

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

Quick Reference

3020-3-R75-01(E)

■ 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.

For Windows Server 2003 and Windows XP Professional:

P-242C-6H97 Job Management Partner 1/Integrated Management - View 09-00

For Windows Server 2008 and Windows Vista:

P-2A2C-6H97 Job Management Partner 1/Integrated Management - View 09-00

For Windows Server 2003:

P-242C-8E97 Job Management Partner 1/Integrated Management - Manager 09-00

For Windows Server 2008:

P-2A2C-8E97 Job Management Partner 1/Integrated Management - Manager 09-00

For Solaris:

P-9D2C-8E92 Job Management Partner 1/Integrated Management - Manager 09-00

For AIX:

P-1M2C-8E92 Job Management Partner 1/Integrated Management - Manager 09-00

■ Trademarks

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

AIX is a registered trademark of the International Business Machines Corp. in the U.S.

HP-UX is a product name of Hewlett-Packard Company.

Itanium is a registered trademark of Intel Corporation or its subsidiaries in the United States and other countries.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and other countries.

Microsoft is a registered trademark of Microsoft Corp. in the U.S. and other countries.

Microsoft Internet Information Services is a product name of Microsoft Corp.

RSA, BSAFE are either registered trademarks or trademarks of RSA Security Inc. in the United States and/or other countries.

RSA Security Inc. All rights reserved.

Solaris is a trademark or registered trademark of Sun Microsystems, Inc. in the United States and other countries.

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

VMware is a registered trademark or trademark of VMware, Inc. in the United States and/or other jurisdictions.

Windows is a registered trademark of Microsoft Corp. in the U.S. and other countries.

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

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

The following program product contains some parts whose copyrights are reserved by Sun Microsystems, Inc.: P-9D2C-8E92.

The following program product contains some parts whose copyrights are reserved by UNIX System Laboratories, Inc.: P-9D2C-8E92.

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.

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

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 RSA BSAFE(R) Cryptographic software from RSA Security Inc.

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.

Printed in Japan.

■ **Edition history**

Edition 1 (3020-3-R75-01(E)): November 2009

■ **Copyright**

All Rights Reserved. Copyright (C) 2009, Hitachi, Ltd.

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.

In this manual, *Job Management Partner 1* is abbreviated as *JP1*, and *JP1/Integrated Management* is abbreviated as *JP1/IM*.

Users who want to learn about JP1/Integrated Management - Manager functions based on the intended use of each function should read this manual first.

The JP1/Integrated Management - Manager manual set contains seven manuals, including this one. For details about the setup and operation methods introduced in this manual, read the pertinent descriptions in the following manuals:

- *Job Management Partner 1/Integrated Management - Manager Overview and System Design Guide* (3020-3-R76(E))
- *Job Management Partner 1/Integrated Management - Manager Configuration Guide* (3020-3-R77(E))
- *Job Management Partner 1/Integrated Management - Manager Administration Guide* (3020-3-R78(E))
- *Job Management Partner 1/Integrated Management - Manager GUI Reference* (3020-3-R79(E))
- *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference* (3020-3-R80(E))
- *Job Management Partner 1/Integrated Management - Manager Messages* (3020-3-R81(E))

Intended readers

This manual is intended for professionals who want to use JP1/Integrated Management - Manager to manage and operate systems.

This manual assumes that the reader has a basic understanding of the following:

- JP1 series products
- JP1/Integrated Management - Manager

Organization of this manual

This manual is organized into the following chapters:

1. *Setting Up a System*

Chapter 1 explains how to define and manage a system configuration, and the preparations that are necessary for monitoring events.

2. *Monitoring a System*

Chapter 2 explains how to temporarily filter events that are displayed in the events list, and how to customize the severity level of events.

3. *Detecting Errors*

Chapter 3 explains how to display multiple events as a single event, and how to automatically execute commands based on the error that is detected.

4. *Troubleshooting Errors*

Chapter 4 explains how to display unlisted events that were issued previously for the purpose of investigating an error, and how to register for later display the corrective action to take for an error.

Related publications

This manual is part of a related set of manuals. The manuals in the set are listed below (with the manual numbers):

- *Job Management Partner 1/Base User's Guide (3020-3-R71(E))*
- *Job Management Partner 1/Integrated Management - Manager Overview and System Design Guide (3020-3-R76(E))*
- *Job Management Partner 1/Integrated Management - Manager Configuration Guide (3020-3-R77(E))*
- *Job Management Partner 1/Integrated Management - Manager Administration Guide (3020-3-R78(E))*
- *Job Management Partner 1/Integrated Management - Manager GUI Reference (3020-3-R79(E))*
- *Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference (3020-3-R80(E))*
- *Job Management Partner 1/Integrated Management - Manager Messages (3020-3-R81(E))*

How to read this manual

Descriptions in this manual are organized as indicated below:

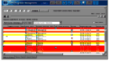
4. Troubleshooting Errors

4.1 Checking the status of previously-issued events

Once you have monitored a system for a while, error-related events that were issued previously may be issued again. Even if you want to check the corrective action you took in the past for such an event, the event may no longer be displayed in the events list. Let's display events that are no longer displayed in the events list to check the status of previously-issued events.


Problem

To check the status of previously-issued events, click the **Refresh** button in the Monitor Events page.




Action

1. By clicking the **Refresh** button, the events list is updated with the latest events.
2. Click the **Refresh** button in the Monitor Events page to check the status of previously-issued events.



Check

Click the **Refresh** button to check whether events that were issued in the past are still displayed in the events list.



4.1.1 Using the event display start-time specification function to specify the display time of events

To display events that are no longer displayed in the Monitor Events page of the Event Console window, use the event display start-time specification function. The event display start-time specification function can be used on the Monitor Events page.

52

Overview of task

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

Problem

This area reveals a problem one may encounter during monitoring.

Action

Corrective action
This area provides the windows, definition files, and settings required to take corrective action. The corrective action to take is detailed in the first part of each section.

Check

This area describes the system status checks to perform after you have taken corrective action. The checks to perform are detailed in the second part of each section.


4. Troubleshooting Errors

and Server Events pages of the Event Console window.

Prerequisite condition:

- The integrated monitoring database must have been configured at the time the events were acquired.

On the Monitor Events page, try displaying an event issued at 09:00:00 on February 23, 2009 that no longer currently displayed arrived at 10:00:00 on February 24, 2009.



Reference:

- See 3.1.9 Displaying event by specifying time in the Administration Guide.
- See 2.2 Monitor Events page in the manual OCU Reference.

You can also use the slider to display previously-issued events.

4.1.2 Verifying that events are displayed from the specified display time

After you have finished specifying the time in the area for specifying the event display start time, check whether events are displayed in the events list beginning from the time you specified.

To check whether events are displayed from the specified time:

- Click the **Display** button in the area for specifying the event display start time. Issued events are displayed in the events list beginning at the specified time. For this example, verify that events issued from 09:00:00 on February 23, 2009 are displayed in the events list on the Monitor Events page.

Keywords:

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

53

Overview of corrective action

This subsection title includes the name of the function needed for the corrective action.

The descriptions in the subsection are limited to the most important parts of each function.

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

References:

Provides references to sections in related manuals.

Keywords:

Provides keywords that are directly and indirectly related to the function.

Tip:

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

Conventions: Abbreviations

This manual uses the following abbreviations for product names:

Abbreviation		Full name or meaning
AIX		AIX(R) 5L 5.2
		AIX(R) 5L 5.3
		AIX(R) 6.1
JP1/Base		Job Management Partner 1/Base
JP1/Integrated Management or JP1/IM	JP1/IM - Manager	Job Management Partner 1/Integrated Management - Manager
	JP1/IM - View	Job Management Partner 1/Integrated Management - View
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 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

Abbreviation	Full name or meaning
Windows Server 2008	Microsoft(R) Windows Server(R) 2008 Enterprise
	Microsoft(R) Windows Server(R) 2008 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

- In this manual, *Windows 2000*, *Windows XP Professional*, *Windows Server 2003*, *Windows Server 2008*, and *Windows Vista* may be referred to collectively as *Windows*.

This manual also uses the following abbreviations:

Abbreviation	Full name or meaning
DB	Database
GUI	Graphical User Interface
HTTP	HyperText Transfer Protocol
IPF	Itanium(R) Processor Family
TXT	Text
URL	Uniform Resource Locator
WWW	World Wide Web

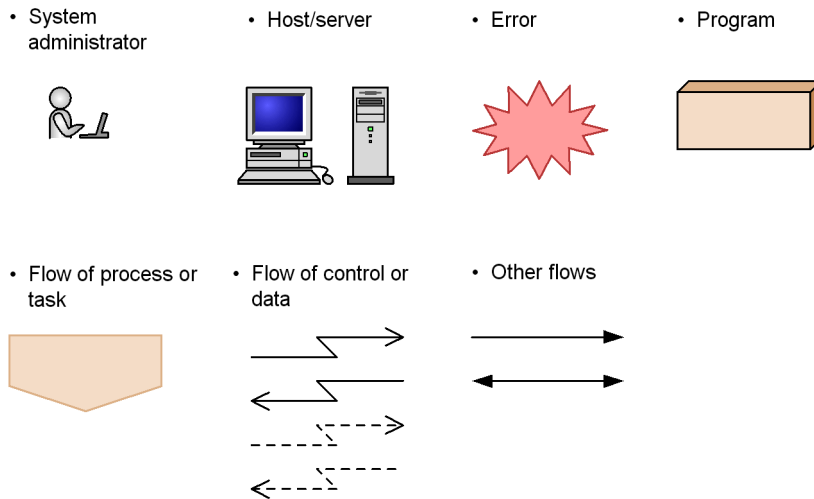
This manual uses the following abbreviations for cross-references to other manuals:

Abbreviation	Full title
<i>Overview and System Design Guide</i>	<i>Job Management Partner 1/Integrated Management - Manager Overview and System Design Guide</i>
<i>Configuration Guide</i>	<i>Job Management Partner 1/Integrated Management - Manager Configuration Guide</i>
<i>Administration Guide</i>	<i>Job Management Partner 1/Integrated Management - Manager Administration Guide</i>

Abbreviation	Full title
<i>GUI Reference</i>	<i>Job Management Partner 1/Integrated Management - Manager GUI Reference</i>
<i>Command and Definition File Reference</i>	<i>Job Management Partner 1/Integrated Management - Manager Command and Definition File Reference</i>
<i>Messages</i>	<i>Job Management Partner 1/Integrated Management - Manager Messages</i>

Conventions: Diagrams

This manual uses the following conventions in diagrams:



Conventions: Fonts and symbols

Font and symbol conventions are classified as:

- General font conventions
- Conventions in syntax explanations

These conventions are described below.

General font conventions

The following table lists the general font conventions:

Font	Convention
Bold	Bold type indicates text on a window, other than the window title. Such text includes menus, menu options, buttons, radio box options, or explanatory labels. For example, bold is used in sentences such as the following: <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>Italics</i>	Italics are used to indicate a placeholder for some actual text provided by the user or system. Italics are also used for emphasis. For example: <ul style="list-style-type: none"> • Write the command as follows: <i>copy source-file target-file</i> • Do <i>not</i> delete the configuration file.
Code font	A code font indicates text that the user enters without change, or text (such as messages) output by the system. For example: <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>

Examples of coding and messages appear as follows (although there may be some exceptions, such as when coding is included in a diagram):

```
MakeDatabase
...
StoreDatabase temp DB32
```

In examples of coding, an ellipsis (...) indicates that one or more lines of coding are not shown for purposes of brevity.

Conventions in syntax explanations

Syntax definitions appear as follows:

```
StoreDatabase [temp|perm] (database-name ...)
```

The following table lists the conventions used in syntax explanations:

Example font or symbol	Convention
<code>StoreDatabase</code>	Code-font characters must be entered exactly as shown.
<i>database-name</i>	This font style marks a placeholder that indicates where appropriate characters are to be entered in an actual command.
SD	Bold code-font characters indicate the abbreviation for a command.

Example font or symbol	Convention
<u>perm</u>	Underlined characters indicate the default value.
[]	Square brackets enclose an item or set of items whose specification is optional.
	Only one of the options separated by a vertical bar can be specified at the same time.
...	An ellipsis (...) indicates that the item or items enclosed in () or [] immediately preceding the ellipsis may be specified as many times as necessary.
()	Parentheses indicate the range of items to which the vertical bar () or ellipsis (...) is applicable.

Conventions: Installation folders for the Windows version of JP1/IM and JP1/Base

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

Product name	Writing convention for 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>
	<i>Scope-path</i>	<i>system-drive:\Program Files\HITACHI\JP1Scope</i>
JP1/Base	<i>Base-path</i>	<i>system-drive:\Program Files\HITACHI\JP1Base</i>

[#]: Denotes the installation folder for each product when a default installation is performed.

For Windows Server 2008 and Windows Vista, the *system-drive:\Program Files* part is determined at installation by an OS environment variable, and may therefore vary depending on the environment.

Conventions: KB, MB, GB, and TB

This manual uses the following conventions:

- 1 KB (kilobyte) is 1,024 bytes.
- 1 MB (megabyte) is 1,024² bytes.
- 1 GB (gigabyte) is 1,024³ bytes.

- 1 TB (terabyte) is $1,024^4$ bytes.

