HITACHI
Inspire the Next

JP1 Version 11

JP1/Integrated Management - Manager Overview and System Design Guide

3021-3-A07-30(E)

Notices

■ Relevant program products

For details about the supported operating system versions and prerequisite service packs and patches for JP1/Integrated Management - Manager and JP1/Integrated Management - View, see the *Release Notes* accompanying each program product.

JP1/Integrated Management - Manager (for Windows):

P-2A2C-8EBL JP1/Integrated Management - Manager 11-50

The above product includes the following:

P-CC2A2C-9MBL JP1/Integrated Management - Manager 11-50 (for Windows Server 2016, Windows Server 2012, Windows Server 2008 R2)

P-CC2A2C-6HBL JP1/Integrated Management - View 11-50 (for Windows Server 2016, Windows 10, Windows 8.1, Windows 8, Windows Server 2012, Windows 7, Windows Server 2008 R2)

JP1/Integrated Management - Manager (for AIX):

P-1M2C-8EBL JP1/Integrated Management - Manager 11-50

The above product includes the following:

P-CC1M2C-9MBL JP1/Integrated Management - Manager 11-50 (for AIX)

P-CC2A2C-6HBL JP1/Integrated Management - View 11-50 (for Windows Server 2016, Windows 10, Windows 8.1, Windows 8, Windows Server 2012, Windows 7, Windows Server 2008 R2)

JP1/Integrated Management - Manager (for Linux):

P-812C-8EBL JP1/Integrated Management - Manager 11-50

The above product includes the following:

P-CC812C-9MBL JP1/Integrated Management - Manager 11-50 (for Linux 7, Linux 6 (x64), Oracle Linux 7, Oracle Linux 6 (x64), CentOS 7, CentOS 6 (x64))

P-CC9W2C-9MBL JP1/Integrated Management - Manager 11-50 (for SUSE Linux 12)

P-CC2A2C-6HBL JP1/Integrated Management - View 11-50 (for Windows Server 2016, Windows 10, Windows 8.1, Windows 8, Windows Server 2012, Windows 7, Windows Server 2008 R2)

■ Trademarks

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

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

IBM, AIX are trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide.

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

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

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

This product includes RSA BSAFE Cryptographic software of EMC Corporation.

■ Microsoft product name abbreviations

This manual uses the following abbreviations for Microsoft product names.

Abbreviation		Full name or meaning
Hyper-V		Microsoft$^{(R)}$ Windows Server$^{(R)}$ 2008 R2 Hyper-V$^{(R)}$
		Microsoft$^{(R)}$ Windows Server$^{(R)}$ 2012 Hyper-V$^{(R)}$
IE	Windows Internet Explorer	Windows$^{(R)}$ Internet Explorer$^{(R)}$
SCVMM		Microsoft$^{(R)}$ System Center Virtual Machine Manager 2008
		Microsoft$^{(R)}$ System Center Virtual Machine Manager 2012
Windows 7		Microsoft$^{(R)}$ Windows$^{(R)}$ 7 Enterprise
		Microsoft$^{(R)}$ Windows$^{(R)}$ 7 Professional
		Microsoft$^{(R)}$ Windows$^{(R)}$ 7 Ultimate
Windows 8		Windows$^{(R)}$ 8 Enterprise
		Windows$^{(R)}$ 8 Pro
Windows 8.1		Windows$^{(R)}$ 8.1 Enterprise
		Windows$^{(R)}$ 8.1 Pro
Windows 10		Windows$^{(R)}$ 10 Enterprise 32-bit
		Windows$^{(R)}$ 10 Enterprise 64-bit
		Windows$^{(R)}$ 10 Home 32-bit
		Windows$^{(R)}$ 10 Home 64-bit
		Windows$^{(R)}$ 10 Pro 32-bit
		Windows$^{(R)}$ 10 Pro 64-bit

Abbreviation		Full name or meaning
Windows Server 2008		Microsoft$^{(R)}$ Windows Server$^{(R)}$ 2008 Datacenter
		Microsoft$^{(R)}$ Windows Server$^{(R)}$ 2008 Enterprise
		Microsoft$^{(R)}$ Windows Server$^{(R)}$ 2008 Standard
Windows Server 2008 R2		Microsoft$^{(R)}$ Windows Server$^{(R)}$ 2008 R2 Datacenter
		Microsoft$^{(R)}$ Windows Server$^{(R)}$ 2008 R2 Enterprise
		Microsoft$^{(R)}$ Windows Server$^{(R)}$ 2008 R2 Standard
Windows Server 2012	Windows Server 2012	Microsoft$^{(R)}$ Windows Server$^{(R)}$ 2012 Datacenter
		Microsoft$^{(R)}$ Windows Server$^{(R)}$ 2012 Standard
	Windows Server 2012 R2	Microsoft$^{(R)}$ Windows Server$^{(R)}$ 2012 R2 Datacenter
		Microsoft$^{(R)}$ Windows Server$^{(R)}$ 2012 R2 Standard
Windows Server 2016		Microsoft$^{(R)}$ Windows Server$^{(R)}$ 2016 Datacenter
		Microsoft$^{(R)}$ Windows Server$^{(R)}$ 2016 Standard

Windows is sometimes used generically, referring to Windows Server 2016, Windows 10, Windows 8.1, Windows 8, Windows Server 2012, Windows 7, and Windows Server 2008 R2.

■ Restrictions

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

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

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

■ Issued

Nov. 2017: 3021-3-A07-30(E)

■ Copyright

Summary of amendments

The following table lists changes in this manual (3021-3-A07-30(E)) and product changes related to this manual.

Changes	Location
For linkage with JP1/Service Support, a new incident registration mode was added to allow any event attributes or character strings to be inherited.	*2.5*, *8.1.1*
A common exclusion-condition in extended mode can now exclude a JP1 event that satisfies the condition from automated-action execution.	*3.2*, *3.2.6*, *3.2.7*, *5.1*, *5.4.4*
A description was added for the common exclusion history file that logs the exclusion processes of common exclusion-conditions.	*3.2.7(5)*
A description was added for the common exclusion-conditions definition history file that logs the definition history of common exclusion-conditions.	*3.2.7(6)*
A note was added for the common exclusion-conditions.	*3.2.7(7)*
The maximum number of repeated event conditions was increased to 2,500. The total size of the definitions of repeated event conditions was increased to 15 MB.	*3.4.3*, *3.4.4*, *3.5.4*, *Appendix D.1(1)*, *Appendix D.1(2)*
Saving event listings (CSV snapshot) now includes action-excluded events.	*3.15.1(3)*
Saving event information from the integrated monitoring database (output of an event report) now includes the following event attributes: • Common exclude conditions group ID (`E.JP1_IMCOMEXCLUDE_ID`) • Common exclude conditions group name (`E.JP1_IMCOMEXCLUDE_NAME`) • Common exclude conditions group target-for-exclusion (`E.JP1_IMCOMEXCLUDE_TARGET`)	*3.15.2(3)*
Defined automated actions can now be enabled or disabled by using the Action Parameter Definitions window or the `jcachange` command.	*5.1*, *5.2*, *5.3*, *5.3.1*, *5.3.3*, *5.4.4*
A note was added for cases where the automated action function requests a large number of agents at once to execute a command.	*5.1*
For automated action definitions, the status of execution conditions can now be retained unless their definitions are changed.	*5.3.3*
A consideration on maintenance was added for excluding error events that are caused by maintenance work from action execution.	*11.1.3(1)(c)*, *12.10.1(2)*, *12.10.2(2)(b)*
The maximum number of hosts that can be managed by one instance of JP1/IM - Manager was increased to 2,500.	*12.1.3*, *Appendix D.1(1)*, *Appendix D.3(1)*
The following files were added to the list of files and folders: • Configuration file for incident inheritance information • Model file for the configuration file for incident inheritance information • Common exclusion history file • Common exclusion-conditions definition history file	*Appendix A.1(2)*, *Appendix A.2(2)*
The maximum number of hosts on which commands can be executed from one instance of JP1/IM - Manager was increased 2,500.	*Appendix D.1(1)*
The maximum number of defined common exclusion-conditions groups (in extended mode) was increased to 2,500. The maximum filter length of the common exclusion-conditions groups (in extended mode) was increased to 15 MB.	*Appendix D.1(1)*

Changes	Location
The maximum number of hosts that can be set in a business group or monitoring group was increased to 2,500.	*Appendix D.3(1)*

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

Preface

This manual provides an overview and describes the functionality and system design of JP1/Integrated Management - Manager and JP1/Integrated Management - View.

In this manual, JP1/Integrated Management is abbreviated to *JP1*, and JP1/Integrated Management - Manager and JP1/Integrated Management - View are generically referred to as *JP1/Integrated Management* or *JP1/IM*.

JP1/IM is a suite of integrated management products that provide the core foundation for performing integrated management of IT systems.

In addition to the integrated management products, the JP1 series of products listed below are mentioned in this manual. For further details, see the documentation accompanying the product.

Product name	Contents covered in this manual
JP1/Integrated Management - Rule Operation	• The role of JP1/Integrated Management - Rule Operation within the JP1/IM series • An overview of the JP1/IM - Rule Operation linkage function
JP1/Service Support	• The role of JP1/Service Support within the JP1 series
JP1/TELstaff	• The role of JP1/Integrated Management - TELstaff within the JP1/IM series
JP1/Integrated Management - Event Gateway for Network Node Manager i	• The role of JP1/Integrated Management - Event Gateway for Network Node Manager i within the JP1/IM series
JP1/Integrated Management - Message Optimizer	• The role of JP1/Integrated Management - Message Optimizer within the JP1/IM series
JP1/Navigation Platform	• The role of JP1/Navigation Platform within the JP1 series • An overview of the JP1/Navigation Platform linkage function
JP1/Automatic Job Management System 3	• The role of JP1/Automatic Job Management System 3 within the JP1 series • An overview of the JP1/AJS linkage function
JP1/Performance Management	• The role of JP1/Performance Management within the JP1 series • An overview of the JP1/PFM linkage function

■ Intended readers

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

- System administrators who are considering introducing JP1/IM to centrally monitor events that occur in the system
- Those who have knowledge of operating systems and applications

■ Organization of this manual

This manual is organized into the following parts:

PART 1: Overview

This part provides an overview of the integrated management products, the JP1 series products, and JP1/IM.

PART 2: Functionality

This part describes the functionality of JP1/IM.

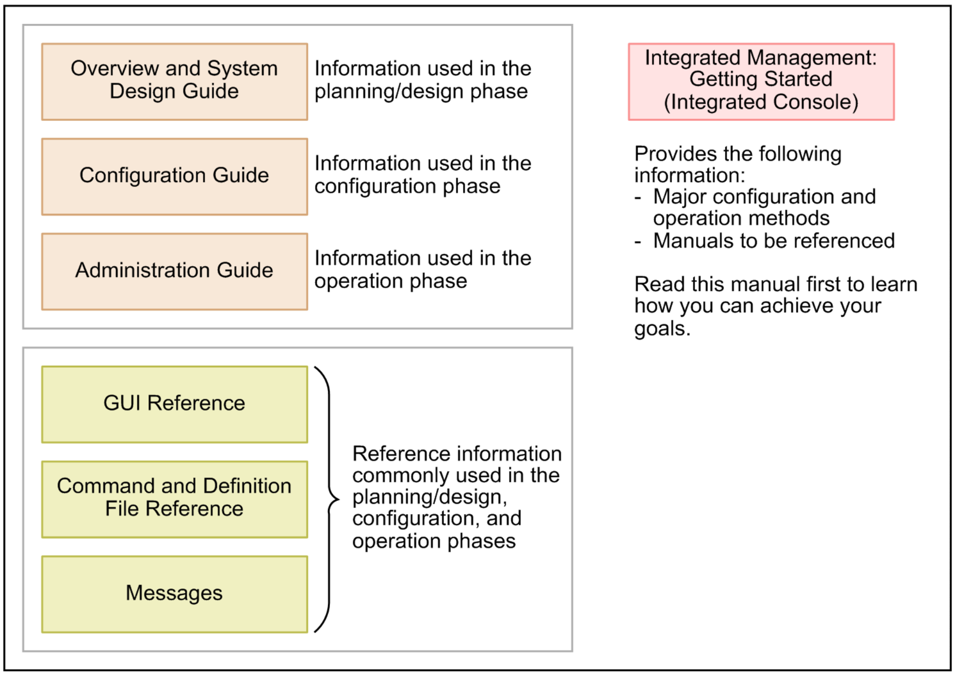
PART 3: Design

This part describes the requirements for the monitoring tasks supported by JP1/IM and the system requirements for achieving those objectives.

■ Manual suite

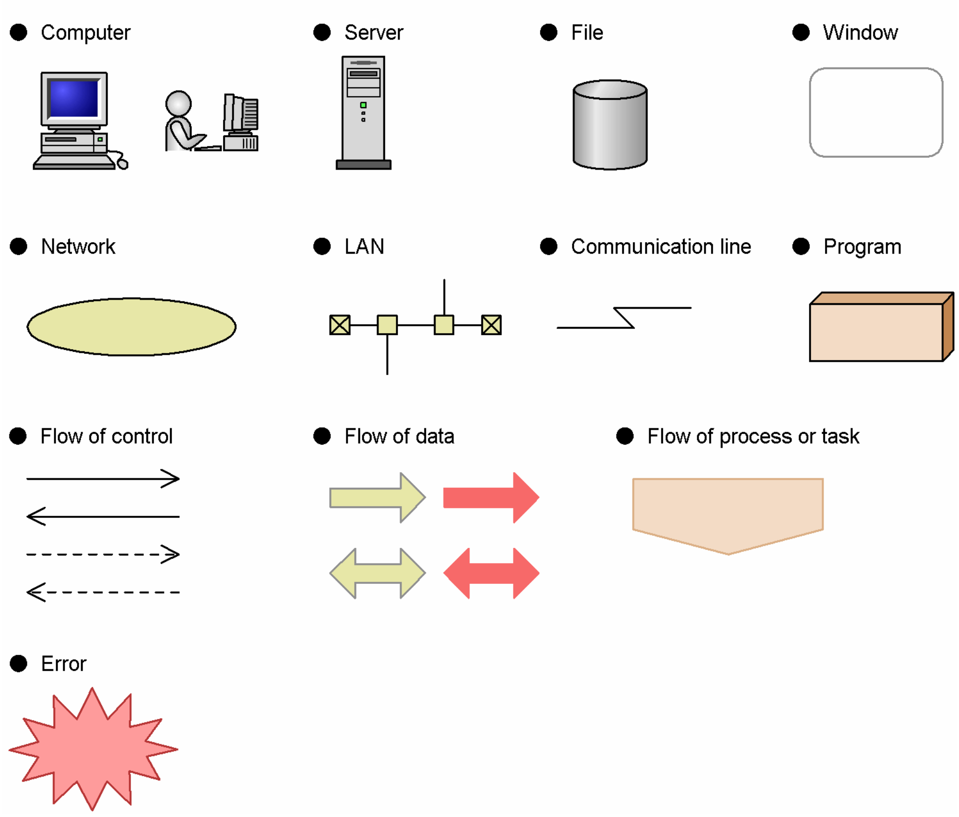
JP1/IM manuals provide necessary information according to the phases in the system life cycle, which include planning and design, configuration, and operation.

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


Overview and System Design Guide
Information used in the planning/design phase
Configuration Guide
Information used in the configuration phase
Administration Guide
Information used in the operation phase
GUI Reference
Command and Definition File Reference
Messages
Reference information commonly used in the planning/design, configuration, and operation phases
Integrated Management: Getting Started (Integrated Console)
Provides the following information:
- Major configuration and operation methods
- Manuals to be referenced
Read this manual first to learn how you can achieve your goals.

■ Conventions: Diagrams

This manual uses the following conventions in diagrams:



■ Conventions: Fonts and symbols

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

Text formatting	Convention
Bold	Bold characters indicate text in a window, other than the window title. Such text includes menus, menu options, buttons, radio box options, or explanatory labels. For example: • From the **File** menu, choose **Open**. • Click the **Cancel** button. • In the **Enter name** entry box, type your name.
Italic	Italic characters indicate a placeholder for some actual text to be provided by the user or system. For example: • Write the command as follows: `copy` *source-file target-file* • The following message appears: `A file was not found. (file =` *file-name*`)` Italic characters are also used for emphasis. For example: • Do *not* delete the configuration file.
`Monospace`	Monospace characters indicate text that the user enters without change, or text (such as messages) output by the system. For example: • At the prompt, enter `dir`. • Use the `send` command to send mail. • The following message is displayed: `The password is incorrect.`

The following table explains the symbols used in this manual:

Symbol	Convention
|	In syntax explanations, a vertical bar separates multiple items, and has the meaning of OR. For example: `A|B|C` means `A`, or `B`, or `C`.
`{ }`	In syntax explanations, curly brackets indicate that only one of the enclosed items is to be selected. For example: `{A|B|C}` means only one of `A`, or `B`, or `C`.
`[ ]`	In syntax explanations, square brackets indicate that the enclosed item or items are optional. For example: `[A]` means that you can specify `A` or nothing. `[B|C]` means that you can specify `B`, or `C`, or nothing.
`...`	In coding, an ellipsis (`...`) indicates that one or more lines of coding have been omitted. In syntax explanations, an ellipsis indicates that the immediately preceding item can be repeated as many times as necessary. For example: `A, B, B, ...` means that, after you specify `A, B,` you can specify B 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 default installation folders of JP1/IM and JP1/Base for Windows are represented as follows:

Product name	Installation folder notation	Default installation folder#
JP1/IM - View	*view-path*	*system-drive*`:\Program Files\Hitachi\JP1CoView`
JP1/IM - Manager	*manager-path*	*system-drive*`:\Program Files\Hitachi\JP1IMM`
	console-path	*system-drive*`:\Program Files\Hitachi\JP1Cons`
	scope-path	*system-drive*`:\Program Files\Hitachi\JP1Scope`
JP1/Base	*base-path*	*system-drive*`:\Program Files\Hitachi\JP1Base`

#: Represents the installation folder when the product is installed in the default location. The location represented by *system-drive*`:\Program Files` is determined at the time of installation by an OS environment variable, and might differ depending on the environment.

■ Conventions: Meaning of "Administrator permissions" in this manual

In this manual, *Administrator permissions* refers to Administrator permissions for the local PC. The local user, domain user, or user of the Active Directory environment can perform tasks requiring Administrator permissions if granted Administrator permissions for the local PC.

■ Conventions: Version numbers

The version numbers of Hitachi program products are usually written as two sets of two digits each, separated by a hyphen. For example:

- Version 1.00 (or 1.0) is written as 01-00.
- Version 2.05 is written as 02-05.

- Version 2.50 (or 2.5) is written as 02-50.
- Version 12.25 is written as 12-25.

The version number might be shown on the spine of a manual as *Ver. 2.00,* but the same version number would be written in the program as *02-00*.

■ Online manual

JP1/IM comes with an HTML manual that you can read in a Web browser.

The HTML manual has the same contents as this manual.

To view the HTML manual:

- In JP1/IM - View, choose **Help** and then **Help Contents**.

Note:

- Depending on the OS settings, the HTML manual might appear in the active window when opened from the **Start** menu.

Contents

Part 1: Overview

Part 2: Functionality

Part 3: Design

1 Overview of JP1/Integrated Management

The integrated management products are a suite of programs for managing an entire corporate information system. With the growing size and complexity of the systems underpinning an enterprise's business operations, management of the system operation is a vital issue. The integrated management products optimize system operations management by offering integrated management tailored to objectives and integration of operational tasks.

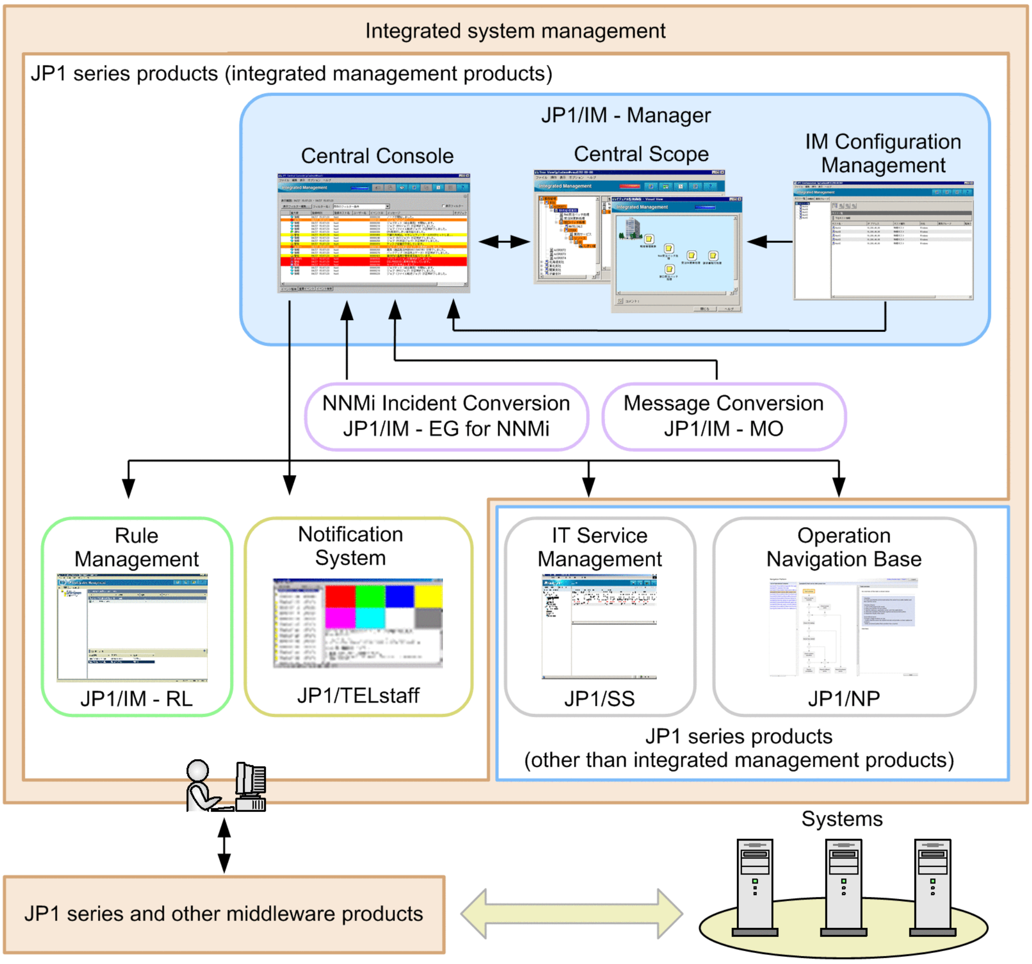
This chapter provides an overview of the integrated management products and the JP1/IM series of products that can be linked with JP1/IM - Manager. The chapter also describes the features and organization of JP1/IM - Manager, which provides the integrated management functionality central to the integrated management products.

1.1 Introducing the integrated management products

The integrated management products are a family of core products for implementing integrated management of an IT system. The integrated management products enable you to centrally manage information about a system's myriad resources, and enable centralized monitoring and operation across the entire IT system.

The integrated management products link with a wide range of middleware, including other JP1 products that provide job management and storage management functionalities. Integrated management products enable integrated system management to be implemented through configuration and operations management on a system-wide basis.

Figure 1–1: Integrated system management by the integrated management products



The integrated management products optimize system management by managing the configuration information created while planning and building the system, as well as the operational information generated during system operation. By providing a core platform for system management, JP1/IM offers full support for the entire workflow - from designing and building the system, through operation, redesign, and rebuild.

1.2 System management issues and integrated management

The need for system management as provided by the integrated management products stems from the various challenges that IT systems present as they become more sophisticated.

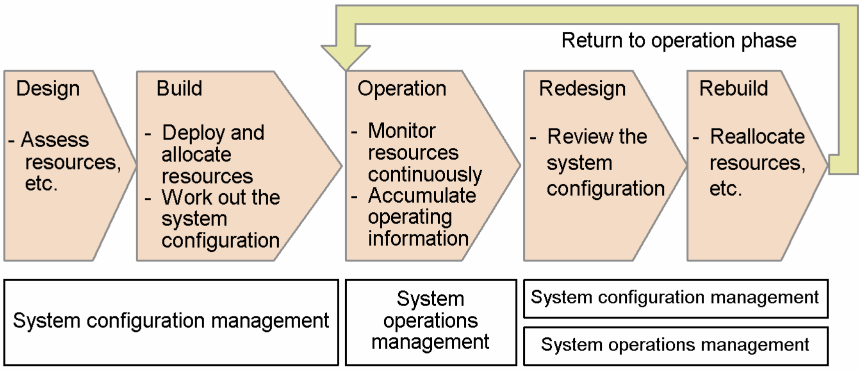
For many enterprises, IT systems are indispensable as the foundation of their business operations. Corporate IT systems are growing in scale and complexity to meet the various demands placed upon them. This in turn makes system management more onerous and costly. Optimizing system operations management is a vital concern.

1.2.1 System life cycle

An IT system comprises a diverse range of resources, including servers, networks, and other hardware, and software-based operations such as job execution and security monitoring.

To make proper use of these various resources, administrative tasks must be carried out on an ongoing basis. These include assessing and re-allocating resources, and quickly detecting and resolving any problems that occur in those resources. The workflow and processes involved in ensuring that the system runs reliably are referred to as the *system life cycle*. The system life cycle consists of five phases: system design, build, operation, redesign, and rebuild. The following figure shows the life cycle phases and associated administrative tasks.

Figure 1–2: System life cycle


Return to operation phase
Design
- Assess resources, etc.
Build
- Deploy and allocate resources
- Work out the system configuration
Operation
- Monitor resources continuously
- Accumulate operating information
Redesign
- Review the system configuration
Rebuild
- Reallocate resources, etc.
System configuration management
System operations management
System configuration management
System operations management

As this figure shows, the administrative tasks differ at each phase of the system life cycle, as does the information that needs to be managed at each phase. The integrated management products optimize management of system information at each phase of the system life cycle and provide a framework of support for stable system operation.

The following describes system management issues and the role of the integrated management products at each phase of the system life cycle.

1.2.2 Issues and the role of the integrated management products at the design and build phase

At the design and build phase, you must first consider how to configure the system as a whole. Then you must plan how to deploy and build the resources needed for the processing that the system will perform. To fulfill these tasks, information about the system components needs to be properly managed. This is referred to as *system configuration management*.

The design and build phase is a repeated process of assessing resources, working out the system configuration, deploying resources, pre-operation testing and debugging.

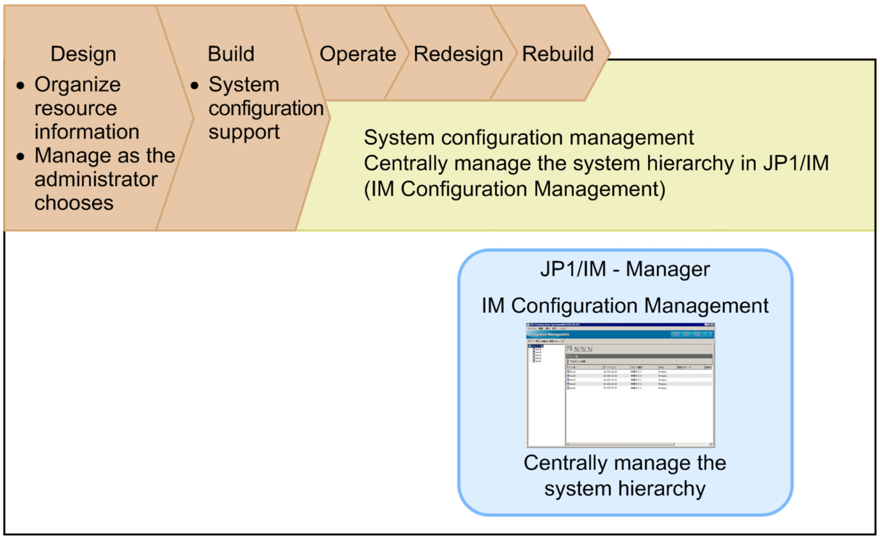
As the resources in a system grow in number, it becomes harder to keep track of them all. Managing the system configuration becomes ever more complex too.

The following table and figure list and describe the product in the integrated management product suite that is provided to support system configuration management.

Table 1–1: Products for system configuration management

Product	Functionality	Role
JP1/IM - Manager	IM Configuration Management	Manages the system hierarchy managed by JP1/IM (IM configuration) and the settings of the hosts that make up the system from the manager by using GUI and supports configuring the system. To use IM Configuration Management, you must set up the IM Configuration Management database.

Figure 1–3: System configuration management


Design
• Organize resource information
• Manage as the administrator chooses
Build
• System configuration support
Operate
Redesign
Rebuild
System configuration management
Centrally manage the system hierarchy in JP1/IM
(IM Configuration Management)
JP1/IM - Manager
IM Configuration Management
Centrally manage the system hierarchy

The integrated management products provide functionality for collecting all resource information in one location, where it can be organized and managed as the administrator chooses. The JP1/IM programs support system configuration management by facilitating the organization and classification of resource information in ways that the administrator finds easiest to manage. This functionality optimizes configuration management even in systems with huge volumes of resource information.

1.2.3 Issues and the role of the integrated management products at the operation phase

To ensure stable system operation during the operation phase, the resources configured in the system need to be monitored round the clock. Monitoring depends on proper management of system operating information and error information. This is referred to as *system operations management*.

In running a system, the processes of monitoring, error detection, investigation, and resolution are handled as a single ongoing cycle.

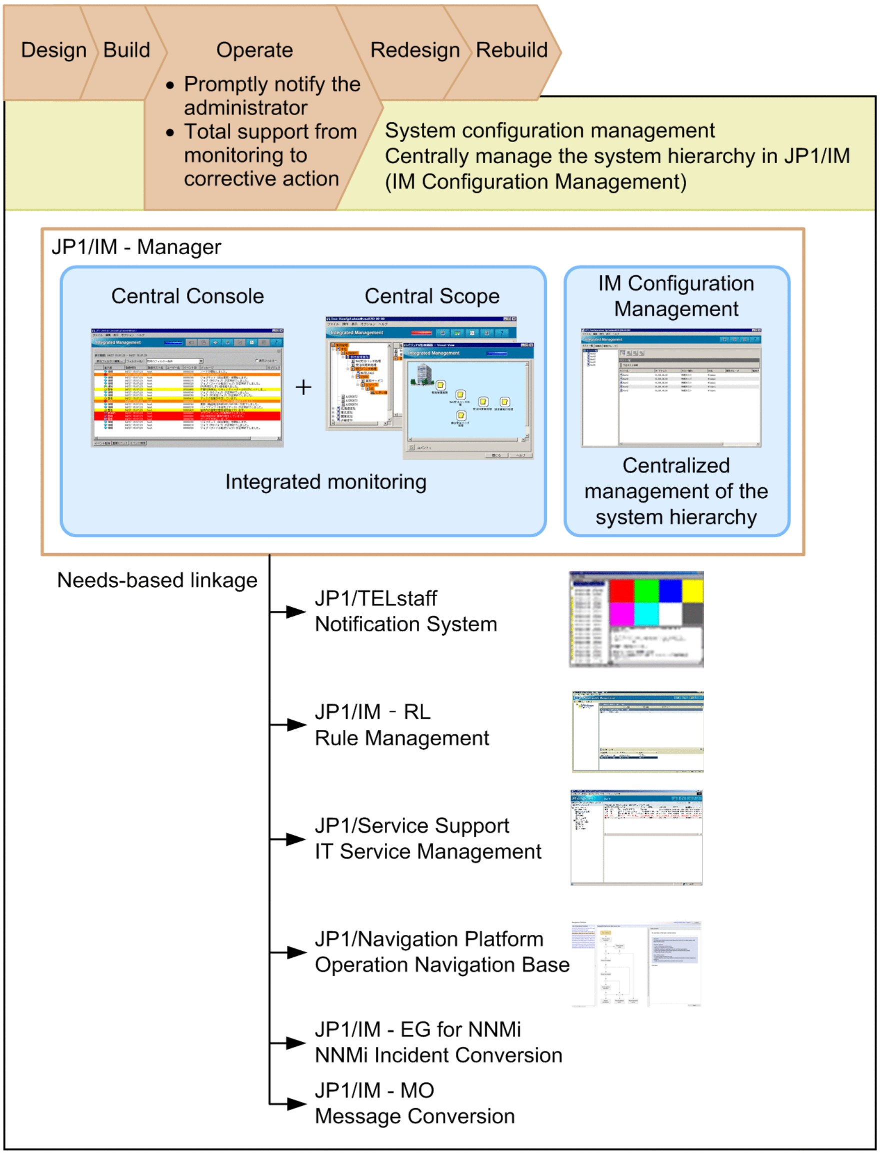
As a system grows in size and complexity, it becomes exponentially more difficult to perform the tasks involved in this operational cycle. The administrator is burdened with a growing workload, and requires a broad range of advanced skills to properly manage the vast array of resources. This puts huge demands on operations management, making the training of system administrators more challenging too.

The following table and figure list and describe the products in the integrated management product suite that are provided to support system operations management, as well as the JP1 series products that are explained in this manual.

Table 1–2: Products for system operations management

Product	Functionality	Role
JP1/IM - Manager	Central Console	Centrally monitors the system as a whole using JP1 events. Integrates all aspects of the operating cycle, from event monitoring to error detection, investigation, and resolution.
	Central Scope	Centrally manages the system based on requirements set by the system administrator, enabling integrated objective-oriented system management.
	IM Configuration Management	Manages the system hierarchy managed by JP1/IM (IM configuration) and the settings of the hosts that make up the system from the manager by using GUI.
JP1/IM - Rule Operation	Rule Management	Defines error-handling procedures and automatically executes actions based on the nature of the error.
JP1/TELstaff	Notification System	Notifies the person in charge of handling failures by telephone or email when a failure is detected.
JP1/Service Support	IT Service Management	Registers queries, failure events, and problems resulting from failure events as items requiring resolution, and centralizes their management.
JP1/IM - EG for NNMi	NNMi Incident Conversion	Converts NNMi incidents managed by NNMi into JP1 events.
JP1/IM - Message Optimizer	Message Conversion	Converts the messages that are output to the JP1/IM console into easy-to-understand messages.
JP1/Navigation Platform	Operation Navigation	Displays application information (operating procedures) applicable to JP1 events.
JP1/AJS	Job Scheduler	Manages automatic job execution.
JP1/PFM	Performance Management	Manages host performance.

Figure 1–4: System operations management



Note: Central Console can be linked with notification System, Incident Management, Rule Management, and IT Service Management.

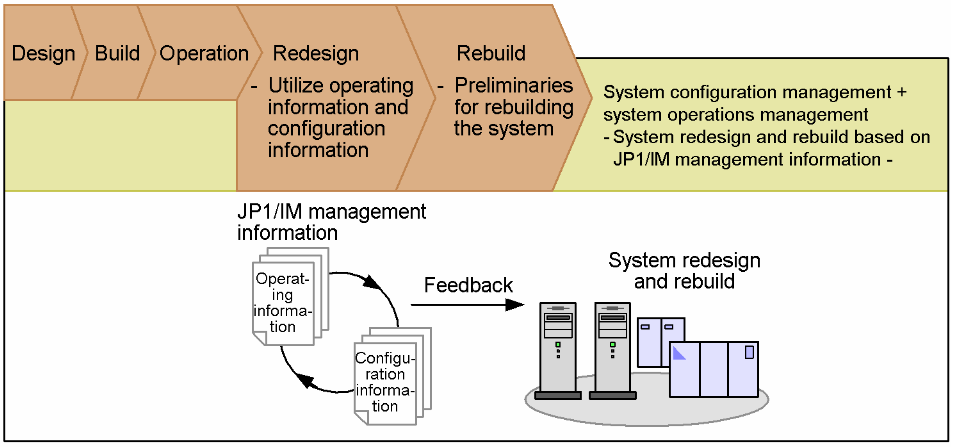
The integrated management products provide a platform for continuous system monitoring and immediate administrator notification whenever a problem occurs, as well as operational tasks such as error identification and investigation. The JP1/IM programs provide integrated operating cycle support, from monitoring through to troubleshooting. JP1/IM optimizes operations management even in large-scale, complex systems.

1.2.4 Issues and the role of the integrated management products at the redesign and rebuild phase

The redesign and rebuild phase entails evaluating performance based on the system operating information, organizing the system configuration information as needed, and rethinking the system configuration.

You will need to redeploy resources if a particular resource is prone to frequent errors that affect job processing performance. Resource redeployment could have far-reaching effects, beyond the resources in the immediate environment. You will need a good understanding of the system configuration information created at the design and build phase, and you will need to select and deploy appropriate resources based on the operating information accumulated during the operation phase.

Figure 1–5: System rebuild


Design
Build
Operation
Redesign
- Utilize operating information and configuration information
Rebuild
- Preliminaries for rebuilding the system
System configuration management + system operations management
- System redesign and rebuild based on JP1/IM management information -
JP1/IM management information
Operat-ing informa-tion
Configu-ration informa-tion
Feedback
System redesign and rebuild

At the redesign and rebuild phase, the integrated management products assist the administrator by optimizing management of the configuration information created at the design and build phase, as well as of the operating information generated at the operation phase, as discussed above. This helps to minimize the administrator's workload when redesigning and rebuilding the system, and maximizes use of the management information accumulated at the design, build, and operation phases.

