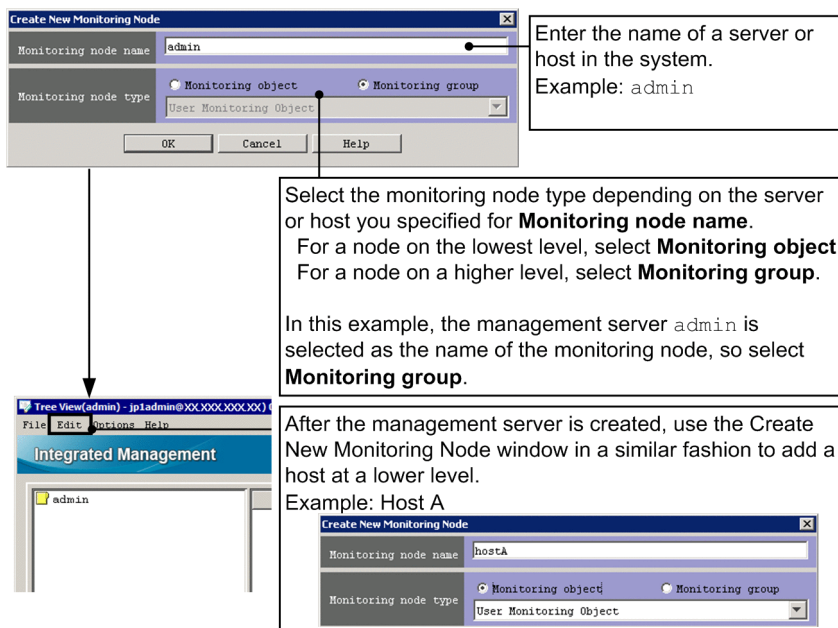
Procedure

1. From the Windows **Start** menu, select **Programs, JP1_Integrated Management - View**, and then **Edit Monitoring Tree**. The Monitoring Tree (Editing) window appears.

After logging in to the central scope, you can also display the Monitoring Tree (Editing) window from the Monitoring Tree window.

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

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



4. In the Monitoring Tree (Editing) window, select **File**, and then **Update Server Tree** to apply the edited tree data to the Monitoring Tree window.

When the Login window appears, enter the JP1 user name and password registered on the authentication server.

Related topics

- 5.3.1 *Opening the Monitoring Tree (Editing) window in the Configuration Guide*
- 5.3.3 *Generating a monitoring tree automatically in the Configuration Guide*
- 4.1 *Logging on to JP1/IM - Manager in the Administration Guide*
- 1.2 *Login window in the manual GUI Reference*
- 3.1 *Overview of the Monitoring Tree window in the manual GUI Reference*
- 3.15 *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 [1.2.1 Overview of a basic configuration system](#).

Prerequisites

Monitoring nodes must exist 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.

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.

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

- *3.9 Properties window in the manual GUI Reference*
- *3.12 Status-Change Condition Settings window in the manual GUI Reference*
- *3.13 Common Condition Settings window in the manual GUI Reference*
- *3.14 Common Condition Detailed Settings window in the manual GUI Reference*

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

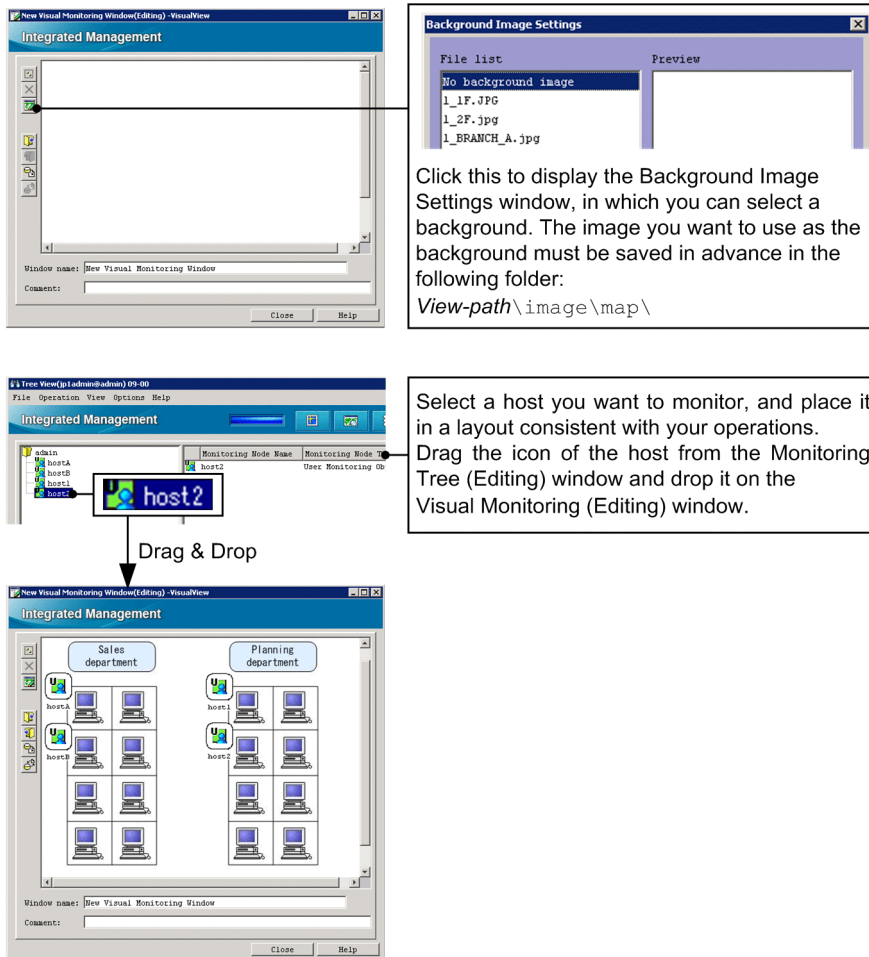
To display hosts in a map format, you first create a Visual Monitoring window. The following describes how to create the Visual Monitoring window from the Visual Monitoring (Editing) window.