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:

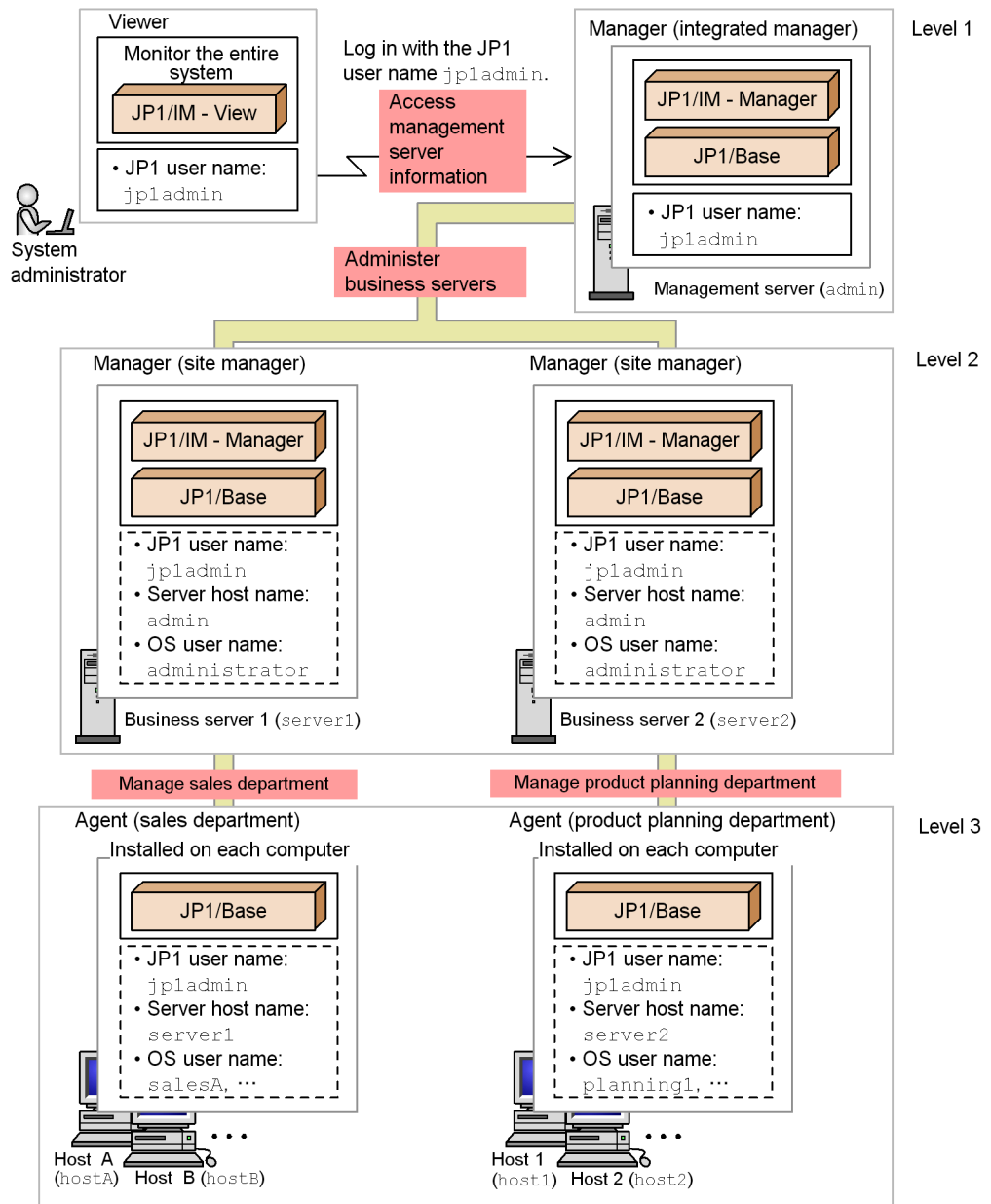
- Version 1.00 (or 1.0) is written as 01-00.
- Version 2.05 is written as 02-05.
- Version 2.50 (or 2.5) is written as 02-50.
- Version 12.25 is written as 12-25.

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*.

Basic system configuration

Systems provided by JP1/IM - Manager consist of managers for administering the system, agents that perform the role of monitored targets, and viewers for monitoring and operating the system. Systems provided by JP1/IM - Manager can be configured hierarchically. The following figure shows a system consisting of three levels.

In this manual, the term *system* means a system provided by JP1/IM - Manager.



Legend: : Information set by means of user mapping.
 JP1 user name: the JP1 user name used to log in.

In this example, the system administrator logs in to a manager called a *management*

server (integrated manager) with the JP1 user name `jp1admin`, from where he or she can use a viewer to monitor the entire system. The integrated manager is used to administer managers called *site managers* designated here as business server 1 and business server 2. Each site manager manages agents in the sales department and the product planning department.

To execute a command during management operations, a JP1 user account must be mapped to the OS user accounts by means of user mapping. For details about the user mapping procedure, see *1.2 Executing a command on a target host*. The following information must be set for the items in the areas indicated by *Information set by means of user mapping* in the legend of the figure above.

- JP1 user name: Specifies the JP1 user that will execute the commands.
- Server host name: Specifies the manager from which the commands will be executed.
- OS user name: Specifies the OS user permissions with which the commands will be executed.

Note:

The appropriate JP1 permissions are required to execute commands.

For details about the system setup procedure, see *1.1 Setting up a basic system*.

The descriptions in this manual assume that all products are version 09-00. They also assume that the integrated monitoring database and the IM configuration management database have been configured for JP1/IM - Manager. For details about the integrated monitoring database and the IM configuration management database, see *1. Installation and Setup (for Windows)* or *2. Installation and Setup (for UNIX)* in the *Configuration Guide*.

JP1 permission levels for system administrators

This manual assumes that the JP1 permission level used by the system administrator is either `JP1_Console_Admin` or `JP1_CF_Admin`.

`JP1_Console_Admin` permissions are needed to operate Central Console and Central Scope.

`JP1_CF_Admin` permissions are needed to operate IM Configuration Management.

Administrator permissions

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

Contents

Preface	i
Intended readers	i
Organization of this manual	ii
Related publications	ii
How to read this manual	iii
Conventions: Abbreviations	iv
Conventions: Diagrams	vi
Conventions: Fonts and symbols	vi
Conventions: Installation folders for the Windows version of JP1/IM and JP1/Base	viii
Conventions: KB, MB, GB, and TB	viii
Conventions: Version numbers	ix
Basic system configuration	ix
JP1 permission levels for system administrators	xi
Administrator permissions	xi
1. Setting Up a System	1
1.1 Setting up a basic system	2
1.1.1 Using IM Configuration Management to set up a system	3
1.1.2 Verifying that the system was set up correctly	5
1.2 Executing a command on a target host	7
1.2.1 Using the user mapping feature to map a JP1 user account to an OS user account	8
1.2.2 Verifying that you can execute a command	10
1.3 Centrally monitoring events that are issued in a system	11
1.3.1 Using Central Console to centrally manage a system	12
1.3.2 Verifying that central monitoring of the system was achieved	14
1.4 Visually monitoring events that are issued in a system	17
1.4.1 Learning how to use Central Scope	17
1.4.2 Verifying that you can monitor events in both tree format and map format	22
2. Monitoring a System	23
2.1 Filtering the events that are displayed	24
2.1.1 Using the view filter to specify conditions	25
2.1.2 Verifying that the events that match the conditions are displayed	26
2.2 Changing the severity level of events to better match your operations	28
2.2.1 Using the severity changing function to change the severity level of events	29
2.2.2 Verifying that the event severity level has been changed	30

2.3	Removing hosts undergoing maintenance from being monitored	32
2.3.1	Using common exclusion conditions in a filter to temporarily remove hosts from being monitored.....	33
2.3.2	Verifying that events from unmonitored hosts are not displayed	34
3.	Detecting Errors	37
3.1	Handling multiple events as a single event.....	38
3.1.1	Associating events with correlation events	39
3.1.2	Verifying that the correlation event is generated	42
3.2	Automatically executing a command when a specific event is generated.....	44
3.2.1	Using the automated action function to execute a command	45
3.2.2	Verifying that the command was executed	46
3.3	Preventing an action that has already been executed once from being executed during a set period of time	47
3.3.1	Using automated action suppression to prevent an action from being executed repeatedly	48
3.3.2	Verifying that the same action does not execute repeatedly	49
4.	Troubleshooting Errors	51
4.1	Checking the status of previously-issued events	52
4.1.1	Using the event display start-time specification function to specify the display time of events	52
4.1.2	Verifying that events are displayed from the specified display time	53
4.2	Searching for events.....	55
4.2.1	Using the search events function to search for events that match a specified condition.....	55
4.2.2	Verifying that the event was found.....	56
4.3	Registering for later display the corrective action to take for previously-issued events	58
4.3.1	Using the event guide function to register the corrective action to take	59
4.3.2	Verifying that the corrective action is registered	60
Index	63

Chapter

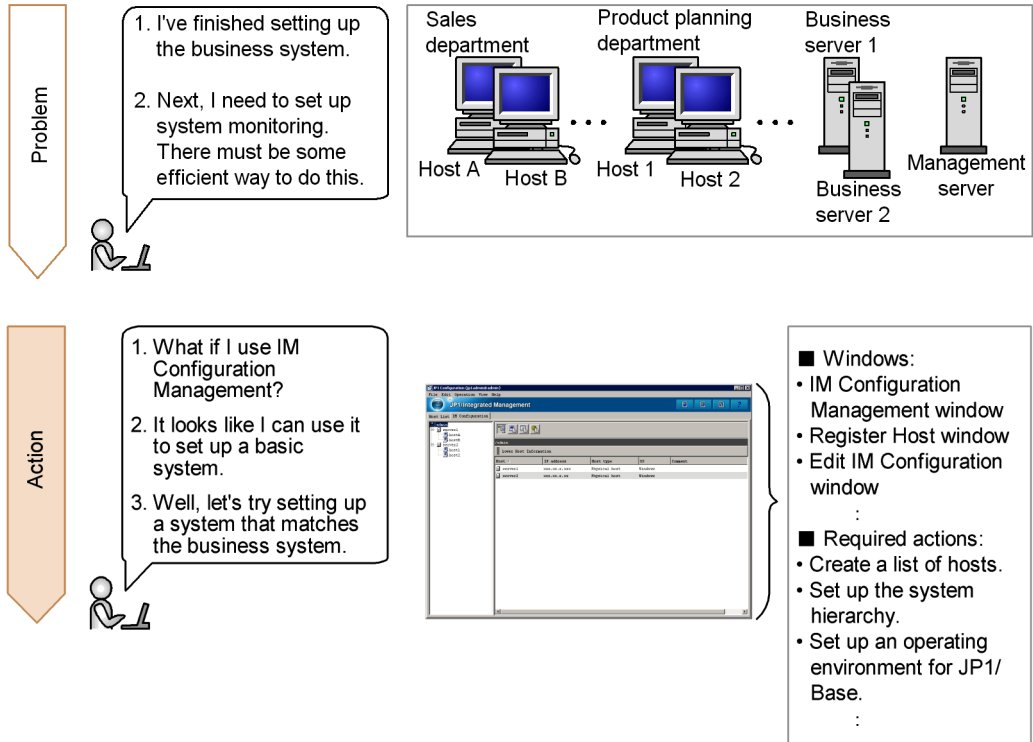
1. Setting Up a System

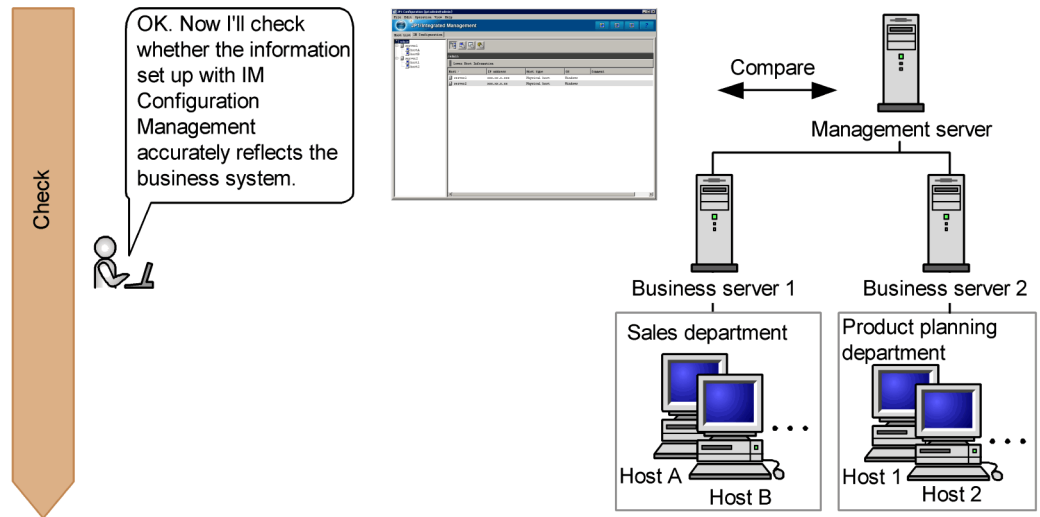
This chapter explains how to define and manage a system configuration, and the preparations that are necessary for monitoring events.

- 1.1 Setting up a basic system
- 1.2 Executing a command on a target host
- 1.3 Centrally monitoring events that are issued in a system
- 1.4 Visually monitoring events that are issued in a system

1.1 Setting up a basic system

JP1/IM - Manager allows you to centrally manage events issued in a business system. This means that the system hierarchy must be defined to follow the business system's organization. There are two ways to define a system hierarchy: by using IM Configuration Management or by using the Configuration Management component provided by JP1/Base. In this section, let's use IM Configuration Management to set up a basic system hierarchy.





1.1.1 Using IM Configuration Management to set up a system

To set up a system, you can use a component called *IM Configuration Management*. IM Configuration Management is one of the components provided by JP1/IM - Manager. It is used to centrally manage the hierarchical configuration of hosts comprising a system.

You use the IM Configuration Management window to set up the system hierarchy.

To display the window:

From the **Start** menu, choose **Programs, JP1_Integrated Management - View**, and then **Configuration Management**. This command sequence displays the Login window. The IM Configuration Management window is displayed once you log in at the Login window.

In the following subsections, you will set up the system described in the *Basic system configuration* section of the Preface.

Prerequisite conditions:

- JP1/Base is installed on the managed hosts.
- JP1/IM - Manager is installed on business server 1 (site manager), business server 2 (site manager), and the management server (integrated manager).

To define a system hierarchy:

1. Register the hosts.
2. Define the system hierarchy.

1. Setting Up a System

The following subsections explain the procedure for each of these steps.