1.3 Features of JP1/IM - Manager

The previous sections introduced the integrated management products as a whole. This section describes JP1/IM - Manager.

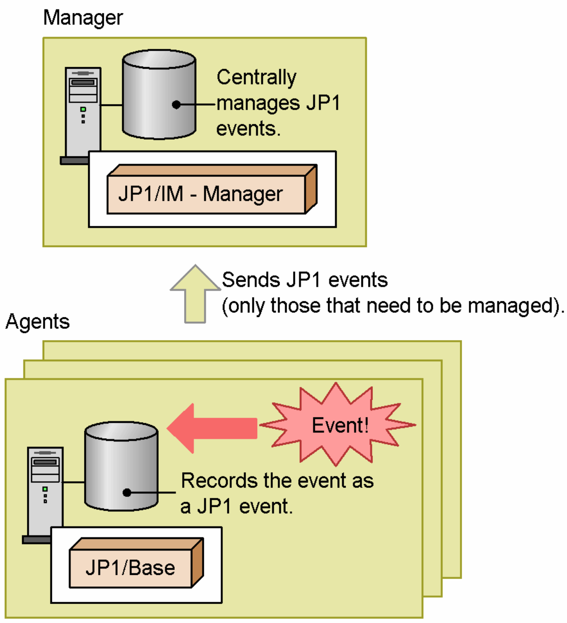
Through the features described below, JP1/IM - Manager integrates monitoring and operation into a unified management process. By simplifying complex tasks, JP1/IM - Manager reduces the workload involved in running a system.

1.3.1 Integrated management using JP1 events

JP1/IM - Manager centrally manages the various events that occur in the system as JP1 events. Events generated by JP1/Base, which provides the core functionality for integrated management, are managed by the agent hosts in the system as JP1 events. The agents forward JP1 events to JP1/IM - Manager for centralized management as needed.

Alternatively, JP1 events accumulated at an agent can be acquired by JP1/IM - Manager and managed at the JP1/IM - Manager side.

Figure 1–6: Integrated management using JP1 events


Manager
Centrally manages JP1 events.
JP1/IM - Manager
Sends JP1 events (only those that need to be managed).
Agents
Event!
Records the event as a JP1 event.
JP1/Base

Implementing integrated management by simply collecting all JP1 events would result in a deluge of events across the system. Severe events could easily be overlooked, making operations management more difficult. Too many events would also place a greater load on the monitoring system. Using event filtering, JP1/IM - Manager selects only those events relevant to operations management, allowing JP1 events to be managed appropriately. The filtering feature gives you various choices: You can select which events to send to JP1/IM - Manager, and which to treat as severe events.

In addition, JP1/IM - Manager can manage the following events:

- Events (such as messages in the log files, the Windows event logs, and SNMP traps managed by HP NNM version 7.5 or earlier) that are converted into JP1 events by JP1/Base event conversion. JP1/IM - Manager can also manage events issued by a user application calling a command or the API.
- Events (such as messages in the log files and the Windows event logs) that are issued on hosts on which JP1/Base has not been installed and that are converted into JP1 events by remote monitoring based on the remote communication settings.

A monitored host for which the remote communication settings have been set is called *a remotely monitored host*.

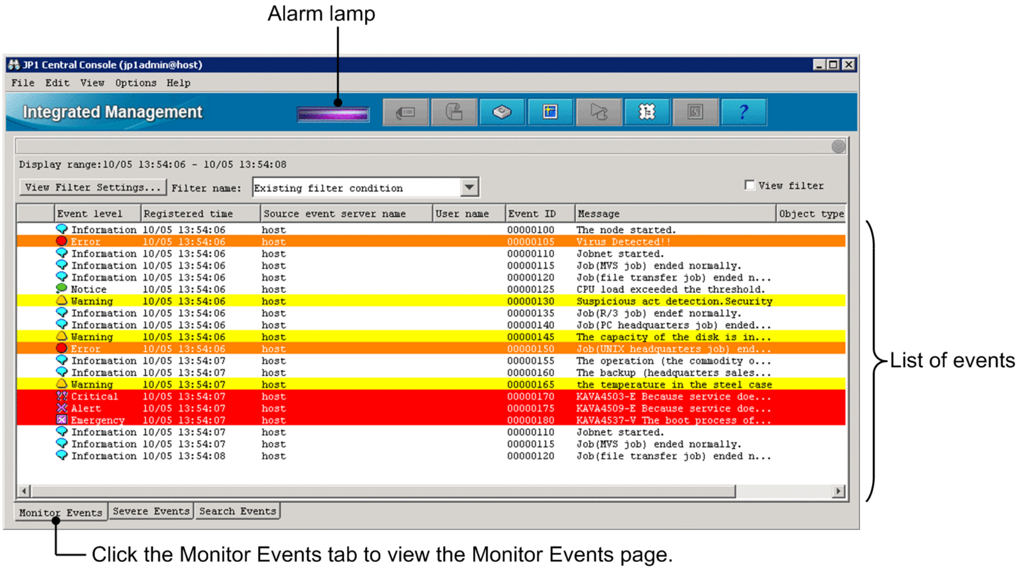
- NNMi incidents converted into JP1 events by JP1/IM - EG for NNMi. For details about NNMi incidents, see the manual *Job Management Partner 1/Integrated Management - Event Gateway for Network Node Manager i Description, User's Guide and Reference*.
- Events handled by a wide variety of non-JP1 products and converted into JP1 events.

1.3.2 Centralized system monitoring

JP1/IM - Manager can centrally monitor the system in its entirety via the Central Console and Central Scope.

The Central Console centrally monitors events in the system by collecting JP1 events as they occur and displaying them in a time series. JP1 events are displayed on the **Monitor Events** page of the Event Console window, so you can monitor everything that is happening across the entire system.

Figure 1–7: Event Console window (Monitor Events page)



JP1 Central Console (jp1admin@host)
File Edit View Options Help
Integrated Management
?
Monitor Events
Severe Events
Search Events

Display range:10/05 13:54:06 - 10/05 13:54:08

View Filter Settings... Filter name: Existing filter condition

□ View filter

Event level	Registered time	Source event server name	User name	Event ID	Message	Object type
Information	10/05 13:54:06	host		00000100	The node started.	
Error	10/05 13:54:06	host		00000105	Virus Detected!!	
Information	10/05 13:54:06	host		00000110	Jobnet started.	
Information	10/05 13:54:06	host		00000115	Job(MVS job) ended normally.	
Information	10/05 13:54:06	host		00000120	Job(file transfer job) ended n...	
Notice	10/05 13:54:06	host		00000125	CPU load exceeded the threshold.	
Warning	10/05 13:54:06	host		00000130	Suspicious act detection.Security	
Information	10/05 13:54:06	host		00000135	Job(R/3 job) endef normally.	
Information	10/05 13:54:06	host		00000140	Job(PC headquarters job) ended...	
Warning	10/05 13:54:06	host		00000145	The capacity of the disk is in...	
Error	10/05 13:54:06	host		00000150	Job(UNIX headquarters job) end...	
Information	10/05 13:54:07	host		00000155	The operation (the commodity o...	
Information	10/05 13:54:07	host		00000160	The backup (headquarters sales...	
Warning	10/05 13:54:07	host		00000165	the temperature in the steel case	
Critical	10/05 13:54:07	host		00000170	KAVA4503-E Because service doe...	
Alert	10/05 13:54:07	host		00000175	KAVA4509-E Because service doe...	
Emergency	10/05 13:54:07	host		00000180	KAVA4537-V The boot process of...	
Information	10/05 13:54:07	host		00000110	Jobnet started.	
Information	10/05 13:54:07	host		00000115	Job(MVS job) ended normally.	
Information	10/05 13:54:08	host		00000120	Job(file transfer job) ended n...	

Alarm lamp

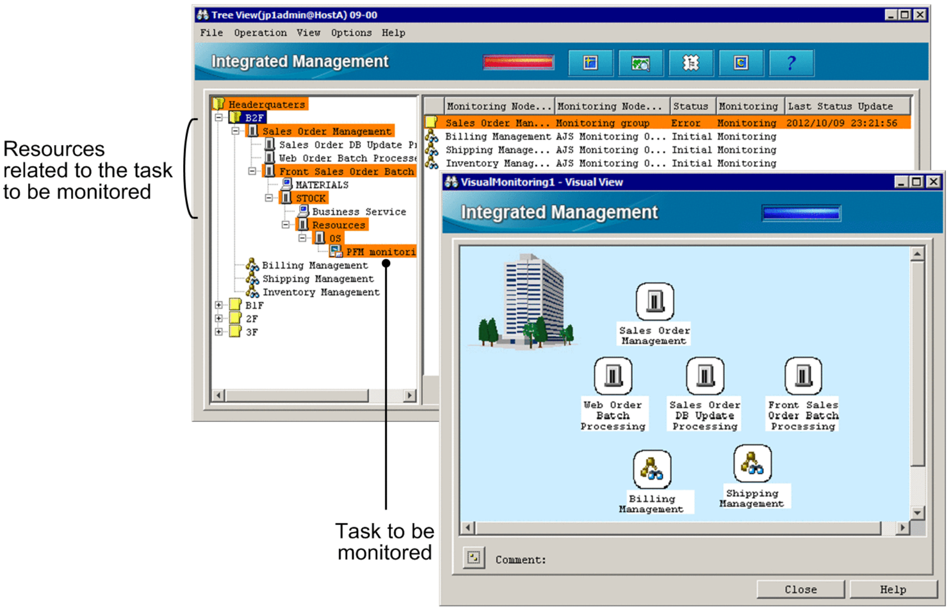
List of events

Click the Monitor Events tab to view the Monitor Events page.

Using the Central Scope, the administrator can centrally monitor the system from any chosen viewpoint. The entire system can be displayed in a tree view matched to your purpose, providing a visual understanding of the relationships between the tasks in progress and system resources. Essential monitoring points can also be mapped geographically, enabling centralized monitoring from the required viewpoints, no matter how large the system.

In the Monitoring Tree window, you can group resources and centrally monitor the system in a tree view. In the Visual Monitoring window, you have a map view of objects you selected in a monitoring tree.

Figure 1–8: Monitoring Tree window

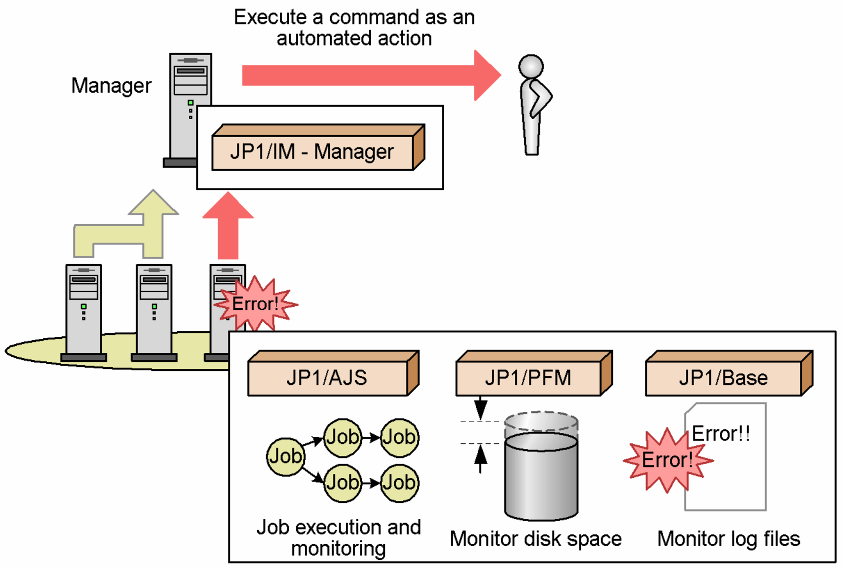


Monitoring Node...	Monitoring Node...	Status	Monitoring	Last Status Update
Sales Order Man...	Monitoring group	Error	Monitoring	2012/10/09 23:21:56
Billing Management	AJS Monitoring O...	Initial	Monitoring	
Shipping Manage...	AJS Monitoring O...	Initial	Monitoring	
Inventory Manag...	AJS Monitoring O...	Initial	Monitoring	

1.3.3 Error detection and reporting

JP1/IM - Manager supports automated actions as a means of detecting and reporting problems in the system. An *automated action* is the automatic execution of a command on a host managed by JP1/IM - Manager when a particular JP1 event is received. Commands for sending an email or making a telephone call can be executed as automated actions, notifying the administrator of any problems occurring in the system.

Figure 1–9: Error reporting using automated actions



Using the Central Scope, the location of a problem can be represented visually in a tree view or map format, allowing on-the-spot judgment of how the problem in the system might affect business operations.

1.3.4 Measures to handle a large number of JP1 events

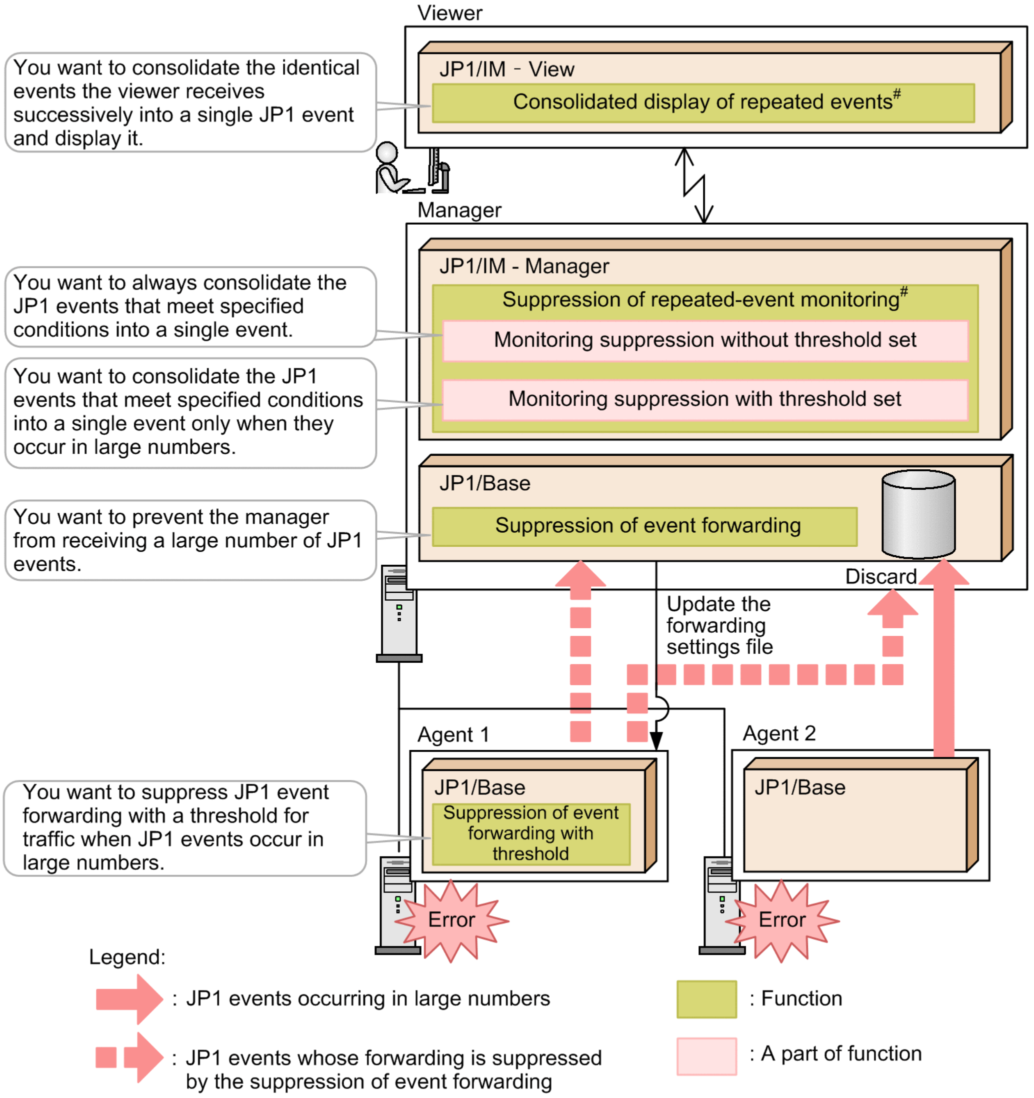
If an event triggers the occurrence of a large number of JP1 events, the JP1 events might fill the relevant event list and cause excessive commands to be automatically executed as automated actions. This might disrupt normal monitoring of JP1 events.

JP1/IM - Manager enables you to take the following measures to handle a large number of JP1 events in combination with the suppression of event transfer by JP1/Base:

- Setting a threshold for JP1 event traffic to suppress event transfer when a large number of JP1 events occur on agents
- Preventing the manager from receiving the JP1 events that have occurred on agents
- Consolidating a large number of JP1 events into a single JP1 event only when those JP1 events meet specified conditions
- Always consolidating the JP1 events that meet specified conditions into a single JP1 event
- Consolidating and displaying identical JP1 events received in succession by the viewer, as a single JP1 event

The following figure shows the measures to handle a large number of JP1 events and corresponding functions of JP1/IM - Manager.

Figure 1–10: Measures to handle a large number of JP1 events and corresponding functions of JP1/IM - Manager


Viewer
JP1/IM - View
Consolidated display of repeated events#
You want to consolidate the identical events the viewer receives successively into a single JP1 event and display it.
Manager
JP1/IM - Manager
Suppression of repeated-event monitoring#
Monitoring suppression without threshold set
Monitoring suppression with threshold set
You want to always consolidate the JP1 events that meet specified conditions into a single event.
You want to consolidate the JP1 events that meet specified conditions into a single event only when they occur in large numbers.
JP1/Base
Suppression of event forwarding
You want to prevent the manager from receiving a large number of JP1 events.
Discard
Update the forwarding settings file
Agent 1
JP1/Base
Suppression of event forwarding with threshold
Agent 2
JP1/Base
You want to suppress JP1 event forwarding with a threshold for traffic when JP1 events occur in large numbers.
Error
Error
Legend:
: JP1 events occurring in large numbers
: JP1 events whose forwarding is suppressed by the suppression of event forwarding
: Function
: A part of function

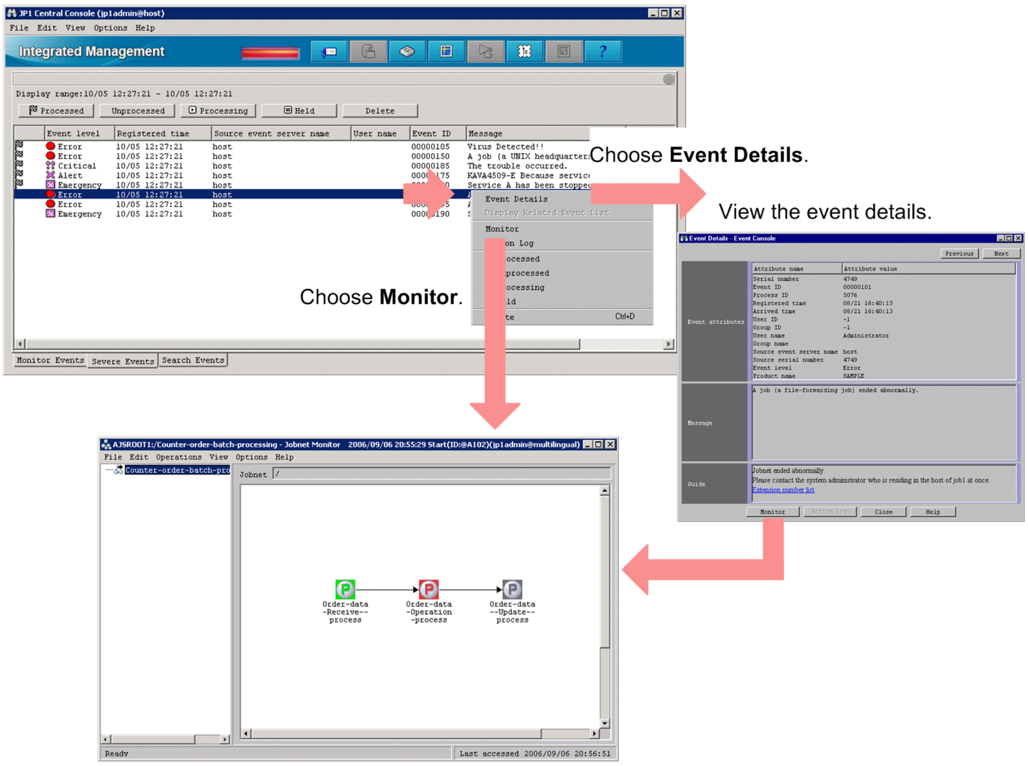
#:The suppression of repeated-event monitoring and the consolidated display of repeated events operate exclusively. You cannot use the two functions together at the same time.

Taking the above measures to handle a large number of JP1 events enables normal monitoring of the system.

1.3.5 Integrated troubleshooting with JP1/IM - Manager

All operational tasks from monitoring to error investigation can be integrated into a single flow of operations based on JP1/IM - Manager. In the Event Console window of the Central Console, you can select a JP1 event and view the event details. You can also directly launch related applications when needed.

Figure 1–11: Error investigation with JP1/IM - Manager



The selected event reports a problem.

JP1 Central Console (jp1admin@host)

Display range:10/05 12:27:21 - 10/05 12:27:21

Event level	Registered time	Source event server name	User name	Event ID	Message
Error	10/05 12:27:21	host		00000105	Virus Detected!!
Error	10/05 12:27:21	host		00000150	A job (a UNIX headquarter
Critical	10/05 12:27:21	host		00000185	The trouble occurred.
Alert	10/05 12:27:21	host		000 175	KAVA4509-E Because servic
Emergency	10/05 12:27:21	host			Service A has been stoppe
Error	10/05 12:27:21	host			
Error	10/05 12:27:21	host			
Emergency	10/05 12:27:21	host		000 190	

Choose **Event Details**.

Choose **Monitor**.

View the event details.

Event Details - Event Console

Attribute name	Attribute value
Serial number	4749
Event ID	00000101
Process ID	5076
Registered time	08/21 16:40:13
Arrived time	08/21 16:40:13
User ID	-1
Group ID	-1
User name	Administrator
Group name	
Source event server name	host
Source serial number	4749
Event level	Error
Product name	SAMPLE

Message: A job (a file-forwarding job) ended abnormally.

Guide: Jobnet ended abnormally.
Please contact the system administrator who is residing in the host of job1 at once.
Extension number list

Previous
Next
Event attributes
Message
Guide
Monitor
Action Log
Close
Help
AJSROOT1:/Counter-order-batch-processing - Jobnet Monitor 2006/09/06 20:55:29 Start(ID:@A102)(jp1admin@multilingual)
File Edit Operations View Options Help
Counter-order-batch-pro
Jobnet /
Order-data -Receive-- process
Order-data -Operation -process
Order-data --Update-- process
Ready
Last accessed 2006/09/06 20:56:51

Monitor startup
Opens JP1/AJS - View where you can directly view the job in which the error that triggered the JP1 event occurred.

Non-JP1 applications required in managing system operations can also be registered, creating an integrated workflow based on JP1/IM - Manager.

1.3.6 Easy-to-build monitoring system

Automatic generation of a monitoring tree in the Central Scope enables you to collect information about the active system and to create a monitoring window. If the system is modified, difference information can be collected and the monitoring window updated.

JP1/IM - Manager definition information can be distributed as a batch to the monitored hosts, allowing even a large-scale system to be configured with ease.

1.3.7 Flexible system configuration

The scalability of JP1/IM's management support means that systems of any size can be managed, from small office systems to large-scale hierarchical systems. Cross-platform systems that incorporate a mixture of Windows, UNIX or UNIX variants, mainframes or other operating systems are also supported.

JP1/IM - Manager also supports networks with firewalls, cluster systems, and other types of system configurations.

1.3.8 Integrated management of the system hierarchy and host settings

In a JP1/IM system, you can hierarchically configure and define managers and agents to centralize the management of systems of any size, from small systems to large systems serving an entire enterprise.

IM Configuration Management enables you to operate the IM configuration management viewer to centrally manage, from the manager, the system hierarchy managed by JP1/IM (IM configuration) and the host settings. To use IM Configuration Management, you must set up the IM Configuration Management database.

IM Configuration Management provides the following functionality:

- Host management

  You can register the hosts in the network as management targets with IM Configuration Management. You can also manage host information, such as the host name and IP address of each registered host.

- Management of the system hierarchy

  You can define the hierarchical structure of the system managed by JP1/IM, and apply information about the hierarchy (configuration definition information) to the system as a whole.

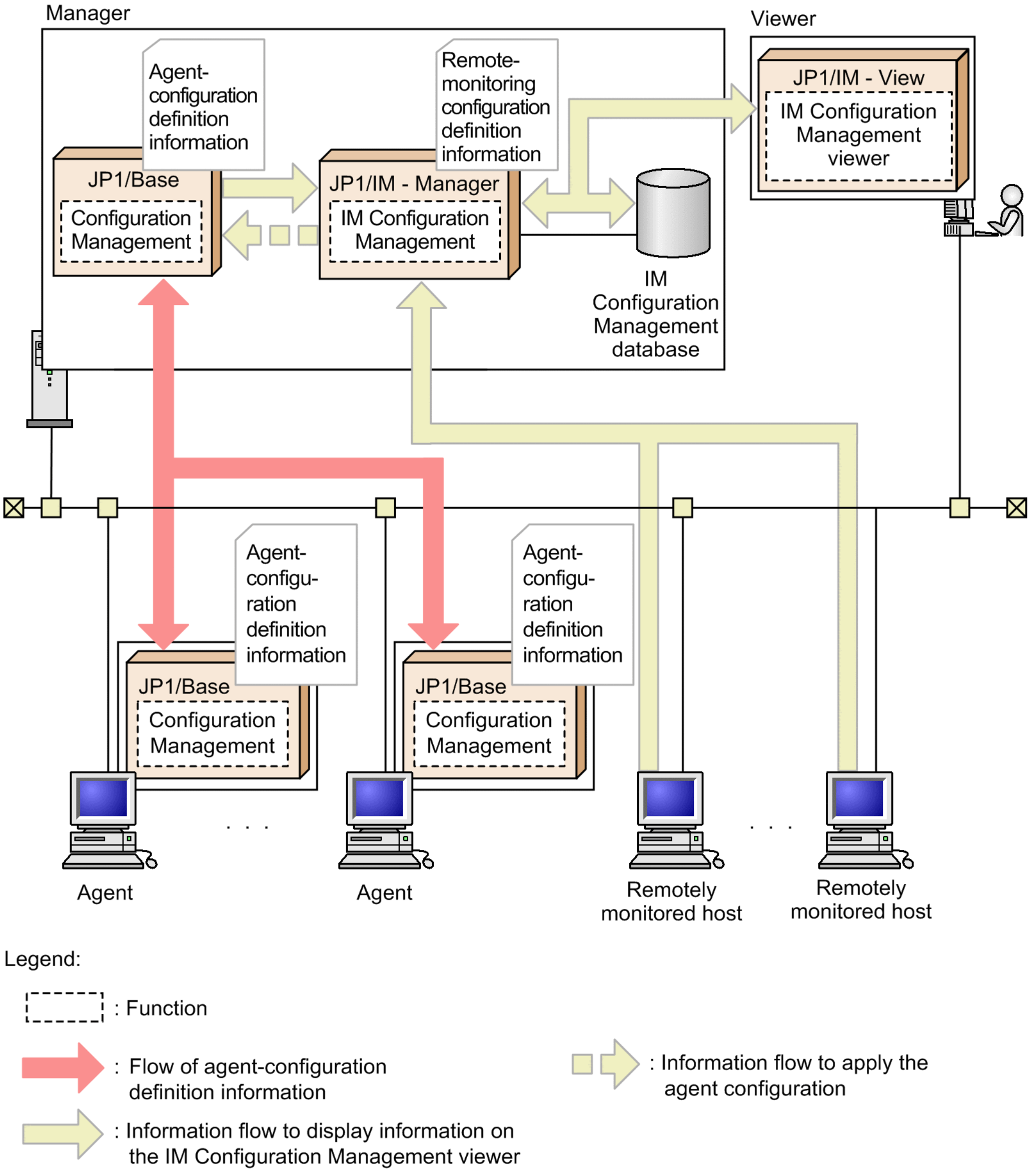
- Profile management

  You can check and edit the definition information (profiles) set in JP1/Base on the hosts that make up the JP1/IM system and for the remotely monitored hosts.

- Management of service activity information

  You can check whether the services on the managed hosts are active.

Figure 1–12: Integrated management of the system hierarchy and host settings

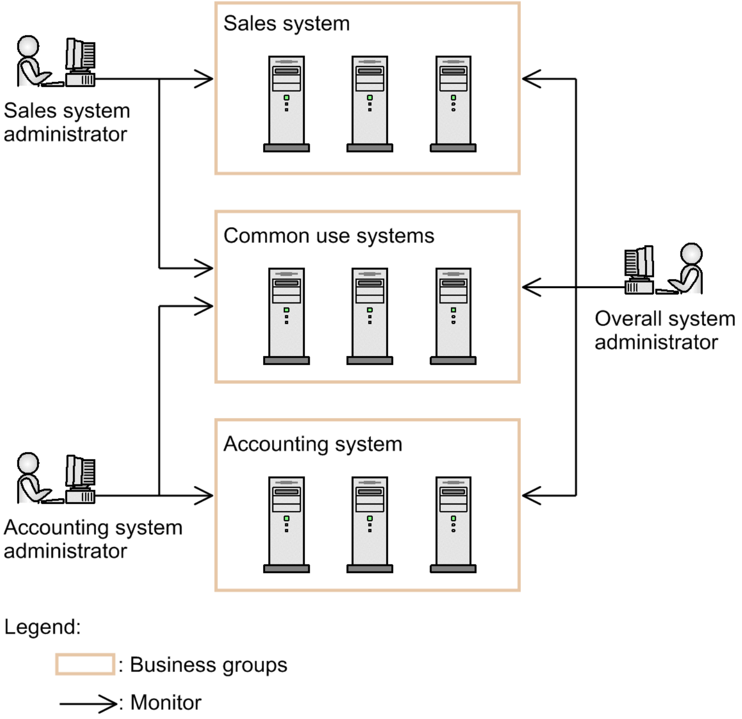


Manager
Agent-configuration definition information
Remote-monitoring configuration definition information
JP1/Base
Configuration Management
JP1/IM - Manager
IM Configuration Management
IM Configuration Management database
Viewer
JP1/IM - View
IM Configuration Management viewer
Agent-configu-ration definition information
JP1/Base
Configuration Management
Agent-configu-ration definition information
JP1/Base
Configuration Management
Agent
Agent
Remotely monitored host
Remotely monitored host
Legend:
: Function
: Flow of agent-configuration definition information
: Information flow to apply the agent configuration
: Information flow to display information on the IM Configuration Management viewer

1.3.9 Monitoring groups based on business operations

You can monitor multiple monitored hosts by grouping them based on business operations. Each of these groups of hosts is called a *business group*. You can limit what can be viewed or operated or from the Event Console window (Central Console) or in the Monitoring Tree window (Central Scope) by business group. This allows you to monitor or handle individual business groups in different ways.

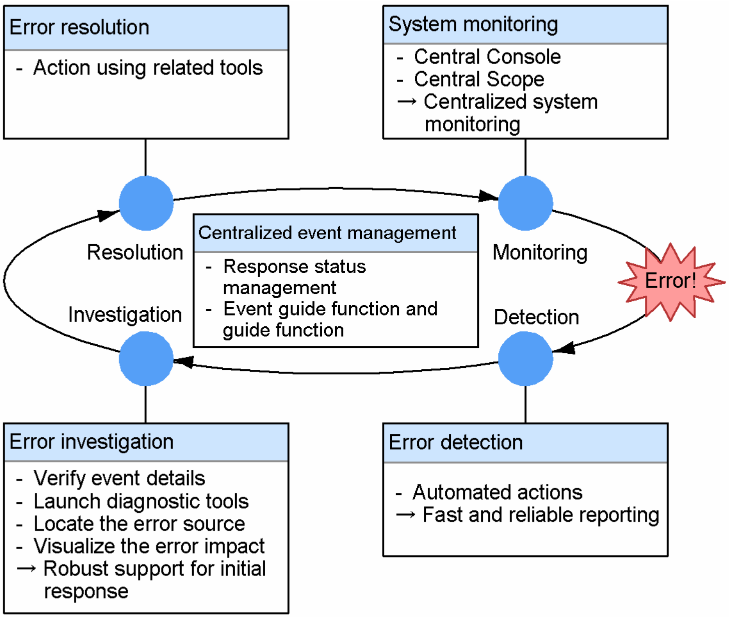
Figure 1–13: Monitoring groups based on business operations


Sales system
Sales system administrator
Common use systems
Overall system administrator
Accounting system
Accounting system administrator
Legend:
: Business groups
: Monitor

1.4 System operation with JP1/IM - Manager

JP1/IM - Manager provides full support for a unified flow of operations from system monitoring through to error detection, investigation, and resolution. The following figure shows the functions that support each phase of the system operating cycle.

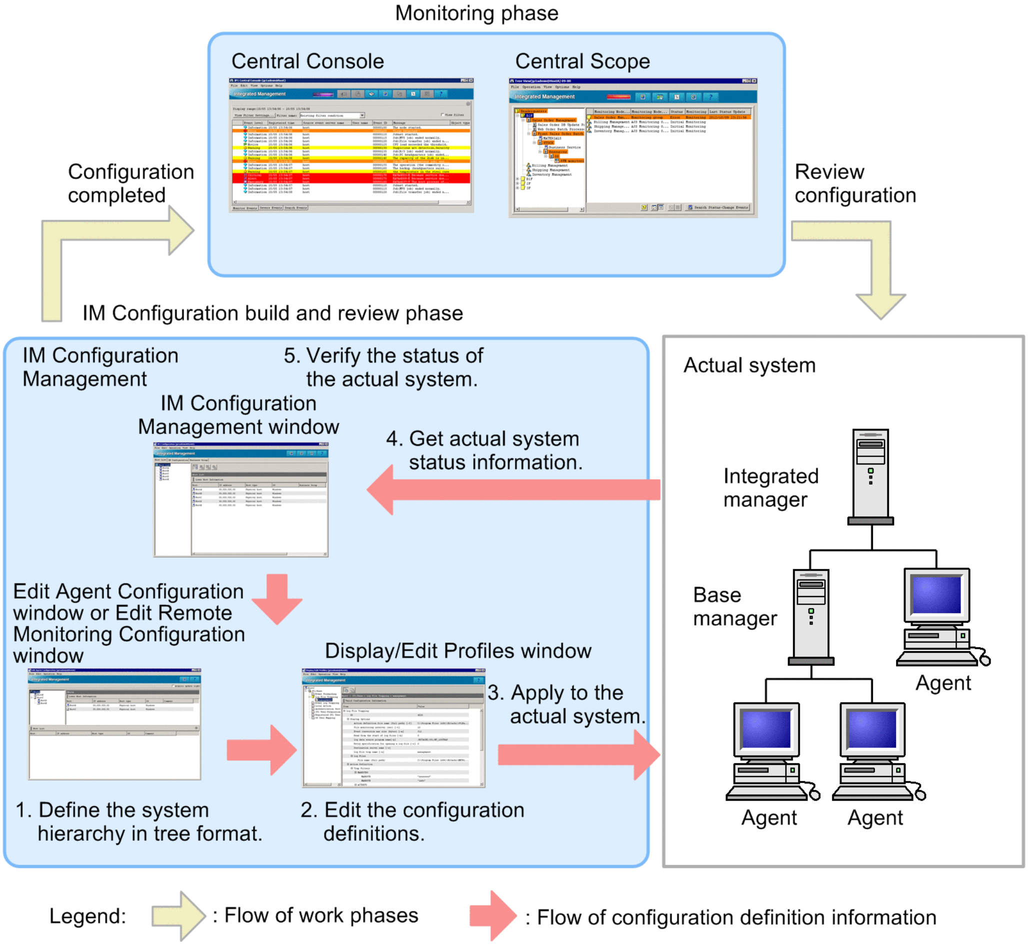
Figure 1–14: System operation with JP1/IM - Manager


Error resolution
- Action using related tools
System monitoring
- Central Console
- Central Scope
→ Centralized system monitoring
Resolution
Centralized event management
- Response status management
- Event guide function and guide function
Monitoring
Error!
Investigation
Detection
Error investigation
- Verify event details
- Launch diagnostic tools
- Locate the error source
- Visualize the error impact
→ Robust support for initial response
Error detection
- Automated actions
→ Fast and reliable reporting

No matter how large or complex the system, JP1/IM - Manager enables a diverse range of resources to be managed in an integrated fashion. By providing the capability to accurately grasp the system status, and to rapidly detect and deal with problems as they occur, JP1/IM - Manager ensures that the entire system runs reliably.

When using IM Configuration Management, you can define the system hierarchy in the IM configuration management viewer, and monitor the system from Central Console and Central Scope.