Prerequisites

Monitoring nodes must exist in the Monitoring Tree window.

Procedure

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



5. Click the  (Update the Visual Monitoring) button to apply the settings of the Visual Monitoring window to the manager.

When the Login window appears, enter the JPI user name and password registered on the authentication server.

Related topics

- [3.4 Visual Monitoring \(Editing\) window in the manual GUI Reference](#)
- [3.5 Visual Monitoring window in the manual GUI Reference](#)
- [5.4.1 Opening an edit window for the Visual Monitoring window in the Configuration Guide](#)
- [5.4.3 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

After you have finished configuring the central scope, use the procedure below to check whether you are able to monitor events in both map format and tree format, in a manner consistent with the system configuration. The following describes how to issue events on host A shown in [1.2.1 Overview of a basic configuration system](#).

Prerequisites

OS user mapping must be completed according to the procedure in [2.2.1 Using the user mapping feature to map a JPI user account to an OS user account](#).

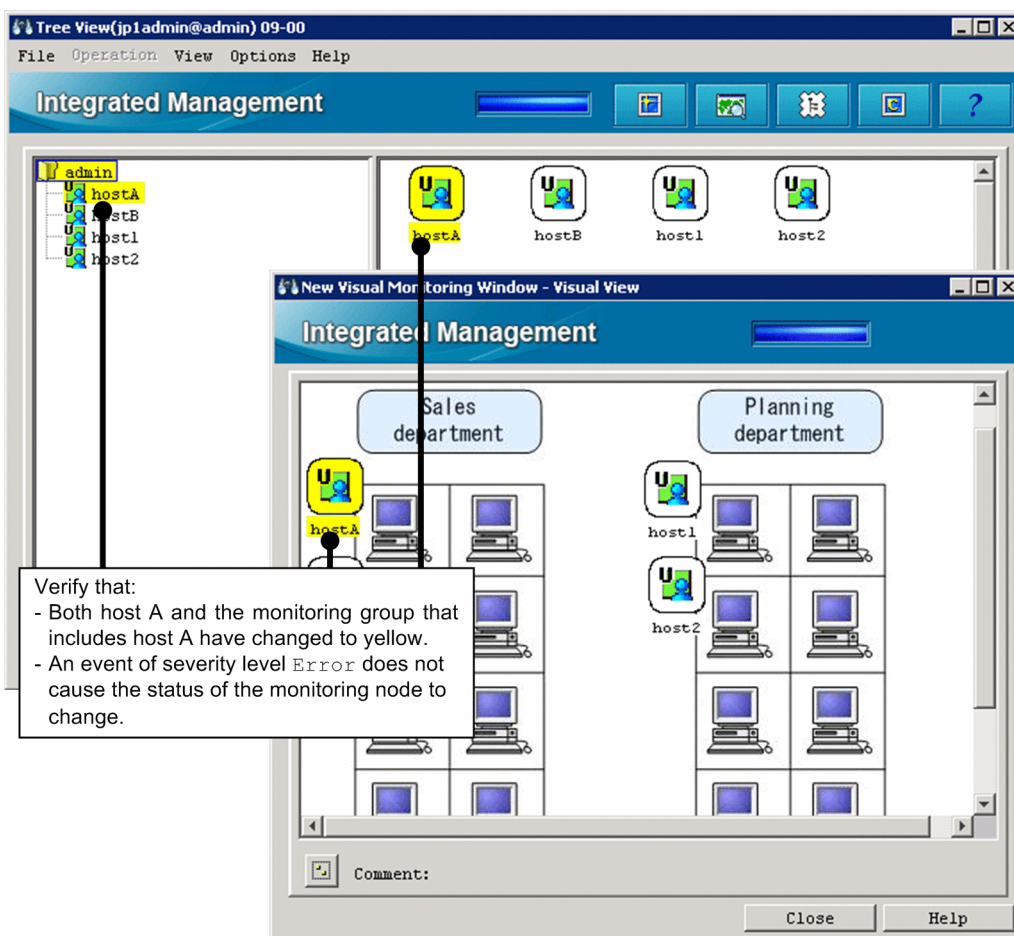
Procedure

1. In the Event Console window, click the **Execute Command** button. The Execute Command window appears.
2. Follow the procedure in [2.2.2 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/jplbase/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: <code>"Base-path\bin\jevsend" -e SEVERITY=Error -m Error Event Issued</code> In Linux: <code>/opt/jplbase/bin/jevsend -e SEVERITY=Error -m Error Event Issued</code>

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

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

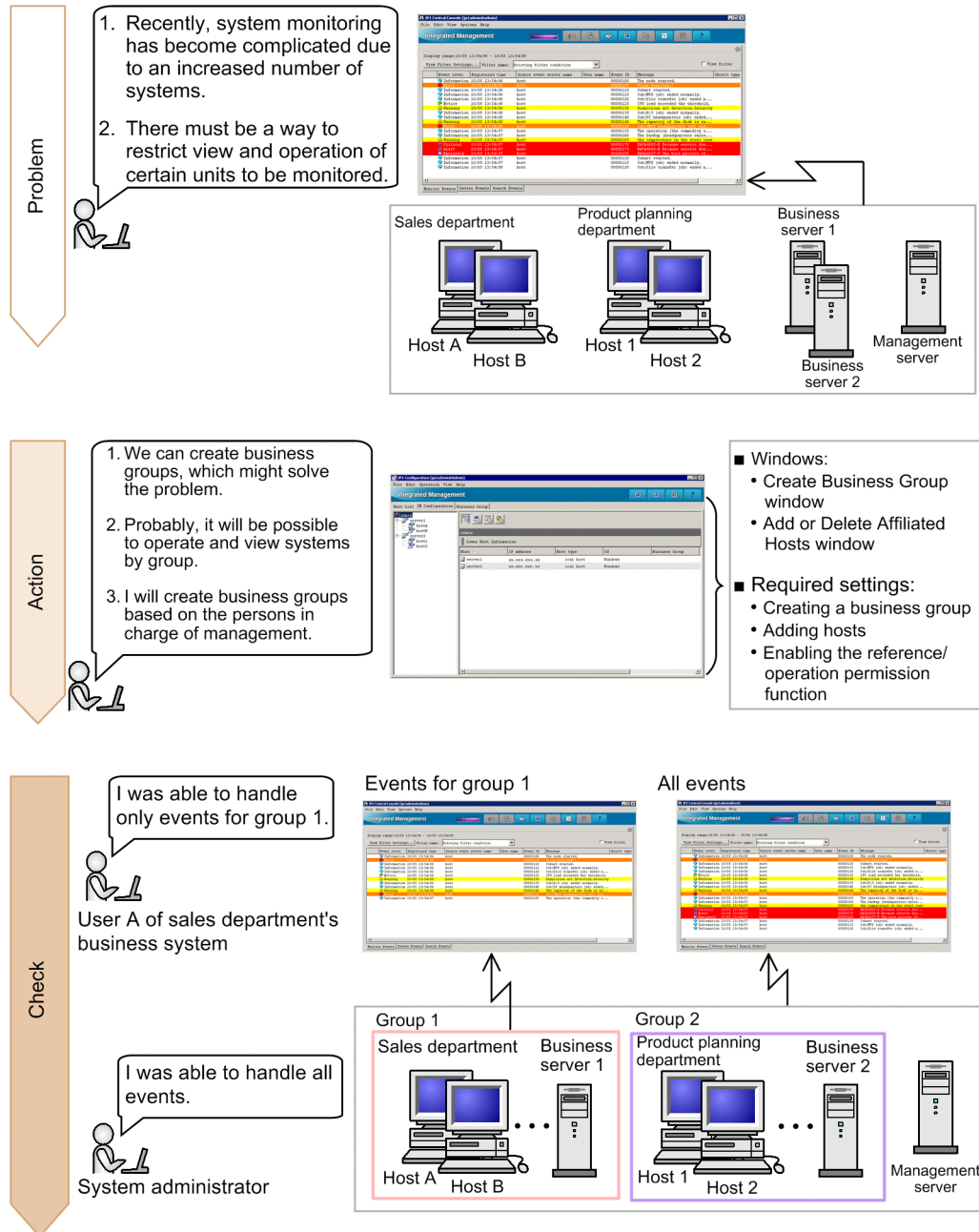
For this example, verify that the status of host A or the monitoring group that includes host A does not change when an event of severity level `Error` is issued.