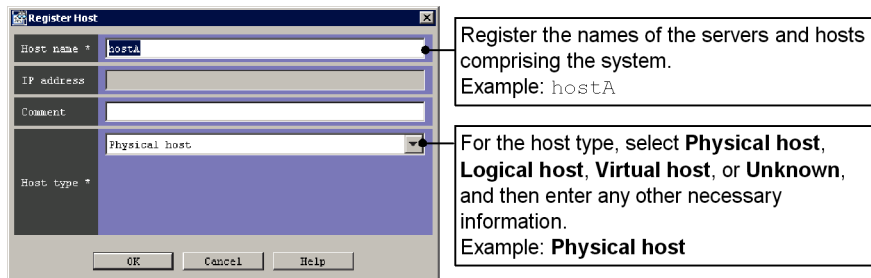
(1) Registering the hosts

You register the hosts in the Register Host window.

To display the window:

To display the Register Host window, select the **Host List** tab, choose **Edit**, and then choose **Register Host**.

Let's register the hosts that comprise the system.



In a similar fashion, register the other servers and hosts according to the system hierarchy.

(2) Defining the system hierarchy

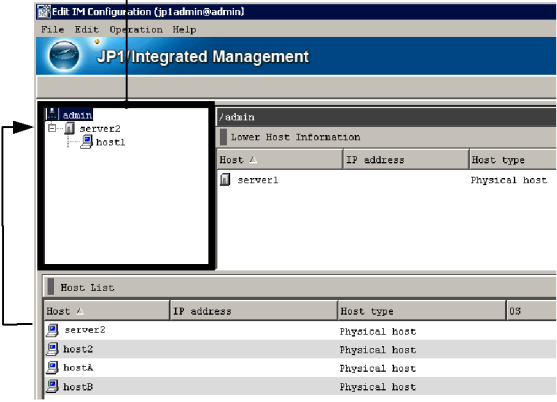
You define the system hierarchy in the Edit IM Configuration window.

To display the window:

To display the Edit IM Configuration window, in the IM Configuration Management window, choose **Edit**, and then **Edit IM Configuration**.

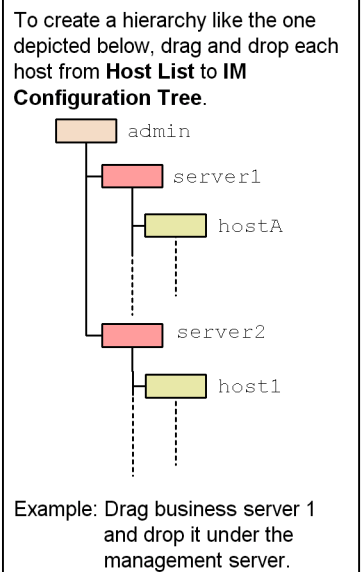
Let's configure the registered hosts according to the hierarchy.

IM Configuration Tree



The screenshot shows the 'IM Configuration Management' window. On the left, a tree view shows a hierarchy starting with 'admin', which contains 'server2' and 'host1'. Below the tree is a 'Host List' table with columns for Host, IP address, Host type, and OS. The table contains entries for server2, host2, hostA, and hostB, all of which are 'Physical host' type.

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



The diagram shows a tree structure. The root node is 'admin' (orange box). Under 'admin' are two nodes: 'server1' (red box) and 'server2' (red box). Under 'server1' is a node 'hostA' (yellow box). Under 'server2' is a node 'host1' (yellow box). Dashed lines indicate the parent-child relationships.

Example: Drag business server 1 and drop it under the management server.

When you have finished setting up the hierarchy, select the **Acquire update right** check box. Then, from the IM Configuration Management window, choose **Operation**, and then **Apply IM Configuration** to register the definitions.

References:

- See 6. *System Hierarchy Management Using IM Configuration Management in the Overview and System Design Guide.*
- See 1.9 *Setting the system hierarchy (when IM Configuration Management is used) in the Configuration Guide.*
- See 1.19.2 *Setting up IM Configuration Management - View in the Configuration Guide.*
- See 8. *Managing the System Hierarchy using IM Configuration Management in the Administration Guide.*
- See 4. *IM Configuration Management Window in the manual GUI Reference.*

1.1.2 Verifying that the system was set up correctly

Check whether the system was set up correctly by IM Configuration Management.

1. Setting Up a System

To check whether the system was set up correctly:

1. In the IM Management Configuration window, select the **IM Configuration** tab.

For this example, verify that the configuration is the same as the configuration shown in the *Basic system configuration* section of the Preface.

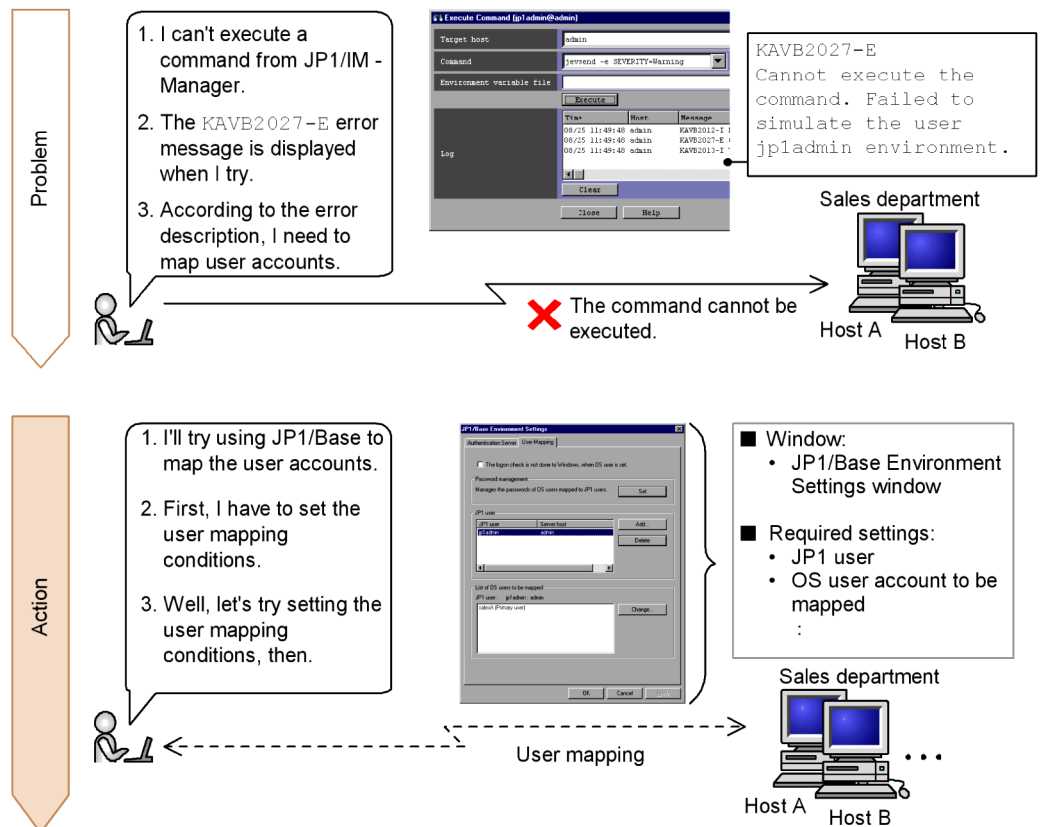


Keywords:

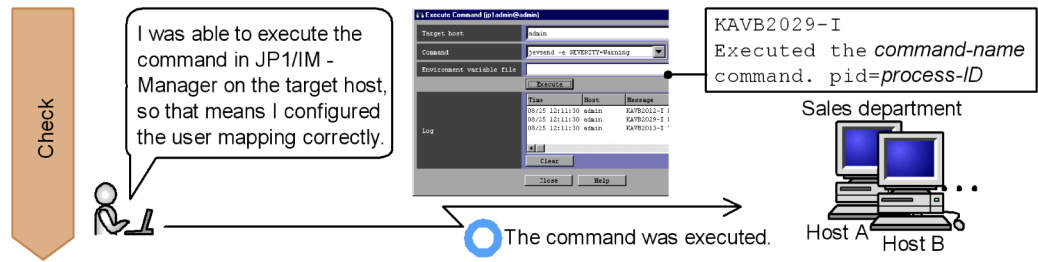
GUI, Configuration Management, configuration, system, IM Configuration Management, monitoring

1.2 Executing a command on a target host

To check the status of processes provided by JP1/IM - Manager on various hosts, or to check the system environment settings, system administrators execute commands in a component called *Central Console*. Central Console is a component provided by JP1/IM - Manager to capture events issued in a system based on a physical perspective for the purpose of facilitating management of system operations. Commands are executed using an OS user account on the target host, which means that the JP1 user executing the command must be mapped to an OS user account on the target host. Let's map a JP1 user to an OS user account, and then execute a command on a target host.



1. Setting Up a System



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

To map the JP1 user account with which commands are executed to an OS user account on a host, you use JP1/Base user mapping. Once user mapping is configured, from a management server, you can execute commands or perform automated actions on a target host in the product planning department or the sales department. For details about how to configure automated actions, see *3.2.1 Using the automated action function to execute a command*.

The following subsections separately explain how to configure user mapping by using a graphical user interface (GUI) and by using a command.

Prerequisite condition:

- Refer to the chapter that describes how to set up user mapping in the *Job Management Partner 1/Base User's Guide*, and make sure all of the prerequisite conditions are met.

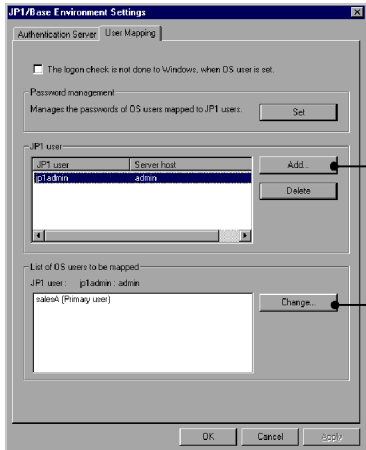
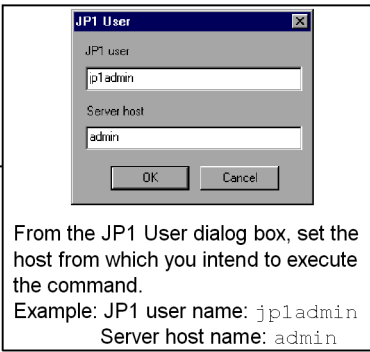
The following subsections explain how to map the JP1 user account used to execute commands (jpladmin) to an OS user account (salesA). Note that user mapping has to be configured for each host.

(1) Using the GUI

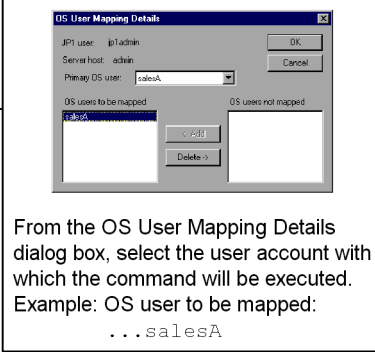
Using the GUI, you configure user mappings in the User Mapping page of the JP1/Base Environment Settings dialog box.

To display the window:

To open the JP1/Base Environment Settings dialog box, from the **Start** menu, choose **Programs, JP1_Base**, and then **Environment Settings**.

From the JP1 User dialog box, set the host from which you intend to execute the command.
Example: JP1 user name: `jpladmin`
Server host name: `admin`



From the OS User Mapping Details dialog box, select the user account with which the command will be executed.
Example: OS user to be mapped:
...`salesA`

 Reference:

- Chapter on setting up user mapping in the *Job Management Partner 1/Base User's Guide*

(2) Using a command

You use `jbssetumap` to set up user mapping. Execute the command as shown below:

```
jbssetumap -u jpladmin
           -sh admin
           -o salesA
```

 References:

- Chapter on setting up user mapping in the *Job Management Partner 1/Base User's Guide*
- Section on the `jbssetumap` command in the *Job Management Partner 1/Base User's Guide*

1.2.2 Verifying that you can execute a command

Once you have finished setting up user mapping for host A as described in *1.2.1 Using the user mapping feature to map a JP1 user account to an OS user account*, check whether you can execute a command from the manager.

First, display the Execute Command window.

To display the window:

To display the Execute Command window, in the Event Console window, click the **Execute Command** button.

To check whether you can execute a command from the manager:

1. For **Target host**, specify the target host on which the command will be executed.

hostA

2. For **Command**, enter the JP1/Base `jevsend` command as follows: `jevsend -e SEVERITY=Warning -m`, and click **Execute**.

The `jevsend -e SEVERITY=Warning -m` command is executed.

For this example, verify that an event is displayed with the message `Executed the command-name command of severity level Warning`.