Figure 1–15: Flow of system configuration and system monitoring with IM Configuration Management (build phase)



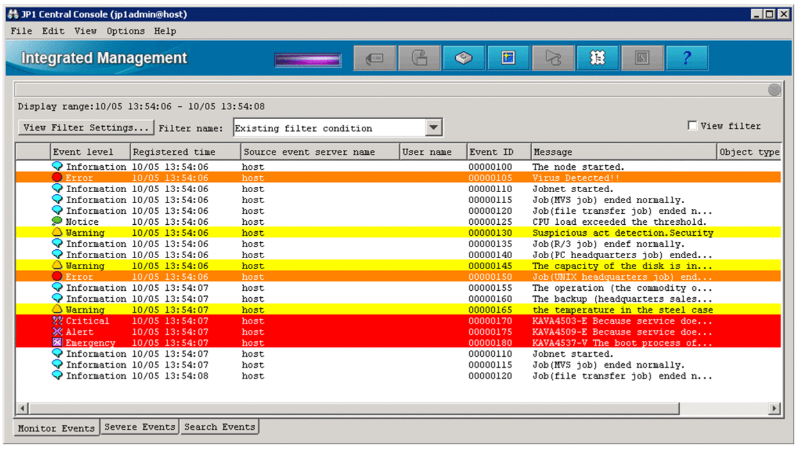
Monitoring phase
Central Console
Central Scope
Configuration completed
Review configuration
IM Configuration build and review phase
IM Configuration Management
5. Verify the status of the actual system.
IM Configuration Management window
4. Get actual system status information.
Edit Agent Configuration window or Edit Remote Monitoring Configuration window
Display/Edit Profiles window
3. Apply to the actual system.
1. Define the system hierarchy in tree format.
2. Edit the configuration definitions.
Actual system
Integrated manager
Base manager
Agent
Agent
Agent
Legend:
: Flow of work phases
: Flow of configuration definition information

1.4.1 System monitoring

(1) System monitoring using the Central Console

Using the Central Console, you can monitor the events occurring in the system in the Event Console window. You do not need to constantly monitor the Event Console window if you have set up automated actions to notify the system administrator when an error occurs.

Figure 1–16: System monitoring from the Central Console

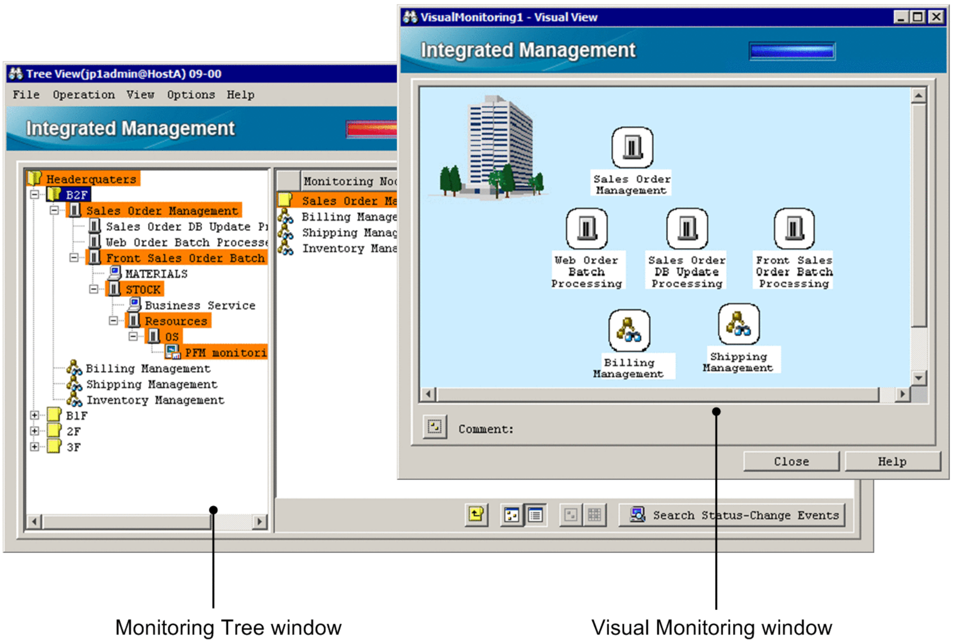


```
Display range:10/05 13:54:06 - 10/05 13:54:08

Filter name: Existing filter condition

Event level  Registered time  Source event server name  User name  Event ID  Message                                  Object type
Information  10/05 13:54:06   host                                 00000100  The node started.
Error        10/05 13:54:06   host                                 00000105  Virus Detected!!
Information  10/05 13:54:06   host                                 00000110  Jobnet started.
Information  10/05 13:54:06   host                                 00000115  Job(MVS job) ended normally.
Information  10/05 13:54:06   host                                 00000120  Job(file transfer job) ended n...
Notice       10/05 13:54:06   host                                 00000125  CPU load exceeded the threshold.
Warning      10/05 13:54:06   host                                 00000130  Suspicious act detection.Security
Information  10/05 13:54:06   host                                 00000135  Job(R/3 job) endef normally.
Information  10/05 13:54:06   host                                 00000140  Job(PC headquarters job) ended...
Warning      10/05 13:54:06   host                                 00000145  The capacity of the disk is in...
Error        10/05 13:54:06   host                                 00000150  Job(UNIX headquarters job) end...
Information  10/05 13:54:07   host                                 00000155  The operation (the commodity o...
Information  10/05 13:54:07   host                                 00000160  The backup (headquarters sales...
Warning      10/05 13:54:07   host                                 00000165  the temperature in the steel case
Critical     10/05 13:54:07   host                                 00000170  KAVA4503-E Because service doe...
Alert        10/05 13:54:07   host                                 00000175  KAVA4509-E Because service doe...
Emergency    10/05 13:54:07   host                                 00000180  KAVA4537-V The boot process of...
Information  10/05 13:54:07   host                                 00000110  Jobnet started.
Information  10/05 13:54:07   host                                 00000115  Job(MVS job) ended normally.
Information  10/05 13:54:08   host                                 00000120  Job(file transfer job) ended n...
```

(2) System monitoring using the Central Scope

Using the Central Scope, you can monitor the system in the Monitoring Tree window and Visual Monitoring window. You do not need to constantly monitor these windows if you have set up automated actions to notify the system administrator when an error occurs.

Figure 1–17: System monitoring using the Central Scope



In the Monitoring Tree window, you can configure the monitoring tree according to your objectives. In the Visual Monitoring window, you can place essential monitoring points on a map or organizational chart, and monitor the system in an intuitive manner matched to your purpose.

1.4.2 Error detection

The products in the JP1 series issue a JP1 event when an error occurs in the system. Specific error messages can also be converted into JP1 events.

JP1 events that need management follow-up are forwarded to JP1/IM - Manager where they are centrally managed. In the Central Scope, the source of an error can be represented visually in a tree view or map format, allowing on-the-spot judgment of how a problem in the system could affect business operations.

1.4.3 Error investigation

JP1/IM - Manager simplifies the investigation of problems occurring in the system by integrating the diagnostic processing into a unified flow of operations based on the Central Console or Central Scope.

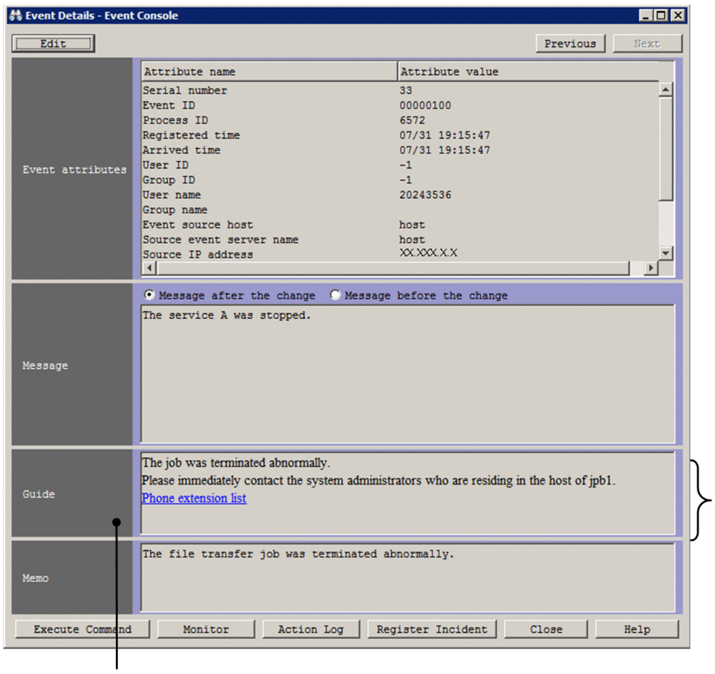
(1) Error investigation with the Central Console

The following describes the diagnostic and troubleshooting processing when using the Central Console.

(a) Event details

First of all, check the details of the detected error event. If you register action methods and procedures in advance, the initial response will be smoother and faster.

Figure 1–18: Troubleshooting advice (event guide information) provided in the Guide area



Attribute name	Attribute value
Serial number	33
Event ID	00000100
Process ID	6572
Registered time	07/31 19:15:47
Arrived time	07/31 19:15:47
User ID	-1
Group ID	-1
User name	20243536
Group name	
Event source host	host
Source event server name	host
Source IP address	XX.XXX.X.X

● Message after the change ○ Message before the change

The service A was stopped.

The job was terminated abnormally.
Please immediately contact the system administrators who are residing in the host of jpb1.
Phone extension list

The file transfer job was terminated abnormally.

Event guide information

View event guide information to find out how to handle a problem.

(b) Event search

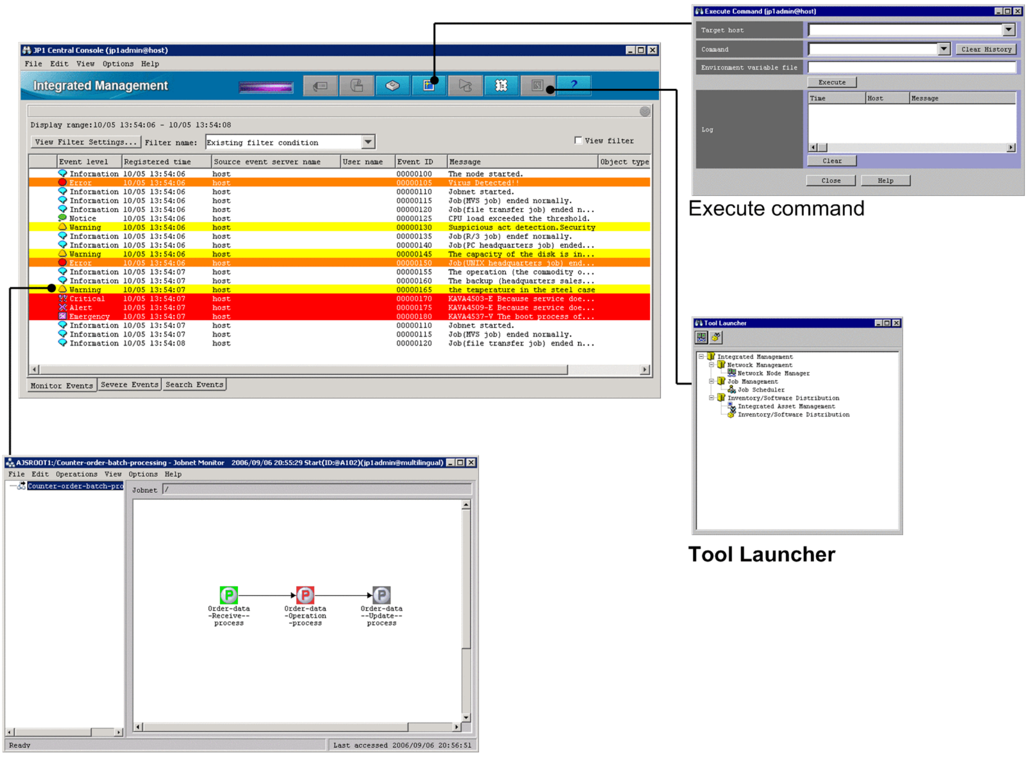
For some problems, you might want to investigate not only the error-notification event but also related events leading up to the event in question, to see what was happening generally at the time the error occurred. In such cases, you can perform an event search.

(c) Event investigation

After verifying the general circumstances by checking the event details and conducting an event search, investigate each event.

From a displayed JP1 event, you can launch the appropriate management application and move by intuitive operation from the monitoring window to the investigation window to begin your diagnosis. You can also execute Windows and UNIX commands on an agent host directly from the Central Console. This makes it easy to perform simple checks or tests because you can execute commands without having to connect to the agent host by telnet or other means.

Figure 1–19: Operations performed from JP1/IM - Manager



JP1 Central Console (jp1admin@host)

Display range:10/05 13:54:06 - 10/05 13:54:08

Filter name: Existing filter condition

☐ View filter

Event level	Registered time	Source event server name	User name	Event ID	Message	Object type
Information	10/05 13:54:06	host		00000100	The node started.	
Error	10/05 13:54:06	host		00000105	Virus Detected!!	
Information	10/05 13:54:06	host		00000110	Jobnet started.	
Information	10/05 13:54:06	host		00000115	Job(MVS job) ended normally.	
Information	10/05 13:54:06	host		00000120	Job(file transfer job) ended n...	
Notice	10/05 13:54:06	host		00000125	CPU load exceeded the threshold.	
Warning	10/05 13:54:06	host		00000130	Suspicious act detection.Security	
Information	10/05 13:54:06	host		00000135	Job(R/3 job) endef normally.	
Information	10/05 13:54:06	host		00000140	Job(PC headquarters job) ended...	
Warning	10/05 13:54:06	host		00000145	The capacity of the disk is in...	
Error	10/05 13:54:06	host		00000150	Job(UNIX headquarters job) end...	
Information	10/05 13:54:07	host		00000155	The operation (the commodity o...	
Information	10/05 13:54:07	host		00000160	The backup (headquarters sales...	
Warning	10/05 13:54:07	host		00000165	the temperature in the steel case	
Critical	10/05 13:54:07	host		00000170	KAVA4503-E Because service doe...	
Alert	10/05 13:54:07	host		00000175	KAVA4509-E Because service doe...	
Emergency	10/05 13:54:07	host		00000180	KAVA4537-V The boot process of...	
Information	10/05 13:54:07	host		00000110	Jobnet started.	
Information	10/05 13:54:07	host		00000115	Job(MVS job) ended normally.	
Information	10/05 13:54:08	host		00000120	Job(file transfer job) ended n...	

Execute Command (jp1admin@host)

Target host	
Command	
Environment variable file	

Time	Host	Message

Execute command

Tool Launcher

- Integrated Management
  - Network Management
    - Network Node Manager
  - Job Management
    - Job Scheduler
  - Inventory/Software Distribution
    - Integrated Asset Management
    - Inventory/Software Distribution

Tool Launcher

AJSROOT1:/Counter-order-batch-processing - Jobnet Monitor 2006/09/06 20:55:29 Start(ID:@A102)(jp1admin@multilingual)

Jobnet /

Last accessed 2006/09/06 20:56:51

File Edit View Options Help
Integrated Management
View Filter Settings...
Monitor Events
Severe Events
Search Events
Execute
Clear History
Log
Clear
Close
Help
File Edit Operations View Options Help
Counter-order-batch-pro
Order-data -Receive-- process
Order-data -Operation -process
Order-data --Update-- process
Ready

Monitor startup

(2) Error investigation with the Central Scope

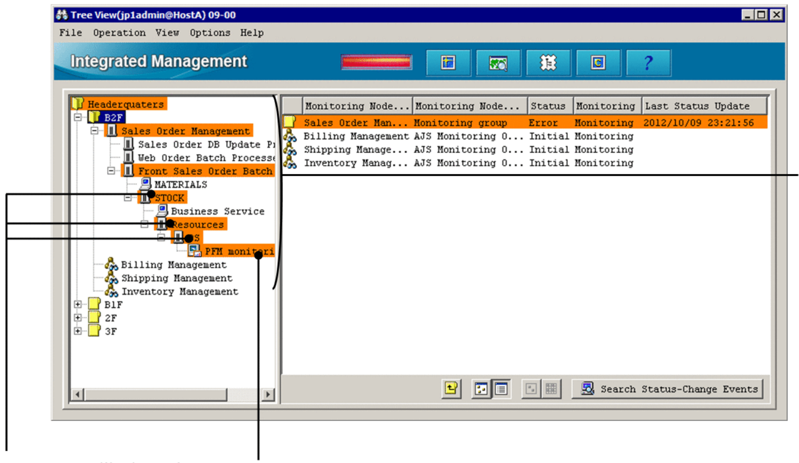
When investigating an error using the Central Scope, first identify the error source, and then link to the Central Console to investigate further.

The following describes the diagnostic and troubleshooting processing when using the Central Scope.

(a) Identifying the source and extent of an error

When an error occurs in the system, the icons representing the affected nodes change to error status in the Monitoring Tree window and Visual Monitoring window. From the upper level of the tree, check the monitoring nodes indicating error status, and identify which resources are likely to be affected by the error.

Figure 1–20: Checking the affected resources



Tree View(jp1admin@HostA) 09-00

File Operation View Options Help

Integrated Management

```
Headerquaters
  B2F
    Sales Order Management
      Sales Order DB Update Pr
      Web Order Batch Processi
      Front Sales Order Batch
        MATERIALS
        STOCK
          Business Service
          Resources
            S
              PFM monitori
    Billing Management
    Shipping Management
    Inventory Management
  B1F
  2F
  3F
```

```
Monitoring Node... Monitoring Node... Status  Monitoring Last Status Update
Sales Order Man... Monitoring group   Error   Monitoring 2012/10/09 23:21:56
Billing Management AJS Monitoring O... Initial Monitoring
Shipping Manage... AJS Monitoring O... Initial Monitoring
Inventory Manag... AJS Monitoring O... Initial Monitoring
```

Drill down from the highest object to identify the trouble spot.

Resources likely to be affected

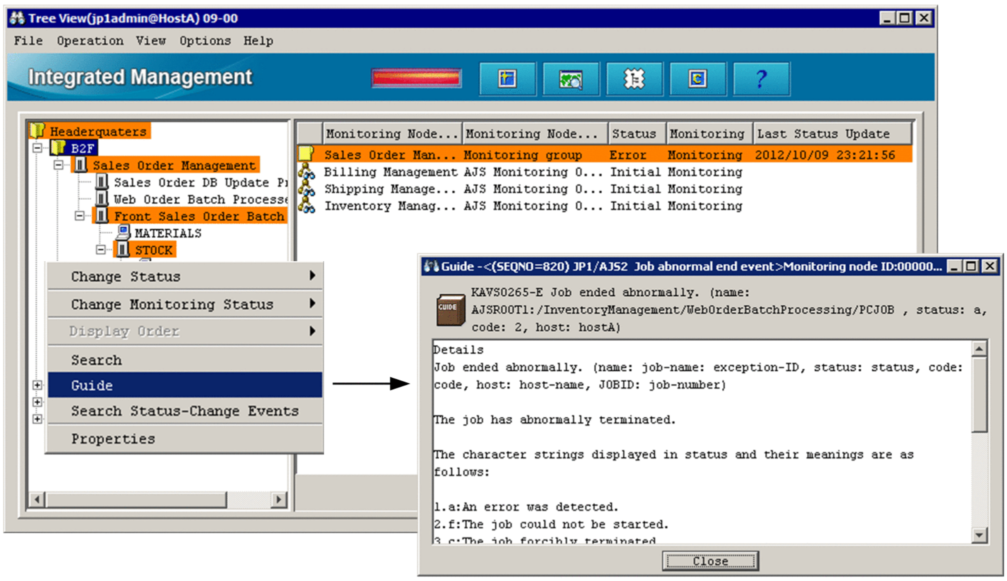
Resource in which the problem occurred

Guide information is a useful means of checking where a problem occurred. The guide function allows you to register operating know-how including troubleshooting procedures for specific problems, and examples of past situations in which certain errors have occurred. Although responding appropriately to whatever problems occur in a diverse range of resources is never easy, the guidance offered by the guide function goes some way toward reducing the system administrator's workload.

Important

Guide information must be registered before it can be viewed. For details about the guide function, see *4.8 Guide function* in this manual and *5.6 Editing guide information* in the *JP1/Integrated Management - Manager Configuration Guide*.

Figure 1–21: Troubleshooting advice provided by the guide function



Tree View(jp1admin@HostA) 09-00

File Operation View Options Help

Integrated Management

```
Headerquaters
  B2F
    Sales Order Management
      Sales Order DB Update Pr
      Web Order Batch Processi
      Front Sales Order Batch
        MATERIALS
        STOCK
```

```
Monitoring Node... Monitoring Node... Status  Monitoring Last Status Update
Sales Order Man... Monitoring group   Error   Monitoring 2012/10/09 23:21:56
Billing Management AJS Monitoring O... Initial Monitoring
Shipping Manage... AJS Monitoring O... Initial Monitoring
Inventory Manag... AJS Monitoring O... Initial Monitoring
```

Guide -<(SEQNO=820) JP1/AJS2 Job abnormal end event>Monitoring node ID:00000...

```
KAVS0265-E Job ended abnormally. (name:
AJSROOT1:/InventoryManagement/WebOrderBatchProcessing/PCJOB , status: a,
code: 2, host: hostA)
```

```
Details
Job ended abnormally. (name: job-name: exception-ID, status: status, code:
code, host: host-name, JOBID: job-number)

The job has abnormally terminated.

The character strings displayed in status and their meanings are as
follows:

1.a:An error was detected.
2.f:The job could not be started.
3.c:The job forcibly terminated
```

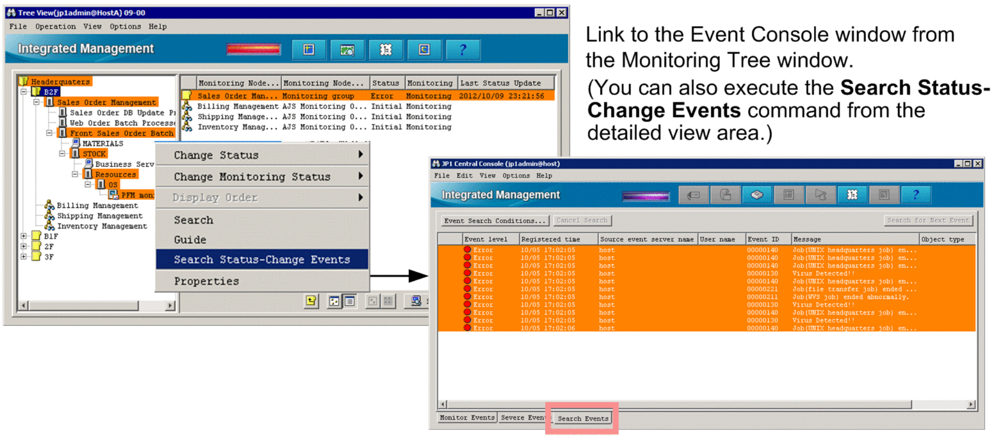
(b) Identifying events that caused the error

After you have identified the node that is in error status, you can discover what event caused the problem.

Select the node that is in error status, and then click the **Search Status-Change Events** command. The Event Console window opens with the **Search Events** page displayed. This page lists the JP1 events that caused the node to change to error status.

Figure 1–22: Identifying events that caused the error

Monitoring Tree window (Central Scope)



Monitoring Node...	Monitoring Node...	Status	Monitoring	Last Status Update
Sales Order Man...	Monitoring group	Error	Monitoring	2012/10/09 23:21:56
Billing Management	AJS Monitoring O...	Initial	Monitoring	
Shipping Manage...	AJS Monitoring O...	Initial	Monitoring	
Inventory Manag...	AJS Monitoring O...	Initial	Monitoring	

Event level	Registered time	Source event server name	User name	Event ID	Message	Object type
Error	10/05 17:02:05	host		00000140	Job(UNIX headquarters job) en...	
Error	10/05 17:02:05	host		00000140	Job(UNIX headquarters job) en...	
Error	10/05 17:02:05	host		00000140	Job(UNIX headquarters job) en...	
Error	10/05 17:02:05	host		00000130	Virus Detected!!	
Error	10/05 17:02:05	host		00000140	Job(UNIX headquarters job) en...	
Error	10/05 17:02:05	host		00000221	Job(file transfer job) ended ...	
Error	10/05 17:02:05	host		00000211	Job(WVS job) ended abnormally.	
Error	10/05 17:02:05	host		00000130	Virus Detected!!	
Error	10/05 17:02:05	host		00000140	Job(UNIX headquarters job) en...	
Error	10/05 17:02:05	host		00000130	Virus Detected!!	
Error	10/05 17:02:06	host		00000140	Job(UNIX headquarters job) en...	

Link to the Event Console window from the Monitoring Tree window.
(You can also execute the **Search Status-Change Events** command from the detailed view area.)

Event Console window (Central Console)

(c) Investigating the error

After you have identified the node in which an error occurred, you can discover what event caused the problem. To locate the event, use the Central Console. By linking to the Central Console, you can investigate the nature of the error that triggered the JP1 event.

1.4.4 Error resolution

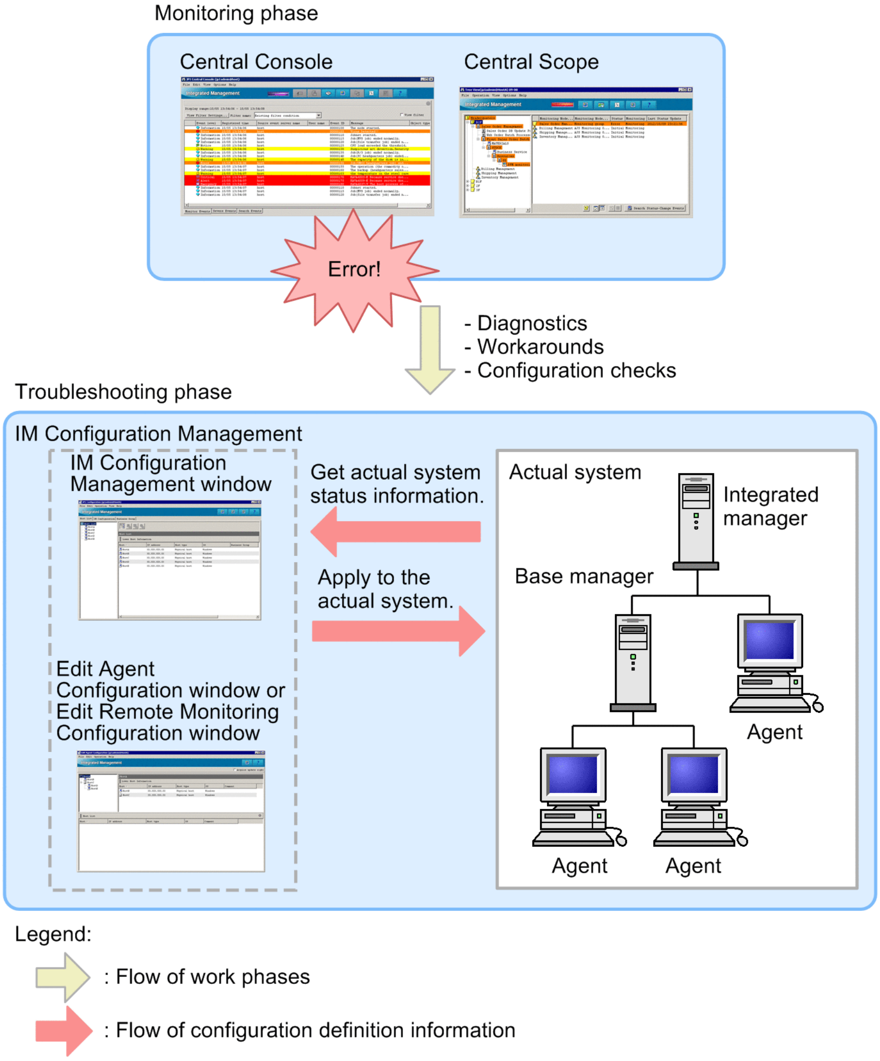
After identifying the location and cause of a problem, take the appropriate action to resolve it.

After resolving the problem, make sure that the system is working normally. Then, in the monitoring tree of the Central Scope, change the status of the objects affected by the error back to **Initial**. You can change the status of monitoring objects individually, or collectively by changing the status of the monitoring group. To restore monitoring objects to **Initial** status individually, select each object and change its status. To restore all the monitoring objects in a monitoring group to **Initial** status in a single operation, select the monitoring group and change its status.

Further errors might be occurring in other resources while you are busy dealing with the original problem. Before you restore the objects' status, take steps to make sure that the entire monitoring group is working normally, including searching for nodes that have error status.

When you are using IM Configuration Management, you can operate the IM configuration management viewer to change the system hierarchy (IM configuration) for error resolution.

Figure 1–23: Flow of system monitoring and system reconfiguration with IM Configuration Management (operation phase)


Monitoring phase
Central Console
Central Scope
Error!
- Diagnostics
- Workarounds
- Configuration checks
Troubleshooting phase
IM Configuration Management
IM Configuration Management window
Get actual system status information.
Apply to the actual system.
Edit Agent Configuration window or Edit Remote Monitoring Configuration window
Actual system
Integrated manager
Base manager
Agent
Agent
Agent
Legend:
: Flow of work phases
: Flow of configuration definition information

1.5 JP1/IM - Manager system configuration

This section describes the component products and configuration of a JP1/IM - Manager system.

1.5.1 Component products of a JP1/IM - Manager system

A JP1/IM - Manager system consists of a *manager* (which performs integrated management of the system), *agents* (which run on the monitored servers), remotely monitored hosts, and a *viewer* (which is used for performing monitoring and operations). Note that remotely monitored hosts can be placed only under the integrated manager or base managers in a tree.

A JP1/IM - Manager system requires the following products, depending on the functionality to be used and the host's role in the system:

- Manager host: JP1/IM - Manager and JP1/Base
- Agent host: JP1/Base
- Viewer host: JP1/IM - View

The viewer program can be used on both manager hosts and agent hosts.

A JP1/IM - Manager system consists of the following component products.

Table 1–3: Component products of a JP1/IM - Manager system

Product name	Product overview
JP1/IM - Manager	Provides the following manager functionality • Central Console • Central Scope • IM Configuration Management
JP1/IM - View	Broadly classified, JP1/IM - View provides four main windows:# • Central Console viewer (for Central Console operations) • Central Scope viewer (for Central Scope operations) • IM configuration management viewer (for IM Configuration Management operations) • Rule operation viewer (for rule management operations) JP1/IM - Manager performs system monitoring and operation using the Central Console viewer and Central Scope viewer.
JP1/Base	Provides the agent functionality. JP1/Base operates as a monitored server and provides the JP1 core functionality, such as JP1 event management and JP1 user management. JP1/Base is a prerequisite product of JP1/IM - Manager.

#: This manual describes the Central Console viewer, Central Scope viewer, and IM configuration management viewer only.

For details about the rule operation viewer, see the *Job Management Partner 1/Integrated Management - Rule Operation System Configuration and User's Guide*.

1.5.2 JP1/IM system hierarchy

A system managed by JP1/IM consists of a *manager* (which performs integrated management of the system), *agents* (which run on the monitored servers), remotely monitored hosts, and a *viewer* (which is used for performing monitoring and operations).

To monitor a host as an agent, JP1/Base must be running on that host. A configuration where JP1/Base is running on the monitored hosts is called an *agent configuration*.

A configuration where remotely connected hosts are monitored is called a *remote monitoring configuration*. This configuration is supported by JP1/IM version 09-50 or later. The remote monitoring configuration has more limitations than the agent configuration. To discuss whether to use the remote monitoring configuration, see *6.2.8 Selection of agent configuration or remote monitoring configuration*. You must set the hosts to be monitored for remote communication in advance. For details about communication settings, see *1.17 Specifying settings for monitoring logs on remotely monitored hosts (for Windows)* or *2.16 Specifying settings for monitoring logs on remotely monitored hosts (for UNIX)* in the *JP1/Integrated Management - Manager Configuration Guide*.

In an agent configuration, JP1/Base runs on each agent host. In a remote monitoring configuration, however, JP1/Base is not required on the remotely monitored hosts.

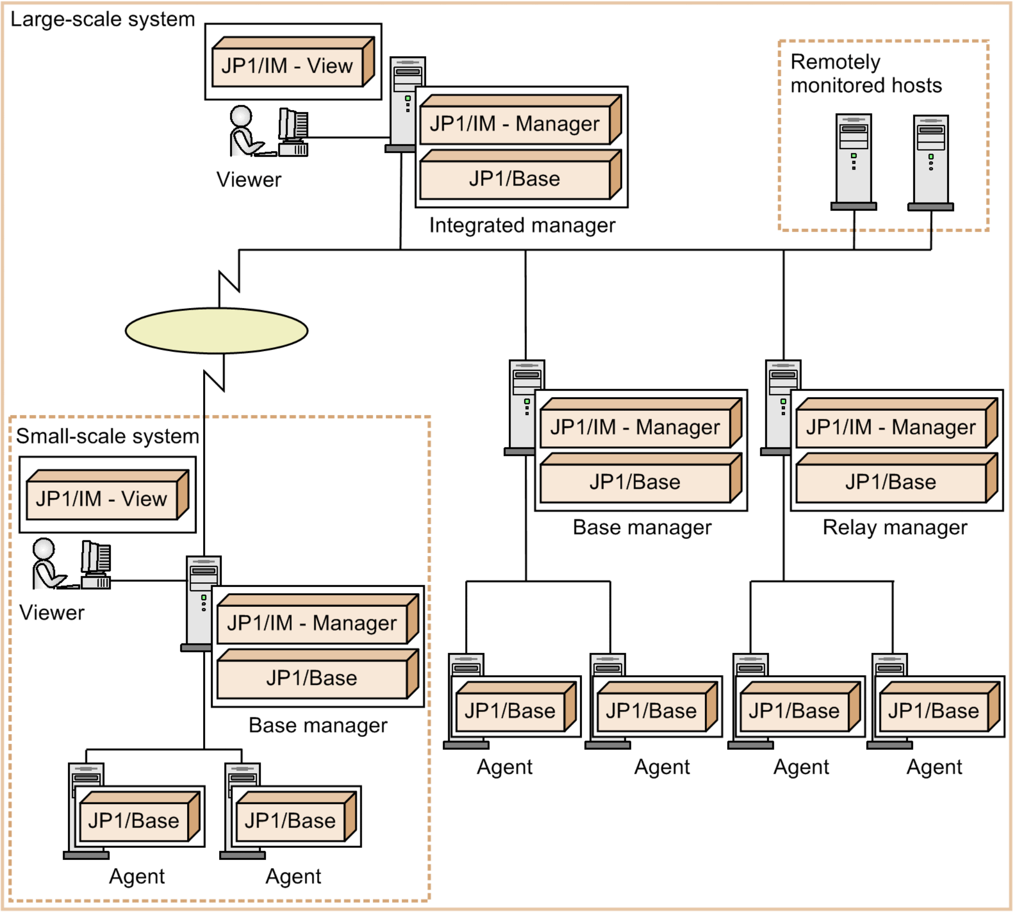
Agent configurations and remote monitoring configurations are collectively referred to as a *system hierarchy* or an *IM configuration*.

To centrally manage the system hierarchy (IM configuration) by using JP1/IM - Manager, you can use the IM Configuration Management functionality provided by JP1/IM - Manager to define the system hierarchy or to distribute the definition information of the system hierarchy (configuration definition information) to hosts.

Alternatively, you can define the system hierarchy using the configuration definition information in JP1/Base in the usual manner. Note that you cannot define the system hierarchy for the remotely monitored hosts in this manner.

In a JP1/IM system, managers can be arranged hierarchically to enable integrated management of systems whatever their size - from a small system serving a regional office to a large-scale system serving the entire enterprise. This allows you to add hosts to those being monitored, and makes it easy to migrate a small system to a large-scale hierarchical system.

Figure 1–24: Scalable system hierarchy



In an agent configuration, you can configure a hierarchical system by placing base managers and relay managers under the integrated manager as shown in the above figure. To configure a hierarchical system, JP1/IM - Manager must be installed on the integrated manager host, base manager hosts, and relay manager host.

In a remote monitoring configuration, you cannot configure a hierarchical system. You must place remotely monitored hosts under the integrated manager or base managers.

The types of manager hosts configured in a JP1/IM system are as follows:

Table 1–4: Types of managers in a JP1/IM system

Type of manager host	Description
Integrated manager	The integrated manager is at the top of the system hierarchy. It performs integrated management of base managers, relay managers, agents (excluding the agents under base managers), and remotely monitored hosts (excluding the remotely monitored hosts under base managers) in the system hierarchy.
Base manager	The base manager is placed between the integrated manager and agents or remotely monitored hosts when agents are managed at individual sites. The integrated manager manages base managers, and each base manager manages the agents and remotely monitored hosts that are placed under them.
Relay manager	Positioned at an intermediate level between the integrated manager and agents to collect events generated at the agent hosts. The relay manager and lower-level agents are managed by the integrated manager. Relay managers cannot be used in a remote monitoring configuration.

Monitored hosts are classified into the following two types:

- Agent
- Remotely monitored host

1.5.3 Support for various system configurations

JP1/IM - Manager supports the following broad range of system configurations, providing flexible integrated management tailored to system requirements.