Related topics

- *2.1 Overview of the Event Console window in the manual GUI Reference*
- *2.38 Execute Command window in the manual GUI Reference*

C. Monitoring Systems on a Business Group Basis

By making groups for each business system, you can restrict what operations users can perform with JP1/IM, and what information users can view with JP1/IM. For example, a system administrator might be able to monitor and operate all business groups, and user A of the sales department might be able to operate only the department's business system. In this section, we will monitor business systems on a group basis.



Tip:

To monitor events visually:

Business groups can also be monitored by using the Monitoring Tree window of the central scope. For details about how to use this window, see 3.4.4(2) *Applying business group information and monitoring group information to the Central Scope monitoring tree* in the *Configuration Guide*.



Keywords:

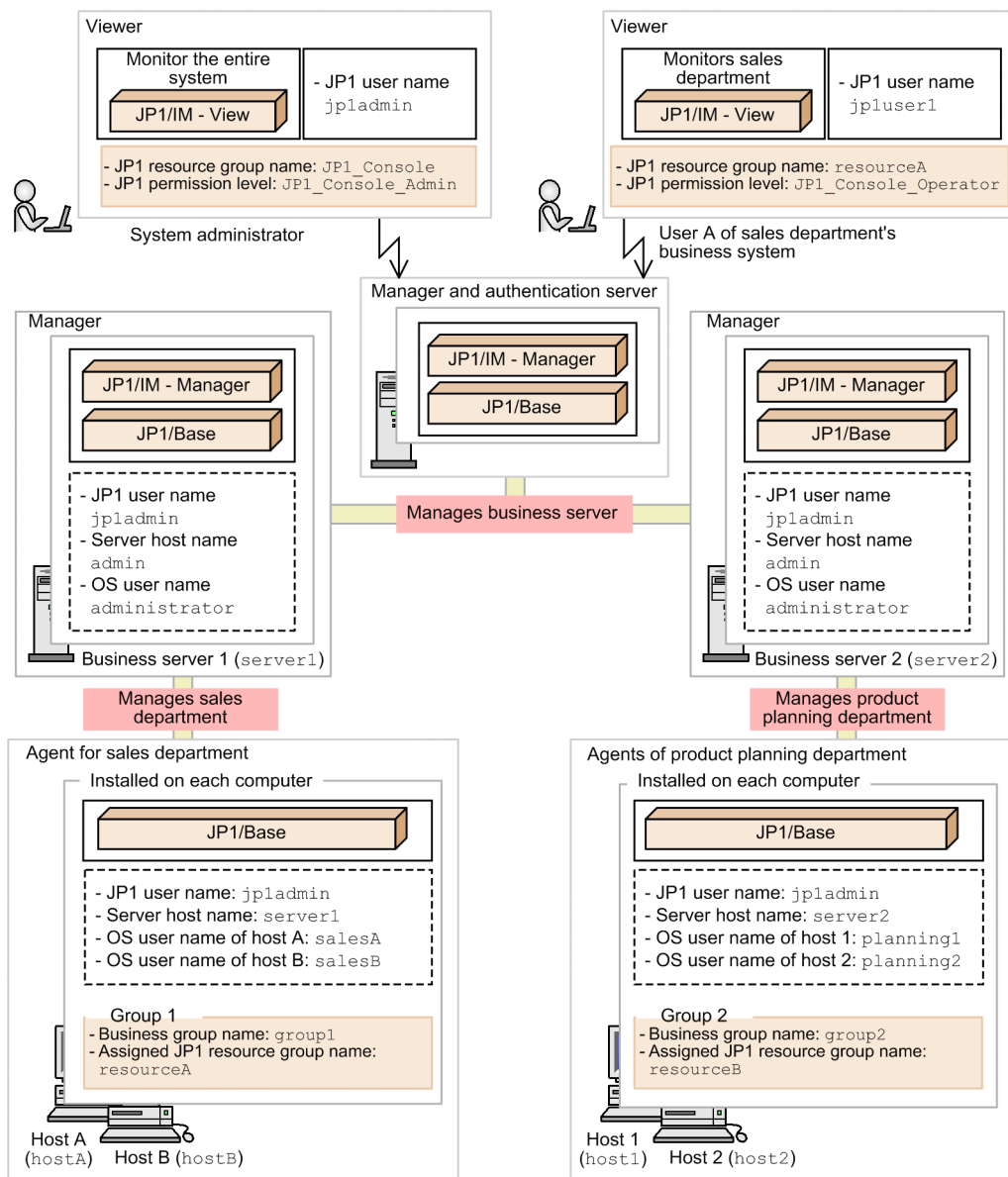
business group, monitoring group, independent monitoring, JP1 user, JP1 resource group, JP1 permission level, restrictions on viewing and operating business groups, multi-tenant

C.1 Procedure for creating business groups

To provide groups of business systems, you need to create *business groups*. A business group is a unit of hosts grouped in IM Configuration Management based on a certain purpose. Use the following procedure to create business groups:

1. Specify the JP1 resource group names and JP1 permission levels for JP1 users of business groups.
2. Enable restrictions on viewing and operating business groups.
3. Create business groups.
4. Register hosts.