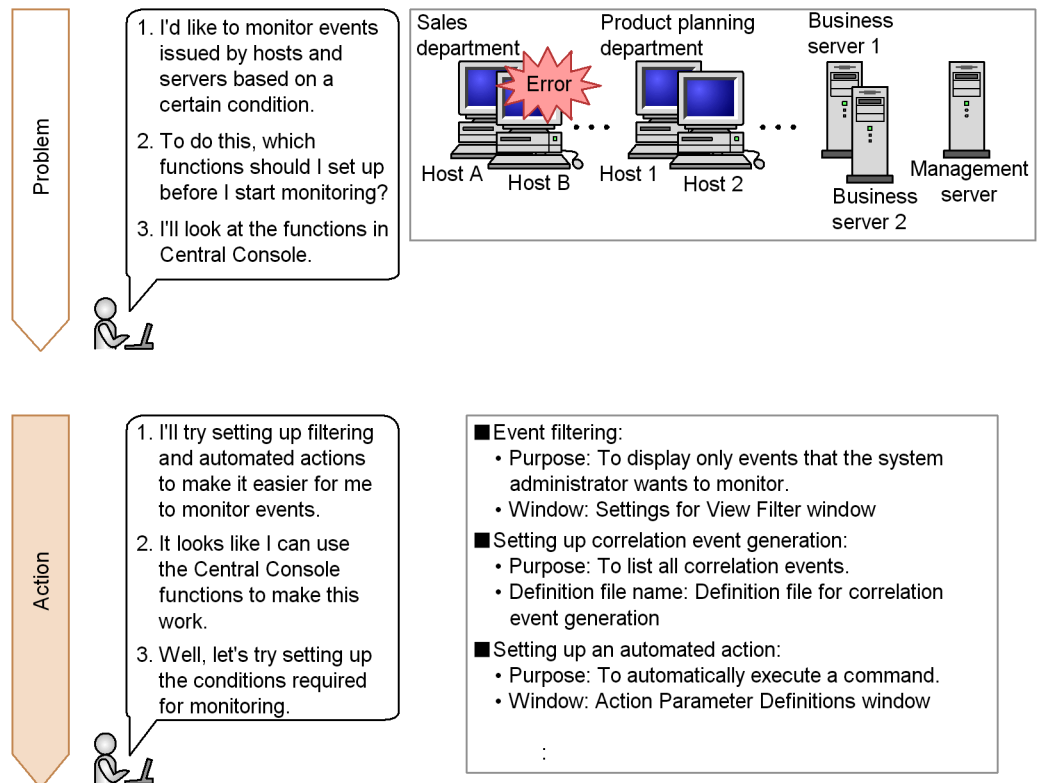


Keywords:

user mapping, mapping, command, relationship

1.3 Centrally monitoring events that are issued in a system

JP1/IM - Manager uses the functions in Central Console to provide you with the ability to centrally monitor events issued by various agents. Although you can manage the events that are issued simply by using the default settings, event management with Central Console affords even more convenience by allowing you to perform such actions as temporarily hiding events that do not need to be monitored, and executing one or more commands based on an event that is issued. Let's customize Central Console, and then centrally monitor the events issued by the system.



1. Setting Up a System

Check

OK. Now I'll check whether the event was issued and whether the command was automatically executed.

Execution of an automated event
(Target: ; Suspended: ; Partially suspended:)

Type	Event level	Original Severity Level	New Severity Level	Action	Registered time	Source ev...
Information	Information	Information	Information		06/21 15:42:04	beat
Warning	Warning	Warning	Warning		06/21 15:42:07	beat
Error	Error	Error	Error		06/21 15:43:11	beat
Information	Information	Information	Information	<input checked="" type="checkbox"/>	06/21 15:42:12	beat
Information	Information	Information	Information		06/21 15:43:12	beat

Generation of a correlation event
(Succeeded: ; Failed:)

1.3.1 Using Central Console to centrally manage a system

To centrally monitor events issued in a system, you must set up event forwarding and some Central Console functions. You can reduce the process load on JP1/IM - Manager by setting up event forwarding such that events that do not need to be monitored are not forwarded. With the Central Console functions, you can monitor from a single location a wide variety of events that are issued during system operations.

To centrally monitor events:

1. Set up event forwarding.
2. Set up the Central Console functions.

The following subsections explain the procedure for each of these steps.

(1) Setting up event forwarding

You set up event forwarding in the Display/Edit Profiles window of IM Configuration Management.

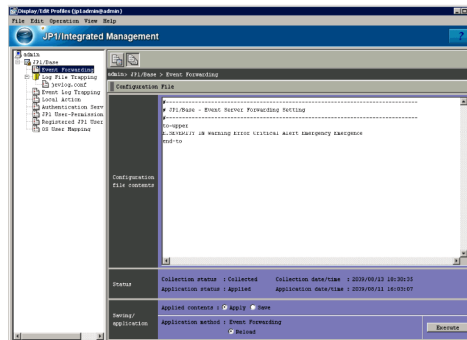
To display the window:

To display the Display/Edit Profiles window, in the IM Configuration Management window, choose **Display**, and then **Display Profiles**.

Prerequisite condition:

- The IM Configuration Management database is configured.

Let's set up event forwarding so that events are forwarded to the management server.



Used to edit the forwarding settings file. The default forwarding format is to-upper. This means that events are forwarded to the higher-level server according to the hierarchy defined in JP1/IM - Manager.

Edit the forwarding settings file if you need to change a forwarding setting for a managed target.


 **References:**


- See 3.1.1 *Monitoring from the Central Console* in the *Overview and System Design Guide*.
- Section on the forwarding settings file (`forward`) in the *Job Management Partner 1/Base User's Guide*.

(2) Setting up the Central Console functions

Explanations in this manual are based on the following Central Console functions. For details about where each function is explained, see the following table.

Table 1-1: Central Console functions in this manual

Central Console function	Overview of Central Console function	 Reference
Event filtering	<p>To display events that are consistent with your monitoring objectives, you can set up event filtering.</p> <p>Event filtering provides the following four types[#] of filters.</p> <ul style="list-style-type: none"> • Event acquisition filter: Filter for selecting JP1 events acquired from JP1/Base • Event receiver filter: Filter for selecting (limiting) events by which individual users can be monitored • Severe events filter: Filter for selecting important JP1 events needed for management • View filter: Filter for temporarily displaying only certain JP1 events 	2.1, 2.3

Central Console function	Overview of Central Console function	 Reference
Correlation event generation	This function generates a new event when a correlated event is issued.	3.1
Automated action	This function automatically executes a command when a specific problem occurs in the system.	3.2, 3.3

#: In addition, event filtering also includes a forwarding filter, which is used in JP1/Base to select events for forwarding to various agents.

1.3.2 Verifying that central monitoring of the system was achieved

From the manager, check to see whether the Central Console functions listed in Table 1-1 and the JP1/Base forwarding filter are set up correctly.

Event filtering:

The following explains how to check the Central Console filters and the JP1/Base forwarding filter.

Event acquisition filter:

See 2.3.2 *Verifying that events from unmonitored hosts are not displayed*.

This subsection explains how to check filtering when common exclusion conditions are used in the event acquisition filter.

Event receiver filter:

By default, this filter displays all events in the events list. Use the following procedure to check whether events are being displayed.

To check whether events are being displayed:

1. Execute the JP1/Base `jevsend` command twice as shown below:

```
jevsend -e SEVERITY=Warning -m Warning Event
jevsend -e SEVERITY=Information -m Information Event
```

An event of severity level `Warning` and an event of severity level `Information` are issued from the management server.

2. View the events list.

For this example, verify that an event of severity level `Warning` and an event of severity level `Information` are displayed.

Severe events filter:

By default, this filter displays only events of severity level `Emergency`, `Alert`, `Critical`, and `Error` in the events list. Use the following

procedure to check whether these events are being displayed.

To check whether Emergency, Alert, Critical, and Error events are being displayed:

1. Using the procedure given in *1.2.2 Verifying that you can execute a command*, enter the following settings in the Execute Command window.

Item	Setting to enter
Target host	hostA
Command	jevsend -e SEVERITY=Alert -m Alert Event jevsend -e SEVERITY=Warning -m Warning Event

On host A, an event of severity level Alert and an event of severity level Warning are issued.

2. Check the **Severe Events** page in the Event Console window of Central Console.

For this example, verify that an event of severity level Alert is displayed and that an event of severity level Warning is not displayed.

View filter:

See *2.1.2 Verifying that the events that match the conditions are displayed*.

Forwarding filter:

By default, this filter forwards only events of severity level Emergency, Alert, Critical, and Error. Use the following procedure to check whether these events are being forwarded.

To check whether Emergency, Alert, Critical, and Error events are being forwarded:

1. Using the procedure given in *1.2.2 Verifying that you can execute a command*, enter the following settings in the Execute Command window.

Item	Setting to enter
Target host	hostA
Command	jevsend -e SEVERITY=Warning -m Warning Event jevsend -e SEVERITY=Information -m Information Event

On host A, an event of severity level Warning and an event of severity level Information are issued.

1. Setting Up a System

2. Check the events list

For this example, verify that an event of severity level `Warning` is displayed and that an event of severity level `Information` is not displayed.

Correlation event generation:

See 3.1.2 *Verifying that the correlation event is generated*.

Automated actions:

See 3.2.2 *Verifying that the command was executed* and 3.3.2 *Verifying that the same action does not execute repeatedly*.



Keywords:

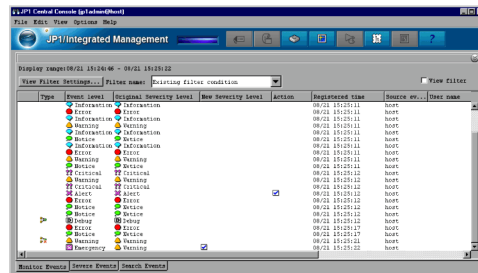
central monitoring, Central Console, event, monitoring, logical

1.4 Visually monitoring events that are issued in a system

In the Event Console window of Central Console, events in the events list are displayed in the order in which they arrive. With the events list, you can identify the host that issued the event, but you cannot quickly determine the extent to which the event impacts the system. By displaying the hierarchy of the hosts and where they are located, you can gain a sense of what impact events issued in the system have on various hosts. Let's visually monitor the events issued in the system to learn how to gain such a feel for the extent of an event's impact.

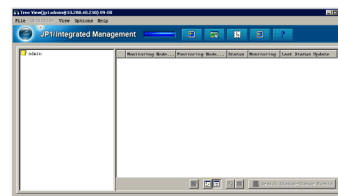
Problem

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

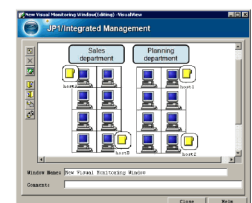
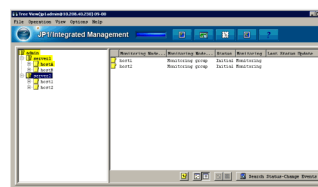
1. It looks as if I can use the Central Scope functions to do this.
2. Well, let's try setting up the conditions for monitoring events visually.



- 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.



1.4.1 Learning how to use Central Scope

To visually monitor events that are issued in a system, system administrators use a

1. Setting Up a System

component called *Central Scope*. Central Scope is a component provided by JP1/IM - Manager to capture events issued in a system based on a logical perspective for the purpose of facilitating management of system operations.

With Central Scope, you can display events that match your monitoring objectives in tree format, or you can display in map format only those points that require monitoring.

Prerequisite conditions:

- A Central Scope database has been created using the `jcsdbsetup` command.
- Central Scope Service is enabled (`jcoimdef -s ON`).

Let's configure Central Scope so that it monitors the system you set up in *1.1 Setting up a basic system*, and so that the status of the monitoring node changes when an event of severity level **Warning** is received from host A.

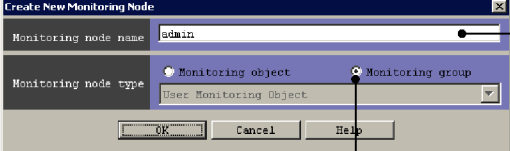
The following subsections explain separately how to set up a tree format and a map format.

(1) Setting up a tree format

To display events in tree format, you add a monitoring node. To add a monitoring node, you work in the Create New Monitoring Node window.

To display the window:


To display the Create New Monitoring Node window, in the Monitoring Tree (Editing) window, choose **Edit**, and then **Create New Monitoring Node**.



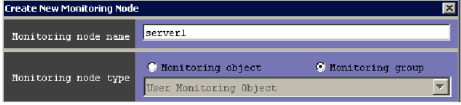

Enter the name of a server or host in the system.
Example: admin

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

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



Once you have created the management server, in a similar fashion, use the Create New Monitoring Node window to create business server 1 and host A.

- For business server 1:
 
- For host A:
 

(2) Setting the properties of the monitoring nodes

By setting the properties of the monitoring nodes, you can do things such as change the icon used by a monitoring node, or change the status of a monitoring node when an event is received. You set the properties of monitoring nodes in the Properties window.

To display the window:

To display the Properties window, select the monitoring node, right-click, and then choose **Properties** in the pop-up menu that appears.

The Properties window for host A opens. Select the **Status-Change Conditions** tab, and then click the **Add** button.

1. Setting Up a System

Status-Change Condition Settings

Change condition

Condition name: HostA Warning Event

Status: Warning

Common condition

Condition: [] Set Common Condition

Individual conditions

Attribute Name	Attribute Value	Condition

Buttons: Add, Edit, Delete

Buttons: OK, Cancel, Help

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.

Common Condition Detailed Settings

Common condition name: HostA

Common condition details

Registration host: hostA Match

Severity: Emergency Alert Critical Error Warning Normal Information Debug

Object type: [] Match

Object name: [] Match

Registration name type: [] Match

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

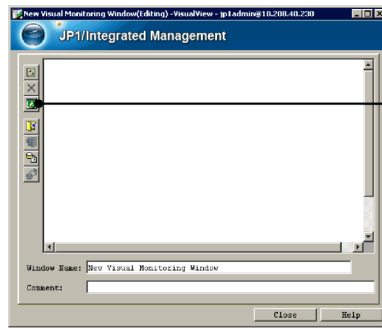
Specify the event severity level.
Example: **Warning**

(3) Setting up a map format

To display hosts in a map format, you first create a Visual Monitoring window. You configure the Visual Monitoring window from the Visual Monitoring (Editing) window.

To display the window:

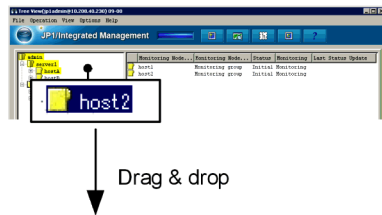
To display the Visual Monitoring (Editing) window, in the Visual Tree (Editing) window, choose **Edit**, and then **Create New Visual Monitoring Window**.



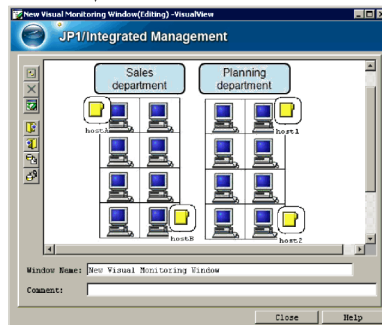
Background Image Settings

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

This displays the Background Image Settings window, in which you can select a background. First, save the image you want to use as the background in the following folder:
View-path\image\map\



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



 **References:**

- See 5.3.1 *Opening the Monitoring Tree (Editing) window* in the *Configuration Guide*.
- See 5.3.3 *Generating a monitoring tree automatically* in the *Configuration Guide*.
- See 5.4.1 *Opening an edit window for the Visual Monitoring window* in the *Configuration Guide*.
- See 5.4.3 *Customizing a Visual Monitoring window* in the *Configuration Guide*.
- See *jcsdbsetup* in Chapter 1 of the manual *Command and Definition File*

Reference.