- Cross-platform support

  JP1/IM - Manager provides agents for a variety of platforms, including Windows, UNIX, and mainframe operating systems. Using these agents, JP1/IM - Manager can seamlessly manage various types of heterogeneous systems.
- Support for individual business groups

  JP1/IM - Manager enables you to monitor hosts by grouping them. For example, you can create a group based on the system used for a particular business operation, or based on which monitored objects are managed by a particular system administrator.
- Support for a variety of network configurations
  - Firewall support

    JP1/IM supports communication through a port-filtering firewall and Network Address Translation (NAT) in static mode. You can deploy JP1/IM in a network configuration that has a firewall installed between a viewer and manager host, or between a manager and agent host.
  - Support for multiple LAN connections

    JP1/IM supports network configurations with JP1/IM hosts connected to multiple LANs. You can set up the JP1/IM host to communicate over a specific LAN.
- Support for cluster systems

  JP1/IM - Manager supports operation in a cluster system.

  In the event of an error, JP1/IM - Manager will fail over and continue working, performing integrated monitoring of the system that runs your business operations.
- Mixed languages and time zones

  JP1/IM supports system configurations that encompass more than one language or time zone, which is unavoidable when managing a global system in its entirety. However, several restrictions apply. Consider the system configuration and operation, referring to *12.1.6 Operation in a multi-language environment*.

2 Overview of Functions

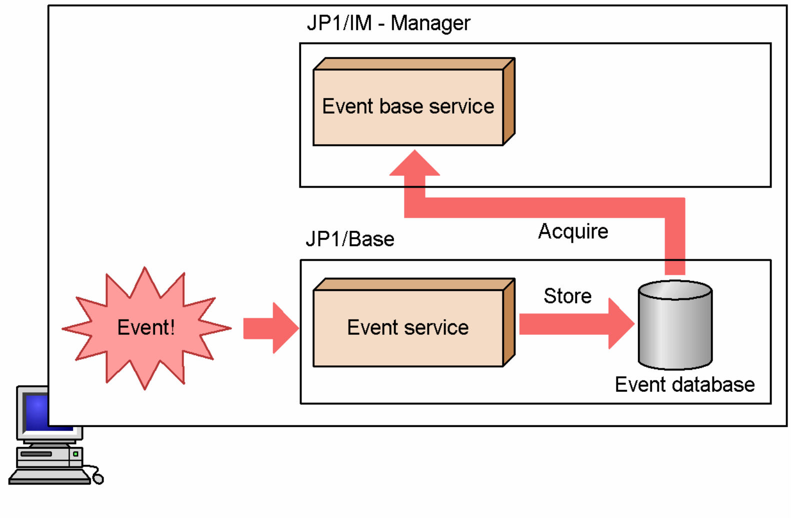
This chapter provides an overview of the functions that are fundamental to JP1/IM - Manager.

2.1 Overview of event management

JP1/IM - Manager centrally manages the various events that occur in the system as *JP1 events*.

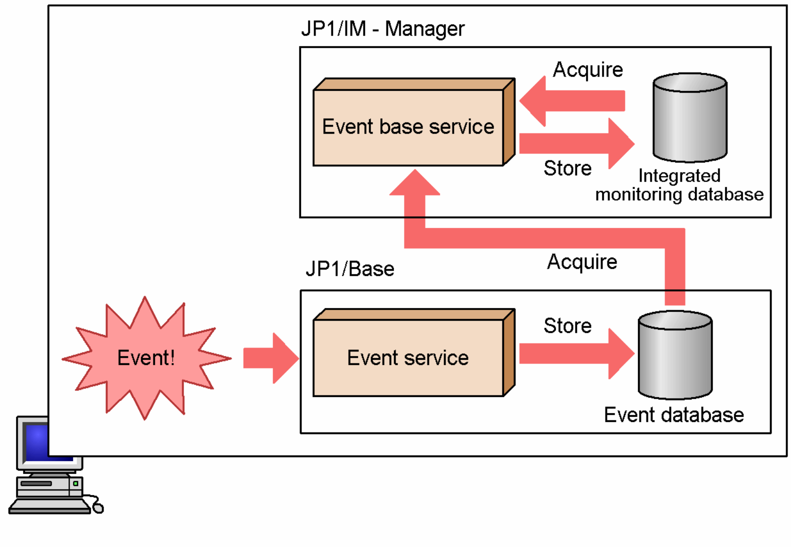
JP1 events are controlled by the JP1/Base event service and are managed by the event database specific to JP1/Base.

Figure 2–1: Overview of JP1 event management



When you use the *integrated monitoring database* provided by JP1/IM - Manager, the event base service of JP1/IM - Manager acquires JP1 events from the JP1/Base event database. JP1/IM - Manager applies JP1/IM - Manager-specific information and stores the acquired JP1 events in the integrated monitoring database. By accessing this JP1 event information in the integrated monitoring database, JP1/IM - Manager can perform processing of various kinds based on the information.

Figure 2–2: Overview of JP1 event management with the integrated monitoring database



For details about how to manage JP1 events on remotely monitored hosts, see *6.6 Managing remotely monitored hosts*.

2.2 Functionality at each phase of the operating cycle

This section describes the functionality provided at each phase of the operating cycle. JP1/IM - Manager consists of four key components: Central Console, Central Scope, IM Configuration Management, and the core functionality.

Central Console

The Central Console centrally manages events in the system based on JP1 events, and enables integrated management of the entire system. For details about system monitoring using the Central Console, see *Chapter 3. Centralized System Monitoring Using the Central Console* and *Chapter 5. Command Execution by Automated Action*.

Central Scope

The Central Scope enables integrated objective-oriented system management via a visual interface, in accordance with requirements set by the system administrator. For details about the Central Scope, see *Chapter 4. Objective-Oriented System Monitoring Using the Central Scope*. To use the Central Scope, you must enable (activate) the central scope service in JP1/IM - Manager. For details about configuring the Central Scope, see *1.18.1 Specifying settings for using the functions of Central Scope (for Windows)* in the *JP1/Integrated Management - Manager Configuration Guide*.

IM Configuration Management

IM Configuration Management enables you to operate the IM configuration management viewer to centrally manage host settings and the system hierarchy managed by JP1/IM (IM configuration). To use IM Configuration Management, you must set up the IM Configuration Management database. For details about IM Configuration Management, see *Chapter 6. System Hierarchy Management Using IM Configuration Management*.

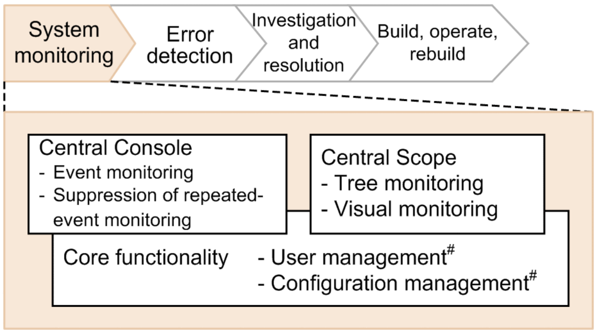
Core functionality

The core functionality includes *process management*, which controls startup, termination, and other operations of JP1/IM - Manager, and *service startup control*, where JP1/Base controls startup of services. For details about the core functionality of JP1/IM - Manager and JP1/Base, see *Chapter 7. JP1/IM Operation Control*.

2.2.1 Functionality for system monitoring

The system needs to be monitored continuously to ensure it is running normally.

Figure 2–3: Functionality for system monitoring



#: JP1/Base functionality

By providing centralized monitoring, the Central Console makes monitoring more efficient, supports early error detection, and reduces management overheads. Even when JP1 events not necessary for monitoring occur in large numbers, you can maintain efficient monitoring by setting repeated event conditions to suppress the display of unnecessary JP1 events that meet the specified conditions.

When the system being monitored is large and complex, problems might be detected successfully, but their impact on operations is never easy to determine. The Central Scope offers visual representation using monitoring windows in a tree or map view, enabling system monitoring from any viewpoint required by the system administrator. You can visually check the area affected by the problem that occurred in the system. This enhances management efficiency and enables preventive action to isolate any problems.

User management and configuration management are part of the core functionality for monitoring the system. User management entails mapping of the JP1 user with the OS user when a JP1 user executes a command. IM Configuration Management manages the system hierarchy.

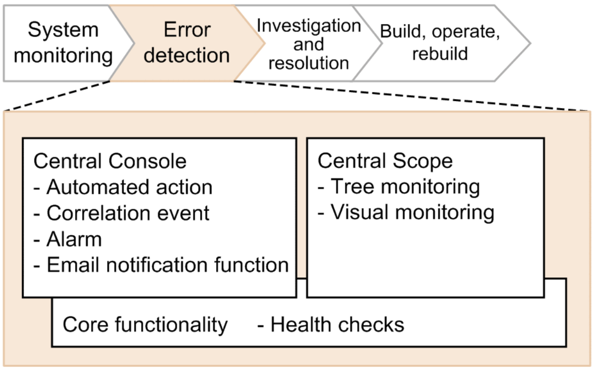
Important

JP1/IM - Manager can only monitor JP1 events that were issued after it began operation. Events that occurred earlier are excluded from monitoring by JP1/IM - Manager.

2.2.2 Functionality for error detection

The following figure shows the functionality for detecting errors.

Figure 2–4: Functionality for error detection



The components used for detecting problems in the system are the Central Console, Central Scope, and the core functionality.

On the Central Console, you can set up automated actions and correlation events in advance to detect errors in the system. An automated action is triggered when a particular event is received and automatically executes a command defined by the user. A correlation event is triggered when multiple correlated events are received and a JP1 event defined by the user is issued. You can use these mechanisms to notify the system administrator of problems by sending emails or issuing notification events.

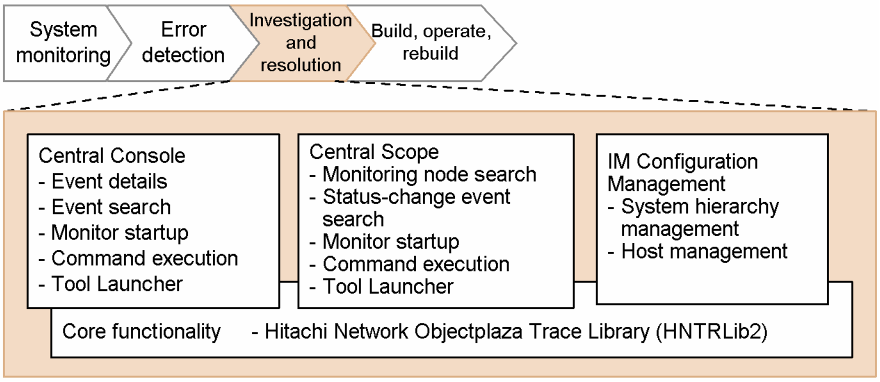
The Central Scope provides tree monitoring and visual monitoring. A JP1 event can be issued from the Central Scope whenever the status of a monitoring node changes, and an automated action can be executed through the Central Console in response to an issued JP1 event. Severe events can be reported by using alarms, and the impact of any errors can be visually represented by changing the icons in the monitoring tree to error status.

The health check provided by the core functionality issues a message or JP1 event whenever an error occurs in a JP1/IM - Manager process. It can also issue a message or JP1 event when an error occurs in a JP1/Base process on the local host or remote host.

2.2.3 Functionality for error investigation and resolution

The following figure shows the functionality used in investigating and resolving errors.

Figure 2–5: Functionality for error investigation and resolution



Error investigation and resolution via the Central Console is based on JP1 events. You can display detailed information about a JP1 event, and search for events related to the JP1 event in question. Error investigation and resolution also applies to starting the application that issued a particular JP1 event or any application, execution of commands, and linkage with other JP1-series products, such as JP1/PFM.

Using the Central Scope, you can search for monitoring nodes related to the problem. You can also change the status or the monitoring status of the monitoring nodes.

To check the change history of the events in which the status of the monitored objects was changed, execute the **Search Status-Change Events** menu command.

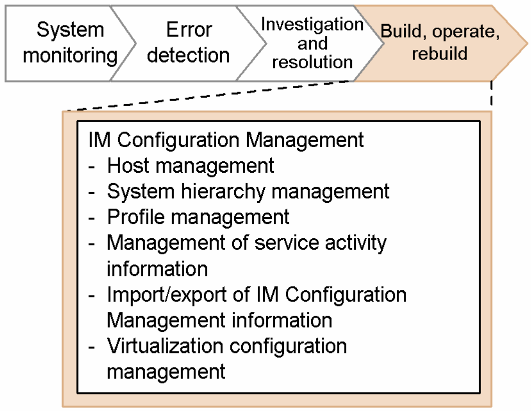
When the range of your investigation extends to the system configuration, use the IM Configuration Management feature. Using IM Configuration Management - View, you can check the status of the host on which the problem occurred, delete that host from the system hierarchy, or apply the hierarchical system information saved in IM Configuration Management to the host. If you do not use IM Configuration Management, you must examine the log information, assess the status of the affected host, and resolve the problem yourself.

Using the Hitachi Network Objectplaza Trace Library (HNTRLib2) with the core functionality, you can output all the trace information generated by the JP1/Base and JP1/IM - Manager processes to a single integrated trace log.

2.2.4 Functionality for building, operating, and rebuilding the system

The following figure shows the functionality used at the build, operation, and rebuild phases.

Figure 2–6: Functionality for building, operating, and rebuilding the system


System monitoring
Error detection
Investigation and resolution
Build, operate, rebuild
IM Configuration Management
- Host management
- System hierarchy management
- Profile management
- Management of service activity information
- Import/export of IM Configuration Management information
- Virtualization configuration management

It is sometimes necessary to rebuild the system or change its configuration during maintenance mode as a means of investigating and resolving an issue. In such cases, review the system hierarchy using the configuration management functionality provided by IM Configuration Management or by JP1/Base.

We recommend that you use the IM Configuration Management functionality if you want to centrally manage the hierarchical structure of the system from JP1/IM - Manager. Using IM Configuration Management - View, you can define the system hierarchy by registering the hosts you want to manage, and adding, moving, or deleting hosts in the hierarchy.

If you choose not to use IM Configuration Management, you can define the system hierarchy using the JP1/Base configuration management functionality. You also have access to the JP1/Base functionality for collecting and distributing the information defined in JP1/Base on the hosts.

Decide in advance whether you want to use IM Configuration Management or the configuration management and definition collection and distribution functionality provided by JP1/Base. For details about these functions and considerations at the design stage, see the following table.

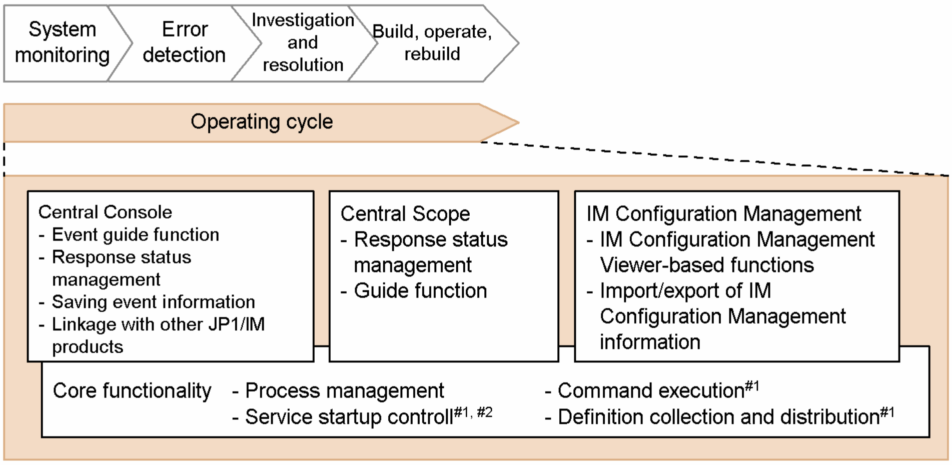
Table 2–1: Details of functions and design considerations

Function	Function details	Design considerations
• IM Configuration Management	• *Chapter 6. System Hierarchy Management Using IM Configuration Management*	• *11.5 Considerations for managing the system hierarchy* • *12.5 Considerations for the system hierarchy*
• JP1/Base configuration management • JP1/Base definition collection and distribution	• *7.4.3 Managing the system hierarchy* • *7.4.5 Collecting and distributing definition information*	

2.2.5 Functionality used throughout the operating cycle

The following figure shows the functions used throughout the operating cycle.

Figure 2–7: Functions used throughout the operating cycle


System monitoring
Error detection
Investigation and resolution
Build, operate, rebuild
Operating cycle
Central Console
- Event guide function
- Response status management
- Saving event information
- Linkage with other JP1/IM products
Central Scope
- Response status management
- Guide function
IM Configuration Management
- IM Configuration Management Viewer-based functions
- Import/export of IM Configuration Management information
Core functionality
- Process management
- Service startup controll#1, #2
- Command execution#1
- Definition collection and distribution#1

#1: JP1/Base function
#2: Windows-only function

The functions in the following table are used throughout the operating cycle.

Table 2–2: Functions used throughout the operating cycle

Component	Function	Description
Central Console	Event guide function	• Displays guidance about methods or procedures for responding to JP1 events.
	Response status management	• Manages actions taken in response to severe events.
	Saving event information	• Saves JP1 event information displayed in JP1/IM - View (exports the information in CSV form). • Saves JP1 event information saved in the integrated monitoring database (outputs event reports).
	Linkage with other JP1 series products	• Registers incidents in JP1/Service Support. • Sends rule start requests to JP1/IM - Rule Operation. • Displays application information (operating procedures) applicable to JP1 events in JP1/Navigation Platform.
Central Scope	Response status management	• Manages the status of monitoring nodes.
	Guide function	• Displays guidance about troubleshooting methods or response procedures.
IM Configuration Management	IM Configuration Management Viewer-based functions	• Manages the status of managed hosts. • Manages the status of the system hierarchy. • Manages the status of the JP1/Base profiles on each host. • Manages the status of the profiles on remotely monitored hosts. • Checks JP1/Base service activity information on each host.
	Import/export of IM Configuration Management information	• Exports management information from IM Configuration Management in case an error occurs, and imports the information at error recovery.
Core functionality	Process management	• Controls JP1/IM - Manager startup, termination, and other operations. • Checks whether JP1/IM - Manager functions are active.
	Service startup control[#1, #2]	• Controls service startup via JP1/Base.

Component	Function	Description
	Command execution#2	• Executes commands from JP1/IM - View. • Executes commands by automated actions.
	Definition collection and distribution#2	• Collects and distributes definition information among JP1/Base hosts.

#1: Windows-only function.

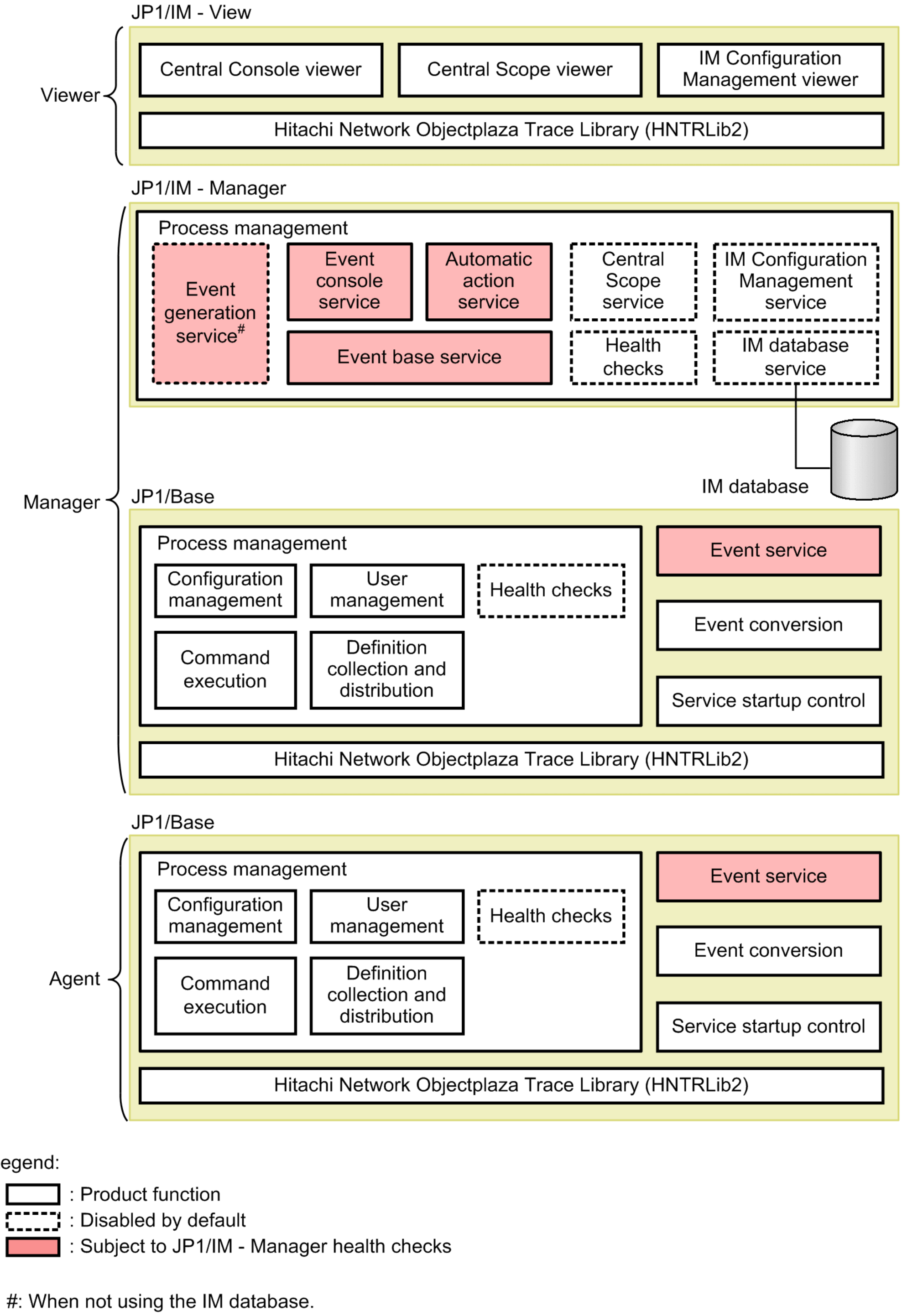
#2: JP1/Base function.

You can manage the system configuration information and collect and distribute definition information using either IM Configuration Management or the core functionality. Consider which method to use before you commence operation. For the function details and design considerations, see *Table 2-1 Details of functions and design considerations*.

2.3 List of functions

The following figure shows the functions of component programs used for system operation monitoring by JP1/IM - Manager.

Figure 2–8: Functions provided by the component products



JP1/IM - Manager is linked with the prerequisite product JP1/Base, and operates using the core functionality provided by JP1/Base. JP1/Base also runs on the agents in the JP1/IM - Manager system. JP1/IM - Manager thus has an inseparable relationship with JP1/Base.

The functions in the figure above are summarized below.

Table 2–3: Summary of product functions

Function		Description	Service name
Central Console	Centralized monitoring using JP1 events	• Monitors JP1 events.	• Central Console viewer
	JP1 event management	• Controls the display of JP1 events in the Central Console viewer.	• Event console service
		• Manages the integrated monitoring database.	• IM database service
		• Acquires JP1 event information from the JP1/Base event service. • Distributes acquired JP1 event information to the JP1/IM - Manager controls (event console service, automatic action service, and central scope service).	• Event base service
		• Controls JP1 events. • Manages the event database.	• JP1/Base
	JP1 event filtering	• Filters JP1 events to select those required.	• Central Console viewer • Event console service • Event base service • Event issue service • JP1/Base
	Automated actions	• Executes a command automatically, conditional on a specific event being detected by the event base service.	• Automatic action service
	Issue of correlation events	• Correlates JP1 events acquired from the JP1/Base event service and registers them as correlation events with JP1/Base.	• Event issue service (when not using the integrated monitoring database) • Event base service (when using the integrated monitoring database)
	Event conversion	• Extracts information from log files and converts it into JP1 events (log file trapping) • Extracts information from the Windows event log and converts it into JP1 events (event log trap conversion) • Extracts information from SNMP traps managed by HP NNM version 7.5 or earlier and converts it into JP1 events (SNMP trap conversion).	• JP1/Base
	Display of user-defined event attributes	• Issues JP1 events from a user application by calling a JP1/Base function.	
	Event guide function	• Displays information about pre-registered response methods and procedures.	• Central Console viewer
	CSV output of information displayed in JP1/IM - View	• Outputs JP1 event information displayed in JP1/IM - View in CSV form.	
	System operation	• Launches a linked application. • Launches an associated application from the Tool Launcher. • Executes a command from JP1/IM - View.	
Central Scope	Tree monitoring	• Centrally monitors objects in a tree view.	• Central Scope viewer

Function		Description	Service name
		• Automatically creates a monitoring window.	• Central Scope service
	Visual monitoring	• Centrally monitors objects in a map view.	
	Guide function	• Displays information about pre-registered response methods and procedures.	
IM Configuration Management[#1]	Host management	• Centrally manages the hosts in the JP1/IM system from the manager.	• IM Configuration Management - View • IM Configuration Management service • IM database service
	System hierarchy management	• Centrally manages the hierarchical structure of the system from the manager. An agent configuration (where JP1/Base is running on agent hosts and the manager host) and a remote monitoring configuration (where remotely connected hosts are monitored) are managed.	
	Management of virtualization configuration information	• Manages the hierarchical structure of the system, including virtual hosts.	
	Business group management	• Monitors multiple monitored hosts by creating a group based on the system used for a particular business operation, or based on which monitored objects are managed by a particular system administrator.	
	Profile management	• Enables you to centrally manage, from the manager, the JP1/Base profiles running on each host or the profiles on the remotely monitored hosts.	
	Management of service activity information	• Checks whether JP1/IM - Manager and JP1/Base services are active on each host.	
	Import/export of IM Configuration Management information	• Exports and imports IM Configuration Management information.	
Core functionality	Process management	• Manages JP1/IM - Manager and its functions.	• Process management
	Health check	• Monitors the status of JP1/IM - Manager processes (other than the central scope service and IM configuration management service on the local host). • Monitors the status of JP1/Base processes.	• Health check • JP1/Base
	Hitachi Network Objectplaza Trace Library (HNTRLib2)	• Stores trace information from JP1/Base, JP1/IM - Manager, JP1/IM - View, and other component products.	• HNTRLib2
	User management	• Manages JP1 users. • Manages command execution permissions.	• JP1/Base
	Configuration management[#2]	• Manages the configuration of the JP1/IM - Manager system.	
	Service startup control	• Controls the service start/stop sequencing of products (including JP1/Base) registered with the Windows service.[#3]	
	Command execution[#2]	• Control command execution. • Manages command execution log files (manager only).	

Function		Description	Service name
	Definition collection and distribution#2	• Collects and distributes definition information related to the JP1/IM - Manager event service.	

#1: Available when the IM Configuration Management database has been set up.

#2: JP1/Base function.

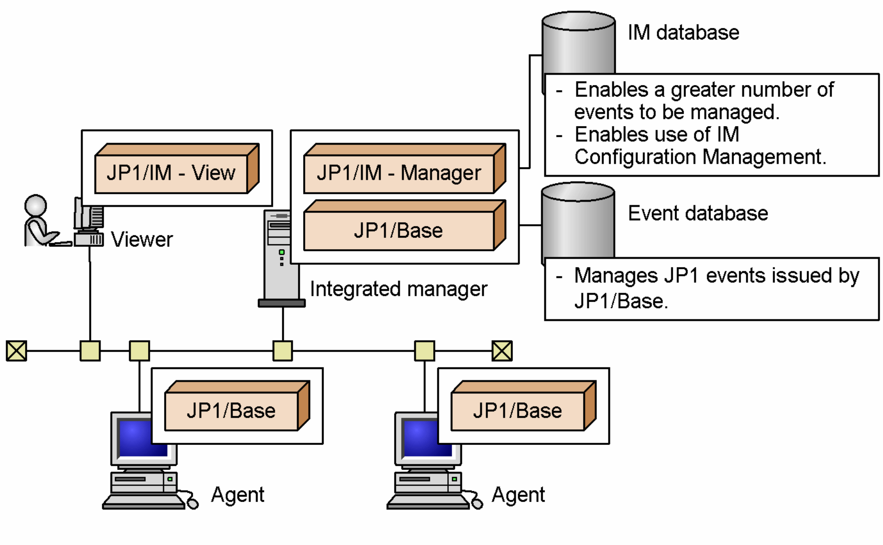
#3: Windows-only function.

2.4 Functions provided by the IM database

JP1/IM - Manager manages JP1 events using its own *IM database* or the event database provided by JP1/Base. Users manage JP1 events by setting up the IM database and the JP1/Base event database.

The following figure shows how the databases are positioned in the system.

Figure 2–9: Positioning of the IM database and JP1/Base event database


IM database
- Enables a greater number of events to be managed.
- Enables use of IM Configuration Management.
JP1/IM - View
Viewer
JP1/IM - Manager
JP1/Base
Integrated manager
Event database
- Manages JP1 events issued by JP1/Base.
JP1/Base
Agent
JP1/Base
Agent

IM database is a generic term for the following two databases:

- *Integrated monitoring database* used by the Central Console component of JP1/IM - Manager
- *IM Configuration Management database* used by the IM Configuration Management component of JP1/IM - Manager

By setting up the integrated monitoring database and IM Configuration Management database according to the functionality you want to use, you can expand the functionality previously available with the JP1/Base event database.

The following table describes the functionality provided by the integrated monitoring database and IM Configuration Management database.

Table 2–4: Functionality provided by the integrated monitoring database and IM Configuration Management database

JP1/IM - Manager component	Database	Available functionality
Central Console	Integrated monitoring database Add memos to JP1 events.	Specify a start time for listing events.
		Change the severity of JP1 events.
		Conduct event searches in the integrated monitoring database.
		Add filtering conditions for JP1 event filtering.
		Add memos to JP1 events.
		Output event reports to the integrated monitoring database.
		Suppress the monitoring of repeated events.
		Set the range of events to be collected at login.

JP1/IM - Manager component	Database	Available functionality
		Change the message display format.
IM Configuration Management	IM Configuration Management database	Manage hosts.
		Manage the system hierarchy.
		Manage virtualization configurations.
		Manage business groups.
		Manage profiles.
		Manage service activity information.
		Import and export IM Configuration Management information.
	Integrated monitoring database and IM Configuration Management database	Manage business groups.

2.5 Preparations for using functions

To use a specific JP1/IM - Manager function, you must complete preparations appropriate to the type of function. The following methods are available for performing the preparations:

- Executing commands
- Specifying parameters in definition files
- Specifying values for items in windows

The table below describes the prerequisite functions, preparations, and configuration methods for using each JP1/IM - Manager function. The settings that are not discussed in this table do not need to be specified because JP1/IM - Manager functions use their initial values. For details about the settings for each function, such as event conditions, see the details for the corresponding function.

Table 2–5: Prerequisite functions, preparations, and configuration methods for using the IM database

Section	Prerequisite function	Preparation for using the function
2.4 Functions provided by the IM database • Integrated monitoring database	--	Specify information such as the size and storage location of the IM database. • Physical hosts Setup information file (`jimdbsetupinfo.conf`) • Logical hosts Cluster setup information file (`jimdbclustersetupinfo.conf`)
		Set up the IM database by using the following command: • `jcodbsetup` command
		Enable the function by using the following command: • `jcoimdef` command (option:`-db ON`)
2.4 Functions provided by the IM database • IM Configuration Management database	--	Specify information such as the size and storage location of the IM database. • Physical hosts Setup information file (`jimdbsetupinfo.conf`) • Logical hosts Cluster setup information file (`jimdbclustersetupinfo.conf`)
		Set up the IM database by using the following command: • `jcfdbsetup` command
		Enable the function by using the following command: • `jcoimdef` command (option: `-cf ON`)

Legend:

--: Not applicable

Table 2–6: Prerequisite functions, preparations, and configuration methods for using the Central Console

Section	Prerequisite function	Preparation for using the function
3.1.1 Monitoring from the Central Console	--	--

Section	Prerequisite function	Preparation for using the function
3.1.4 Restrictions on viewing and operating business groups	Integrated monitoring database IM Configuration Management Event-source-host mapping	Enable the function by using the following command: • `jcoimdef` command (option: `-bizmonmode ON`)
3.2.2 Event acquisition filter	--	--
3.2.3 Event receiver filter	--	--
3.2.4 Severe events filter	--	--
3.2.5 View filter	--	--
3.2.6 Defining filter conditions • Common exclusion conditions (basic mode)	--	Use the following command to change from extended mode to basic mode: `jcochcefmode` command (option: `-m normal`)
3.2.6 Defining filter conditions • Common exclusion conditions (extended mode)	--	Change JP1/Base regular expressions to extended regular expressions. For details, see the *JP1/Base User's Guide*.
		Use the following command to change from basic mode to extended mode: • `jcochcefmode` command (option: `-m extended`)
3.3 Issue of correlation events	--	Enable the function by using the following command: • `jcoimdef` command (option: `-egs ON`)
3.4 Suppressing display of repeated events	Integrated monitoring database	Enable the function by using the following command: • `jcoimdef` command (option: `-storm ON`)
3.4.10 Suppressing repeated-event display by the consolidated display of repeated events	--	Disable the repeated event monitoring suppression function by using the following command: • `jcoimdef` command (option: `-storm OFF`) Enable the function in the following window: • Preferences window
3.5 Suppressing monitoring of a large number of events	Integrated monitoring database	Enable the function by using the following command: • `jcoimdef` command (option: `-storm ON`)
3.6 Searching for events	--	--
3.7 Changing the event level (severity) of JP1 events	Integrated monitoring database	Enable the function by using the following command: • `jcoimdef` command (option: `-chsev ON`)
3.8 Changing the message display format	Integrated monitoring database	--
3.9 Mapping of the event source hosts	Integrated monitoring database	Enable the function by using the following command: • `jcoimdef` command (option: `-hostmap ON`)
3.10 Event guide function	--	--
3.11 Setting memo entries	Integrated monitoring database	Enable the function by using the following command: • `jcoimdef` command (option: `-memo ON`)

Section	Prerequisite function	Preparation for using the function
3.12 Adding program-specific attributes	--	--
3.13 Displaying program-specific extended attributes and specifying them in event conditions	--	--
3.14 Displaying user-defined event attributes	--	--
3.15 CSV output of information displayed in JP1/IM - View	--	--
3.16 Specifying the event display start-time	Integrated monitoring database	--
3.17 Range of events to be collected at login	Integrated monitoring database	Enable the function in the following window: • Preferences window
3.18 Specifying the event display period	--	--
3.19.1 Launching a linked product by monitor startup	--	--
3.19.2 Tool Launcher	--	--
3.19.3 Executing commands on managed hosts from JP1/IM - View	--	--
3.19.4 Executing commands on client hosts	--	--
3.19.5 Inheriting event information when a command is executed	--	--
3.20 Email notification function (for Windows only)	--	In the following definition file, specify the information needed for email transmission, such as the mail server's host name, authentication method, authentication account name, and password: • Email environment definition file (`jimmail.conf`)
Chapter 5. Command Execution by Automated Action	--	--

Legend:

--: Not applicable

Table 2–7: Prerequisite functions, preparations, and configuration methods for using Central Scope

Section	Prerequisite function	Preparation for using the function
4.1 Overview of Central Scope functions	--	Set up a monitoring object database by using the following command: • `jcsdbsetup` command
		Enable the function by using the following command: • `jcoimdef` command (option: `-s ON`)
4.2 Monitoring tree	Central Scope	--
4.3 Automatically generating a monitoring tree	Central Scope	--
4.4 Editing a monitoring tree	Central Scope	--

Section	Prerequisite function	Preparation for using the function
4.5 Visual monitoring	Central Scope	--
4.7 Searching for monitoring nodes or status change events	Central Scope	--
4.8 Guide function	Central Scope	--
4.9 Completed-action linkage function	Central Scope	--
4.10.1 Tool Launcher	Central Scope	--

Legend:

--: Not applicable

Table 2–8: Prerequisite functions, preparations, and configuration methods for using IM Configuration Management

Section	Prerequisite function	Preparation for using the function
Chapter 6. System Hierarchy Management Using IM Configuration Management	IM Configuration Management database	Enable the function by using the following command: • `jcoimdef` command (option: `-cf ON`)
6.1 Host management	IM Configuration Management	--
6.2 System hierarchy management	IM Configuration Management	--
6.3 Virtualization configuration management	IM Configuration Management	--
6.4 Managing business groups	IM Configuration Management	--
6.5 Profile management	IM Configuration Management	--
6.6 Managing remotely monitored hosts	IM Configuration Management	To perform remote monitoring, configure the OSs on both the manager host and the monitored host. For details about the OS settings, see the following: • *1.17 Specifying settings for monitoring logs on remotely monitored hosts (for Windows)* or *2.16 Specifying settings for monitoring logs on remotely monitored hosts (for UNIX)* in the *JP1/Integrated Management - Manager Configuration Guide*
6.7 Management of service activity information	IM Configuration Management	--
6.8 Exporting and importing IM Configuration Management information	IM Configuration Management	--

Legend:

--: Not applicable

Table 2–9: Prerequisite functions, preparations, and configuration methods for controlling JP1/IM - Manager operation

Section	Prerequisite function	Preparation for using the function
7.1 JP1/IM - Manager process management	--	--

Section	Prerequisite function	Preparation for using the function
7.2 JP1/IM - Manager health check function	--	Enable the function by using the following definition file: - Health check definition file (`jcohc.conf`)

Legend:

--: Not applicable

Table 2–10: Prerequisite functions, preparations, and configuration methods for linking with other products

Section	Prerequisite function	Preparation for using the function
8.1 Linking with JP1/Service Support	--	Define the URL for JP1/Service Support's WWW page used for registering incidents: - Definition file for manually registering incidents (`incident.conf`) Define the attributes or strings of JP1 events to be registered as incidents in the following file: - Configuration file for incident inheritance information (`incident_info.conf`)
8.2 Linking with JP1/Navigation Platform	Central Console's event guide	--
8.3 Linking with JP1/IM - Rule Operation	--	Enable the function by using the following command: - `jcoimdef` command (option: `-rule ON`)
		Register the host name for JP1/IM - Rule Operation: - `jcoimdef` command (option: `-rulehost` *host-name*)
8.4 Linking with VMware vCenter Operations Manager	IM Configuration Management	--
8.5 Linking with OpenStack	--	--
8.6 Linking with another system that uses the REST API of JP1/AO	--	--
8.7 Linking with JP1/AJS	Launching linked products by monitor startup	--
	Tool Launcher	--
	Central Console's event guide	--
	Automated action (mail transmission)	--
8.8 Linking with JP1/PFM	--	Define the URL for the target JP1/PFM - Web Console. - Performance report display definition file (`performance.conf`)
	Launching linked products by monitor startup	--
	Tool Launcher	--
Linking with BJEX or JP1/AS	--	Enable the function by using the following command: - `jcoimdef` command (option: `-resevent ON`)

Legend:

--: Not applicable

Table 2–11: Preparation for outputting data to the operation log

Section	Prerequisite function	Preparation for using the function
Appendix K. Operation Log Output	--	Specify whether to output data to the operation log, the output destination, the size of the operation log, and the maximum number of files that can be saved. • Operation log definition file (`imm_operationlog.conf`)

Legend:

--: Not applicable

2.6 JP1/IM - Manager service

JP1/IM - Manager (for Windows) provides the services below.