The following describes how to create business groups for business systems in the configuration shown below, which is changed from the basic system configuration shown in [1.2.1 Overview of a basic configuration system](#).



Legend:

[] : Information set by means of user mapping

[] : Business group settings

JP1 user name : JP1 user name used to log in

Note that the system hierarchy is assumed to have been configured as shown in the above figure by using IM Configuration Management.

(1) Settings of the user permission level file to be created

The table below shows the information specified in the user permission level file created in *C.1(2) Specifying the JP1 resource group names and JP1 permission levels for JP1 users of business groups*. The table also shows the corresponding JP1 user name, JP1 resource group name, and JP1 permission level.

Specification details

Specification in the user permission level file	JP1 user name, JP1 resource group name, and JP1 permission level that will be set
jpladmin:JP1_Console=JP1_Console_Admin,JP1_C F_Admin	JP1 user name: jpladmin

Specification in the user permission level file	JP1 user name, JP1 resource group name, and JP1 permission level that will be set
	JP1 resource group name: JP1_Console JP1 permission levels: - JP1_Console_Admin - JP1_CF_Admin
jpluser1:sigenA=JP1_Console_Operator	JP1 user name: jpluser1 JP1 resource group name: sigenA JP1 permission level: JP1_Console_Operator

(2) Specifying the JP1 resource group names and JP1 permission levels for JP1 users of business groups

To limit the business groups that can be viewed and operated by JP1/IM users, you need to specify the JP1 resource group name and JP1 permission level for each JP1 user. To do this, perform the following procedure on the primary authentication server of the system.

Prerequisites

The following conditions must be satisfied:

- The primary authentication server is set up.
- The JP1 user is registered on the primary authentication server.
- The OS user who will execute the `jbsaclreload` command has Administrator or root permissions.

Procedure

1. On the primary authentication server, specify settings in the JP1/Base user permission level file (JP1_UserLevel) as follows:

```
-----
jpladmin:JP1_Console=JP1_Console_Admin,JP1_CF_Admin
jpluser1:sigenA=JP1_Console_Operator
-----
```

The user permission level file is stored in the following location:

In Windows:

Base-path\conf\user_acl\

In Linux:

/etc/opt/jplbase/conf/user_acl/

2. Execute the following `jbsaclreload` command to apply the settings of the user permission level file to JP1/Base on the primary authentication server:
 - In Windows:
 "*Base-path*\bin\jbsaclreload"
 - In Linux:

/opt/jplbase/bin/jbsaclreload

Related topics

- Description of how to configure user management in the *JP1/Base User's Guide*

(3) Enabling restrictions on viewing and operating business groups

To limit the business groups that can be viewed and operated by JP1/IM users, you enable restrictions on viewing and operating business groups. Perform this operation on managers.

Prerequisites

The following conditions must be satisfied:

- The integrated monitoring database has been configured and enabled according to *1.3.4(3) Setting up an integrated monitoring database (for Windows)* or *1.4.4(3) Setting up an integrated monitoring database (for Linux)*.
- The IM Configuration Management database has been configured and enabled according to *1.3.4(4) Setting up an IM Configuration Management database (for Windows)* or *1.4.4(4) Setting up an IM Configuration Management database (for Linux)*.
- The OS user who will execute the `jcoimdef` command has Administrator or `root` permissions.

Procedure

1. Execute the following `jcoimdef` command to enable user mapping for the source host:
 - In Windows:
`"Console-path\bin\jcoimdef" -hostmap ON`
 - In Linux:
`/opt/jplcons/bin/jcoimdef -hostmap ON`
2. Execute the following `jcoimdef` command to enable restrictions on viewing and operating business groups:
 - In Windows:
`"Console-path\bin\jcoimdef" -bizmonmode ON`
 - In Linux:
`/opt/jplcons/bin/jcoimdef -bizmonmode ON`
3. Restart JP1/IM - Manager and JP1/IM - View.