- See *jcoimdef* in Chapter 1 of the manual *Command and Definition File Reference*.

1.4.2 Verifying that you can monitor events in both tree format and map format

After you have finished configuring Central Scope, check whether you are able to monitor events in both map format and tree format in a manner consistent with the system.

To check event monitoring:

1. Using the procedure given in *1.2.2 Verifying that you can execute a command*, enter the following settings in the Execute Command window.

Item	Setting to enter
Target host	hostA
Command	jevsend -e SEVERITY=Warning -m Warning Event Issued jevsend -e SEVERITY=Error -m Error Event Issued

On host A, an event of severity level `Warning` and an event of severity level `Error` are issued.

2. Check the events in the Monitoring Tree and Visual Monitoring windows.

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

For this example, when the event of severity level `Warning` is issued, verify that host A and the monitoring group that includes host A change to yellow. In addition, confirm that the event of severity level `Error` does not cause host A and the monitoring group to change.



Keywords:

GUI, visual, event, tree, graphical, monitoring tree, Central Scope, aim, visual

Chapter

2. Monitoring a System

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

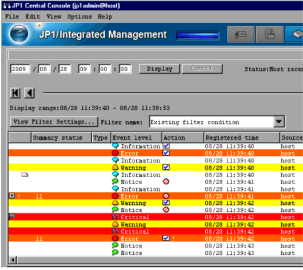
- 2.1 Filtering the events that are displayed
- 2.2 Changing the severity level of events to better match your operations
- 2.3 Removing hosts undergoing maintenance from being monitored

2.1 Filtering the events that are displayed

When you use Central Console - View to monitor events, events issued by hosts are displayed in the events list. If conditions such as the host and severity level have been established, you can display only the events you want to monitor according to the conditions that are set. Let's specify conditions to temporarily filter the events that are displayed.

Problem

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



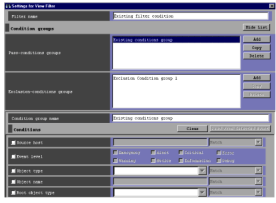
Sales department

Error
 Information
 Warning
 Information
 Notice
 Information
 Error
 :

Host B

Action

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



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



2.1.1 Using the view filter to specify conditions

You use the view filter to filter the events that are displayed. To set up the view filter, you use the Settings for View Filter window of Central Console.

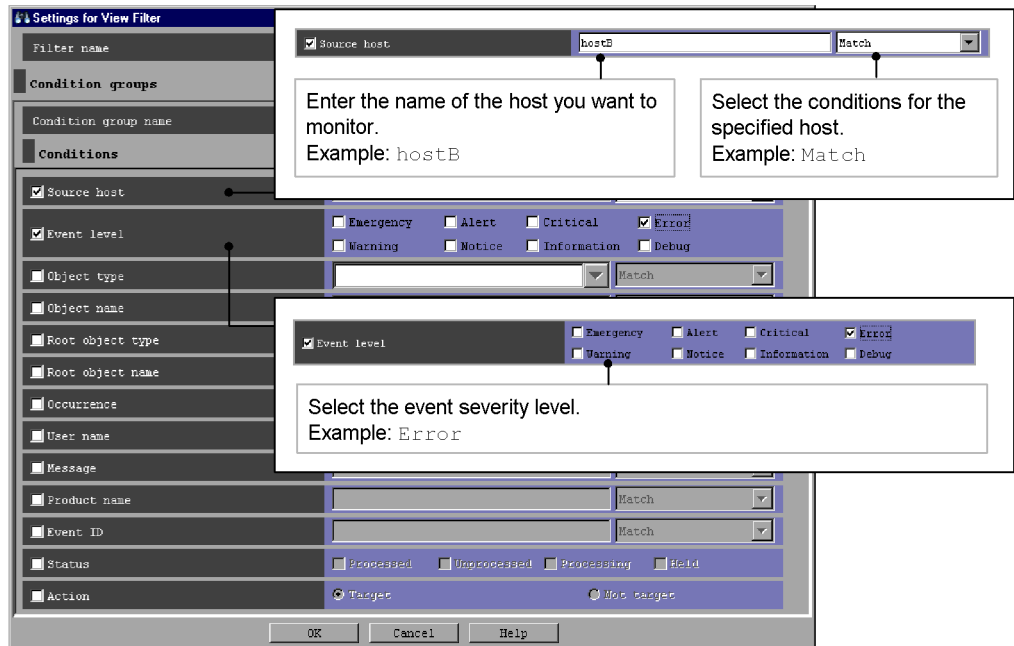
To display the window:

To display the Settings for View Filter window, in the Monitor Events page of the Event Console window, click **View Filter Settings**.

Prerequisite conditions:

- None

Let's specify settings to display in the events list only events of severity level Error issued by host B.



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

 *References:*

- See 4.2.1 *Settings for view filters* in the *Configuration Guide*.
- See 2.20 *Settings for View Filter window* in the manual *GUI Reference*.

2.1.2 Verifying that the events that match the conditions are displayed

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

To check whether the events that match the conditions are being displayed:

1. Select the **View filter** check box in the Event Console window.

The events that match the specified conditions are displayed in the events list.

For this example, verify that events of severity level **Error** issued by host B are displayed.



Keywords:

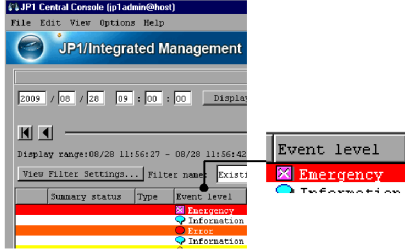
display, event, specific, filtering, view filter

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

In JP1/IM - Manager, the event severity level is 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 may not match the severity of the event. So that you can monitor events with severity levels that are consistent with your system operations, you may want to try changing the severity level of events to better match your operations.

Problem

1. The severity level of the events does not seem to match our operations.
2. There must be a way to change the severity level settings for events.

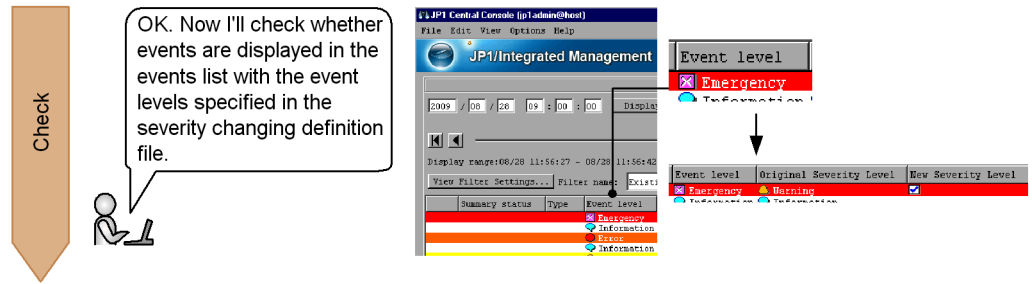


Summary status	Type	Event level
		Emergency
		Information
		Emergency
		Information
		Information

Action

1. I'll try formulating event severity levels that match our operations.
2. It looks like I can use the severity changing function to change event severity levels.
3. Well, let's try specifying a condition to change the event severity level from Warning to Emergency.

- File name: Severity changing definition file (jcochsev.conf)
- Condition settings:
 - Definition name
 - Event comparison condition
 - Event severity level after change
 -



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

You use the event severity changing function to change the severity level of events to better match your operations. You configure the severity changing function using the severity changing definition file.

Prerequisite conditions:

- The integrated monitoring database is configured.
- The event severity changing function is enabled.

Let's configure the system so that the severity level of events issued by host A that match warning is changed to a severity level of Emergency.

Using a text editor, open the severity changing definition file (`jcochsev.conf`), which is in the following location:

- Windows:

`Console-path\conf\chsev\jcochsev.conf`

`shared-folder\jp1cons\conf\chsev\jcochsev.conf` (logical host)

- UNIX:

`/etc/opt/jp1cons/conf/chsev/jcochsev.conf`

`shared-directory/jp1cons/conf/chsev/jcochsev.conf` (logical host)

Specify the settings as follows.

```
DESC_VERSION=1
def severity-level-change-1
  cnd
    E.SEVERITY IN Warning
    B.SOURCESERVER IN hostA
  end-cnd
sev Emergency
```

```
end-def
```

The following table explains these specifications.

Specification	Explanation
<pre>cnd E.SEVERITY IN Warning B.SOURCESERVER IN hostA end-cnd</pre>	<p>Specifies a comparison condition for the purpose of comparing events. Specify these conditions as follows:</p> <ul style="list-style-type: none"> To match the severity level of Warning: E.SEVERITY IN Warning To match host A as the event-issuing source: B.SOURCESERVER IN hostA
<pre>sev Emergency</pre>	<p>Specifies the severity level to which events matching the event conditions are changed. Specify the severity level as follows:</p> <ul style="list-style-type: none"> To change the severity level to Emergency: sev Emergency

To register the specified settings in JP1/IM, execute the `jco_spmd_reload` command on the manager to restart JP1/IM - Manager.



References:

- See *11.1.6 Considerations for changing JP1 event levels* in the *Overview and System Design Guide*.
- See *4.9 Setting the severity changing function* in the *Configuration Guide*.
- See *Severity changing definition file (jcochsev.conf)* in Chapter 2 of the manual *Command and Definition File Reference*.

2.2.2 Verifying that the event severity level has been changed

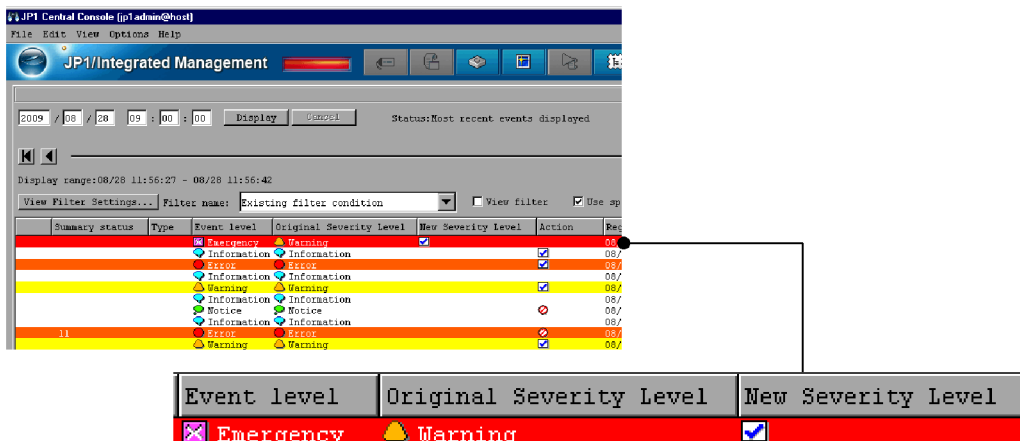
After you have finished specifying the conditions for the severity changing function, check whether events are displayed in the events list showing the changed severity level of events.

1. Using the procedure given in *1.2.2 Verifying that you can execute a command*, enter the following settings in the Execute Command window.

Item	Setting to enter
Target host	hostA
Command	<code>jvsend -e SEVERITY=Warning</code>

On host A, an event of severity level warning is issued.

For this example, verify that the event level was changed to Emergency, and that the events list is displayed as follows:



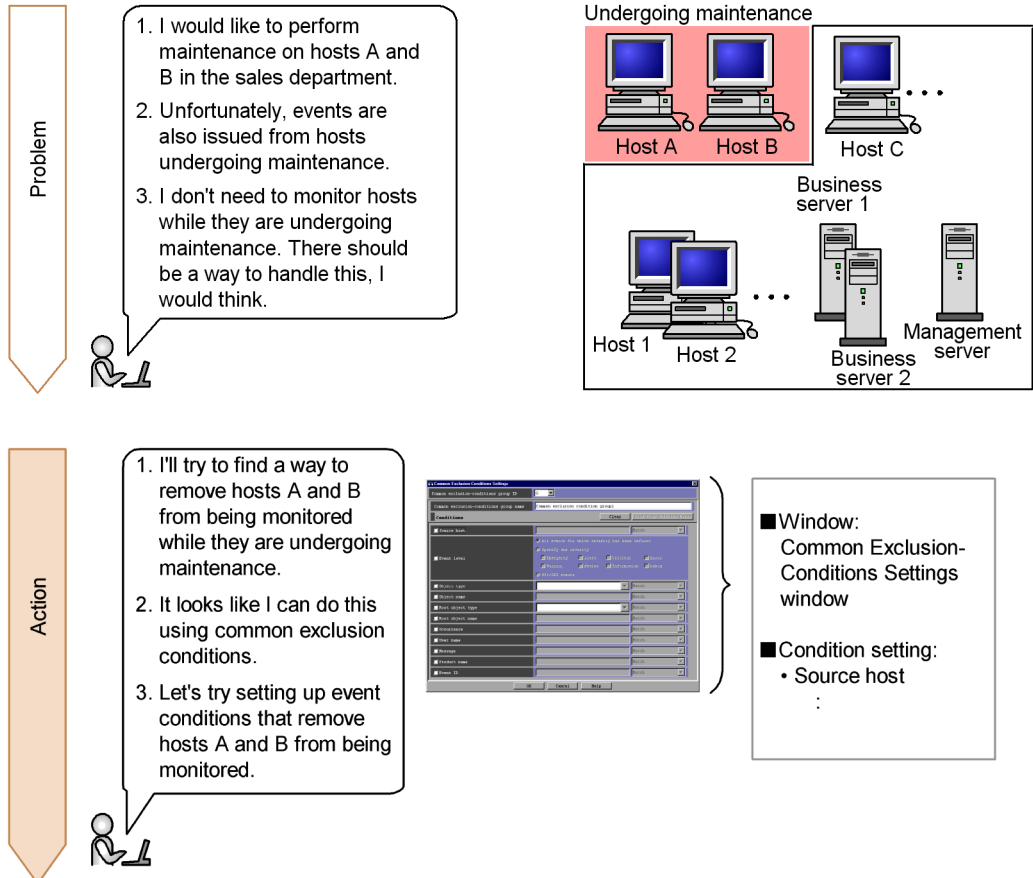
By default, the **Original severity level** and **New severity level** column headings are not displayed in the events list. We recommend that you use the Preferences window to configure Central Console to display these items.