In the following table, italic character strings indicate variables.

Table 2–12: JP1/IM - Manager services

Displayed name	Service name	Startup type	Description
`JP1/IM-Manager`	`JP1_Console`	Manual	JP1/IM - Manager service (Central Console, Central Scope, and IM Configuration Management) on a physical host
`JP1/IM-Manager DB Server`#1	`HiRDBEmbeddedEdition_JM0`	Manual	IM database service on a physical host
`JP1/IM-Manager DB Cluster Service`#1	`HiRDBClusterService_JM0`	Manual	Not used in JP1/IM - Manager
`JP1/IM-Manager_`*logical-host-name*#2	`JP1_Console_`*logical-host-name*	Manual	JP1/IM - Manager service (Central Console, Central Scope, and IM Configuration Management) on a logical host (*logical-host-name*)
`JP1/IM-Manager DB Server_`*logical-host-name*#3, #4	`HiRDBEmbeddedEdition_JM`<*n*>#6	Manual	IM database service on a logical host (*logical-host-name*)
`JP1/IM-Manager DB Cluster Service_`*logical-host-name*#3, #5	`HiRDBClusterService_JM`<*n*>#6	Manual	A service that controls the internal status of the IM database on a logical host (*logical-host-name*)

#1: This service is registered only when the IM database for the physical host is set up.

#2: This service is registered only when a logical host is set up.

#3: This service is registered only when the IM database for the logical host is set up.

#4: This service is controlled by `JP1/IM-Manager DB Cluster Service_`*logical-host-name*. Do not use this service for operation of a logical host in a non-cluster system. For operation of a logical host in a non-cluster system, this service does not stop if `JP1/IM-Manager DB Cluster Service_`*logical-host-name* is stopped.

#5: Use this service for operation of a logical host in a non-cluster system.

#6: <*n*> is a number from 1 to 9. This number is the same as the value specified for `LOGICALHOSTNUMBER` in the cluster setup information file. For details, see *Cluster setup information file (jimdbclustersetupinfo.conf)* in *Chapter 2. Definition Files* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

Important

In the **Log on** settings of the above services, do not change **System Account** in the initial settings. Do not select the **Allow service to interact with desktop** option. If this option is selected, the service might not function normally.

3 Centralized System Monitoring Using the Central Console

This chapter describes how to monitor the system using the Central Console.

3.1 Centralized monitoring using JP1 events

The JP1/IM Central Console centrally monitors major events occurring in the system, such as network problems and server failures, based on JP1 events.

This section describes the following functions used to perform centralized monitoring:

- Monitoring from the Central Console
- Filtering of JP1 events
- Issue of correlation events
- Monitoring repeated events
- Searching for events
- Event guide function
- Setting memo entries
- Display of user-defined event attributes
- CSV output of information displayed in JP1/IM - View
- System operations from JP1/IM

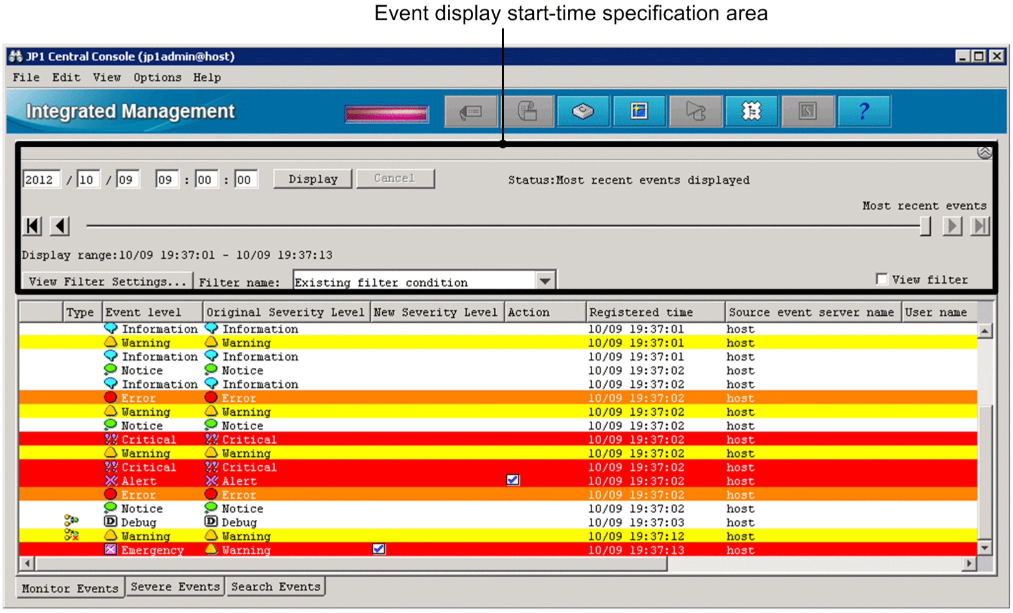
When you use the integrated monitoring database, expanded functionality is available for centralized monitoring, as described in the following table.

Table 3–1: Expanded functionality when using the integrated monitoring database

Item	Expanded functionality
Specifying the event display start-time	You can specify the event display start-time for the JP1 events to be displayed in the event list.
Changing the severity of a JP1 event	You can set a severity changing definition to change the severity of the JP1 event that meets the condition specified by the definition.
Changing the message displayed for a JP1 event	You can set a display message change definition to change the message displayed for a JP1 event that satisfies specified conditions.
Searching for events in the integrated monitoring database	You can specify the event database or integrated monitoring database as the database in which to search for events.
Adding filtering conditions for JP1 event filtering	More filtering conditions can be used for the view filter and the event receiver filter.
Adding memo entries	When the memo entry setting function is enabled, you can add memo entries for the JP1 events registered in the integrated monitoring database.
Outputting event reports about the events in the integrated monitoring database	You can output the information about JP1 events stored in the integrated monitoring database in CSV format.
Suppressing monitoring of repeated events	You can set repeated event conditions to suppress the display of JP1 events (that meet set conditions) in the event list and execute corresponding automated actions.
Specifying the range of events to be collected at login	You can specify the period of occurrence for the events that JP1/IM - View acquires from the integrated monitoring database of JP1/IM - Manager when you log in to JP1/IM - Manager.

The following figure shows the window for monitoring JP1 events.

Figure 3–1: JP1 event monitoring in the Event Console window



Event display start-time specification area

2012 / 10 / 09 09 : 00 : 00

Status:Most recent events displayed

Most recent events

Display range:10/09 19:37:01 - 10/09 19:37:13

Filter name: Existing filter condition

□ View filter

	Type	Event level	Original Severity Level	New Severity Level	Action	Registered time	Source event server name	User name
		Information	Information			10/09 19:37:01	host	
		Warning	Warning			10/09 19:37:01	host	
		Information	Information			10/09 19:37:01	host	
		Notice	Notice			10/09 19:37:02	host	
		Information	Information			10/09 19:37:02	host	
		Error	Error			10/09 19:37:02	host	
		Warning	Warning			10/09 19:37:02	host	
		Notice	Notice			10/09 19:37:02	host	
		Critical	Critical			10/09 19:37:02	host	
		Warning	Warning			10/09 19:37:02	host	
		Critical	Critical			10/09 19:37:02	host	
		Alert	Alert		☑	10/09 19:37:02	host	
		Error	Error			10/09 19:37:02	host	
		Notice	Notice			10/09 19:37:02	host	
		Debug	Debug			10/09 19:37:03	host	
		Warning	Warning			10/09 19:37:12	host	
		Emergency	Warning	☑		10/09 19:37:13	host	

The Event Console window shows a list of JP1 events. JP1 events are managed by JP1/Base, and can be optimally viewed using the various functions provided by JP1/IM.

In the above Event Console window, the area for event display start-time specification is displayed. This area appears only when you use the integrated monitoring database.

Display in the Event Console window

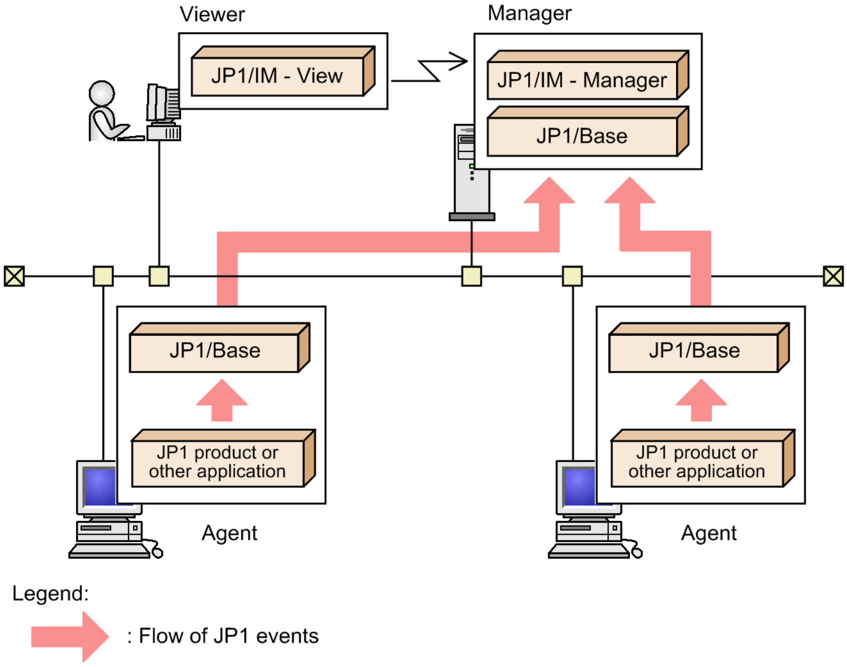
JP1/IM attaches an icon to each event to indicate its level of severity (one of the attributes of JP1 events). This enables visual identification when the user views an event listing.

The event levels of JP1 events are ☒ `Emergency`, ✕ `Alert`, `Critical`, ● `Error`, △ `Warning`, `Notice`, `Information`, and 🄳 `Debug`.

3.1.1 Monitoring from the Central Console

The Central Console centrally manages JP1 events that were generated on agents and received at the manager. JP1 events issued on agents are filtered, and only the JP1 events that need to be monitored are forwarded to the manager.

Figure 3–2: Overview of JP1 event monitoring from the Central Console



JP1 events are displayed in a time series in the Event Console window. The window has three pages, which you can display as required by clicking the appropriate tab. In some cases, JP1 events might be selected by the filtering function during the pre-processing for display in JP1/IM - View. This is explained below in *3.2 Filtering of JP1 events*. JP1 events might be consolidated by repeated-event monitoring during pre-processing for display in JP1/IM - View. This is explained in *3.4 Suppressing display of repeated events*.

The Event Console window has the following three types of pages:

Monitor Events page

The **Monitor Events** page displays JP1 events in the order received at the manager. Use this page to view events generated in the system in a time series.

JP1 events acquired from the JP1/Base event service on the manager are displayed.

The view filter function is available on the **Monitor Events** page. Users can choose how to filter the JP1 events displayed on the **Monitor Events** page.

When a large number of identical events occur in a short space of time, they can be summarized on the **Monitor Events** page using the function for consolidating repeated events.

The **Monitor Events** page can also display JP1 events consolidated by repeated-event monitoring.

Severe Events page

The **Severe Events** page lists only those JP1 events considered to be severe events.

A *severe event* is a JP1 event that needs to be addressed, such as a failure of some sort. By default, JP1 events whose event level is `Emergency`, `Alert`, `Critical`, or `Error` are defined as severe events.

When a severe event occurs, the alarm lamp in JP1/IM - View flashes to inform the user.

You can use the view filter function on the **Severe Events** page.

You can freely filter JP1 events to separate out those to be displayed on the **Severe Events** page.

The **Severe Events** page can also display JP1 events consolidated by repeated-event monitoring.

Search Events page

The **Search Events** page displays the results of an event search conducted on a host from JP1/IM - View.

Because only severe events are forwarded to a manager, you must perform an event search if you want to view normal JP1 events. For example, you can use the **Search Events** page to retrieve events immediately before and after a JP1 event indicating a problem when you want to find out what was happening at the time.

You can also use the **Search Events** page to display old events that have been removed from the JP1/IM - View's scroll buffer.

For an overview of the event search, see *3.6 Searching for events*.

You can perform the following operations and settings for the JP1 events displayed in the Event Console window:

- Specify a start time for listing JP1 events

  When you use the integrated monitoring database, you can change the JP1 events listed in the Event Console window of JP1/IM - View by specifying a date and time or by moving the slider in the event display start-time specification area. After you specify a start time for listing JP1 events, among the JP1 events generated after the specified start time (the date and time displayed in the event display start-time text boxes or the date and time displayed on the slider), only those JP1 events that match the applied filter conditions are searched from the integrated monitoring database and displayed in the Event Console window. This allows you to see JP1 events when the maximum number of viewable events (JP1/IM - View's scroll buffer size) has been exceeded and there are too many events to fit into the Event Console window all at once.

  The event display start-time specification area does not appear in the **Search Events** page.

- View JP1 event details

  You can view detailed attribute information about JP1 events. You can also view operating advice, such as troubleshooting procedures, if event guide information has been preset for a selected JP1 event. When you use the integrated monitoring database, you can set and display memos by enabling the function for entering memos in JP1 events. When a memo has been set, the 📝 icon appears to the left of the listed event.

- Specify a period for listing JP1 events

  Using the event display period specification, you can set a base time and a period of days for listing events. For example, suppose the current time is 9:15 am on July 8, and you set the display period as follows:

  - **Base time**

    09:00

  - **Display period**

    2 days

  With this setting, the listing will cover JP1 events that have occurred since 9:00 am on the previous day (July 7).

- Launch linked applications by monitor startup

  You can launch the GUI of a linked product associated with a selected JP1 event.

- View the execution results of automated actions

  You can view the execution result of an automated action executed in response to a JP1 event.

  The execution results of automated actions cannot be displayed in the **Search Events** page.

- Change the display items for JP1 events

  The following information can be displayed as JP1 event information in the Event Console window:

  Items displayed by default:

  Event level, **Registered time**, **Source host**, **User name**, **Event ID**, **Message**, **Object type**, and **Action**.

  Items not displayed by default:

  Start time, **End time**, **Product name**, **Object name**, **Root object type**, **Root object name**, **Arrived time**, **Occurrence**, **Serial number**, **Source process ID**, **Source user ID**, **Source group ID**, **Source user name**, **Source group name**, **Source serial number**, **Type**, **Action type**, **Source IP address**, **Object ID**, **Return**

code, **Relation Event serial number**, **Correlation event generation condition name**, **Suppressed event ID**, **Repeated event condition name**, **Monitoring ID**, **Log file trap name**, and **Extended attribute**.

In addition to the above items, when you use the integrated monitoring database, **Original severity level**, **New severity level**, **Changed display message**, **New display message**, **Display message change definition**, **Memo, Common exclude conditions group ID**, **Common exclude conditions group name**, and **Common exclude conditions group target-for-exclusion** are also not displayed by default. **Original severity level** and **New severity level** are displayed when the severity changing function is enabled. **Changed display message**, **New display message**, and **Display message change definition** are displayed when the display message change function is enabled. **Memo** is displayed when the memo functionality is enabled. When you use mapping of the event source hosts, **Event source host name** is displayed by default in addition to the above items.

For **Extended attribute**, the information specified in the definition file for the extended event attributes (extended file) is displayed.

You can change the display items and their order to suit your purpose.

In addition to the above display items, icons representing the event status and the presence of an event memo are displayed in JP1 event listings. These icons appear in front of the event name in the Event Console window. The memo icon does not appear unless you are using the integrated monitoring database.

Event-specific information and other information not covered by the above display items can be displayed in the Event Console window by mapping the event-specific information to one of the above display items. In this case, # is prefixed to the displayed information.

The following items are not displayed in the Web-based JP1/IM - View.

Items that are not displayed in the Web-based JP1/IM - View:

Source IP address, **Return code**, **Relation Event serial number**, **Correlation event generation condition name**, **Suppressed event ID**, **Repeated event condition name**, **Monitoring ID**, **Log file trap name**, **Extended attribute**, **Changed display message**, **New display message**, **Display message change definition**, **Common exclude conditions group ID**, **Common exclude conditions group name**, **Common exclude conditions group target-for-exclusion**

- Set the response status of JP1 events

  You can set the response status of JP1 events. Any of the following four statuses can be set, according to how events are processed and the action already taken: **Processed**, **Processing**, **Held**, and **Unprocessed**. You can check the settings in the **Monitor Events** page, **Severe Events** page, or **Search Events** page. The response status is represented by an icon.

  The response statuses that can be set and displayed differ for each page, as shown in the following table.

Table 3–2: Differences in response status settings among pages in the Event Console window

Page	Specifiable response statuses	Number of events whose response status can be set in one operation	Update of other pages when response status changes[#1]
Monitor Events	Processed, Processing, Held, Unprocessed	Multiple	Automatically updated
Severe Events	Processed, Processing, Held, Unprocessed, Delete[#2]	Multiple	Automatically updated
Search Events	Processed, Processing, Held, Unprocessed	Multiple	After next search

#1: When a response status is set on another page, the **Monitor Events** page or **Severe Events** page is automatically updated to reflect the changed status (provided the **Apply** check box is selected for **Automatic refresh** in the Preferences window). Otherwise, you can update the response status in the **Monitor Events** page and **Severe Events** page by choosing **View** and then **Refresh**, or by clicking the **Refresh** button. To refresh the **Search Events** page, you must perform another search.

#2: When **Delete** is set for a JP1 event on the **Severe Events** page, that JP1 event is no longer listed on the page. Because the events deleted on the **Severe Events** page are not deleted from the event database and integrated database, they might appear on other pages and, if so, their response status can still be set.

The events once deleted on the **Severe Events** page cannot be redisplayed on the page.

You can also set the response status in the Related Events window, which opens from the Event Console window. You can set and display the same statuses as on the page from which you opened the Related Events window.

You can also generate a JP1 event whenever a response status changes. This allows you to record a history of the actions taken.

- Highlighting

  You can apply a background color to the JP1 events displayed in the Event Console window (the default is no highlighting). If you set the background colors to be used, JP1 events are highlighted according to their event levels when they are displayed on the **Monitor Events**, **Severe Events**, or **Search Events** page of the Event Console window.

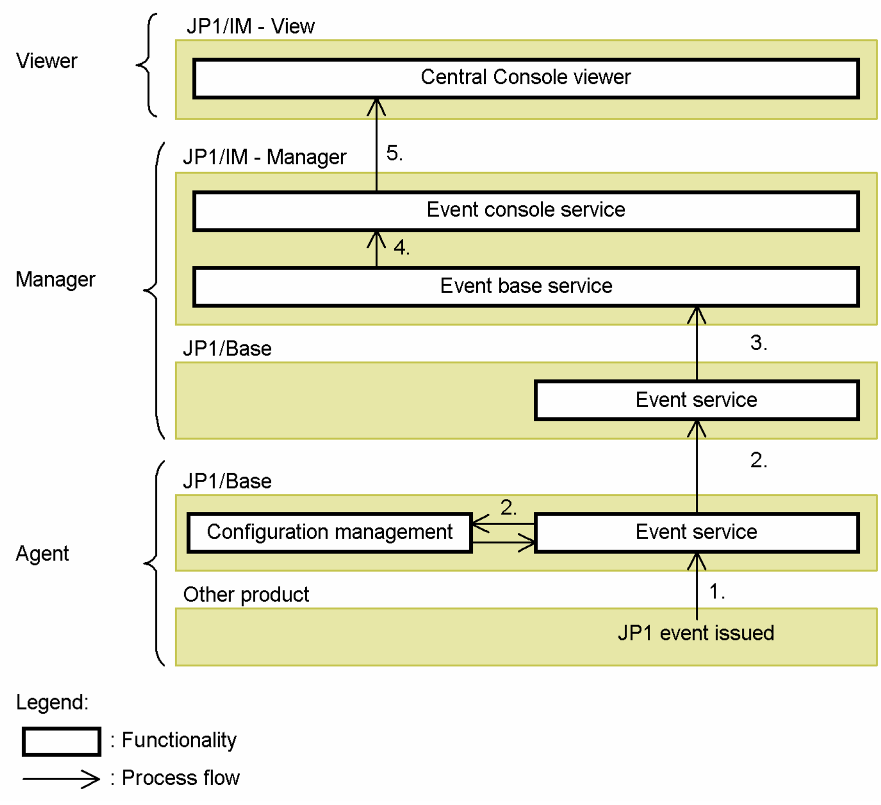
  When you use the integrated monitoring database, events are highlighted according the user-defined event level.

  You can change the background color by using the system color definition file (`systemColor.conf`). For details, see *System color definition file (systemColor.conf)* (*Chapter 2. Definition Files*) in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

3.1.2 Flow of processing for JP1 event monitoring

The following describes how JP1/IM and JP1/Base are inter-linked in event monitoring. This example shows the flow of processing where a JP1 event generated in an agent is displayed on a window on the viewer.

Figure 3–3: Flow of processing for JP1 event monitoring



The flow of processing is described below, following the numbers in the figure:

1. The agent issues a JP1 event, which is registered with its event service.
2. The JP1 event registered with the event service is forwarded to the destination defined by the forwarding setting file of JP1/Base.
3. Information about the registered JP1 event is acquired by the event base service.

4. The event console service acquires the JP1 event information from the event base service.
5. The JP1 event acquired by the event console service is monitored from the viewer.

For details about the event service, see *7.4.2 Managing JP1 events using JP1/Base*. For details about configuration management, see *7.4.3 Managing the system hierarchy*. For details about the event base service, see *3.1.3 Internal control of JP1 events by JP1/IM - Manager*.

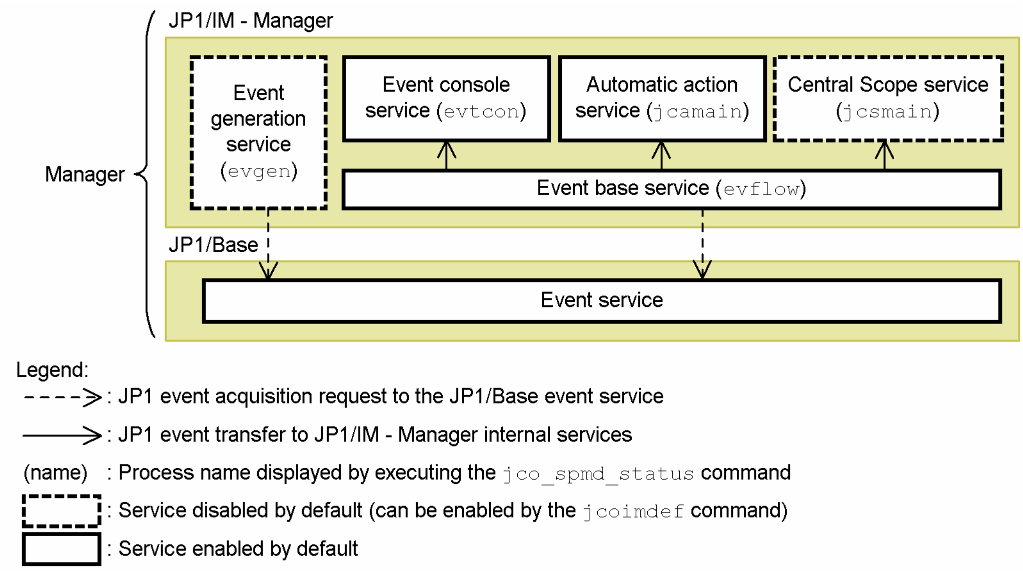
3.1.3 Internal control of JP1 events by JP1/IM - Manager

Internal processing in JP1/IM - Manager is based on information about JP1 events collected from the event database in JP1/Base and from the integrated monitoring database in JP1/IM - Manager.

(1) JP1 event control when not using the integrated monitoring database

If you do not use the integrated monitoring database, JP1 events are collected from the JP1/Base event database by the JP1/IM - Manager's event base service and event generation service.

Figure 3–4: Internal control of JP1 events by JP1/IM - Manager (when the integrated monitoring database is not used)


JP1/IM - Manager
Manager
Event generation service (evgen)
Event console service (evtcon)
Automatic action service (jcamain)
Central Scope service (jcsmain)
Event base service (evflow)
JP1/Base
Event service
Legend:
- - - -> : JP1 event acquisition request to the JP1/Base event service
——> : JP1 event transfer to JP1/IM - Manager internal services
(name) : Process name displayed by executing the jco_spmd_status command
: Service disabled by default (can be enabled by the jcoimdef command)
: Service enabled by default

The JP1 events acquired by these two services are processed in various ways after they have been filtered by the event acquisition filter according to set conditions.

Processing of acquired JP1 events by the event base service

JP1/IM - Manager sends JP1 events from the event base service to the event console service, the automatic action service, and the central scope service. After the event base service receives notification from all of these services that they have received the JP1 events, it executes the next processing task. Therefore, if a large number of JP1 events are issued, the processing of JP1 events might be delayed. We recommend that you filter JP1 events and use only the necessary events for management.

Using the `jcoimdef` command, you can adjust the JP1 event acquisition and transfer processing performed by the event base service (for example, you can change the event acquisition start location, or the transfer timeout period and retry setting). For details, see *jcoimdef* in *Chapter 1. Commands* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

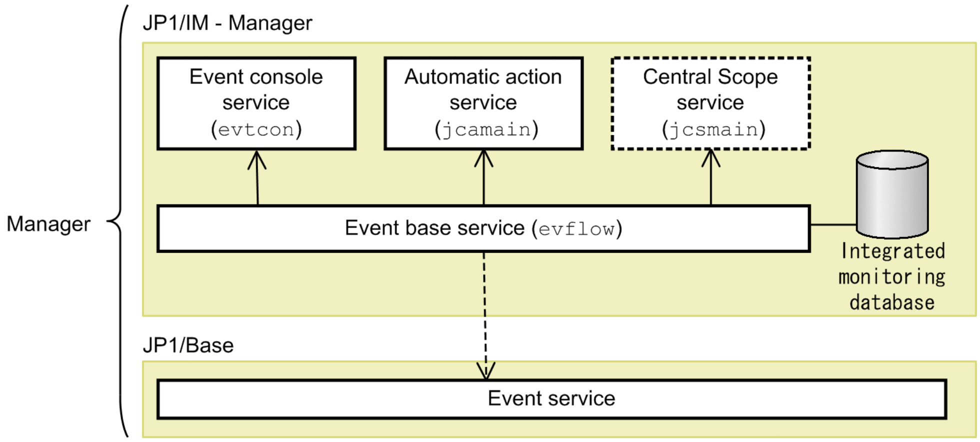
Processing of acquired JP1 events by the event generation service

This service performs correlation event issue based on issue definitions. For details, see *3.3 Issue of correlation events*.

(2) JP1 event control when using the integrated monitoring database

When you use the integrated monitoring database, JP1 events are collected from the JP1/Base event database by the JP1/IM - Manager's event base service. The acquired JP1 events are stored in the integrated monitoring database.

Figure 3–5: Internal control of JP1 events by JP1/IM - Manager (when the integrated monitoring database is used)


JP1/IM - Manager
Manager
Event console service (evtcon)
Automatic action service (jcamain)
Central Scope service (jcsmain)
Event base service (evflow)
Integrated monitoring database
JP1/Base
Event service

Legend:

-----> : JP1 event acquisition request to the JP1/Base event service

——> : JP1 event transfer to JP1/IM - Manager internal services

(name) : Process name displayed by executing the `jco_spmd_status` command

⬚ : Service disabled by default (can be enabled by the `jcoimdef` command)

□ : Service enabled by default

The event base service acquires JP1 events and executes various processing tasks.

If you execute the `jcoimdef` command with -1 specified for the -b option, the event base service acquires JP1 events from the next event after the event that has the oldest serial number (the event at which JP1/IM - Manager stopped last time) among the JP1 events processed before JP1/IM - Manager is stopped. -1 specified for the -b option, JP1 event is acquired depends on whether the event was processed before JP1/IM - Manager stopped.

For JP1 events that were processed before JP1/IM - Manager stopped:

JP1 events are acquired from the integrated monitoring database, where the event acquisition filter is not used.

For JP1 events that were not processed before JP1/IM - Manager stopped:

JP1 events are acquired from the JP1/Base event database.

These JP1 events have been filtered by the event acquisition filter. JP1 events acquired from the event database are stored in the integrated monitoring database.

Processing of acquired JP1 events by the event base service

In the event base service, JP1/IM - Manager generates a correlation event according to the correlation event generation definition. Then, JP1/IM - Manager sends JP1 events from the event base service to the event console service, the automatic action service, and the central scope service. After the event base service receives notification from all of these services that they have received the JP1 events, it executes the next processing task. Therefore, if a large number of JP1 events are issued, the processing of JP1 events might be delayed. We recommend that you filter JP1 events and use only the necessary events for management.

Using the `jcoimdef` command, you can adjust the JP1 event acquisition and transfer processing performed by the event base service (for example, you can change the event acquisition start location, or the transfer timeout and retry setting). For details, see *jcoimdef* in *Chapter 1. Commands* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

3.1.4 Restrictions on viewing and operating business groups

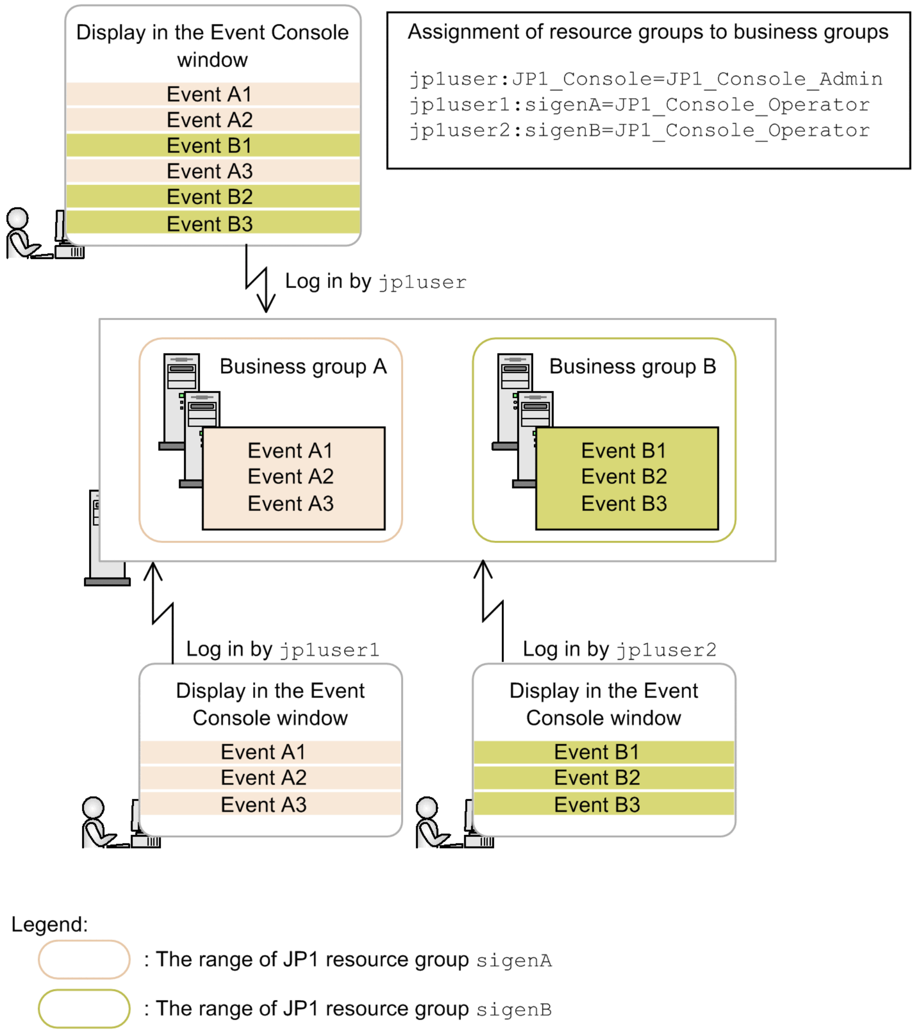
The system administrator can restrict what JP1 users are able to view and operate on. This is called *restrictions on viewing and operating business groups*.

If restrictions on viewing and operating business groups are enabled, a user can view and operate on only the JP1 events issued within the assigned business group. This prevents users from unintentionally operating on JP1 events in other business groups.

If restrictions on viewing and operating business groups are enabled, the following windows display only the JP1 events issued within the assigned business group:

- Event Console window
- Related Events window
- Event Details window

Figure 3–6: The range of JP1 events that can be viewed and operated



```
jp1user:JP1_Console=JP1_Console_Admin
jp1user1:sigenA=JP1_Console_Operator
jp1user2:sigenB=JP1_Console_Operator
```

In this example, resource group `sigenA` is assigned to business group A, and resource group `sigenB` is assigned to business group B.

For details about how to enable restrictions on viewing and operating business groups, see *4.20 Setting reference and operation restrictions on business groups* in the *JP1/Integrated Management - Manager Configuration Guide*.

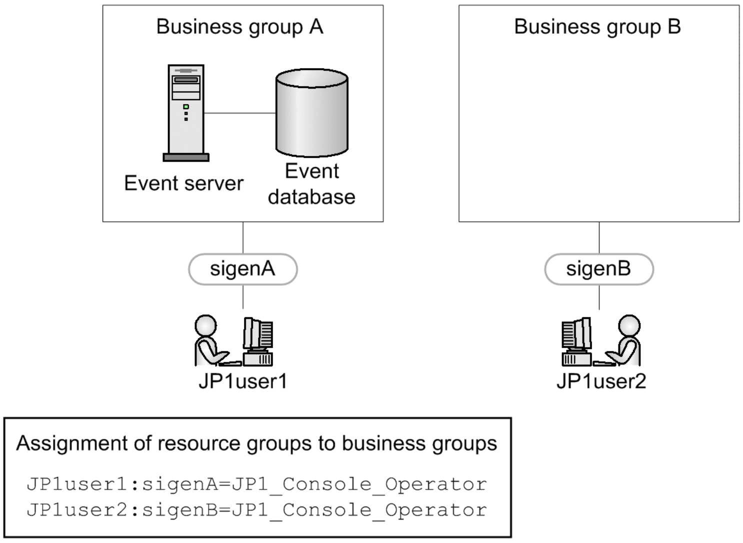
When you change the configuration of business groups, note the following:

- When moving the JP1/Base event server to another business group, initialize the event database.

  If you do not initialize the event database, the JP1 users in the business group to which the event server is moved will be able to view and operate on JP1 events saved in the event database. Therefore, be sure to initialize the event database.

  As an example, assume that business groups are configured as in the following figure.