Related topics

- *3.1.4 Restrictions on viewing and operating business groups* in the *Overview and System Design Guide*
- *4.12 Setting event source host mapping* in the *Configuration Guide*
- *4.17 Setting reference and operation restrictions on business groups* in the *Configuration Guide*
- `jcoimdef` in *1. Commands* in the manual *Command and Definition File Reference*

(4) Creating business groups and adding affiliated hosts to them

To limit the business groups that can be viewed and operated by JP1/IM users, you create business groups and then specify which business group manages which host.

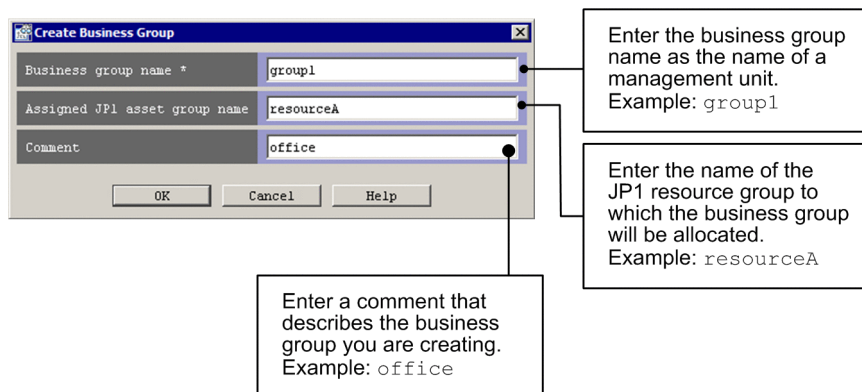
Prerequisites

The following conditions must be satisfied:

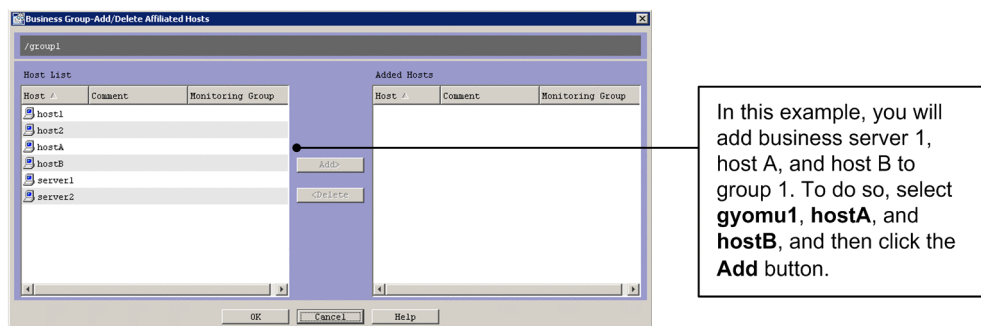
- The restrictions on viewing and operating business groups are enabled according to *C.1(3) Enabling restrictions on viewing and operating business groups*.
- Monitored hosts are registered in IM Configuration Management.

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, on the the **Business Groups** page, select the **Acquire update right** check box at the upper right of the page.
4. Right-click the root node on the **Business Groups** page. In the pop-up menu that appears, select **New**. The Create Business Group window appears.
5. Create a business group according to the following figure:



6. On the **Business Groups** page, in the tree area, select the node of the business group to which you want to add hosts.
7. Right-click the selected node and, in the command menu that opens, select **Add or Delete Affiliated Hosts**. The Add or Delete Affiliated Hosts window opens.
8. Add hosts to the business group according to the following figure:



9. In the IM Configuration Management window, on the **Business Groups** page, select **Operation, Business Group**, and then **Apply Business Group** to apply the business group settings to IM Configuration Management.

10. Clear the **Acquire update right** check box.

Related topics

- *6.4 Managing business groups* in the *Overview and System Design Guide*
- *3.4 Setting business groups* in the *Configuration Guide*
- *4.1 IM Configuration Management window* in the manual *GUI Reference*
- *4.14 Create Business Group window* in the manual *GUI Reference*

C.2 Verifying that the business group settings are specified correctly

The following describes how to check events for each JP1 user in the Event Console window to verify that the business group settings are specified correctly.

Procedure

1. Log in to JP1/IM - Manager (central console).
 - If you are a system administrator:
Log in as `jpladmin`.
 - If you are user A, who will manage the business system at the sales department:
Log in as `jpluser1`.
2. In the Event Console window, check events.
 - If you are a system administrator:
You can view and manage all events.
 - If you are user A, who will manage the business system at the Sales department:
You can view and manage only events issued from the hosts defined in group 1.