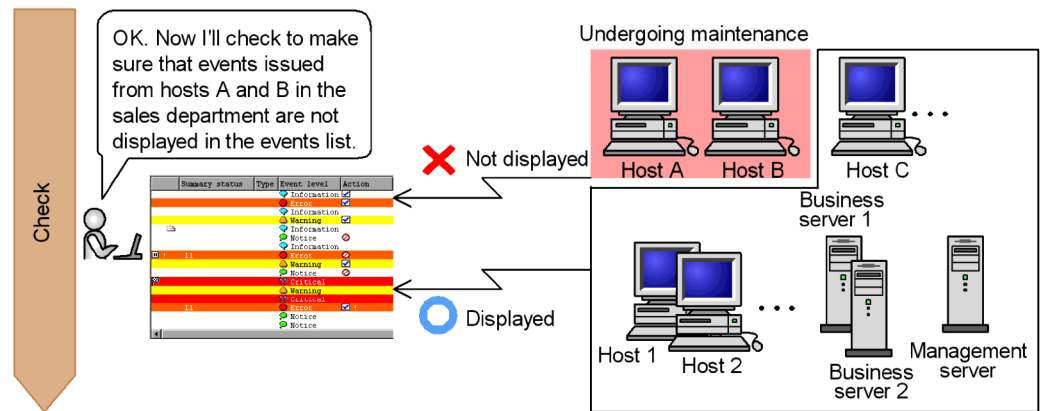
Keywords:

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

2.3 Removing hosts undergoing maintenance from being monitored

Whenever you restart a server on a host that is undergoing maintenance, a large number of events that are not needed for monitoring the system are issued. This means that events not needed for monitoring the system are displayed in the events list, making it difficult to check those events that are needed. Let's remove a couple of hosts that are undergoing maintenance from being monitored so that these unnecessary events are not displayed.





Note:

If you need to perform maintenance on an entire system that includes JP1/IM - Manager, perform the maintenance in order of higher hosts to lower hosts.

2.3.1 Using common exclusion conditions in a filter to temporarily remove 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.

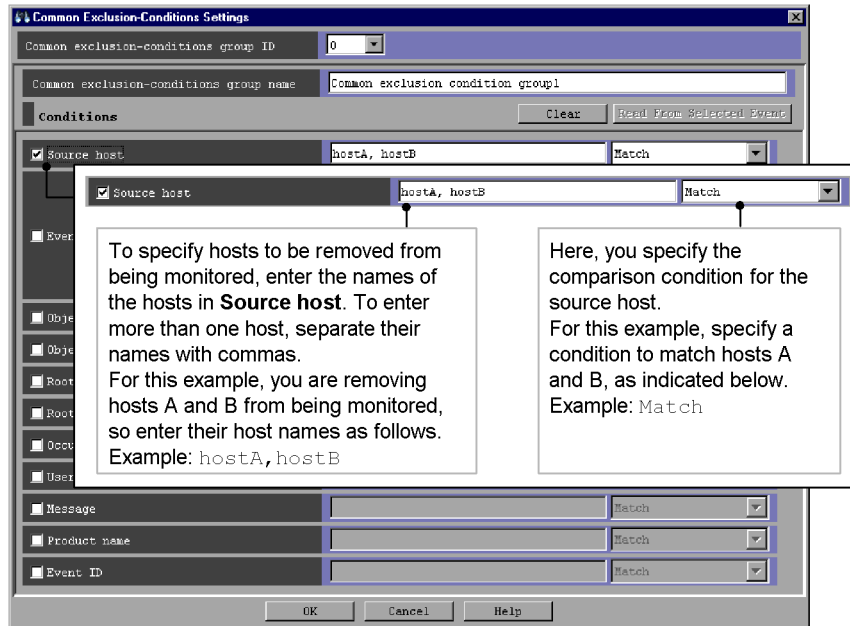
To display the window:

To display the Common Exclusion-Conditions Settings window, in the Event Acquisition Conditions List window, click the **Add** button under the area for the common exclusion conditions groups.

Prerequisite conditions:

- None

For example, let's configure Central Console to remove events issued by hosts A and B from being monitored while these hosts are undergoing maintenance.



 **References:**

- See 3.2.6 *Defining filter conditions* in the *Overview and System Design Guide*.
- See 12.10 *Considerations for JP1/IM system-wide maintenance* in the *Overview and System Design Guide*.
- See 4.2.4 *Settings for event acquisition filters* in the *Configuration Guide*.
- See 2.15 *Common Exclusion-Conditions Settings window* in the manual *GUI Reference*.

2.3.2 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 being displayed in the events list.

To verify that events from the unmonitored hosts are not being displayed:

1. Click the **OK** button in the Common Exclusion-Condition Settings window.
The Event Acquisition Conditions List window is displayed.
2. Click the **OK** button in the Event Acquisition Conditions List window.

The System Environment Settings window appears.

3. Click **Apply** in the System Environment Settings window.

The specified conditions are defined.

4. Using the procedure given in *1.2.2 Verifying that you can execute a command*, enter the following settings in the Execute Command window.

Item	Setting to enter
Target host	hostA
Command	jevsend -e SEVERITY=Warning -m Command executed from host A.

On host A, an event of severity level Warning is issued.

5. Repeat step 4. Enter the following settings in the Execute Command window.

Item	Setting to enter
Target host	hostB
Command	jevsend -e SEVERITY=Warning -m Command executed from host B.

On host B, an event of severity level Warning is issued.

6. Repeat step 4. Enter the following settings in the Execute Command window.

Item	Setting to enter
Target host	hostC
Command	jevsend -e SEVERITY=Warning -m Command executed from host C.

On host C, an event of severity level Warning is issued.

For this example, verify that only events of severity level Warning that are issued by host C are displayed in the events list, and that events of severity level Warning that are issued by hosts A and B are not displayed in the events list.



Keywords:

item, filter, common exclusion condition, specific, host

Chapter

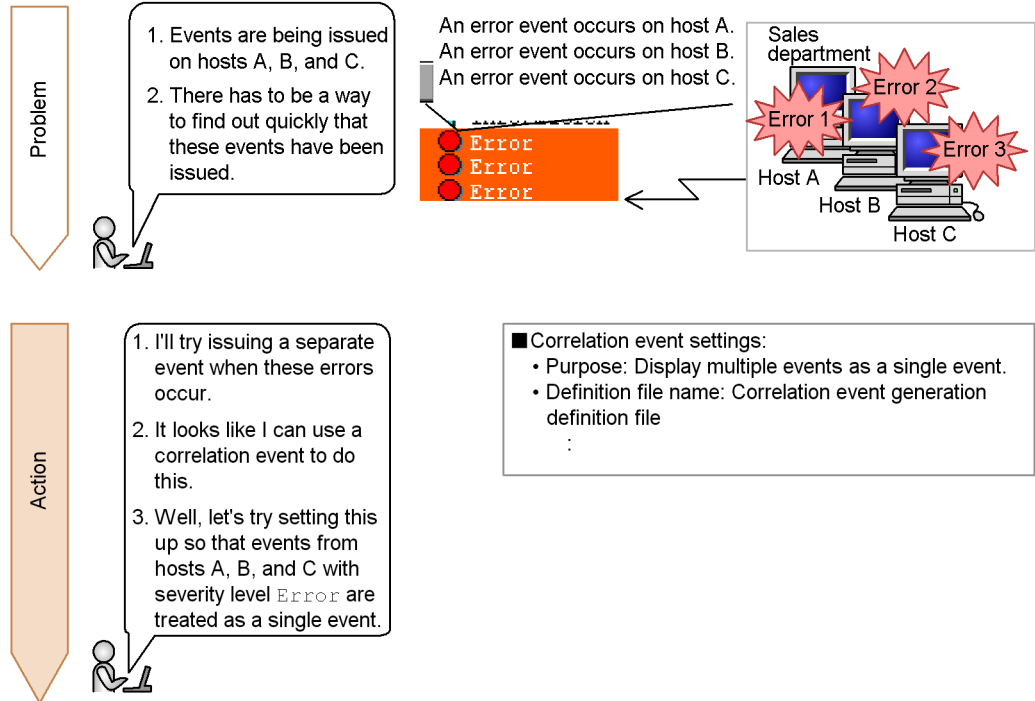
3. Detecting Errors

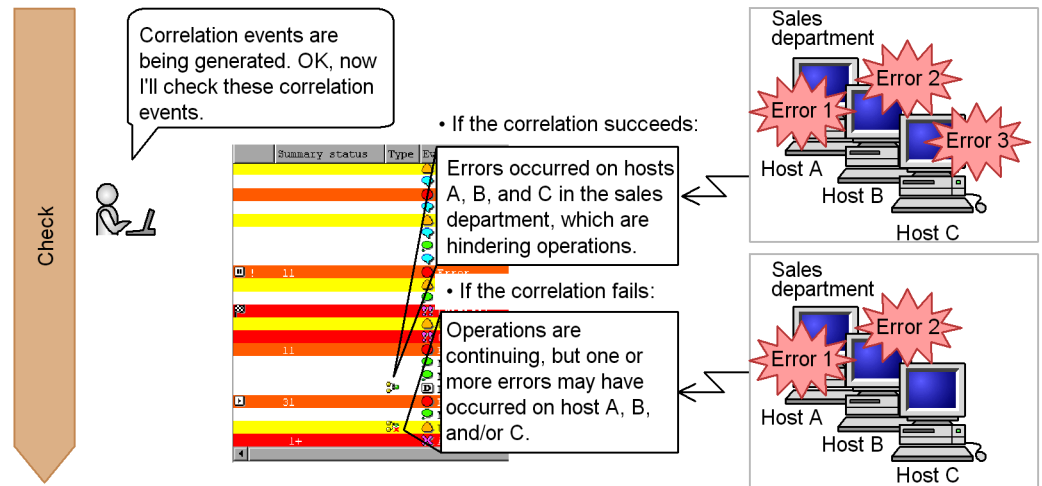
This chapter explains how to display multiple events as a single event, and how to automatically execute commands based on the error that is detected.

- 3.1 Handling multiple events as a single event
- 3.2 Automatically executing a command when a specific event is generated
- 3.3 Preventing an action that has already been executed once from being executed during a set period of time

3.1 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 coupled events are issued, you may need to quickly take action appropriate for these events. To help single out important events that need to be dealt with quickly, you can treat multiple events as a single issue.





3.1.1 Associating events with correlation events

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

Prerequisite condition:

- The correlation event generation function is enabled.

Let's specify settings to generate the following events when a correlation either succeeds or fails.

When the correlation succeeds:

- Condition for a successful correlation:

Events of severity level `Error` are issued from hosts A, B, and C within 60 seconds of one another.

- Event that is generated:

An event of severity level `Warning` is generated with the message `Errors occurred on hosts A, B, and C in the sales department, which are hindering operations.`

When the correlation fails:

- Condition for a failed correlation:

Error-level events issued from host A, B, and/or C do not satisfy the condition set for a successful correlation.

3. Detecting Errors

- Event that is generated:

An event with severity level Information is generated with the message Operations are continuing, but one or more errors may have occurred on host A, B, and/or C.

Using a text editor, open a correlation event generation definition file (example: def1.conf) which is in the following location:

- Windows: *any-folder*
- UNIX: *any-directory*

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

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==hostC
TYPE=combination
SUCCESS_EVENT=E.SEVERITY:Warning,B.MESSAGE:"Errors occurred on
hosts A, B, and C in the sales department, which are hindering
operations."
FAIL_EVENT=E.SEVERITY:Information,B.MESSAGE:"Operations are
continuing, but one or more errors may have occurred on host A,
B, and/or C."
```

The following table explains these specifications:

Specification	Explanation
<pre>CON=E.SEVERITY==Error,B.SOURCESERVER==hostA CON=E.SEVERITY==Error,B.SOURCESERVER==hostB CON=E.SEVERITY==Error,B.SOURCESERVER==hostC</pre>	<p>Specifies the event conditions used in specifying a correlation event generation condition. Specify as follows to set error-level events issued by hostA as a condition.</p> <ul style="list-style-type: none"> • Set the severity level to match Error: E.SEVERITY==Error • Set the event-issuing host to match host A: E.SOURCESERVER==hostA <p>In a similar fashion, specify error-level events issued by host B and host C as conditions.</p>

Specification	Explanation
TYPE=combination	<p>Specifies the type of the correlation event generation condition that is defined. Specify as follows to set the combination of host A, host B, and host C as a condition.</p> <ul style="list-style-type: none"> • TYPE=combination
SUCCESS_EVENT=E.SEVERITY:Warning,B.MESSAGE: "Errors occurred on hosts A, B, and C in the sales department, which are hindering operations."	<p>Specifies the correlation event that is generated if the correlation event generation condition succeeds.</p> <p>Specify as follows to generate an event of severity level warning with the message Errors occurred on hosts A, B, and C in the sales department, which are hindering operations.</p> <ul style="list-style-type: none"> • Specify an event of severity level warning: E.SEVERITY:Warning • Specify the message to display: B.MESSAGE:"Errors occurred on hosts A, B, and C in the sales department, which are hindering operations."

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

You can store `def1.conf` anywhere you like (Example: `C:\jplim`).

Execute the `jcoegschange` command on the manager as follows to register the definitions:

```
jcoegschange -f C:\jplim\def1.conf
```



References:

- See *3.3 Issue of correlation events* in the *Overview and System Design Guide*.
- See *4.4 Setting correlation event generation* in the *Configuration Guide*.
- See *5.1.7 Displaying and handling correlation events* in the *Administration Guide*.
- See *jcoegschange* in Chapter 1 of the manual *Command and Definition File Reference*.
- See *Correlation event generation definition file* in Chapter 2 of the manual *Command and Definition File Reference*.

3.1.2 Verifying that the correlation event is generated

After you have finished specifying the correlation event conditions, check whether the correlation event is generated according to your specifications.

To check whether the correlation event is generated as specified:

- Using the procedure given in 1.2.2 *Verifying that you can execute a command*, enter the following settings in the Execute Command window.

Item	Setting to enter
Target host	hostA
Command	jevsend -e SEVERITY=Error

On host A, verify that an event of severity level `Error` is generated.



- Change the name of the target host to `hostB`, and repeat step 1.

On host B, verify that an event of severity level `Error` is generated.

- Change the name of the target host to `hostC`, and repeat step 1.

On host C, verify that an event of severity level `Error` is generated.

Under **Type** in the events list, the fact that a correlation event was generated is indicated by the following icons:

Type	Explanation
	Indicates that the correlation event was successful.
	Indicates that the correlation event was not successful.

For this example, verify that the icon indicating that the correlation event was successful is displayed in the events list.

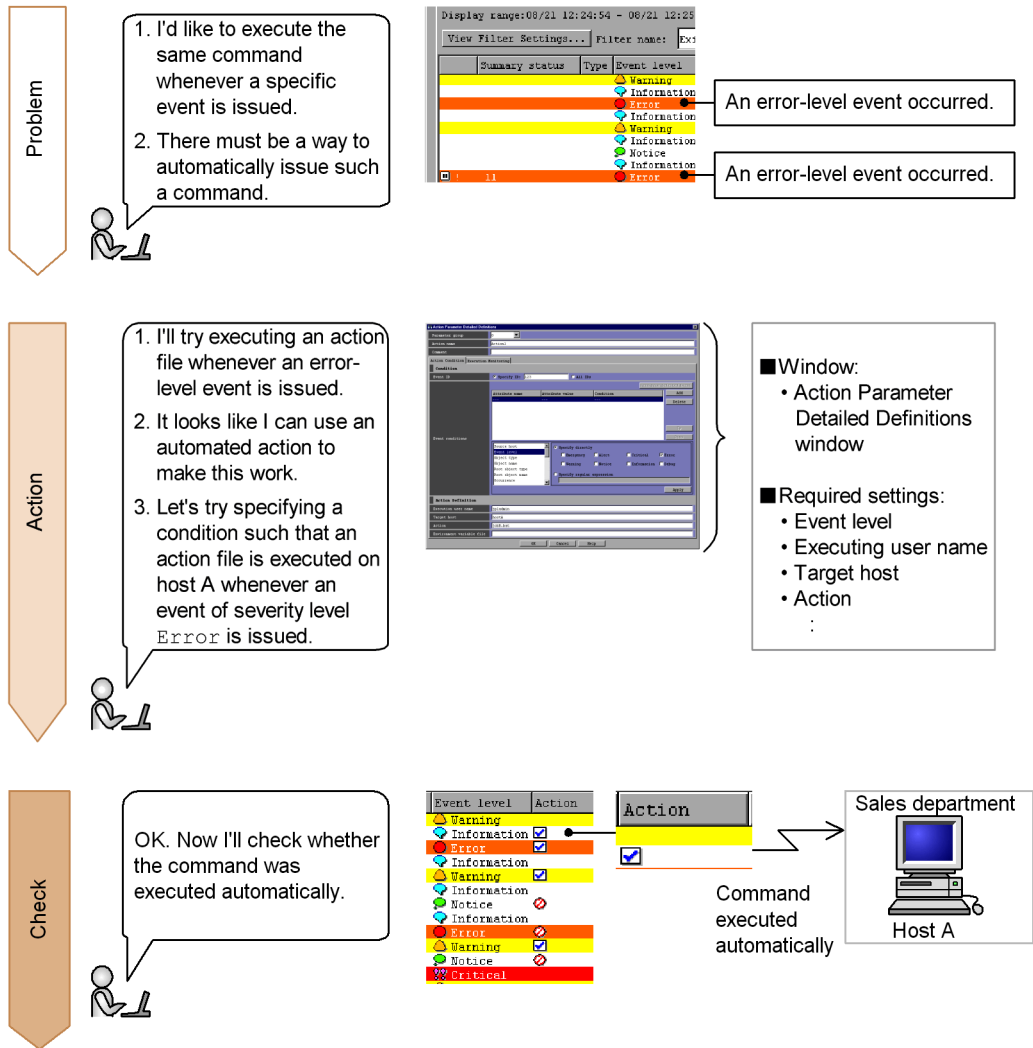


Keywords:

correlation event, severity, consolidation, summary, event, succeeded, failed, generate, do not generate

3.2 Automatically executing a command when a specific event is generated

When an event is issued, the system administrator may execute one or more commands as a means of handling the event. Executing a particular command every time a specific event occurs is a burden to the system administrator. To reduce the workload, let's configure Central Console so that a command is automatically executed whenever a specific event is issued.



3.2.1 Using the automated action function to execute a command

To automatically execute a command, you use the automated action function. You 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 use variables and specify information included in events.

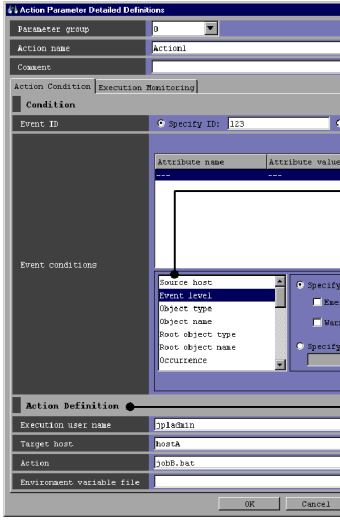
To display the window:

To display the Action Parameter Detailed Definitions window, in the Action Parameter Definitions window, click either the **Add** or the **Edit** button.

Prerequisite conditions:

- None

Let's specify that, when an event of severity level **Error** is issued, the error action batch file (.bat) that is stored in C:\jplim will be executed on the Windows computer host A (hostA).



Condition: Specify an event condition for triggering an event by which an automated action is executed.

For this example, specify as indicated below to set events of severity level **Error** as the condition.

Source host	Event level	Object type	Object name	Root object type	Root object name
	<input type="checkbox"/> Emergency <input type="checkbox"/> Alert <input type="checkbox"/> Critical <input checked="" type="checkbox"/> Error <input type="checkbox"/> Warning <input type="checkbox"/> Notice <input type="checkbox"/> Information <input type="checkbox"/> Debug				

Action Definition: Specify the automated action that is executed when an event specified in **Condition** occurs.

For 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 host A.
Example: hostA
- **Action:** Execute an error action batch file (.bat) stored in C:\jplim.
Example: C:\jplim\jobB.bat



Reference:

- See 2.25.1 *Action Parameter Detailed Definitions window* in the manual *GUI Reference*.

3.2.2 Verifying that the command was executed

After you have finished configuring the automated action, check whether the command executes according to your specifications.

To check whether the command executes as specified:

1. Click the **OK** button in the Action Parameter Detailed Definitions window.
The Action Parameter Definitions window is displayed.
2. Click the **Apply** button in the Action Parameter Definitions window.
The specified settings are updated.
3. Using the procedure given in 1.2.2 *Verifying that you can execute a command*, enter the following settings in the Execute Command window.

Item	Setting to enter
Target host	hostA
Command	jevsend -e SEVERITY=Error

On host A, an event of severity level `Error` is issued.

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

For this example, verify that an automated action that executes event action batch file (.bat) on Windows computer host A was triggered when an event of severity level `Error` was issued.



Keywords:

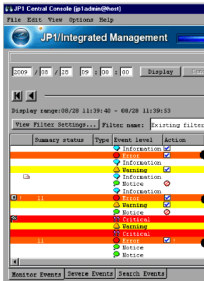
automated action, command, Automatic Action Service

3.3 Preventing an action that has already been executed once from being executed 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 the 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

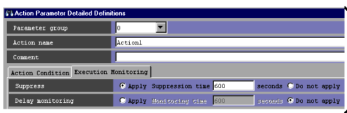
1. If I set up an action file to be executed, it will execute every time the same event occurs.
2. The action file needs to execute only once. There has to be some way I can deal with this.



The action executes every time the same event is issued.

Action

1. I'll try setting this up so that the automated action doesn't execute repeatedly.
2. It looks like I can use automated action suppression to do this.
3. Let's try setting conditions so that, once the action file executes, it won't execute again for 10 minutes.



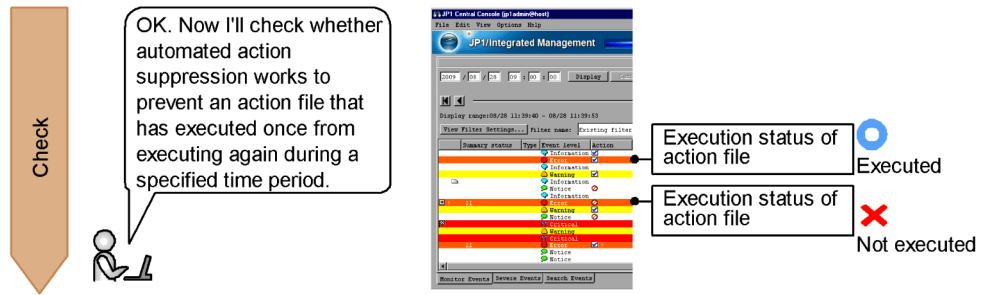
■ Window:

- Action Parameter Detailed Definitions window

■ Required setting:

- Suppress
- :

3. Detecting Errors



3.3.1 Using automated action suppression to prevent an action from being executed repeatedly

To prevent an action that has executed once from being executed for a set period of time, you use automated action suppression. You set up automated action suppression in the Action Parameter Detailed Definitions window.

To display the window:

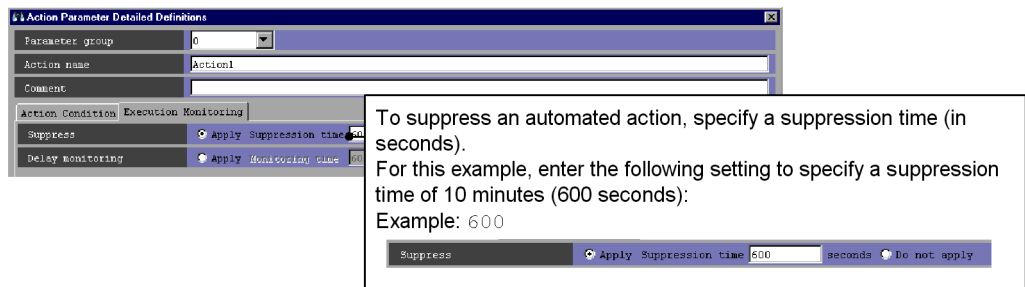
To display the Action Parameter Detailed Definitions window, in the Action Parameter Definitions window, click either the **Add** or the **Edit** button.

Prerequisite conditions:

- None

Let's specify that the automated action set in 3.2.1 *Using the automated action function to execute a command* does not execute for 10 minutes (600 seconds).

In the Action Parameter Detailed Definitions window, select the **Execution Monitoring** tab.



References:

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

- See 4.3.4 *Setting suppression of automated action execution* in the *Configuration Guide*.
- See 2.25.1 *Action Parameter Detailed Definitions window* in the manual *GUI Reference*.

3.3.2 Verifying that the same action does not execute repeatedly

After you have finished setting up suppression of automated actions, make sure that the same action does not execute repeatedly.


To make sure that the action does not execute repeatedly:

1. Click the **OK** button in the Action Parameter Detailed Definitions window.
The Action Parameter Definitions window is displayed.
2. Click the **Apply** button in the Action Parameter Definitions window.
The specified settings are updated.
3. Using the procedure given in 1.2.2 *Verifying that you can execute a command*, enter the following settings in the Execute Command window.



Item	Setting to enter
Target host	hostA
Command	jevsend -e SEVERITY=Error

On host A, an event of severity level `Error` is issued.


4. Repeat step 3.
On host A, an event of severity level `Error` is issued.
5. In 10 minutes, repeat step 3 again.
On host A, an event of severity level `Error` is issued.

If the automated action was suppressed, an automated action suppression icon () is displayed under **Action** in the events list.

For this example, verify that the following is displayed under **Action** in the events list.

- The first time the command is executed:
The execution trigger icon is displayed ().
- The second time the command is executed:
The automated action suppression icon is displayed ().

3. Detecting Errors

- The third time the command is executed:
Because the ten minutes specified as the suppression time have elapsed, the execution trigger icon is displayed ().



Keywords:

automated action, generate, severity, time, suppression

Chapter

4. Troubleshooting Errors

This chapter explains how to display unlisted events that were issued previously for the purpose of investigating an error, and how to register for later display the corrective action to take for an error.

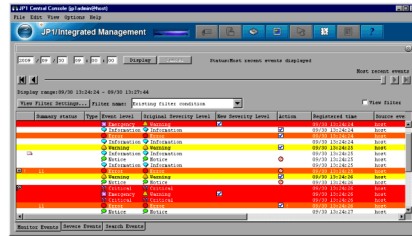
- 4.1 Checking the status of previously-issued events
- 4.2 Searching for events
- 4.3 Registering for later display the corrective action to take for previously-issued events

4.1 Checking the status of previously-issued events

Once you have monitored a system for a while, error-related events that were issued previously may be issued again. Even if you want to check the corrective action you took in the past for such an event, the event may no longer be displayed in the events list. Let's display events that are no longer displayed in the events list to check the status of previously-issued events.


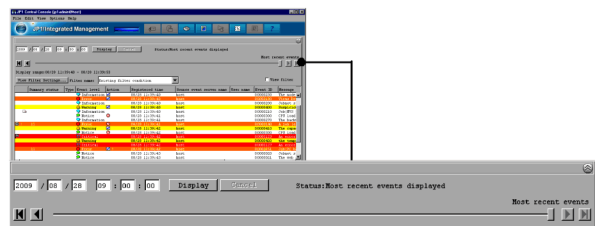
Problem

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


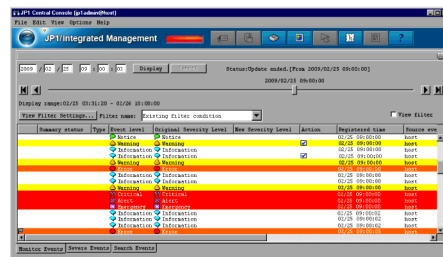
Action

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.

4.1.1 Using the event display start-time specification function to specify the display time of events

To display events that are no longer displayed on the **Monitor Events** page of the Event Console window, you use the event display start-time specification function.

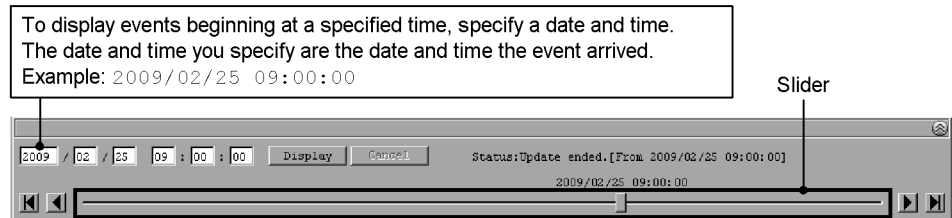
The event display start-time specification function can be used on the **Monitor Events**

and **Severe Events** pages of the Event Console window.

Prerequisite condition:

- The integrated monitoring database is configured.[#]
#: The integrated monitoring database must have been configured at the time the events were acquired.

On the **Monitor Events** page, try displaying an event issued at 09:00:00 on February 25, 2009 when the earliest event currently displayed arrived at 10:00:00 on February 26, 2009.



References:

- See 5.1.9 *Displaying events by specifying time* in the *Administration Guide*.
- See 2.2 *Monitor Events page* in the manual *GUI Reference*.

You can also use the slider to display previously-issued events.

4.1.2 Verifying that events are displayed from the specified display time

After you have finished specifying the time in the area for specifying the event display start time, check whether events are displayed in the events list beginning from the time you specified.

To check whether events are displayed from the specified time:

1. Click the **Display** button in the area for specifying the event display start time.
Issued events are displayed in the events list beginning at the specified time.

For this example, verify that events issued from 09:00:00 on February 25, 2009 are displayed in the events list on the **Monitor Events** page.

Keywords:

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



Tip:

Attaching a memo to an event

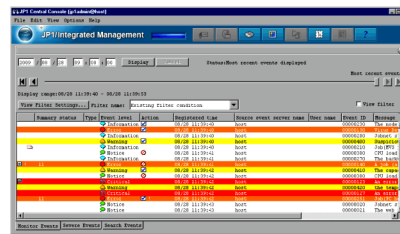
By attaching a memo to an event, you can record a note indicating the status of the investigation conducted on the event. For details about how to attach a memo, see *3.7 Setting memo entries* in the *Overview and System Design Guide*.

4.2 Searching for events

In the course of investigating an error, you may need to check whether other events related to the error have been issued, in addition to the ones currently displayed in the events list. However, at the time of the investigation, such events may have already been cleared from the events list. Let's search for events that have been cleared from the events list by specifying event conditions.

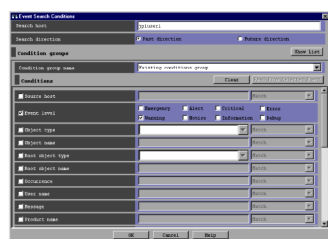
Problem

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



Action

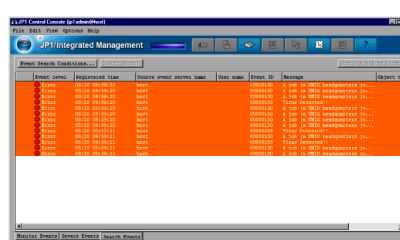
1. I'd like to find error-level events.
2. It looks like I can use the search events function to do this.



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

Check

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



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

To search for events, you use the search events function. You set the conditions for the search events function in the Event Search Conditions window.

To display the window:

To display the Event Search Conditions window, click the **Events Search Conditions** button on the **Search Events** page.

Prerequisite condition:

- The integrated monitoring database is configured.#

#: The integrated monitoring database must be configured only if you want to specify the integrated monitoring database as a search target.

Let's search for events of severity level warning.

Used to specify the event search condition.
For this example, specify an event level of **Warning**.
Example: **Warning**



References:

- See 3.5 *Searching for events* in the *Overview and System Design Guide*.
- See 5.5.1 *Search method* in the *Administration Guide*.

4.2.2 Verifying that the event was found

After you have specified the event search conditions, check whether the event you wanted to find is displayed on the **Search Events** page.

To check whether the event you wanted to find is displayed:

1. Click the **OK** button in the Event Search Conditions window.

Events matching the specified condition are displayed on the **Search Events** page.

For this example, verify that events of severity level warning are displayed.

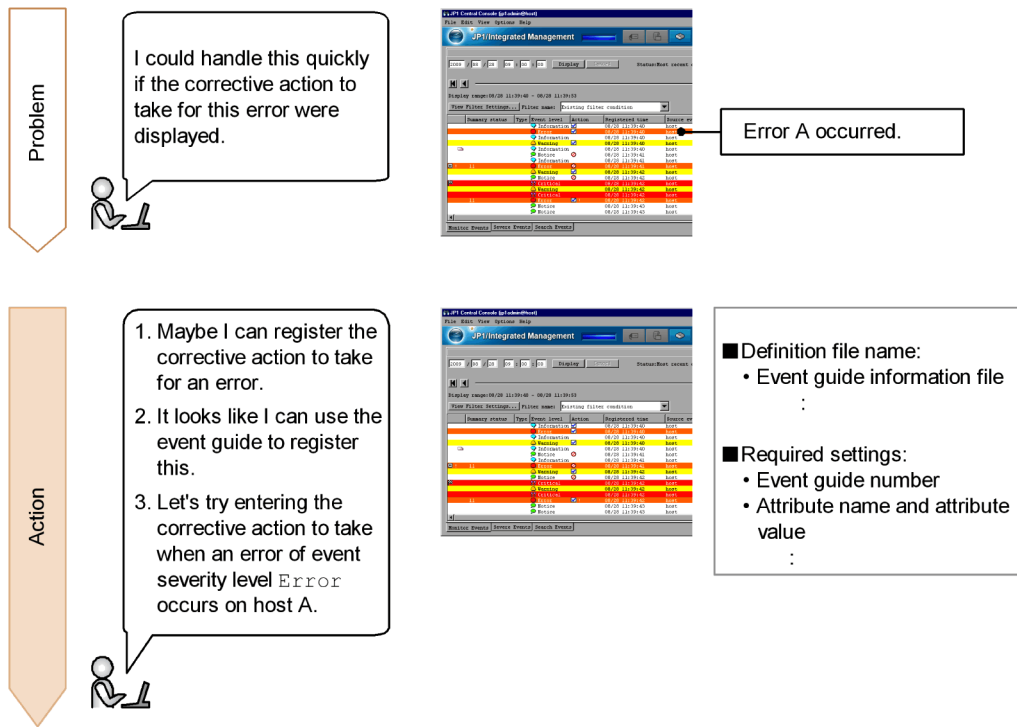


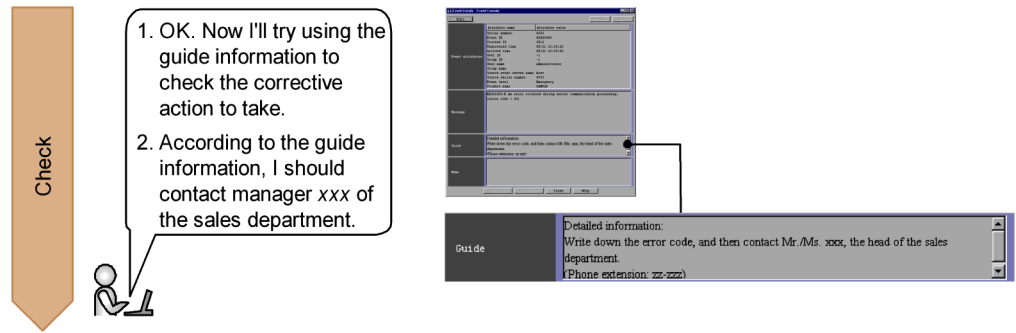
Keywords:

search event function, searching, investigation

4.3 Registering for later display the corrective action to take for previously-issued events

When an error occurs in a system, the system administrator handles the error according to the corrective action most appropriate for that error. However, it is almost impossible for the system administrator to keep track of the most appropriate corrective action for each case. To reduce the administrative workload on the system administrator, you can register the corrective action to take for an event so that it is displayed later.





4.3.1 Using the event guide function to register the corrective action to take

To register for later display the corrective action to take for events, you use the event guide function. To use the event guide function, you create an event guide information file named `jco_guide.txt`.

Prerequisite conditions:

- None

Let's register for later display the error handling to use when a user process on host A in the sales department terminates abnormally with an event of severity level Error.

Enter the following specifications in `jco_guide.txt`:

```
DESC_VERSION=1
[EV_GUIDE_1]
#Contact Information in Case of Abnormal Termination
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]
```

The following table explains these specifications:

Specification	Explanation
EV_COMP=E.SEVERITY:Error EV_COMP=B.SOURCESERVER:hostA	Specifies comparison conditions for the purpose of comparing events. Specify these conditions as follows: <ul style="list-style-type: none"> To match the severity level of Error: EV_COMP=E.SEVERITY:Error To match host A as the event-issuing source: 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 display in the event guide.

Save the event guide information file that you created in the following location:

- Windows:
 - Console-path*\conf\guide\
shared-folder\jplcons\conf\guide\ (logical host)
- UNIX:
 - /etc/opt/jplcons/conf/guide/
shared-directory/jplcons/conf/guide/ (logical host)

The defined settings are registered after you execute the `jco_spm�_reload` command or restart JP1/IM - Manager.

Restart JP1/IM - View as well if JP1/IM - View is connected.



References:

- See 4.6.1 *How to edit event guide information* in the *Configuration Guide*.
- See *Event guide information file (jco_guide.txt)* in Chapter 2 of the manual *Command and Definition File Reference*.

4.3.2 Verifying that the corrective action is registered

After you have finished using the event guide function to set the event guide information, check whether the corrective action you set for the event is registered.

To check whether the corrective action is registered:

- Using the procedure given in 1.2.2 *Verifying that you can execute a command*, enter the following settings in the Execute Command window.

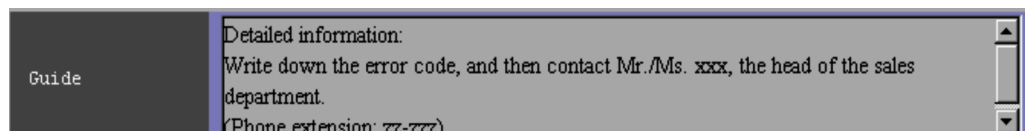
Item	Setting to enter
Target host	hostA
Command	jvsend -e SEVERITY=Error

On host A, an error-level event is issued.

2. Select the issued event in the events list and, in the Event Console window, choose **View**, and then **Event Details**.

Event guide information for the selected event is displayed in the Event Details window.

For this example, verify that the following is displayed:



Keywords:

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



Tip:

To start an application that is linked to the 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 *4.12 Setting monitor startup for linked products* in the *Configuration Guide*.

Index

A

abbreviations defined iv
Action Parameter Detailed Definitions window 45, 48
automated action function 45
automatic command execution 44

B

basic system configuration ix

C

Central Console
 associating events with correlation events 39
 automated action function 45
 automated action suppression 48
 common exclusion condition 33
 event display start-time specification function 52
 event guide function 59
 search events function 55
 severity changing function 29
 using 12
 view filter 25
Central Scope
 setting up map format 20
 setting up tree format 18
 using 17
common exclusion condition 33
Common Exclusion-Conditions Settings window 33
conventions
 abbreviations iv
 diagrams vi
 fonts and symbols vi
 KB, MB, GB and TB viii
 version numbers ix
correlation event generation definition file 40
correlation events 39
Create New Monitoring Node window 18

D

diagram conventions vi
Display/Edit Profiles window 12

E

Edit IM Configuration window 4
event acquisition filter 13
event display start-time specification function 52
event guide function 59
event guide information file 59
event receiver filter 13
Event Search Conditions window 56
events, searching for 55
Execute Command window 10

F

filtering events that are displayed 24
font conventions vi
forwarding filter 14

G

GB meaning viii

H

hosts
 registering 4
 removing from being monitored 32

I

IM Configuration Management
 defining system hierarchy 4
 registering hosts 4
 using 3
IM Configuration Management window 3

J

JP1/Base Environment Settings dialog box 8

K

KB meaning viii

M

map format 20

mapping JP1 user to OS user 8

MB meaning viii

multiple events, handling as single event 38

P

preventing action from executing during set time period 47

previously-issued events

checking status of 52

registering corrective action to take for 58

Properties window 19

R

Register Host window 4

S

search events function 55

Settings for View Filter window 25

setup

basic system 2

centrally managing events 11

command execution 7

visually monitoring events 17

severe events filter 13

severity changing definition file 29

severity changing function 29

severity level of events, changing 28

suppression 48

symbol conventions vi

syntax conventions vii

system hierarchy, defining 4

T

TB meaning viii

tree format 18

U

user mapping 8

V

version number conventions ix

view filter 13, 25

Visual Monitoring (Editing) window 20

Reader's Comment Form

We would appreciate your comments and suggestions on this manual. We will use these comments to improve our manuals. When you send a comment or suggestion, please include the manual name and manual number. You can send your comments by any of the following methods:

- Send email to your local Hitachi representative.
- Send email to the following address:
WWW-mk@itg.hitachi.co.jp
- If you do not have access to email, please fill out the following information and submit this form to your Hitachi representative:

Manual name:	
Manual number:	
Your name:	
Company or organization:	
Street address:	
Comment:	

(For Hitachi use)