Figure 3–7: Configuration of business groups

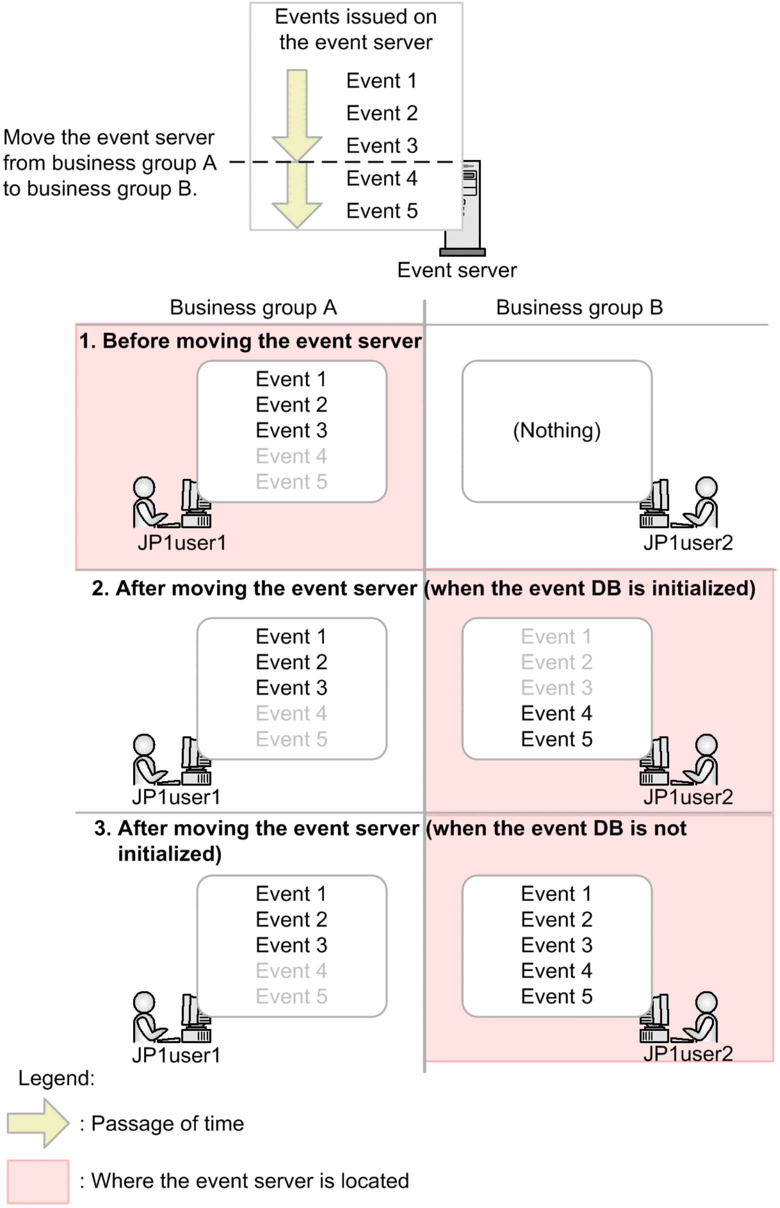


Assignment of resource groups to business groups

```
JP1user1:sigenA=JP1_Console_Operator
JP1user2:sigenB=JP1_Console_Operator
```

Now move the event server in business group A to business group B.

Figure 3–8: Moving the event server



The following explains the above example, in the order of the numbers in the figure:

1. Before the event server is moved, JP1 events issued on the event server (`Event1`, `Event2`, and `Event3`) can be viewed and operated on in business group A. In business group B, no JP1 events can be viewed and operated on yet.

2. After the event server is moved, JP1 events issued before the event server is moved (`Event1`, `Event2`, and `Event3`) can be viewed and operated on in business group A. In business group B, JP1 events issued after the event server is moved (`Event4` and `Event5`) can be viewed and operated on.

3. If the event database is not initialized when the event server is moved, JP1 events issued before the event server is moved can also be viewed and operated on in business group B.

For details about how to initialize the event database, see the description about initialization of the event database in the chapter for setting the event service environment in the *JP1/Base User's Guide*.

- Do not forward events between different business groups.

If you forward events between different business groups, JP1 events from different business groups are saved in the event server. This enables you to view and operate on JP1 events from business groups that you are not monitoring. Check and, if necessary, revise the forwarding settings for JP1 events before setting business groups.

- Use an authentication server whose JP1/Base version is 07-00 or later.

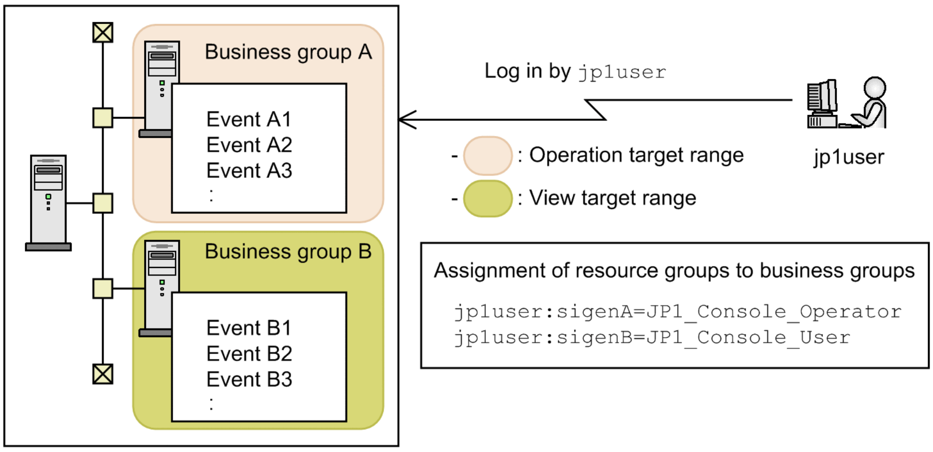
  When you enable restrictions on viewing and operating business groups, you cannot log in to JP1/IM - Manager if you use an authentication server whose JP1/Base version is earlier than 07-00.

For details about business groups, see *6.4 Managing business groups*.

(1) Settings when multiple business groups are assigned to a JP1 user

You can assign multiple JP1 resource groups that can be viewed and operated to a JP1 user. You can also assign different JP1 permission levels for the individual resource groups. This enables operation as shown in the following figure, where a user can operate on some of the displayed JP1 events and can view other displayed JP1 events.

Figure 3–9: Control of viewing and operating business groups by using combinations of JP1 resource groups and JP1 permission levels



Assignment of resource groups to business groups

```
jp1user:sigenA=JP1_Console_Operator
jp1user:sigenB=JP1_Console_User
```

Legend:

🟠 : The range of JP1 resource group `sigenA`

🟡 : The range of JP1 resource group `sigenB`

(2) Assigning a JP1 resource group and permission level to a JP1 user

If restrictions on viewing and operating business groups are enabled, operations allowed for a JP1 user depend on the combination of the JP1 resource group and JP1 permission level assigned to the user. Check and, if necessary, revise the assigned JP1 resource group and JP1 permission level of the user.

For details about operations allowed for each combination of JP1 resource group and JP1 permission level, see *E.1(2) Operating permissions required when restrictions on viewing and operating business groups are enabled*.

When restrictions on viewing and operating business groups are enabled, even JP1 users who are restricted from viewing and operating business groups can perform the following operations:

- Set the view filter
- Display the event list and event details
- Display event-information mapping
- Monitor repeated events

- Output a CSV file of the event list
- Display the severe event list
- Change the action status of JP1 events (when the Event Console window is used)
- Change settings of memo entries
- Search for events
- Display correlation events
- Execute commands, and display and click command buttons
- Display event guide information
- Start monitor windows and the Tool Launcher window
- Manually register incidents (JP1/Service Support)
- Link with BJEX and JP1/AS to list response-waiting events, enter responses to response-waiting events, release response-waiting events from the accumulate-and-hold state, and monitor the accumulation status

For details about JP1 permission levels when restrictions on viewing and operating business groups are disabled, see *E.1(1) Operating permissions required when restrictions on viewing and operating business groups are disabled*.

(3) How to specify business groups

When the conditions below are met, you can specify the path to a business group for an event condition or the name of the execution host (command execution target host). By doing so, you need only to change what hosts belong to a business group or monitoring group, and you do not need to change the definitions.

- The IM Configuration Management database is enabled.
- Business groups or monitoring groups are defined in the IM Configuration Management database.
- The integrated monitoring database is enabled.
- Restrictions on viewing and operating business groups are enabled.
- Mapping of the event source hosts is enabled.

When these conditions are not met, even if you specify a business group for an event condition or the name of the execution host (command execution target host), it is handled as a host name rather than as a business group.

The following table describes the correspondence between the attributes for which a business group can be specified as an event condition and the functions.

Table 3–3: Correspondence between the attributes for event conditions and the functions

Function	Attributes		
	Source host (`B.SOURCESERVER`)	Destination event server name (`B.DESTSERVER`)	Event source host name (`E.JP1_SOURCEHOST`)
Severe event definition	Y	N	Y
Event search	Y	N	Y
Filtering using the event acquisition filter (common exclusion-conditions in extended mode)	Y	N	Y
Filtering using the event receiver filter	Y	N	Y
Filtering using the view filter	Y	N	Y

Function	Attributes		
	Source host (B.SOURCESERVER)	Destination event server name (B.DESTSERVER)	Event source host name (E.JP1_SOURCEHOST)
Automated action	Y	N	Y
Correlation event generation	Y	Y	Y
Severity change	Y	Y	Y
Changing the message display format	Y	Y	Y
Filter file for output of an event report	Y	N	Y
Mapping of the event source host	Y	Y	N
Suppression of repeated-event monitoring	Y	N	Y

Legend:

Y: Can be specified.

N: Cannot be specified. (The attribute does not exist.)

When you specify a business group for an event condition, you can specify `IN` (match) or `NOTIN` (do not match) as the operator.

If a condition for specifying a business group in a path representation is satisfied or the operator is neither `IN` (match) nor `NOTIN` (do not match), the business group is handled as a host name even if the business group is specified for the event condition and the target (host targeted by the command).

Note that an event condition is determined to be not satisfied when no host exists in the specified business group.

You can specify the name of the execution host (command execution target host) when an automated action is executed, action results are displayed, a command button is defined, or a command is executed. The following shows example specifications of paths.

Example: When specifying a host in the business group `Personnel system` for an event condition:

```
/Personnel system
```

Example: When specifying the monitoring group `AP server` in the business group `Personnel system` for an event condition:

```
/Personnel system/AP server
```

After a business group or monitoring group is applied, the name of the business group or monitoring group specified in the definitions below in the Central Console is changed to the latest name. Note that, if a business group or monitoring group is deleted, the name (specified in the Central Console) of the business group or monitoring group changes to a double slash (`//`) and is invalidated.

- Severe event definition
- Event search conditions
- Event acquisition filter (common exclusion-conditions in extended mode)
- Event receiver filter
- View filter
- Correlation event generation definition
- Automatic action definition

- Conditions for updating list of action results
- Command button definition
- Severity change definition
- Display message change definition
- Event-source-host mapping definition
- Repeated event condition

3.2 Filtering of JP1 events

JP1/IM and JP1/Base filter JP1 events and process only the necessary events. For example, you can forward only the JP1 events necessary for management to the manager, or filter JP1 events to be displayed on the viewer.

JP1/IM and JP1/Base provide the following five types of filtering:

- Forwarding filter
- Event acquisition filter
- Event receiver filter
- Severe events filter
- View filter

By combining those filters, you can filter JP1 events and process only the necessary events. The position of the event acquisition filter (in the above five filters) differs depending on whether the integrated monitoring database is used.

Figure 3–10: Filters provided by JP1/IM and JP1/Base (when not using the integrated monitoring database)

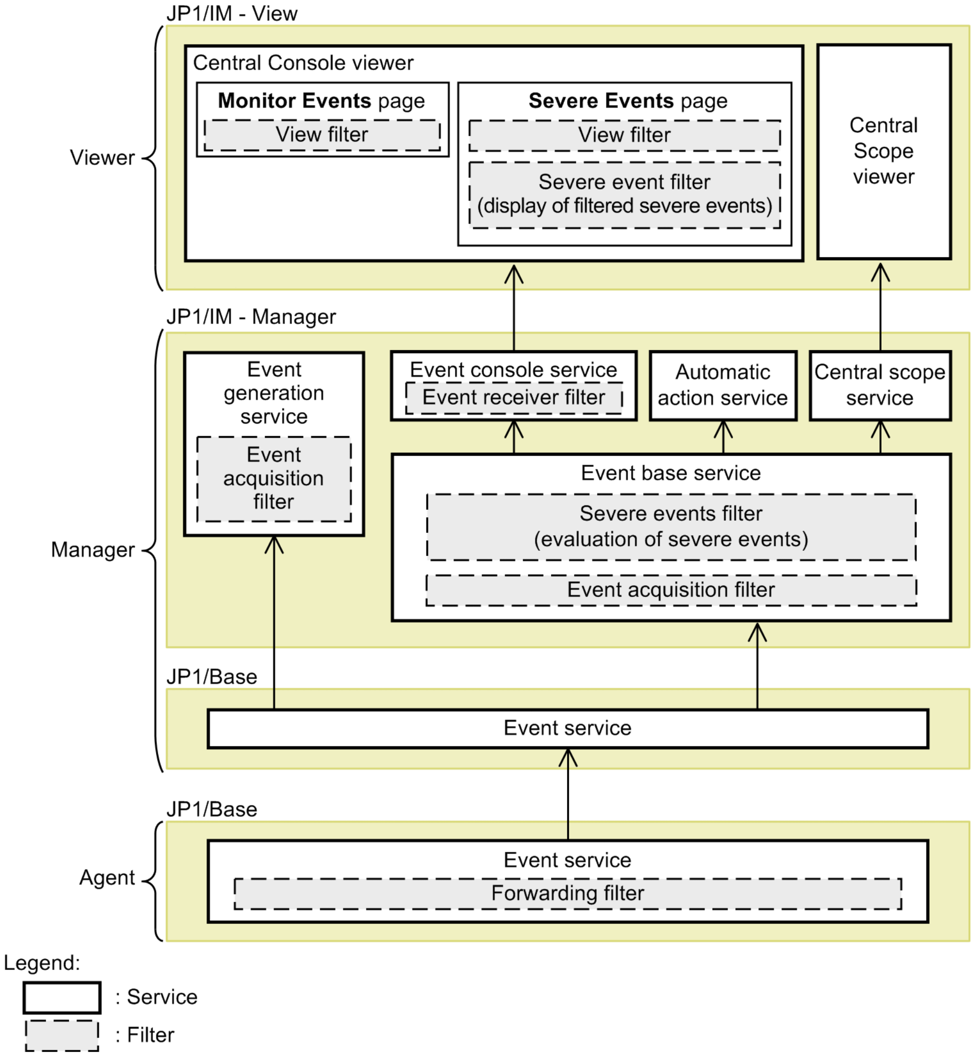
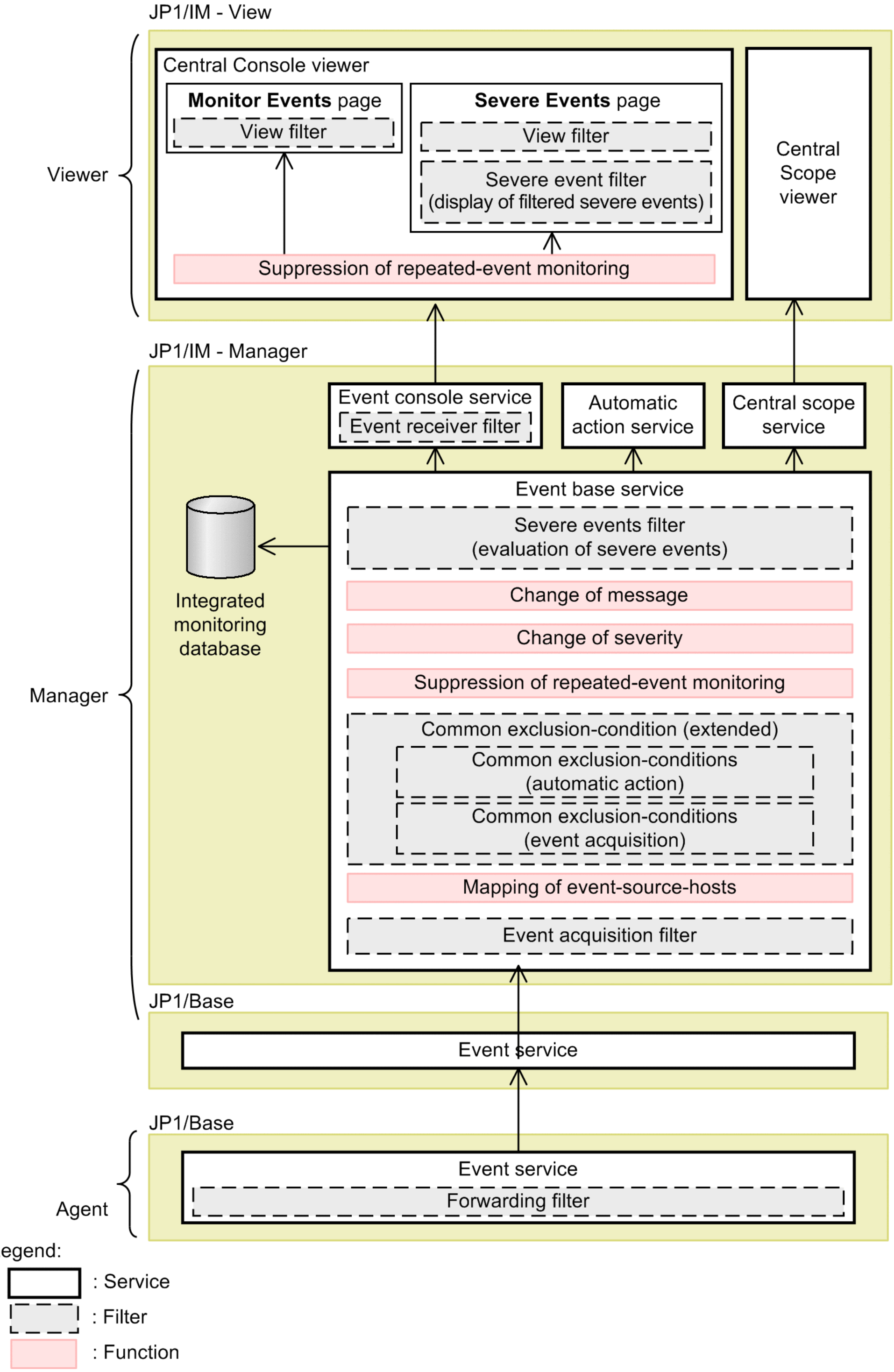


Figure 3–11: Filters provided by JP1/IM and JP1/Base (when using the integrated monitoring database)



The service components differ depending on whether the integrated monitoring database is used, but the processing of JP1/IM does not differ.

When the integrated monitoring database is used, JP1 events that passed through the event acquisition filter are stored into the integrated monitoring database.

The five filters are described next, in the order in which they are applied, starting from the issuing source.

3.2.1 Forwarding filter

The forwarding filter is used by JP1/Base to filter the JP1 events to be forwarded to another host.

JP1/IM performs centralized monitoring, where events generated on individual agents are issued as JP1 events and forwarded to the manager. Each agent filters the monitored JP1 events, and then forwards the filtered events to the higher manager. You can specify these target JP1 events in a forwarding filter. A forwarding filter can also be used to reduce JP1 event traffic when the load on a manager needs to be restricted or the network has limited capacity.

Forwarding filters are specific to each instance of JP1/Base. A forwarding settings file can be edited on each agent individually, or you can distribute forwarding setting information in a batch from a manager to the agents.

For details about the forwarding settings file, see the chapter where forwarding of JP1 events and definition files are described in the *JP1/Base User's Guide*.

3.2.2 Event acquisition filter

The event acquisition filter is used by (the event base service of) JP1/IM - Manager to filter JP1 events acquired from JP1/Base. You can set multiple conditions in the manager before using this filter and then switch and use one of the conditions.

For the event acquisition filter, define the conditions of JP1 events that need to be monitored by JP1/IM - Manager. Generally, the JP1 events indicating that severe events were generated within the monitoring system are the JP1 events that need to be monitored by JP1/IM - Manager. After the JP1 events pass through the event acquisition filter, they become the following JP1 events:

- JP1 events monitored on the **Monitor Events** page or **Severe Events** page of the Event Console window
- JP1 events that trigger automated actions
- JP1 events that change the status of a monitoring object
- JP1 events that issue a correlation event (correlation source events)

For example, if the manager of JP1/IM and a product that issues a large number of normal events are running on the same machine (such as when JP1/AJS issues events for successful execution of jobs), JP1 events required for system monitoring might be buried in those events. In such case, you can use the event acquisition filter to acquire only the JP1 events to be monitored, so that system monitoring will not be adversely affected.

Event acquisition filters reside in JP1/IM - Manager and can be set from JP1/IM - View. They affect all JP1/IM functions, including JP1 event monitoring, automated actions, and object status monitoring.

If the `LANG` environment variable set for JP1/IM - Manager and the `LANG` environment variable set for the JP1/Base event server are different, the event acquisition filter does not operate normally.

If the integrated monitoring database is used, JP1 events that pass through the event acquisition filter are saved.

Note

- To display events in JP1/SES format in JP1/IM - View, you must change the event acquisition filter settings to acquire JP1/SES events. The default settings do not display JP1/SES events.
- If you are not using the integrated monitoring database, the event acquisition filter also applies to the event generation service.

The event generation service is inactive by default. When it is started, however, the filter definitions in effect for the event base service are also applied to the event generation service.

If you are using the event acquisition filter (for compatibility), the event generation service operates without any filter conditions.

For details about the event generation service, see *3.3 Issue of correlation events*.

- Mapping of the event source hosts is available for JP1 events acquired from the event service. Therefore, for event acquisition filter conditions used when JP1 events are acquired, you cannot specify the event source hosts.

Setting multiple event acquisition filters

You can set multiple event acquisition filters.

For example, if you want to change the type of JP1 events collected or the host from which they are acquired according to the time of day (business hours or night time), you can set different event acquisition filters for the different times of day and switch between them.

Events issued when an event acquisition filter is switched

When you switch to a different event acquisition filter, JP1/IM - Manager issues JP1 events (event IDs 00003F13 and 00003F20) reporting the changed filter conditions. The messages give the name of the filter now in effect and the arrival time and serial number of the last event received by JP1/IM - Manager before the filter was switched.

These JP1 events (event IDs 00003F13 and 00003F20) report that the new event acquisition filter came into effect from the first event received by JP1/IM - Manager after the event corresponding to the arrival time and serial number given in the messages. That is, the filter change and JP1 event issue do not occur at the same time.

For example, if a large number of other JP1 events were issued at the time the filter was switched, there might be a delay before the JP1 events (event IDs 00003F13 and 00003F20) reporting the changed filter conditions appear in the Event Console window. This could mean that the first JP1 event acquired with the new filter appears before the JP1 events reporting the filter change.

To identify the first JP1 event acquired with the new event acquisition filter, check the messages (event IDs 00003F13 and 00003F20) to find the last JP1 event acquired before the change. (Subsequent JP1 events will have been acquired with the new event acquisition filter.)

For details about the JP1 events (event IDs 00003F13 and 00003F20), see *Chapter 3. JP1 Events* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*. Note that these JP1 events are not issued when the event acquisition filter is operating in compatibility mode.

3.2.3 Event receiver filter

The event receiver filter filters (or restricts) JP1 events that can be monitored by each JP1 user. Only one event receiver filter can be set for each JP1 user on one manager.

To monitor the system operation using JP1/IM, the user must log in to a manager from JP1/IM - View. Multiple JP1 users can separately monitor different monitoring ranges if each JP1 user's monitoring range is restricted. In this case, you can use the event receiver filter to filter the JP1 events displayed in the Event Console window for each JP1 user.

Event receiver filters reside in JP1/IM - Manager and can be set from JP1/IM - View. They affect the **Monitor Events** page, **Severe Events** page, and **Search Events** page of the Event Console window.

When restrictions on viewing and operating business groups are enabled, you can also use the event receiver filter to restrict the JP1 event range to be monitored by JP1 users.

For details about restrictions on viewing and operating business groups, see *3.1.4 Restrictions on viewing and operating business groups*.

3.2.4 Severe events filter

The severe events filter displays, on the **Severe Events** page, only the JP1 events that possibly need handling and highly affect the system (from among the JP1 events to be monitored by JP1/IM).

Only one such filter can be set on each manager. Because the filter settings are managed on the manager, the same severe events filter is applied to all viewers that connect to that manager.

Some JP1 events, such as emergency notices and error reports, require an immediate response from the operator. In JP1/IM, such JP1 events are known as *severe events*.

The **Severe Events** page of the Event Console window is specifically for managing severe events.

When a severe event occurs, the alarm lamp flashes in JP1/IM - View to notify the user. You can manage the response status of severe events on the **Severe Events** page.

Events whose event level is `Emergency`, `Alert`, `Critical`, or `Error` are defined as severe events in the default severe events filter.

By customizing the default filter, you can select the event levels you want to define as severe events. You can also exclude specific JP1 events that are normally classed as severe events by specifying the event ID or other attribute.

The severe events filter resides in JP1/IM - Manager and JP1/IM - View. JP1 events are judged by the severe events filter in JP1/IM - Manager, and the filtered JP1 events are displayed in JP1/IM - View. The server events filter can be set from JP1/IM - View. They affect the **Severe Events** page of the Event Console window.

3.2.5 View filter

A view filter is used to temporarily display only specific JP1 events among those to be displayed on the **Monitor Events** or **Severe Events** page of the Event Console window. Multiple view filters can be defined for a specific monitoring user of a viewer, and users can switch view filters by easy operation.

View filters reside in, and can be set from, JP1/IM - View. Event filters affect the **Monitor Events** and **Severe Events** pages of the Event Console window.

The view filter conditions are saved in JP1/IM - Manager for each user and for each of the following JP1/IM - View versions:

- The view filter set in JP1/IM - View 07-00
- The view filter set in JP1/IM - View 07-10 to 07-51
- The view filter set in JP1/IM - View 08-00 to 08-10
- The view filter set in JP1/IM - View 08-50
- The view filter set in JP1/IM - View 09-00 to 09-10
- The view filter set in JP1/IM - View 09-50 to 10-50
- The view filter set in JP1/IM - View 11-00 or later

If the manager does not have the view filter whose version corresponds to the connected JP1/IM - View, the conditions of the view filter one version earlier than the version of the connected JP1/IM - View are acquired.

3.2.6 Defining filter conditions

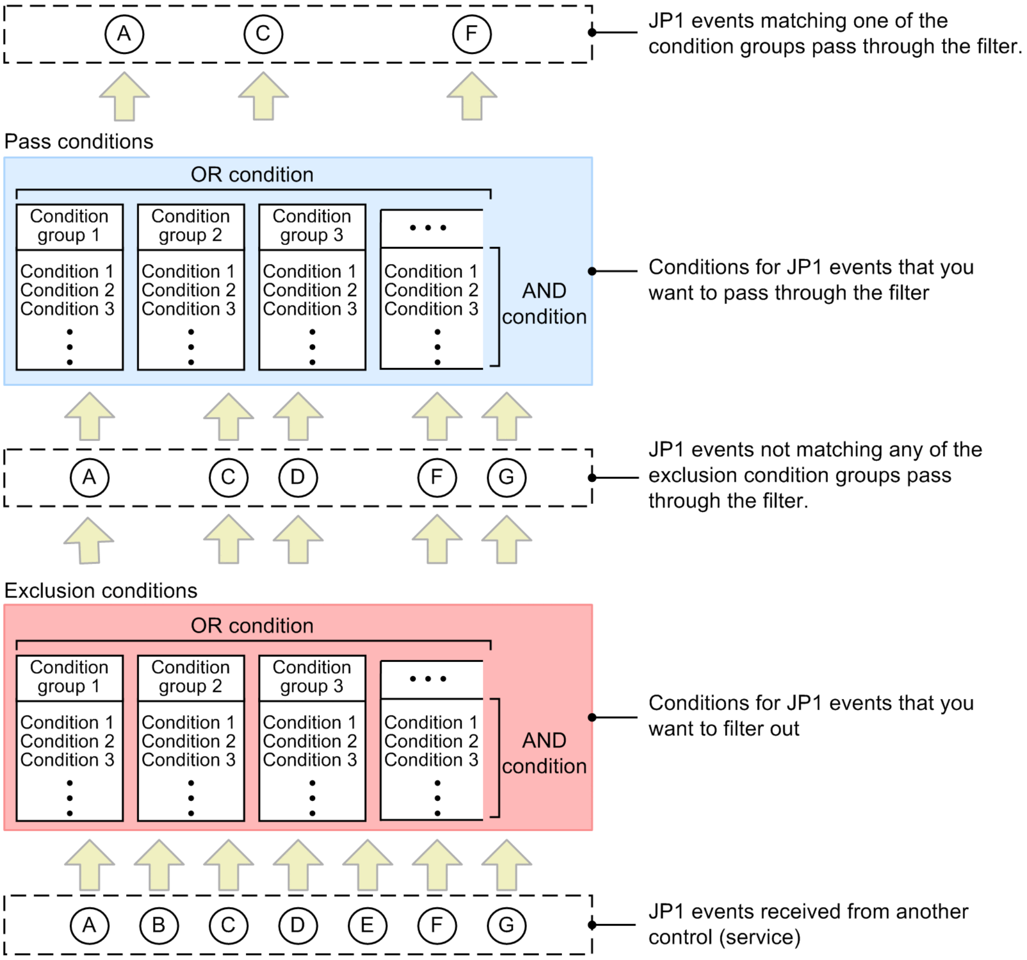
The conditions of the event acquisition filter, event receiver filter, severe events filter, view filter, and the filter that can be defined for event search can be either exclusion-conditions or pass conditions. *Exclusion-conditions* are a set of conditions for JP1 events that you do not want to display (acquire). *Pass conditions* are a set of conditions for JP1 events that you do want to display (acquire). As a separate class of conditions, there are also *common exclusion-conditions*, which allow you to disable or apply a condition group in an event acquisition filter. Filter conditions apply in the following order of precedence: common exclusion-conditions, exclusion-conditions, and pass conditions.

You can define a combination of common exclusion-conditions, exclusion-conditions, or pass conditions in a *condition group*. A condition group contains one or more conditions, and is satisfied when all the defined conditions are satisfied. That is, the conditions in a filter are related by an AND condition.

When a filter consists of exclusion-conditions and pass conditions, combined into multiple condition groups of either type, those JP1 events matching the conditions in one of the exclusion-condition groups are filtered out, and those JP1 events matching the conditions in one of the pass condition groups pass through the filter and are transferred to the higher-level control (see *Figure 3-10 Filters provided by JP1/IM and JP1/Base (when not using the integrated monitoring database)* and *Figure 3-11 Filters provided by JP1/IM and JP1/Base (when using the integrated monitoring database)*). That is, the condition groups of exclusion-conditions or pass conditions are related by an OR condition.

The following figure shows how a filter works.

Figure 3–12: Event transfer through a filter to higher-level control


A
C
F
JP1 events matching one of the condition groups pass through the filter.
Pass conditions
OR condition
Condition group 1
Condition group 2
Condition group 3
• • •
Condition 1
Condition 2
Condition 3
AND condition
Conditions for JP1 events that you want to pass through the filter
A
C
D
F
G
JP1 events not matching any of the exclusion condition groups pass through the filter.
Exclusion conditions
OR condition
Condition group 1
Condition group 2
Condition group 3
• • •
Condition 1
Condition 2
Condition 3
AND condition
Conditions for JP1 events that you want to filter out
A
B
C
D
E
F
G
JP1 events received from another control (service)

Except for the JP1/Base forwarding filter, you define filter conditions in JP1/IM - View.

For details about common exclusion-conditions, see *3.2.7 Common exclusion-conditions*.

(1) Exclusion-conditions

Exclusion-conditions filter out events. JP1 events that match any one of the defined condition groups do not pass through the filter. Exclusion-conditions take precedence over pass conditions. To define exclusion-conditions, JP1/Base version 09-00 or later is required on the JP1/IM - Manager host.

You can define exclusion-conditions in an event acquisition filter, event receiver filter, severe events filter, view filter, and in event searches.

(2) Pass conditions

Pass conditions display (acquire) events. JP1 events that match any one of the defined condition groups pass through the filter.

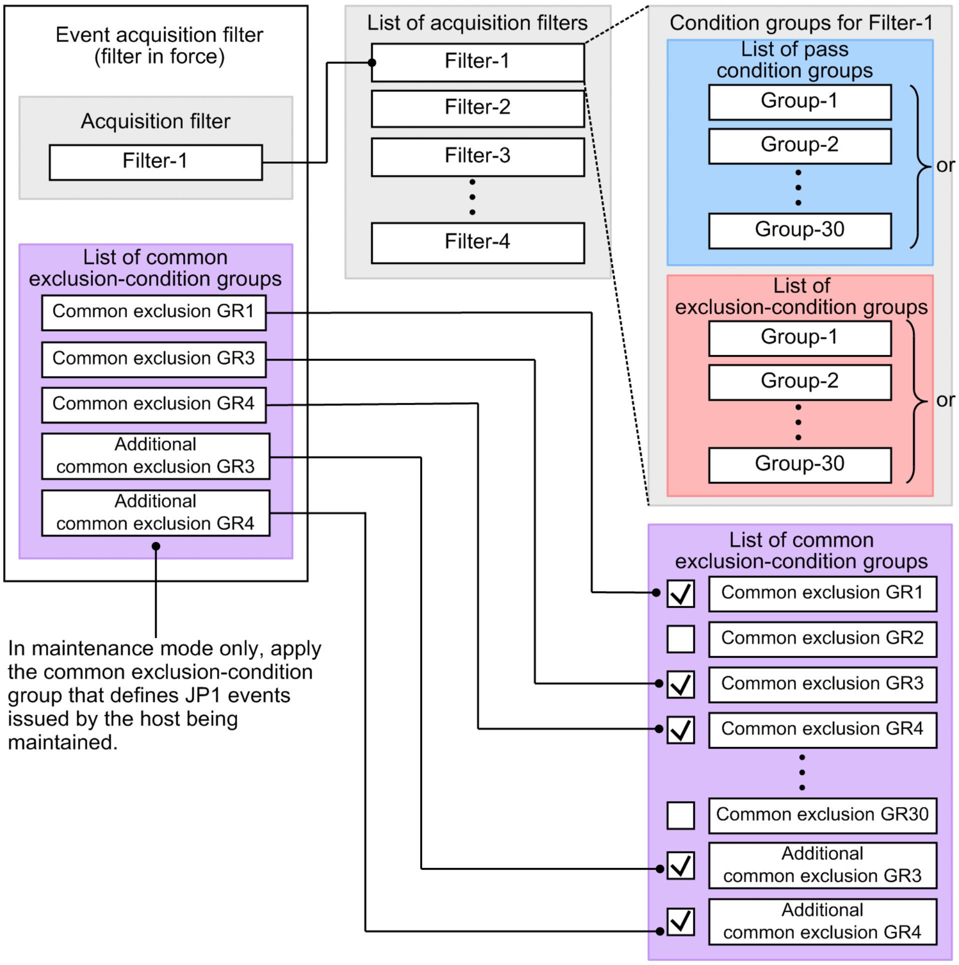
You can define pass conditions in an event acquisition filter, event receiver filter, severe events filter, view filter, and in event searches.

3.2.7 Common exclusion-conditions

Common exclusion-conditions form part of an event acquisition filter and consist of a group of conditions for filtering out JP1 events or excluding JP1 events from automated-action execution. You can apply or disable each group. In maintenance mode, for example, you can set a common exclusion-condition group to temporarily prevent JP1 events from being collected or exclude them from automated-action execution when the events are issued by the host you are working on, without having to change the pass conditions or exclusion-conditions in the event acquisition filter. If you have defined multiple event acquisition filters, and switch among them as required, the common exclusion-conditions you set apply to whichever filter is in force.

Of the conditions defined in an event acquisition filter, common exclusion-conditions take precedence over exclusion-conditions, which take precedence over pass conditions. The following figure shows the relationships among the common exclusion-conditions, exclusion-conditions, and pass conditions in event acquisition filters.

Figure 3–13: Relationships among the filter conditions in event acquisition filters


Event acquisition filter (filter in force)
Acquisition filter
Filter-1
List of common exclusion-condition groups
Common exclusion GR1
Common exclusion GR3
Common exclusion GR4
Additional common exclusion GR3
Additional common exclusion GR4
In maintenance mode only, apply the common exclusion-condition group that defines JP1 events issued by the host being maintained.
List of acquisition filters
Filter-1
Filter-2
Filter-3
Filter-4
Condition groups for Filter-1
List of pass condition groups
Group-1
Group-2
Group-30
or
List of exclusion-condition groups
Group-1
Group-2
Group-30
or
List of common exclusion-condition groups
☑ Common exclusion GR1
□ Common exclusion GR2
☑ Common exclusion GR3
☑ Common exclusion GR4
□ Common exclusion GR30
☑ Additional common exclusion GR3
☑ Additional common exclusion GR4

There are two types of operation modes for common exclusion-conditions: basic mode and extended mode. You can execute the `jcochcefmode` command to switch between basic mode and extended mode. In extended mode, you can filter events by **Registered time**, **Arrived time**, **Start time**, **End time**, **Event source host name**, and other items. You can also filter the event conditions by specifying the date and time, or execute the `jcochfilter` command to switch whether to enable or disable each group of conditions. However, for regular expressions, you can use only the extended regular expressions. After you switch to extended mode, you can return to basic mode. For details about basic mode and extended mode, see *3.2.7(1) Difference between basic mode and extended mode of common exclusion-conditions*. This manual describes information common to basic mode and extended mode if not otherwise specified.

For details about how to define common exclusion-conditions and how to switch the operation modes, see *4.2.4(3) Setting common exclusion-conditions* in the *JP1/Integrated Management - Manager Configuration Guide*.

You can specify an appropriate target on a common exclusion-condition, depending on whether to prevent JP1 events from being collected or exclude JP1 events from automated-action execution. For details, see *3.2.7(2) Exclusion target of a common exclusion-condition*.