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/IM-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)

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
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

Service name	Port numbers	Description
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 (JP1/IM - Central Console)
jplimrt	20237/tcp	JP1/IM - Manager -> JP1/Base
jplimcmda	20238/tcp	JP1/IM - View -> JP1/IM - Manager (JP1/IM - Central Console) JP1/IM - Manager (JP1/IM - 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 (JP1/IM - Central Scope)
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/IM-Manager DB Server	20700/tcp	JP1/IM - Manager -> JP1/IM-Manager DB Server
jplimcf	20702/tcp	JP1/IM - View -> JP1/IM - Manager (IM Configuration Management)
jplimfcs	20701/tcp	Firewall setup is unnecessary because all communication takes place on the machine on which JP1/IM - Manager is installed.
jimmail	25/tcp ^{#2}	JP1/IM - Manager -> Mail server (SMTP) (without authentication)
	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

- *7.3 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/IM-Manager	JP1_Console	Manual	JP1/IM - Manager (central console, central scope, and IM Configuration Management) service for physical hosts
JP1/IM-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>3.2.3 Event receiver filter</i> in the <i>Overview and System Design Guide</i>• <i>3.2.4 Severe events filter</i> in the <i>Overview and System Design Guide</i>• <i>4.2.2 Settings for event receiver filters</i> in the <i>Configuration Guide</i>• <i>4.2.3 Settings for severe events filters</i> in the <i>Configuration Guide</i>• <i>2.10 Severe Event Definitions window</i> in the manual <i>GUI Reference</i>• <i>2.28 Settings for Event Receiver Filter window</i> in the manual <i>GUI Reference</i>
Remote monitoring [#]	You can monitor log files on monitored hosts without JP1/Base installed.	<ul style="list-style-type: none">• <i>6.2.8 Selection of agent configuration or remote monitoring configuration</i> in the <i>Overview and System Design Guide</i>• <i>6.6 Managing remotely monitored hosts</i> in the <i>Overview and System Design Guide</i>• <i>1.18 Settings for monitoring logs on remotely monitored hosts</i> in the <i>Configuration Guide</i>• <i>2.17 Settings for monitoring logs on remotely monitored hosts</i> in the <i>Configuration Guide</i>• <i>4.7 Remote Monitoring Settings window</i> in the manual <i>GUI Reference</i>• <i>4.20 System Common Settings window</i> in the manual <i>GUI Reference</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>12.3.8 Configuration for operation in a cluster system</i> in the <i>Overview and System Design Guide</i>• <i>6. Operation and Environment Configuration in a Cluster System</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>6.3 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>
Linkage with other JP1/IM series products	JP1/IM can be linked with products such as JP1/IM - Service Support and JP1/IM - Navigation	<ul style="list-style-type: none">• <i>8. Linking with Other Products</i> in the <i>Overview and System Design Guide</i>• <i>8. Settings for Linking to Other Integrated Management Products</i> in the <i>Configuration Guide</i>

Function	Overview	Related topics
	Platform to monitor systems.	
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>3.5.9 Suppressing the forwarding of a large number of events in the Overview and System Design Guide</i> • <i>11.1.7 Considerations for suppressing the forwarding of a large number of events in the Overview and System Design Guide</i> • <i>5.1.7 Suppressing event forwarding when a lot of events occur in the Administration 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 2000		Microsoft(R) Windows(R) 2000 Advanced Server Operating System
		Microsoft(R) Windows(R) 2000 Professional Operating System
		Microsoft(R) Windows(R) 2000 Server Operating System
Windows 7		Microsoft(R) Windows(R) 7 Enterprise
		Microsoft(R) Windows(R) 7 Professional
		Microsoft(R) Windows(R) 7 Ultimate
Windows 8		Microsoft(R) Windows(R) 8 Enterprise
		Microsoft(R) Windows(R) 8 Pro
Windows 8.1		Windows(R) 8.1 Enterprise
		Windows(R) 8.1 Pro
Windows Server 2003	Windows Server 2003	Microsoft(R) Windows Server(R) 2003, Enterprise Edition
		Microsoft(R) Windows Server(R) 2003, Standard Edition
	Windows Server 2003 (x64)	Microsoft(R) Windows Server(R) 2003, Enterprise x64 Edition
		Microsoft(R) Windows Server(R) 2003, Standard x64 Edition
	Windows Server 2003 R2	Microsoft(R) Windows Server(R) 2003 R2, Enterprise Edition
		Microsoft(R) Windows Server(R) 2003 R2, Standard Edition
	Windows Server 2003 R2 (x64)	Microsoft(R) Windows Server(R) 2003 R2, Enterprise x64 Edition
		Microsoft(R) Windows Server(R) 2003 R2, Standard x64 Edition
Windows Server 2008	Windows Server 2008	Microsoft(R) Windows Server(R) 2008 Enterprise
		Microsoft(R) Windows Server(R) 2008 Standard
	Windows Server 2008 (IPF)	Microsoft(R) Windows Server(R) 2008 for Itanium-based Systems
	Windows Server 2008 (x64)	Microsoft(R) Windows Server(R) 2008 Enterprise x64
		Microsoft(R) Windows Server(R) 2008 Standard x64
	Windows Server 2008 R2 (x64)	Microsoft(R) Windows Server(R) 2008 R2 Datacenter x64