You can also use additional common exclusion-conditions. You can define additional common exclusion-conditions by using monitored JP1 events while the system is operating. You can use additional common exclusion-conditions only when common exclusion-conditions are in extended mode. For details about additional common exclusion-conditions, see *3.2.7(3) Additional common exclusion-conditions*.

The following shows the difference between common exclusion-conditions and additional common exclusion-conditions:

- Common exclusion-conditions
  Used to exclude pre-defined JP1 events when the system is configured so that they cannot be collected or included in automated-action execution.
- Additional common exclusion-conditions
  Used to exclude JP1 events that are determined to be unnecessary during monitoring when the system is operating so that they cannot be collected or included in automated-action execution. If an additional common exclusion-condition is determined to be a necessary exclusion-condition when the system is operating, the system administrator can change the additional common exclusion-condition to a common exclusion-condition.

For smoother operations, you can use common exclusion-conditions and additional common exclusion-conditions as follows as the situation demands:

- When the system is configured
  Use the Common Exclusion-Conditions Settings window or execute the `jcochfilter` command with the `-ef` option specified to define the JP1 events not to be monitored by the system. These are the common exclusion-conditions defined in advance.
- When the system is operating
  In the event list in the Event Console window, select the JP1 events that are determined to be unnecessary during monitoring and define them as additional common exclusion-conditions.
- When the system is reconfigured
  Use the Event Acquisition Conditions List window to edit or delete the additional common exclusion-conditions accumulated during system operation. You can also change a JP1 event that is not monitored by the system or included in automated-action execution from an additional common exclusion-condition to a common exclusion-condition.

(1) Difference between basic mode and extended mode of common exclusion-conditions

The following table compares what you can do when common exclusion-conditions are switched into extended mode with what you can do when common exclusion-conditions are in basic mode. Common exclusion-conditions operate in basic mode by default and after JP1/IM - Manager is installed.

Table 3–4: Comparison between what you can do with basic mode and extended mode of common exclusion-conditions

What you can do with common exclusion-conditions	Basic mode	Extended mode
Filter events by **Registered time** and **Arrived time**	N	Y
Filter events by **Start time** and **End time**	N	Y
Filter events by **Event source host name**	N	Y
Filter events by **Extended attribute**	Y	Y
Compare events by using JP1-specific regular expressions or basic regular expressions	Y	N
Compare events by using extended regular expressions	Y	Y
Define a group of conditions for each agent host	N	Y
Set whether to activate or deactivate common exclusion-conditions for each group of common exclusion-conditions	Y	Y
Add a group of common exclusion-conditions you want to activate or deactivate	N	Y
Specify a period of time for which a group of conditions is applied	N	Y
Write comments	N	Y
Set additional common exclusion-conditions based on the JP1 events occurring while the system is operating	N	Y
Exclude a JP1 event that satisfies a condition	Y	Y
In the JP1 events that was collected, exclude a JP1 event that satisfies a condition from automated-action execution	N	Y

Legend:

Y: Available

N: Not available

The following table describes the difference between basic mode and extended mode of common exclusion-conditions.

Table 3–5: Difference between basic mode and extended mode of common exclusion-conditions

Item	Basic mode	Extended mode
Attributes of event conditions	Basic attributes: • Event ID (`B.ID`) • Source host (`B.SOURCESERVER`) • Message (`B.MESSAGE`)	Basic attributes: • Event ID (`B.ID`) • Registered reason (`B.REASON`) • Source process ID (`B.PROCESSID`) • Registered time (`B.TIME`) • Arrived time (`B.ARRIVEDTIME`) • Source user ID(`B.USERID`) • Source group (`B.GROUPID`) • Source user name (`B.USERNAME`) • Source group name (`B.GROUPNAME`) • Source host (`B.SOURCESERVER`) • Source IP address (`B.SOURCEIPADDR`) • Message (`B.MESSAGE`)
	Common extended attributes: • Event level (`E.SEVERITY`) • User name (`E.USER_NAME`)	Common extended attributes: • Event level (`E.SEVERITY`) • User name (`E.USER_NAME`)

Item	Basic mode	Extended mode
	- Product name (`E.PRODUCT_NAME`) - Object type (`E.OBJECT_TYPE`) - Object name (`E.OBJECT_NAME`) - Root object type (`E.ROOT_OBJECT_TYPE`) - Root object name (`E.ROOT_OBJECT_NAME`) - Occurrence (`E.OCCURRENCE`)	- Product name (`E.PRODUCT_NAME`) - Object type (`E.OBJECT_TYPE`) - Object name (`E.OBJECT_NAME`) - Root object type (`E.ROOT_OBJECT_TYPE`) - Root object name (`E.ROOT_OBJECT_NAME`) - Object ID (`E.OBJECT_ID`) - Occurrence (`E.OCCURRENCE`) - Start time (`E.START_TIME`) - End time (`E.END_TIME`) - Result code (`E.RESULT_CODE`) - Event source host name (`E.JP1_SOURCEHOST`)
	Extended attribute Can be defined.	Extended attribute Can be defined.
Comparison types of event conditions#	- Match - Does not match - First characters - Is contained - Is not contained - Regular expression	- Match - Does not match - First characters - Is contained - Is not contained - Regular expression - Time
Regular expressions	- JP1-specific regular expressions - Basic regular expressions - Extended regular expressions	Extended regular expressions
Maximum number of common exclusion-conditions groups that can be defined	30 groups (filter length: 64 kilobytes or shorter)	2,500 groups (Filter length: 15 megabytes or shorter)
Contents of definition	- Common exclusion-conditions group ID - Common exclusion-conditions group name - Event conditions	- Common exclusion-conditions group ID - Common exclusion-conditions group name - Event conditions - Comment - Conditions Apply Period - Target for exclusion
Method of activating or deactivating common exclusion-conditions	- System Environment Settings window - `-e` option in the `jcochfilter` command	- System Environment Settings window - `-e`, `-on`, and `-off` options in the `jcochfilter` command
Applicable period	--	On the **Conditions Apply Period** page in the Common Exclusion-Condition Settings (Extended) window, you can set the applicable period.
Setting method	Common Exclusion-Conditions Settings window	- Common Exclusion-Condition-Settings (Extended) window - Common exclusion-conditions extended definition file and the `-ef` option in the `jcochfilter` command

Legend:

--: Not applicable.

#: Comparison types of event conditions differ depending on the selected attribute. For details, see the following:

- For basic mode:

2.15 Common Exclusion-Conditions Settings window in the manual *JP1/Integrated Management - Manager GUI Reference*.

- For extended mode:

  2.16 Common Exclusion-Condition Settings (Extended) window in the manual *JP1/Integrated Management - Manager GUI Reference*.

(2) Exclusion target of a common exclusion-condition

You can select an exclusion target of a common exclusion-condition from the following two options:

- Preventing a JP1 event from being collected when the event satisfies the common exclusion-condition

  This option is used to exclude a specified JP1 event from monitoring by preventing the event from being collected. This option is available in basic mode and extended mode. During maintenance work, for example, if you want to prevent JP1 events from being collected only when the events are issued from a host undergoing maintenance, you can just select this option, rather than changing existing event acquisition filter definitions.
- Excluding a collected JP1 event from automated-action execution when the event satisfies the common exclusion-condition

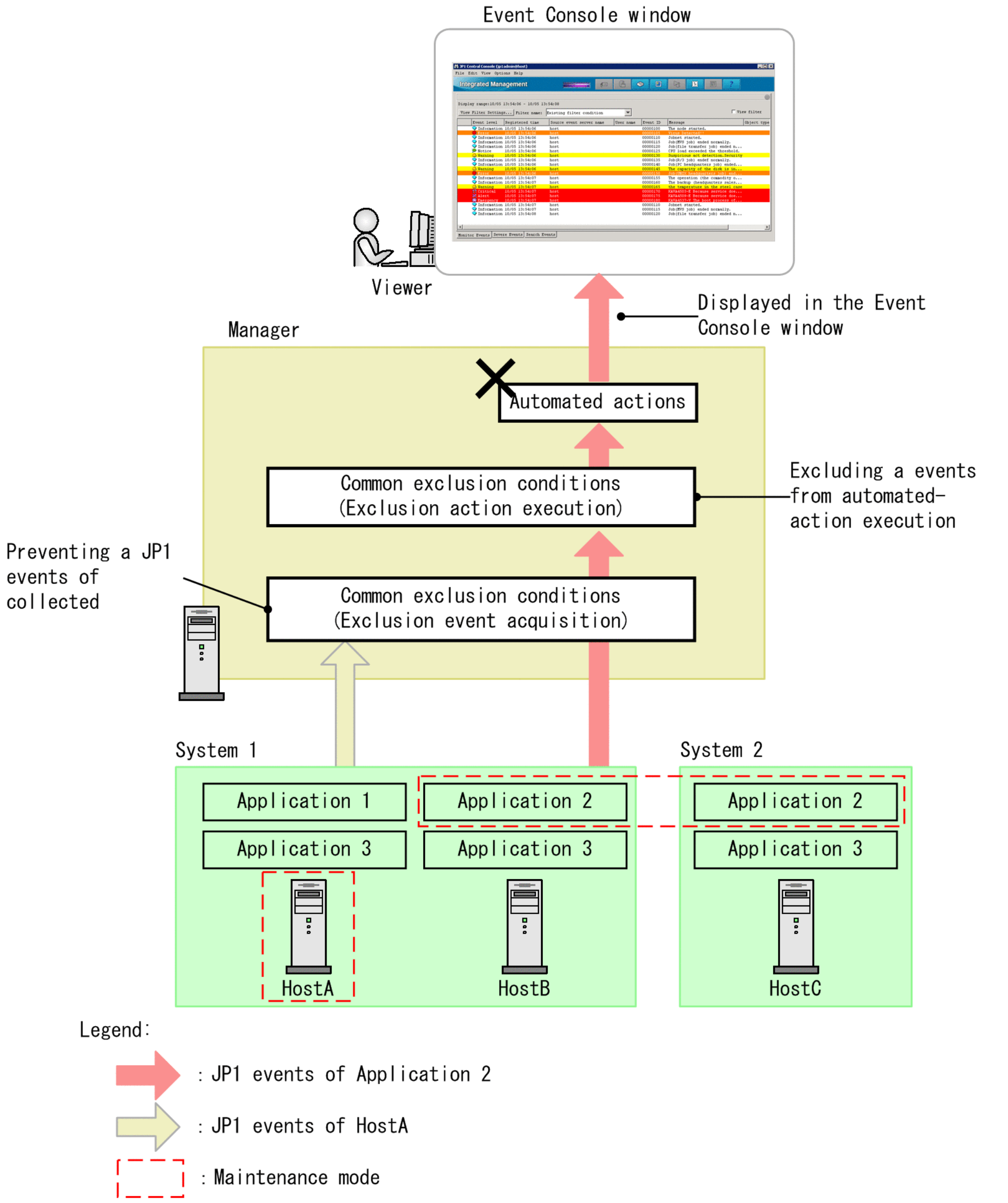
  This option is used to collect JP1 events but exclude a specified JP1 event from automated-action execution. This option is available only in extended mode. During maintenance work, for example, if you want to exclude JP1 events from automated-action execution only when the events are issued from a host undergoing maintenance, you can just select this option, rather than changing existing automated action definitions.

The following figure shows an overview of common exclusion-conditions.

Figure 3–14: Overview of common exclusion-conditions

Common exclusion-conditions

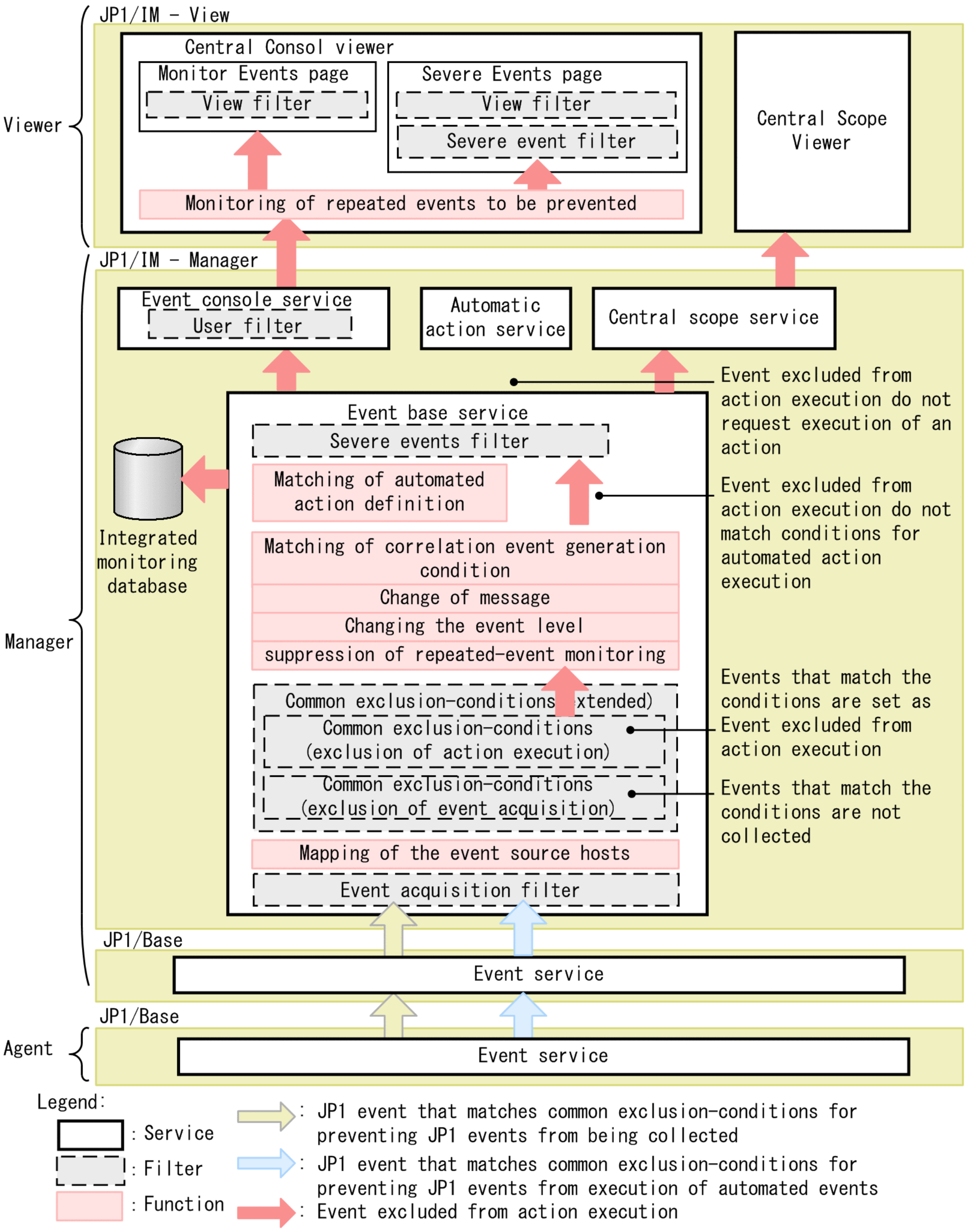
Apply	Maintenance mode	Event conditions	Exclusion target
	System 1	Business group name= System 1	Preventing JP1 events
Y	Application 2	Product name=Application 2	Excluding a collected event from action execution
Y	HostA	Event source host name=HostA	Preventing JP1 events


Event Console window
Viewer
Displayed in the Event Console window
Manager
Automated actions
Common exclusion conditions (Exclusion action execution)
Excluding a events from automated-action execution
Preventing a JP1 events of collected
Common exclusion conditions (Exclusion event acquisition)
System 1
System 2
Application 1
Application 2
Application 3
Application 3
Application 2
Application 3
HostA
HostB
HostC
Legend:
: JP1 events of Application 2
: JP1 events of HostA
: Maintenance mode

JP1 events issued from HostA undergoing maintenance are excluded from monitoring by a common exclusion-condition that prevents the events from being collected. JP1 events issued from Application 2 undergoing maintenance are excluded from automated-action execution by a common exclusion-condition that prevents the events from being included in automated-action execution.

The following figure shows service components for common exclusion-conditions.

Figure 3–15: Service components for common exclusion-conditions



JP1/IM - View
Viewer
Central Consol viewer
Monitor Events page
View filter
Severe Events page
View filter
Severe event filter
Monitoring of repeated events to be prevented
Central Scope Viewer
JP1/IM - Manager
Event console service
User filter
Automatic action service
Central scope service
Event excluded from action execution do not request execution of an action
Event base service
Severe events filter
Matching of automated action definition
Event excluded from action execution do not match conditions for automated action execution
Integrated monitoring database
Matching of correlation event generation condition
Change of message
Changing the event level
suppression of repeated-event monitoring
Manager
Common exclusion-conditions (extended)
Common exclusion-conditions (exclusion of action execution)
Common exclusion-conditions (exclusion of event acquisition)
Events that match the conditions are set as Event excluded from action execution
Events that match the conditions are not collected
Mapping of the event source hosts
Event acquisition filter
JP1/Base
Event service
JP1/Base
Agent
Event service
Legend:
: Service
: Filter
: Function
: JP1 event that matches common exclusion-conditions for preventing JP1 events from being collected
: JP1 event that matches common exclusion-conditions for preventing JP1 events from execution of automated events
: Event excluded from action execution

An event that satisfies a common exclusion-condition that prevents JP1 events from being included in automated-action execution is called an action-excluded event.

The event conditions of common exclusion-condition that prevents JP1 events from being included in automated-action execution are defined independently from the execution conditions of automated action definitions. That is, you can use a single common exclusion-condition to collectively exclude multiple JP1 events from automated-action execution even when the events match different automated action definitions.

Common exclusion-condition that prevents JP1 events from being included in automated-action execution take precedence over whether automated action definitions are enabled or disabled.

Setting a common exclusion-condition that prevents JP1 events from being included in automated-action execution does not affect existing action definitions. When a common exclusion-condition is set and, as a result, no action in an action definition will not be executed, the status (enabled or disabled) of the action definition remains the same. That is, an action with AND-joined conditions and the status of the automated action function are as follows:

- Action with AND-joined conditions

  When a common exclusion-condition is set to exclude a JP1 event from automated-action execution and, as a result, an AND-joined condition is not satisfied, the action is not executed. The action definition including the unsatisfied AND-joined condition remains enabled. The action is not executed even when other AND-joined conditions are satisfied.
- Status of the automated action function

  The status of the automated action function does not change to standby as long as there is an enabled action definition. This is true if no action in the action definition will be executed due to a common exclusion-condition is set to exclude a JP1 event from automated-action execution.

When the integrated monitoring database is used, the event attributes (program-specific extended attributes) listed below are added to an action-excluded event. The attributes can be used as program-specific extended attributes in functions except for the event-source-host mapping function.

- Common exclude conditions group ID (`E.JP1_IMCOMEXCLUDE_ID`)
- Common exclude conditions group name (`E.JP1_IMCOMEXCLUDE_NAME`)
- Common exclude conditions group target-for-exclusion (`E.JP1_IMCOMEXCLUDE_TARGET`)

(3) Additional common exclusion-conditions

The additional common exclusion-conditions are used by defining the monitored JP1 events during system operations. Selecting a JP1 event in the Event Console window or Related Events window sets an additional common exclusion-condition.

To use the additional common exclusion-conditions, you must have the `JP1_Console_Admin` permission. Also, you must switch the common exclusion-conditions into extended mode. You can define the additional common exclusion-conditions for the following JP1 events:

- JP1 events registered in the event database of a manager host to which JP1 JP1/IM - View logged in, or in the integrated monitoring database
- JP1 events registered in the event database of agent hosts

You can set the additional common exclusion-conditions in the Common Exclusion-Condition Settings (Extended) window, which can be displayed as follows:

- In the Event Console window, select a JP1 event, and select **View**>**Exclude by Common Exclusion-Conditions**.
- In the Event Console window, select a JP1 event, and from the pop-up menu displayed by right-clicking, select **Exclude by Common Exclusion-Conditions**.
- In the Related Events window, select a JP1 event, and from the pop-up menu displayed by right-clicking, select **Exclude by Common Exclusion-Conditions**.

The attribute name and value of the selected JP1 event are displayed and are automatically input as event conditions. The common exclusion-conditions group name and comments are also input and automatically displayed. For details about this window, see *2.16 Common Exclusion-Condition Settings (Extended) window* in the manual *JP1/Integrated Management - Manager GUI Reference*. Note that the window cannot be displayed when you are using the Web page version of JP1/IM - View. For details about the event attribute names that can be specified for event conditions, see *Common-exclusion-conditions display item definition file (common_exclude_filter_attr_list.conf)* in *Chapter 2. Definition Files* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

The defined additional common exclusion-conditions can be edited, deleted, or changed into common exclusion-conditions in the Event Acquisition Conditions List window.

For details about this window, see *2.14 Event Acquisition Conditions List window* in the manual *JP1/Integrated Management - Manager GUI Reference*.

For details about how to set additional common exclusion-conditions, see *5.5.4 Setting an additional common exclusion-condition to exclude a JP1 event from the monitoring target or action execution* in the *JP1/Integrated Management - Manager Administration Guide*.

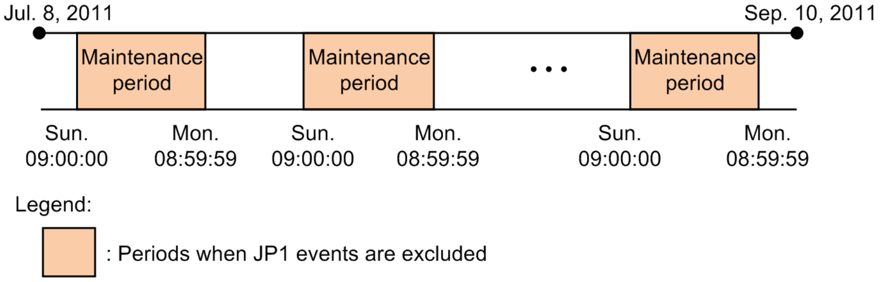
(4) Applicable period of a common exclusion-condition

By changing the mode of common exclusion-conditions of the event acquisition filter to extended mode, you can specify an applicable period of a condition for preventing JP1 events from being collected or excluding them from automated-action execution. During the applicable period, the common exclusion-condition in extended mode can prevent JP1 events from being collected or exclude them from automated-action execution only when the events occur during the applicable period.

For example, when the maintenance time for a monitored host is fixed to a certain time, you can specify the applicable period to prevent JP1 events that would occur on the host during the maintenance conducted at certain date and time or at a certain day of the week from being collected or exclude such events from automated-action execution, or to disable conditions groups by restricting the period.

The following example applies common exclusion-conditions in extended mode from 9:00 on Sunday to 9:00 on the next Monday during July 8 in 2011 to September 10 in 2011, according to the maintenance schedule for the monitored host. Note that the applicable period includes the start time, but not the end time. In this example, the applicable period is every week from 09:00:00 on Sunday to 08:59:59 on the following Monday.

Figure 3–16: Applicable period of a common exclusion-condition



The time is set according to the time zone designed for the machine on which JP1/IM - Manager is running.

Thus, specifying the applicable period might enable JP1 event filtering without the need of changing conditions groups, or activating or deactivating the common exclusion-conditions. JP1 events that occurred during the applicable period is determined by comparing the **Arrived time** (`B.ARRIVEDTIME`) of the JP1 event. Note that you can specify the applicable period for each conditions group. To use the applicable period, common exclusion-conditions groups must be enabled.

You can specify the applicable period on the **Conditions Apply Period** page in the Common Exclusion-Condition Settings (Extended) window. For details about the Common Exclusion-Condition Settings (Extended) window, see *2.16 Common Exclusion-Condition Settings (Extended) window* in the manual *JP1/Integrated Management - Manager GUI Reference*.

(5) Information included in a common exclusion history file

JP1/IM - Manager logs the history of the following processes into a common exclusion history file:

- A JP1 event arrives at JP1/IM - Manager but the event is not collected.
- A collected JP1 event is excluded from automated-action execution.
- A common exclusion-conditions definition is applied or changed.

A common exclusion history file is named as follows:

`comexclude`*n*#`.log`

# *n is an integer from* 1 to 5.

Common exclusion history files are stored in the following locations:

In Windows:

Physical hosts:

console-path`\operation\comexclude`

Logical hosts:

shared-folder`\operation\comexclude`

In UNIX:

Physical hosts:

`/var/opt/jp1cons/operation/comexclude`

Logical hosts:

shared-directory`/operation/comexclude`

A common exclusion history file is created if it does not exist in the location at any of the times listed below. This is based on the assumption that the operation mode of common exclusion-conditions is set to extended mode.

- When JP1/IM - Manager starts
- When JP1/IM - Manager is running and JP1/IM - Manager receives a JP1 event that satisfies a common exclusion-condition
- When JP1/IM - Manager is running and a common exclusion-conditions definition is applied to JP1/IM - Manager
- When JP1/IM - Manager is running and a common exclusion-conditions definition is enabled or disabled

A log entry in a common exclusion history file is generated in the following format:

serial-number process-time process-description

The *serial-number* is a serial number in the common exclusion history. The serial number can be from `00000001` to `99999999`. When the number reaches `99999999`, it is reset to `00000001`. The serial number is also reset to `00000001` when JP1/IM - Manager restarts. The *process-time* is written in the following format: *YYYY*`/`*MM*`/`*DD hh*`:`*mm*`:`*ss*`.`*SSS* (where *YYYY* is the year, *MM* month, *DD* day, *hh* hour, *mm* minute, and *ss*`.`*SSS* second).

The following table describes what information is included in the *process-description*.

Table 3–6: Processes to be logged in the common exclusion history file

No.	Common exclusion process to be logged	Information included in the process description
1	Exclusion is made according to common exclusion-conditions.	The ID and name of the common exclusion-conditions group that caused the exclusion, and the information of the excluded event are logged.

No.	Common exclusion process to be logged	Information included in the process description
		• When an event is excluded from the target to be collected: `Exclude the event from acquiring.` (`event[SEQNO=` *event-database-serial-number-of-the-excluded-JP1-event* `ID=` *event-ID* `SOURCESERVER=` *event-source-server-name* `ARRIVEDTIME=` *arrival-time* `SEVERITY=` *severity*`] common exclusion-conditions[ID=` *common-exclusion-conditions-group-ID* `NAME=` *common-exclusion-conditions-group-name*`]`) (line break) • When a collected event is excluded from action execution: `Exclude the acquired event from action-executing.` (`event[SEQNO=` *event-database-serial-number-of-the-excluded-JP1-event* `ID=` *event-ID* `SOURCESERVER=` *event-source-server-name* `ARRIVEDTIME=` *arrival-time* `SEVERITY=` *severity*`] common exclusion-conditions[ID=` *common-exclusion-conditions-group-ID* `NAME=` *common-exclusion-conditions-group-name*`]`) (line break) The placeholders indicate the following: *event-database-serial-number-of-the-excluded-JP1-event* Indicates the event database serial numbers. Format: 0 to 2,147,483,647 *event-ID* Indicates the event ID (`B.ID` or `B.IDBASE`). Format: *basic-information*`[:`*extended-information*`]` *event-source-server-name* Indicates the source server of the event (`B.SOURCESERVER`) *arrival-time* Indicates the arrival time (`B.ARRIVEDTIME`). Format: *yyyy*`/`*MM*`/`*dd_hh:mm:ss* *severity* Indicates the severity (`E.SEVERITY`). *common-exclusion-conditions-group-ID* Indicates the ID of the common exclusion conditions group that caused the exclusion. For common exclusion-condition: 0 to 2499 For additional common exclusion-condition: A0 to A2499 *common-exclusion-conditions-group-name* Indicates the condition name of the common exclusion conditions group that caused the exclusion.
2	A common exclusion-conditions definition is updated.#	A message is logged indicating that a common exclusion-conditions definition is updated. `The common exclusion-conditions extended definition was updated.` (line break) `The additional common exclusion-conditions definition was updated.` (line break)

#: An update is triggered by the following actions:

- Start JP1/IM - Manager.
- Update by using the **Exclude by Common Exclusion-Conditions** menu in the System Environment Settings window in JP1/IM - View.
- Update by using the `jcochfilter -ef` command.
- Enable a common exclusion-condition (with the `-e` or `-on` option of the `jcochfilter` command)
- Disable a common exclusion-condition (with the `-e` or `-off` option of the `jcochfilter` command)

The details of an update are logged in the common exclusion-conditions definition history file.

The following is an example of a common exclusion history file:

```
00000001 2017/04/01 12:30:25.131 The common exclusion-conditions extended
definition was updated.
00000002 2017/04/01 12:30:25.229 The additional common exclusion-conditions
definition was updated.
00000003 2017/04/01 12:35:04.100 Exclude the event from acquiring.
(event[SEQNO=10001 ID=4704 SOURCESERVER=hostA
ARRIVEDTIME=2017/04/01_12:35:05 SEVERITY=Emergency] common exclusion-
conditions[ID=1 NAME= hostA maintenance])
00000004 2017/04/01 12:35:35.342 Exclude the acquired event from action-
executing. (event[SEQNO=10005 ID=4201 SOURCESERVER=hostB
ARRIVEDTIME=2017/04/01_12:35:36 SEVERITY=Alert] common exclusion-
conditions[ID=A2 NAME= hostB maintenance])
```

(6) Information included in a common exclusion-conditions definition history file

JP1/IM - Manager logs the definition history of common exclusion-conditions into a common exclusion-conditions definition history file. This file helps you check the detailed definition of a certain common exclusion-conditions group, for example, whose ID or name is found in a common exclusion history file containing the history of exclusion processes.

A common exclusion-conditions definition history file is named as follows:

`comexcludeDefn#.log`

#: *n* is an integer 1 or 5.

Common exclusion-conditions definition history files are stored in the following locations:

In Windows:

Physical hosts:

console-path`\operation\comexclude`

Logical hosts:

shared-folder`\operation\comexclude`

In UNIX:

Physical hosts:

`/var/opt/jp1cons/operation/comexclude`

Logical host:

shared-directory`/operation/comexclude`

A common exclusion-conditions definition history file is created if it does not exist in the location at any of the times listed below. This is based on the assumption that the operation mode of common exclusion-conditions is set to extended mode.

- When JP1/IM - Manager starts
- When JP1/IM - Manager is running and a common exclusion-conditions definition is applied to JP1/IM - Manager
- When JP1/IM - Manager is running and a common exclusion-conditions definition is enabled or disabled

A log entry in a common exclusion-conditions definition history file is generated in the following format:

`{+ | -}`*serial-number process-time process-description*

The *serial-number* is a serial number in the common exclusion-conditions definition history. The serial number can be from `00000001` to `99999999`. When the number reaches `99999999`, it is reset to `00000001`. The serial number is also reset to `00000001` when JP1/IM - Manager restarts. The *process-time* is written in the following format: *YYYY*`/`*MM*`/`*DD hh*`:`*mm*`:`*ss*`.`*SSS* (where *YYYY* is the year, *MM* month, *DD* day, *hh* hour, *mm* minute, and *ss*`.`*SSS* second).

Generally, a log entry of a process is written in one line and a plus sign (+) is appended to the top of the line. When a log entry of a process spans multiple lines, a plus sign (+) is appended to the top of the line indicating the start of the process and a minus sign (-) is appended to the top of each subsequent line.

The following table describes what information is included in the process description.

Table 3–7: Processes to be logged in the common exclusion-conditions definition history file

No.	Common exclusion process to be logged	Information included in the process description
1	A common exclusion-conditions definition is updated (by using the System Environment Settings window in JP1/IM - View, or the `jcochfilter -ef` command).	The contents of the applied common exclusion-conditions definition (dump of the definition file) are logged. Line 1: `The common exclusion-conditions extended definition was updated.` (line break) Line 2 and later: *contents-of-the-updated-system-common-exclusion-conditions-extended-definition-file* When the updated definition has an additional common exclusion-conditions extended definition, the information above is followed by the contents of the additional common exclusion-conditions extended definition file. Line 1: `The additional common exclusion-conditions definition was updated.` (line break) Line 2 and later: *contents-of-the-updated-additional-common-exclusion-conditions-extended-definition-file*
2	An additional common exclusion-conditions definition is added (by using **Exclude by Common Exclusion-Conditions** in JP1/IM - View).	The contents of the registered additional common exclusion-conditions definition are logged. Line 1: `The additional common exclusion-conditions definition was registered.` (line break) Line 2 and later: *contents-of-the-registered-additional-common-exclusion-conditions-definition*
3	A common exclusion-condition is enabled (by using the `jcochfilter -e/-on` command).	The ID of the enabled common exclusion-condition is logged. • When an ID is specified: `The common exclusion condition became enabled. (common exclusion condition group IDs =` *common-exclusion-conditions-group-ID*`[,`*common-exclusion-conditions-group-ID*`])` (line break) • When `ALL` is specified: `All common exclusion conditions became enabled.`
4	A common exclusion-condition is disabled (by using the `jcochfilter -e/-off` command).	The ID of the disabled common exclusion-condition is logged. • When an ID is specified: `The common exclusion condition became disabled. (common exclusion condition group IDs =` *common-exclusion-conditions-group-ID*`[,`*common-exclusion-conditions-group-ID*`])` (line break) • When an ID is not specified: `All common exclusion conditions became disabled.`(line break)

The following is an example of a common exclusion-conditions definition history file:

```
+00000001 2017/04/01 12:30:25.131 The common exclusion-conditions extended
definition was updated.
-DESC_VERSION=1
-
```

```
-def hostA maintenance
-    cmt limit:2017/04/31
-    id 1
-    valid true
-    date 20170401-20170431
-    week 1,2,3,4,5,6
-    rtime 1000-1200
-    cnd
-        B.ID IN 00000001
-        E.SEVERITY IN Emergency Alert
-        B.SOURCESERVER IN hostA
-    end-cnd
-end-def
-The additional common exclusion-conditions definition was updated.
-DESC_VERSION=2
-
-def hostB maintenance
-    cmt limit:2017/04/31
-    id A2
-    valid true
-    ex-target action
-    date 20170401-20170431
-    week 1,2,3,4,5,6
-    rtime 1000-1200
-    cnd
-        B.ID IN 00000002
-        E.SEVERITY IN Emergency Alert
-        B.SOURCESERVER IN hostB
-    end-cnd
-end-def
+00000002 2017/04/01 12:40:51.849 The additional common exclusion-
conditions definition was registered.
-def hostC maintenance
-    cmt limit:2017/04/31
-    id A3
-    valid true
-    ex-target action
-    date 20170401-20170431
-    week 1,2,3,4,5,6
-    rtime 1000-1200
-    cnd
-        B.ID IN 00000001
-        E.SEVERITY IN Emergency Alert
-        B.SOURCESERVER IN hostC
-    end-cnd
-end-def
```

00000003 2017/04/01 12:45:41.009 The common exclusion condition became enabled.

(7) Notes on common exclusion-conditions

- The total number of common exclusion-conditions and additional common exclusion-conditions must be 2,500 or fewer, and the total size must be 15 MB or smaller.
- JP1 events that common execution conditions prevent from being collected are excluded from the event monitoring targets. The excluded events are no longer displayed in the event list in the Event Console window. When you set common exclusion-conditions, carefully check the settings for event conditions and exclusion targets.

- If you execute the jcochfilter command with the -ef option specified to apply the extended definitions of common exclusion-conditions, all the defined common exclusion-conditions are replaced. All the definitions of additional common exclusion-conditions that were added during event monitoring will be lost, so be careful.
- The load on JP1/IM - Manager increases in proportion to the number of common exclusion-conditions and their contents, which might cause the number of monitored JP1 events per unit time to decrease. You should consider consolidating filter conditions for multiple hosts into one condition, for example, by using a regular expression in the filter condition.

3.3 Issue of correlation events

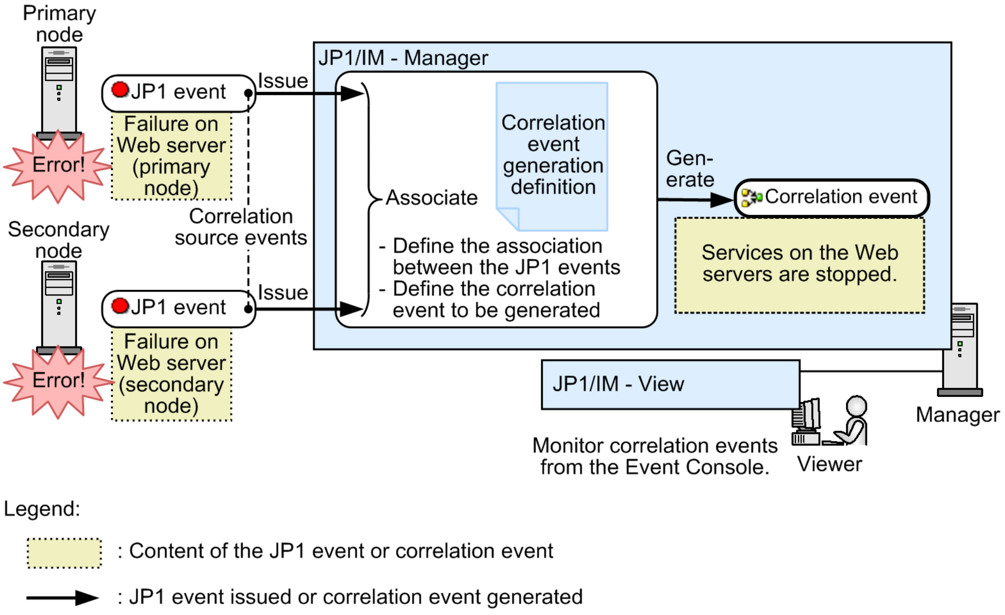
JP1/IM - Manager can issue a new JP1 event whenever two or more related JP1 events are issued. The new event is known as a *correlation event*. The correlation event and the association between the JP1 events can be defined by the user as a *correlation event generation definition*.