Abbreviation		Full name
		Microsoft(R) Windows Server(R) 2008 R2 Enterprise x64
		Microsoft(R) Windows Server(R) 2008 R2 Standard x64
Windows Server 2012	Windows Server 2012	Microsoft(R) Windows Server(R) 2012 Datacenter
		Microsoft(R) Windows Server(R) 2012 Standard
	Windows Server 2012 R2	Microsoft(R) Windows Server(R) 2012 R2 Datacenter
		Microsoft(R) Windows Server(R) 2012 R2 Standard
Windows Vista		Microsoft(R) Windows Vista(R) Business
		Microsoft(R) Windows Vista(R) Enterprise
		Microsoft(R) Windows Vista(R) Ultimate
Windows XP Professional		Microsoft(R) Windows(R) XP Professional Operating System

Windows is sometimes used generically, referring to Windows 8.1, Windows 8, Windows Server 2012, Windows 7, Windows Server 2008, Windows Vista, Windows Server 2003, Windows XP Professional, and Windows 2000.

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>Job Management Partner 1 Version 10 Job Management Partner 1/Integrated Management - Manager Overview and System Design Guide</i>
Configuration Guide	<i>Job Management Partner 1 Version 10 Job Management Partner 1/Integrated Management - Manager Configuration Guide</i>
Administration Guide	<i>Job Management Partner 1 Version 10 Job Management Partner 1/Integrated Management - Manager Administration Guide</i>
GUI Reference	<i>Job Management Partner 1 Version 10 Job Management Partner 1/Integrated Management - Manager GUI Reference</i>
Command and Definition File Reference	<i>Job Management Partner 1 Version 10 Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference</i>
Messages	<i>Job Management Partner 1 Version 10 Job Management Partner 1/Integrated Management - Manager Messages</i>
JP1/Base User's Guide User's Guide	<i>Job Management Partner 1 Version 10 Job Management Partner 1/Base User's Guide</i>

Abbreviations for product names

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

Abbreviation		Full name
JP1/IM	JP1/IM - Manager	Job Management Partner 1/Integrated Management - Manager
	JP1/IM - Service Support [#]	Job Management Partner 1/Integrated Management - Service Support
	JP1/IM - View	Job Management Partner 1/Integrated Manager - View

Abbreviation		Full name
Linux	Linux 6.1 (x86)	Red Hat Enterprise Linux (R) Server 6.1 (32-bit x86)
	Linux 6.1 (x64)	Red Hat Enterprise Linux (R) Server 6.1 (64-bit x86_64)
	Linux 5.1 (x86)	Red Hat Enterprise Linux (R) 5.1 (x86)
	Linux 5.1 (x64)	Red Hat Enterprise Linux (R) 5.1 (AMD/Intel 64)

#: For JP1/IM - Service Support, this manual provides only an overview of the functions related to JP1/IM - Manager and JP1/IM - View described in this manual.

Acronyms

This manual uses the following acronyms:

Acronym	Meaning
AMD	Advanced Micro Devices
DNS	Domain Name System
GUI	Graphical User Interface
HTML	Hyper Text Markup Language
HTTP	HyperText Transfer Protocol
IP	Internet Protocol
IPF	Itanium(R) Processor Family
LAN	Local Area Network
NIC	Network Interface Card
SNMP	Simple Network Management Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TXT	Text
UNC	Universal Naming Convention
URL	Uniform Resource Locator
WWW	World Wide Web

Installation folders for JP1/IM and JP1/Base for Windows (x86 environment)

The table below lists the installation folders for JP1/IM and JP1/Base for Windows in an x86 environment. For Windows 8.1, Windows 8, Windows Server 2012, Windows 7, Windows Server 2008, and Windows Vista, the location represented by *system-drive:\Program Files* is determined by an OS environment variable when the product is installed. Therefore, the actual installation folder might differ depending on the environment.

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

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

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

Installation folders for JP1/IM and JP1/Base for Windows (x64 environment)

The table below lists the installation folders for JP1/IM and JP1/Base for Windows. For Windows 8.1, Windows 8, Windows Server 2012, Windows 7, Windows Server 2008, and Windows Vista, the location represented by ***system-drive***: \Program Files (x86) is determined by an OS environment variable when the product is installed. Therefore, the actual installation folder might differ depending on the environment.

Product name	Installation folder	Default installation folder [#]
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

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

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 provided by JP1/IM - Manager for use with the central console functionality

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 conditions

Conditions that determine repeated events for which monitoring is to be suppressed. JP1 event attributes and operators are used to set repeated event conditions

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

view filter

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