The related JP1 event that triggers the correlation event is known as a *correlation source event*. You can define multiple correlation source events, or just one.

For example, suppose JP1/IM - Manager is managing Web servers in a cluster system. If a failure occurs in succession on both the primary node and secondary node, the service provided by the Web servers on these nodes will stop. By associating the JP1 event reporting a failure on the primary node with the JP1 event reporting a failure on the secondary node, and defining a correlation event, you can ensure a speedy response.

The following figure shows the relationships between a correlation event, correlation event generation definition, and correlation source events, based on the above Web server example.

Figure 3–17: Relationships between correlation event, correlation event generation definition, and correlation source events


Primary node
Error!
JP1 event
Failure on Web server (primary node)
Issue
Correlation source events
Secondary node
Error!
JP1 event
Failure on Web server (secondary node)
Issue
JP1/IM - Manager
Associate
Correlation event generation definition
- Define the association between the JP1 events
- Define the correlation event to be generated
Gen-erate
Correlation event
Services on the Web servers are stopped.
Manager
JP1/IM - View
Monitor correlation events from the Event Console.
Viewer
Legend:
: Content of the JP1 event or correlation event
: JP1 event issued or correlation event generated

The JP1 events issued from the Web servers on the primary and secondary nodes are sent to the manager. The two JP1 events are associated and a *correlation event* is issued, according to the *correlation event generation definition*. The JP1 events that triggered the correlation event are known as *correlation source events*.

There are two kinds of correlation events: A *correlation approval event* is issued when a correlation is established; a *correlation failure event* is issued when no correlation is established.

Event issued when a correlation is established

You can issue a correlation approval event when the specified events all arrive within a set timeout period, as in these examples:

1. Two Web servers are configured in a cluster system. Errors on the primary node issue event A, and errors on the secondary node issue event B.
2. To detect that services on the Web servers have stopped, write a correlation event generation definition that issues a correlation approval event (event C) when both event A and event B are issued.

Event issued when no correlation is established

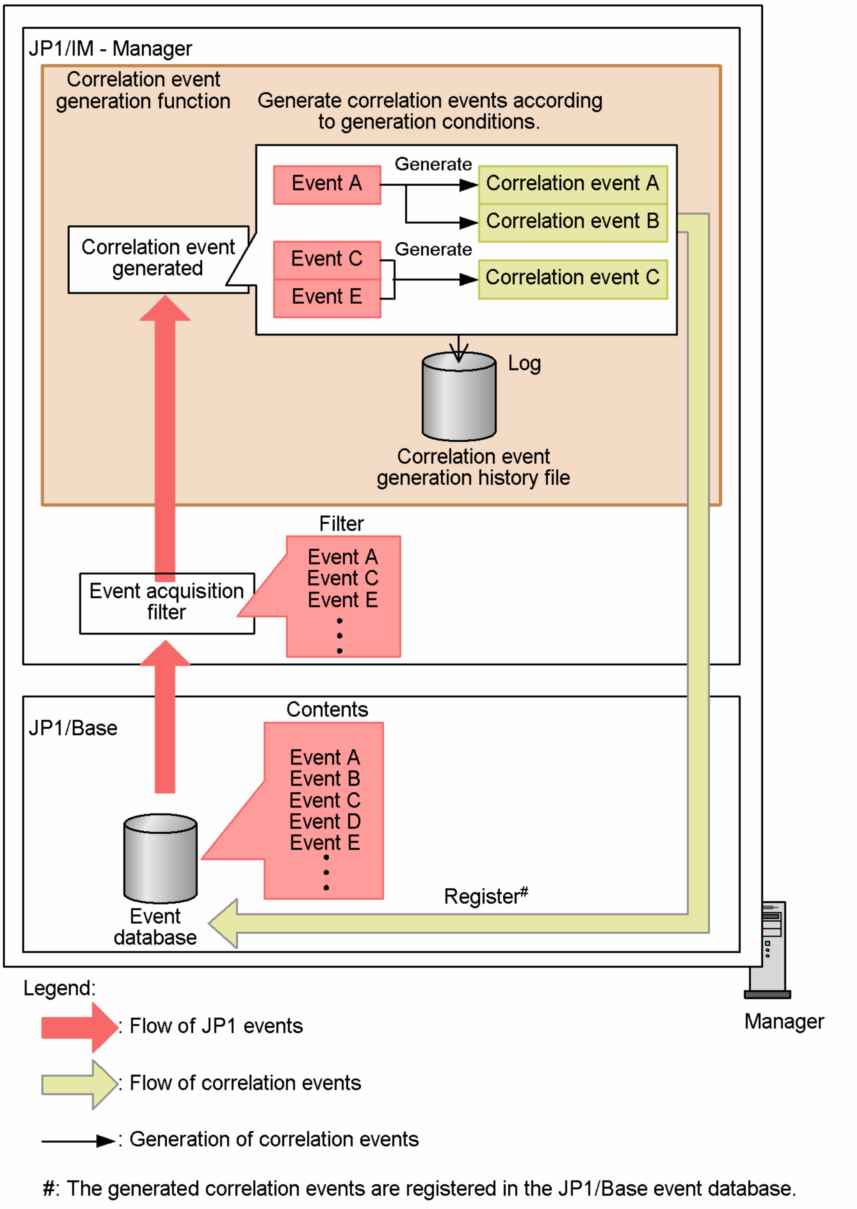
You can issue a correlation failure event when the specified events do not all arrive within the timeout period, as in these examples:

1. Two Web servers are configured in a cluster system. Errors on the primary node issue event A, and errors that occur at failover to the secondary node issue event B.
2. To detect that services on the Web servers have stopped, write a correlation event generation definition that issues a correlation failure event (event C) if event B does not arrive within the set timeout period after event A is issued.

The JP1 events registered with the JP1/Base event database are acquired by JP1/IM - Manager through an event acquisition filter. JP1/IM - Manager then issues correlation events, based on the settings in the correlation event generation definition. These correlation events are also registered with the JP1/Base event database. This processing is known as *correlation event issue*.

The following figure shows an overview of correlation event issue.

Figure 3–18: Overview of correlation event issue



#: The generated correlation events are registered in the JP1/Base event database.

The following describes correlation event issue in further detail.

3.3.1 Correlation event issue

Correlation events are issued by the following JP1/IM - Manager processes:

- When not using the integrated monitoring database: Event issue service
- When using the integrated monitoring database: Event base service

The event generation service and event base service provide the *correlation event generation function*.

This function is positioned internally as shown below.

Figure 3–19: Position of the correlation event generation function (when not using the integrated monitoring database)

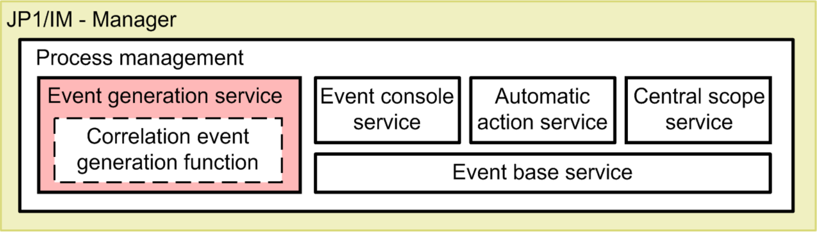
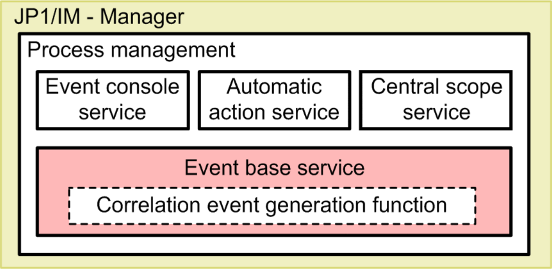


Figure 3–20: Position of the correlation event generation function in the event base service (when using the integrated monitoring database)



When you use the integrated monitoring database, the correlation event generation function is provided by the event base service. This means that event correlation processing can be synchronized with transfer of events to the event console service.

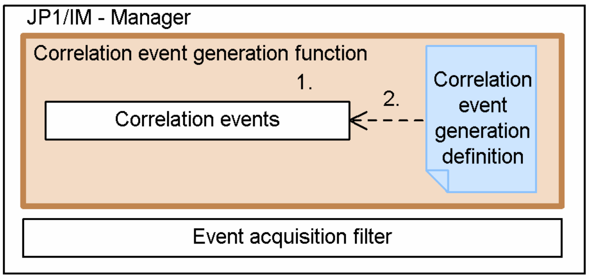
(1) Processing at startup of the correlation event generation function

When JP1/IM - Manager starts, the correlation event generation function reads the correlation event generation definition in preparation for issuing correlation events.

If you are not using the integrated monitoring database, by default the event generation service does not start when JP1/IM - Manager starts. You must enter a setting using the `jcoimdef` command to start this service at JP1/IM - Manager startup. When you use the integrated monitoring database, the event base service starts automatically but the correlation event generation function is disabled by default. You must use the `jcoimdef` command to enable the function.

The following figure shows the processing at startup of the correlation event generation function.

Figure 3–21: Processing at startup of the correlation event generation function


JP1/IM - Manager
Correlation event generation function
1.
2.
Correlation events
Correlation event generation definition
Event acquisition filter

1. Started by the process management (`jco_spmd`) in the same way as other services.
2. Read at startup

The flow of processing is described below, following the numbers in the figure:

1. The correlation event generation function is started by the process management functionality.

   The correlation event generation function is started and stopped by the process management in the same way as other JP1/IM - Manager services.

   If you are not using the integrated monitoring database, by default the event generation service does not start when JP1/IM - Manager starts. You must enter a setting using the `jcoimdef` command to start this service at JP1/IM - Manager startup. When you use the integrated monitoring database, the event base service starts automatically but the correlation event generation function is disabled by default. You must use the `jcoimdef` command to enable the function.

2. The correlation event generation function reads the correlation event generation definition held internally.

   The correlation event generation function behaves according to the internally recorded correlation event generation definition. For this reason, if you edit the correlation event generation definition file, you must apply the changes using the `jcoegschange` command; otherwise, the service operation will remain unchanged.

   The default definition does not issue correlation events. To issue correlation events, you must edit the correlation event generation definition file and execute the `jcoegschange` command to apply the settings.

Note

To change a correlation event generation definition, use the `jcoegschange` command.

You can update an issue definition while the correlation event generation function is active. If the service is stopped, you can update the definition to be used from the next run.

However, you cannot edit a correlation event generation definition while the function is in the process of starting or stopping.

(2) JP1 event acquisition after startup of the correlation event generation function

The processing of JP1 events after the correlation event generation function starts sometimes differs depending on whether you are using the integrated monitoring database. The following describes the flow of processing in each case.

(a) Correlation processing when not using the integrated monitoring database

Once started, the correlation event generation function associates the correlation event generation definitions with events acquired by the event generation service and issues correlation events.

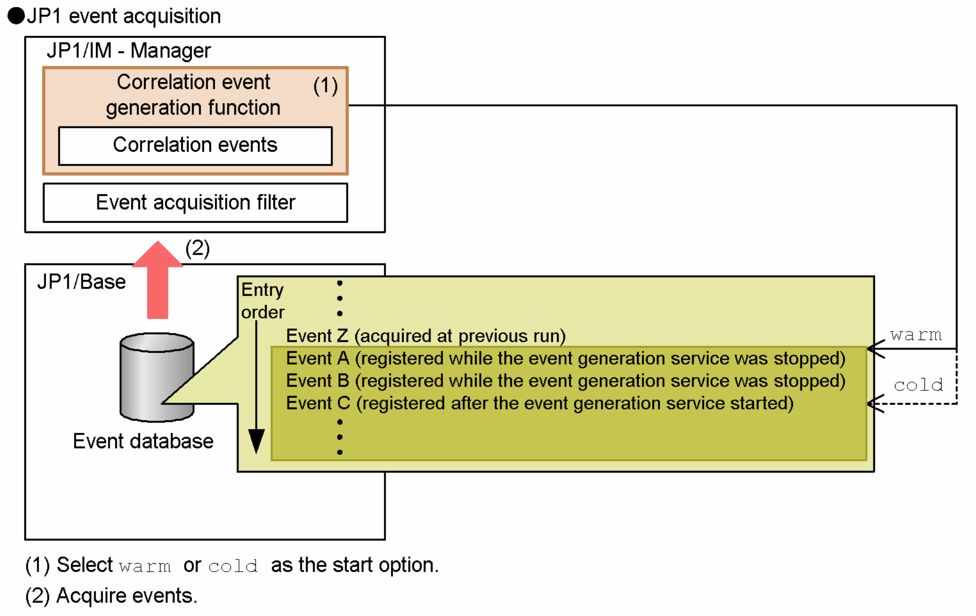
You can select the location in the JP1/Base event database at which the event generation service begins event acquisition after startup. To set the location, select either `cold` or `warm` start mode. These are referred to collectively as *start options*. Using the start options, you can specify whether to resume correlation processing from the previous run. The start options are described in the table below.

Table 3–8: Start options for correlation event issue

Start option	Description
`cold` start	Begins acquiring JP1 events that have been registered in the JP1/Base event database since the correlation event generation function started. Stops the correlation processing that was being executed before JP1/IM - Manager stopped. When JP1/IM - Manager is restarted, the function's previous execution status no longer applies.
`warm` start	Begins acquiring JP1 events registered in the JP1/Base event database, starting from the JP1 event following the last one acquired when the function stopped at the previous run. Records the correlation processing that was being executed before JP1/IM - Manager stopped. When JP1/IM - Manager is restarted, the function's previous execution status takes effect. The default is `warm` start.

The following figure shows the differences between a `cold` start and `warm` start in commencing JP1 event acquisition.

Figure 3–22: Differences in starting acquisition of JP1 events



●JP1 event acquisition
JP1/IM - Manager
Correlation event generation function
(1)
Correlation events
Event acquisition filter
(2)
JP1/Base
Event database
Entry order
Event Z (acquired at previous run)
Event A (registered while the event generation service was stopped)
Event B (registered while the event generation service was stopped)
Event C (registered after the event generation service started)
warm
cold
(1) Select warm or cold as the start option.
(2) Acquire events.

If JP1 events up to event Z have been acquired when the correlation event generation function stops, acquisition will commence from event A (the next event registered after event Z) if the service is restarted in `warm` mode. If the service is restarted in `cold` mode, acquisition will commence from event C (the first event registered after the function restarts).

By default, the correlation event generation function starts in `warm` mode. This is appropriate in most circumstances, but if you do not need to correlate events issued while the function was stopped, switch to `cold` start mode.

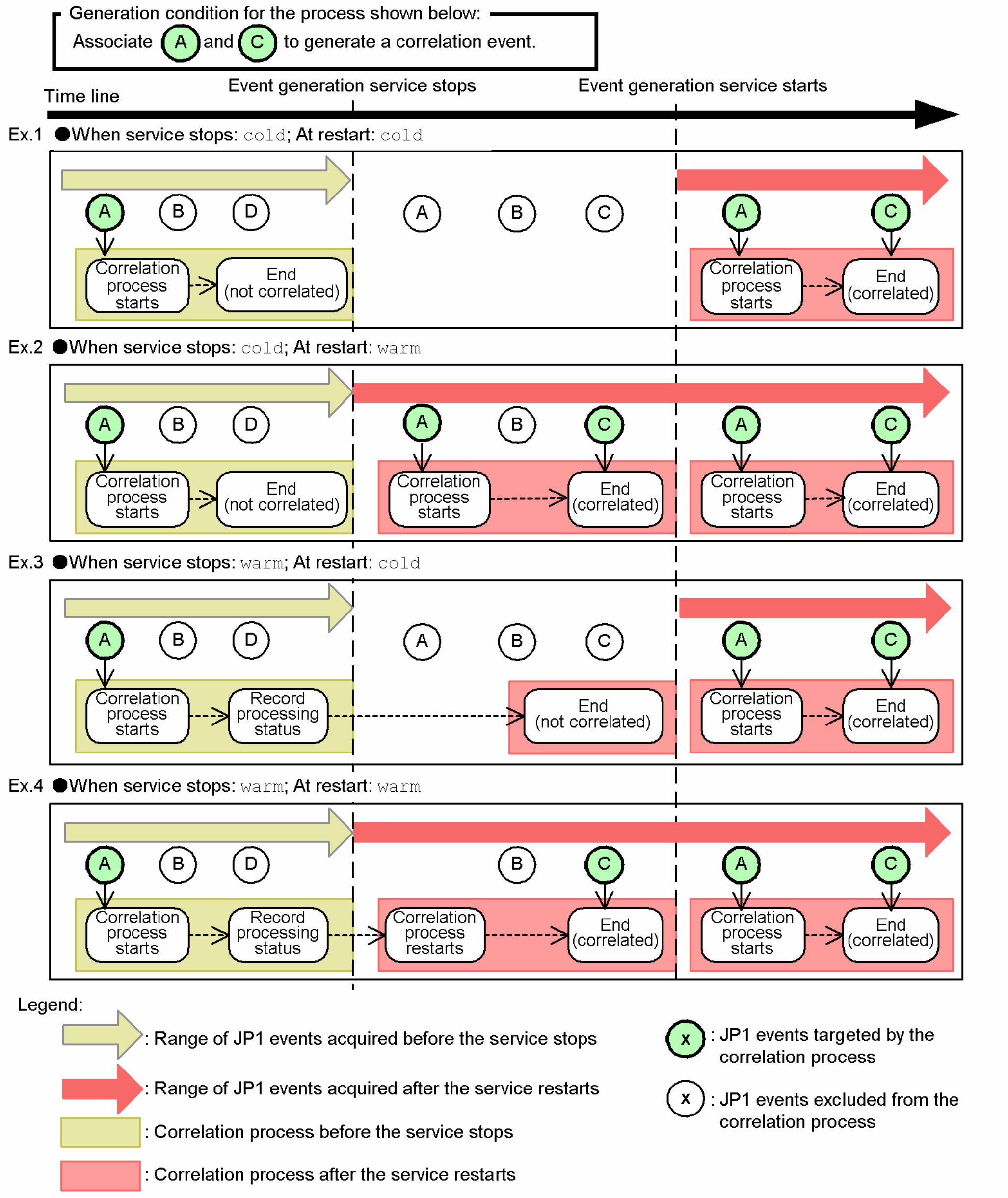
We recommend that you use `warm` starts when running JP1/IM - Manager in a cluster system. If you use `cold` starts, the service will not acquire JP1 events issued while JP1/IM - Manager is being failed over.

Only those JP1 events selected by an event acquisition filter are acquired by the correlation event generation function. For details about event acquisition filters, see *3.2 Filtering of JP1 events*.

■ Correlation processing examples (when not using the integrated monitoring database)

The following figure shows the processing to issue correlation event issue when a `cold` start is specified and when a `warm` start is specified.

Figure 3–23: Correlation processing when the event generation service stops and after it restarts (when not using the integrated monitoring database)



Generation condition for the process shown below:
Associate A and C to generate a correlation event.
Time line
Event generation service stops
Event generation service starts
Ex.1 ●When service stops: cold; At restart: cold
A
B
D
Correlation process starts
End (not correlated)
A
B
C
A
C
Correlation process starts
End (correlated)
Ex.2 ●When service stops: cold; At restart: warm
A
B
D
Correlation process starts
End (not correlated)
A
B
C
Correlation process starts
End (correlated)
A
C
Correlation process starts
End (correlated)
Ex.3 ●When service stops: warm; At restart: cold
A
B
D
Correlation process starts
Record processing status
A
B
C
End (not correlated)
A
C
Correlation process starts
End (correlated)
Ex.4 ●When service stops: warm; At restart: warm
A
B
D
Correlation process starts
Record processing status
B
C
Correlation process restarts
End (correlated)
A
C
Correlation process starts
End (correlated)
Legend:
: Range of JP1 events acquired before the service stops
: Range of JP1 events acquired after the service restarts
: Correlation process before the service stops
: Correlation process after the service restarts
x : JP1 events targeted by the correlation process
x : JP1 events excluded from the correlation process

The following describes how the correlation process behaves in the examples in *Figure 3-23 Correlation processing when the event generation service stops and after it restarts (when not using the integrated monitoring database)*.

Example 1:

If the `cold` start option applies when the event generation service stops and when it is restarted, the correlation processing behaves as follows:

When the event generation service stops

- Processing ends and information about all target JP1 events is discarded.
- The processing contents are logged to a correlation event generation history file.

After the event generation service restarts:

- Acquisition starts from the JP1 events registered after restart.
- The service reads the correlation event generation definition, and starts processing accordingly.

Example 2:

If the `cold` start option applies when the event generation service stops, and `warm` applies when it is restarted, the correlation processing behaves as follows:

When the event generation service stops

- Processing ends and information about all target JP1 events is discarded.
- The processing contents are logged to a correlation event generation history file.

After the event generation service restarts:

- Acquisition starts from the JP1 event following the last one acquired when the service stopped at the previous run.
- The service re-reads the correlation event generation definition, and starts processing accordingly.

Example 3:

If the `warm` start option applies when the event generation service stops, and `cold` applies when it is restarted, the correlation processing behaves as follows:

When the event generation service stops

- Information about the JP1 events being correlated, the processing contents, and the information in the correlation event generation definition are output to an internal log to record the processing status.
- The processing contents are logged to a correlation event generation history file.

After the event generation service restarts:

- All information about JP1 events being correlated when the service stopped at the previous run is discarded.
- Acquisition starts from the JP1 events registered after the restart.
- The service reads the correlation event generation definition, and starts processing accordingly.

Example 4:

If the `warm` start option applies when the event generation service stops and when it is restarted, the correlation processing behaves as follows:

When the event generation service stops

- Information about the JP1 events being correlated, the processing contents, and the information in the correlation event generation definition are output to an internal log to record the processing status.
- The processing contents are logged to a correlation event generation history file.

After the event generation service restarts:

- Acquisition starts from the JP1 event following the last one acquired when the service stopped at the previous run.
- The service re-reads the correlation event generation definition, and starts processing accordingly.
- The service references the internal log and resumes processing from the JP1 events being correlated, if any, when the previous run stopped.

  However, if you change the correlation event generation definition after the service stops and before it restarts, all information about JP1 events being correlated at the end of the previous run is discarded (same behavior as for a `cold` start).

Important

If the event generation service ends abnormally, information about the JP1 events being correlated cannot be recorded. Therefore, at the next run, the service will behave as for a `cold` start: Information about the JP1 events being correlated at the end of the previous run is discarded, and acquisition starts from the JP1 events registered after the service restarts.

The event generation service terminates abnormally when:

- The event generation service process is forcibly terminated (`kill`)
- The process is forcibly terminated by the `jcogencore` command.
- The system is forcibly powered off.

(b) Correlation processing when using the integrated monitoring database

Once started, the correlation event generation function associates the correlation event generation definitions with events acquired by the event base service and issues correlation events.

You can select the location in the JP1/Base event database at which the event base service begins event acquisition after startup. Set the location by executing the `jcoimdef` command with the `-b` option specified.

The correlation processing behaves differently depending on the combination of acquisition start location and start option, as follows:

Table 3–9: Correlation processing behavior

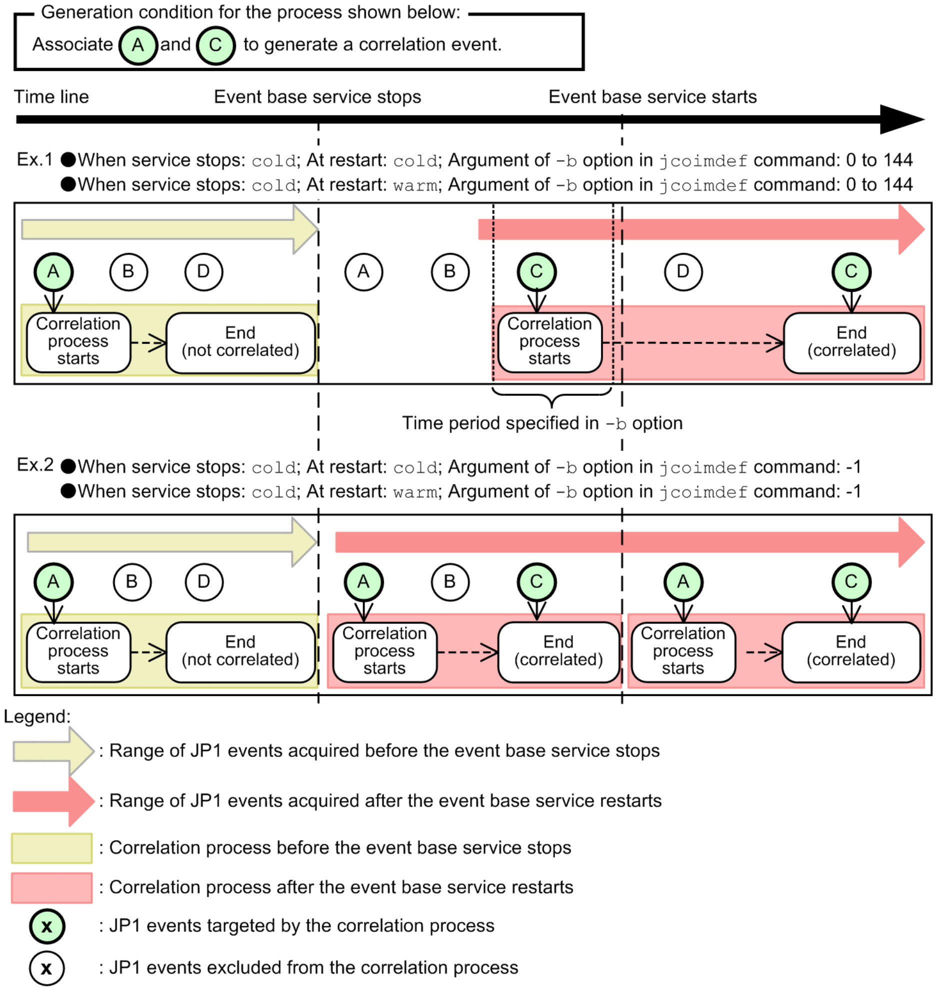
Start option	Value of the -b option	Correlation processing
`warm`	-1 (default)	The status of the JP1 events being correlated is inherited. Acquisition starts from the JP1 event following the last one acquired when the service stopped at the previous run. If no JP1 events had been acquired at the end of the previous run, acquisition starts from the oldest JP1 event registered in the event database.
	0 to 144	Message `KAJV2316-W` is output and the status of JP1 events being correlated is not inherited.
`cold`	-1 to 144	All correlation processing stops and ends. The status of JP1 events being correlated is not inherited.

JP1 events already processed by the correlation event generation function are not subject to correlation processing a second time.

■ Correlation processing examples (when using the integrated monitoring database)

The following figure shows the processing to issue correlation event when a `cold` start is specified and when a `warm` start is specified.

Figure 3–24: Correlation processing when the event base service stops (in cold start mode) and when it restarts


Generation condition for the process shown below:
Associate A and C to generate a correlation event.
Time line
Event base service stops
Event base service starts
Ex.1 ●When service stops: cold; At restart: cold; Argument of -b option in jcoimdef command: 0 to 144
●When service stops: cold; At restart: warm; Argument of -b option in jcoimdef command: 0 to 144
A
B
D
Correlation process starts
End (not correlated)
A
B
C
D
C
Correlation process starts
End (correlated)
Time period specified in -b option
Ex.2 ●When service stops: cold; At restart: cold; Argument of -b option in jcoimdef command: -1
●When service stops: cold; At restart: warm; Argument of -b option in jcoimdef command: -1
A
B
D
Correlation process starts
End (not correlated)
A
B
C
Correlation process starts
End (correlated)
A
C
Correlation process starts
End (correlated)
Legend:
: Range of JP1 events acquired before the event base service stops
: Range of JP1 events acquired after the event base service restarts
: Correlation process before the event base service stops
: Correlation process after the event base service restarts
x : JP1 events targeted by the correlation process
x : JP1 events excluded from the correlation process

The following describes how the correlation processing behaves in the examples in *Figure 3-24Correlation processing when the event base service stops (in cold start mode) and when it restarts*.

Example 1:

If the `cold` or `warm` start option applies when the event base service starts, and a value in the range 0 to 144 is specified in the `-b` option of the `jcoimdef` command, the correlation processing behaves as follows:

When the event base service stops

- Processing ends and information about all target JP1 events is discarded.
- The processing contents are logged to a correlation event generation history file.

After the event base service restarts:

- Acquisition starts at the number of hours specified in the `jcoimdef` command's `-b` option prior to the restart time.
- The service reads the correlation event generation definition, and starts processing accordingly.

Example 2:

If the `cold` or `warm` start option applies when the event base service starts, and -1 is specified in the `-b` option of the `jcoimdef` command, the correlation processing behaves as follows:

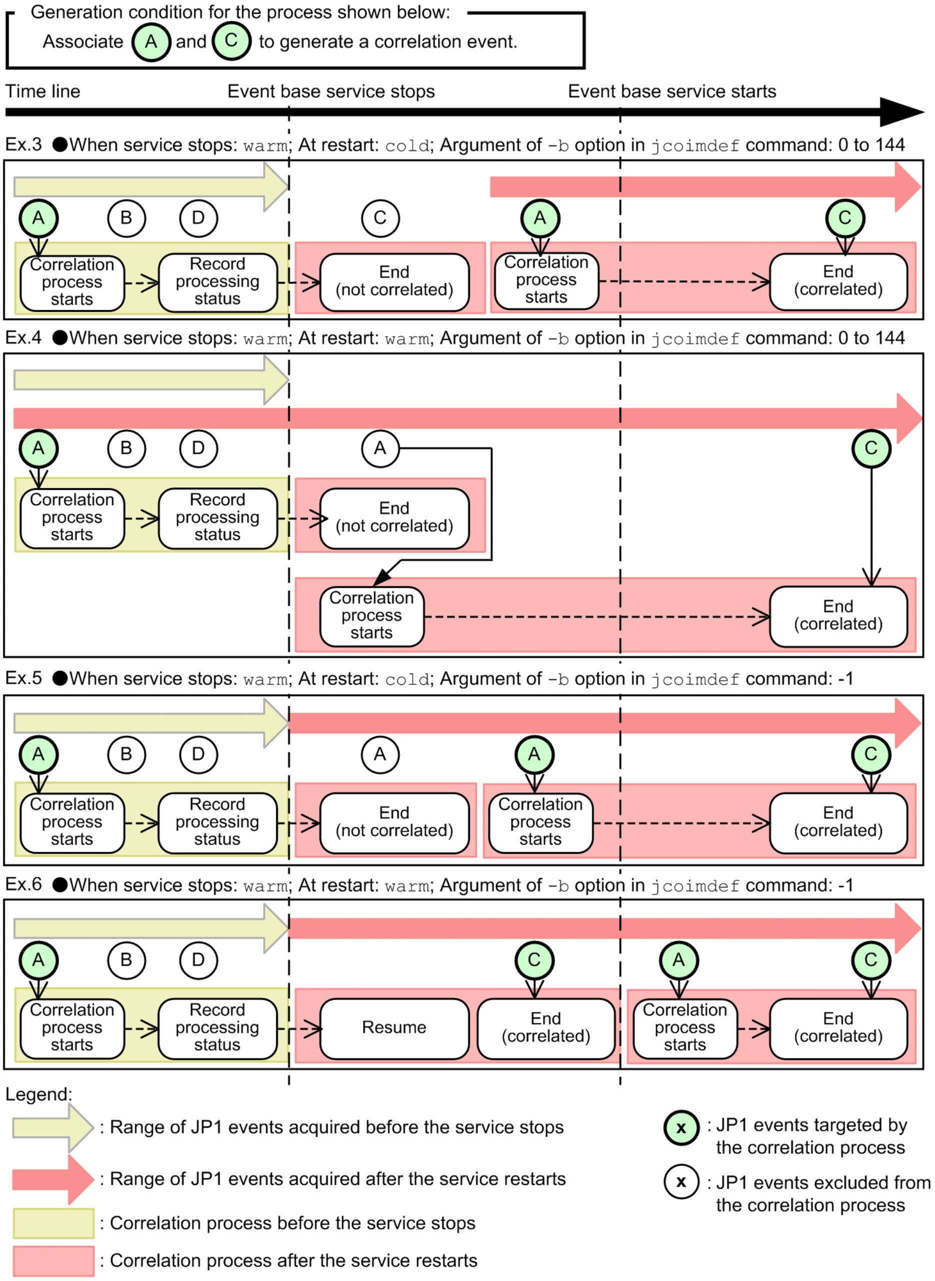
When the event base service stops

- Processing ends and information about all target JP1 events is discarded.
- The processing contents are logged to a correlation event generation history file.

After the event base service restarts:

- Acquisition starts from the JP1 event following the last one acquired when the service stopped at the previous run.
- The service re-reads the correlation event generation definition, and starts processing accordingly.

Figure 3–25: Correlation processing when the event base service stops (in warm start mode) and when it restarts



Generation condition for the process shown below:
Associate A and C to generate a correlation event.
Time line
Event base service stops
Event base service starts
Ex.3 ●When service stops: warm; At restart: cold; Argument of -b option in jcoimdef command: 0 to 144
A
B
D
C
A
C
Correlation process starts
Record processing status
End (not correlated)
Correlation process starts
End (correlated)
Ex.4 ●When service stops: warm; At restart: warm; Argument of -b option in jcoimdef command: 0 to 144
A
B
D
A
C
Correlation process starts
Record processing status
End (not correlated)
Correlation process starts
End (correlated)
Ex.5 ●When service stops: warm; At restart: cold; Argument of -b option in jcoimdef command: -1
A
B
D
A
A
C
Correlation process starts
Record processing status
End (not correlated)
Correlation process starts
End (correlated)
Ex.6 ●When service stops: warm; At restart: warm; Argument of -b option in jcoimdef command: -1
A
B
D
C
A
C
Correlation process starts
Record processing status
Resume
End (correlated)
Correlation process starts
End (correlated)
Legend:
: Range of JP1 events acquired before the service stops
: Range of JP1 events acquired after the service restarts
: Correlation process before the service stops
: Correlation process after the service restarts
x : JP1 events targeted by the correlation process
x : JP1 events excluded from the correlation process

The following describes how the correlation processing behaves in the examples in *Figure 3-25 Correlation processing when the event base service stops (in warm start mode) and when it restarts*.

Example 3:

If the cold start option applies when the event base service starts, and a value in the range 0 to 144 is specified in the -b option of the jcoimdef command, the correlation processing behaves as follows:

When the event base service stops

- Information about the JP1 events being correlated, the processing contents, and the information in the correlation event generation definition are output to an internal log to record the processing status.
- The processing contents are logged to a correlation event generation history file.

After the event base service restarts:

- All information about JP1 events being correlated when the service stopped at the previous run is discarded.
- Acquisition starts at the number of hours specified in the jcoimdef command's -b option prior to the restart time.
- The service reads the correlation event generation definition, and starts processing accordingly.

Example 4:

If the warm start option applies when the event base service starts, and a value in the range 0 to 144 is specified in the -b option of the jcoimdef command, the correlation processing behaves as follows:

When the event base service stops

- Information about the JP1 events being correlated, the processing contents, and the information in the correlation event generation definition are output to an internal log to record the processing status.
- The processing contents are logged to a correlation event generation history file.

After the event base service restarts:

- Acquisition starts at the number of hours specified in the jcoimdef command's -b option prior to the restart time.
- The service re-reads the correlation event generation definition, and starts processing accordingly.
- The service references the internal log and starts processing from the JP1 events that have not yet been correlated.

Example 5:

If the cold start option applies when the event base service starts, and -1 is specified in the -b option of the jcoimdef command, the correlation processing behaves as follows:

When the event base service stops

- Information about the JP1 events being correlated, the processing contents, and the information in the correlation event generation definition are output to an internal log to record the processing status.
- The processing contents are logged to a correlation event generation history file.

After the event base service restarts:

- Acquisition starts from the JP1 event following the last one acquired when the service stopped at the previous run.
- The service re-reads the correlation event generation definition, and starts processing accordingly.

Example 6:

If the warm start option applies when the event base service starts, and -1 is specified in the -b option of the jcoimdef command, the correlation processing behaves as follows:

When the event base service stops

- Information about the JP1 events being correlated, the processing contents, and the information in the correlation event generation definition are output to an internal log to record the processing status.
- The processing contents are logged to a correlation event generation history file.

After the event base service restarts:

- Acquisition starts from the JP1 event following the last one acquired when the service stopped at the previous run.
- The service re-reads the correlation event generation definition, and starts processing accordingly.
- The service references the internal log and resumes processing from the JP1 events being correlated, if any, when the previous run stopped.

Important

If the event base service ends abnormally, information about the JP1 events being correlated cannot be recorded. Therefore, at the next run, the service will behave as for a `cold` start: Information about the JP1 events being correlated at the end of the previous run is discarded, and acquisition starts from the JP1 events registered after the service restarts.

The event base service terminates abnormally when:

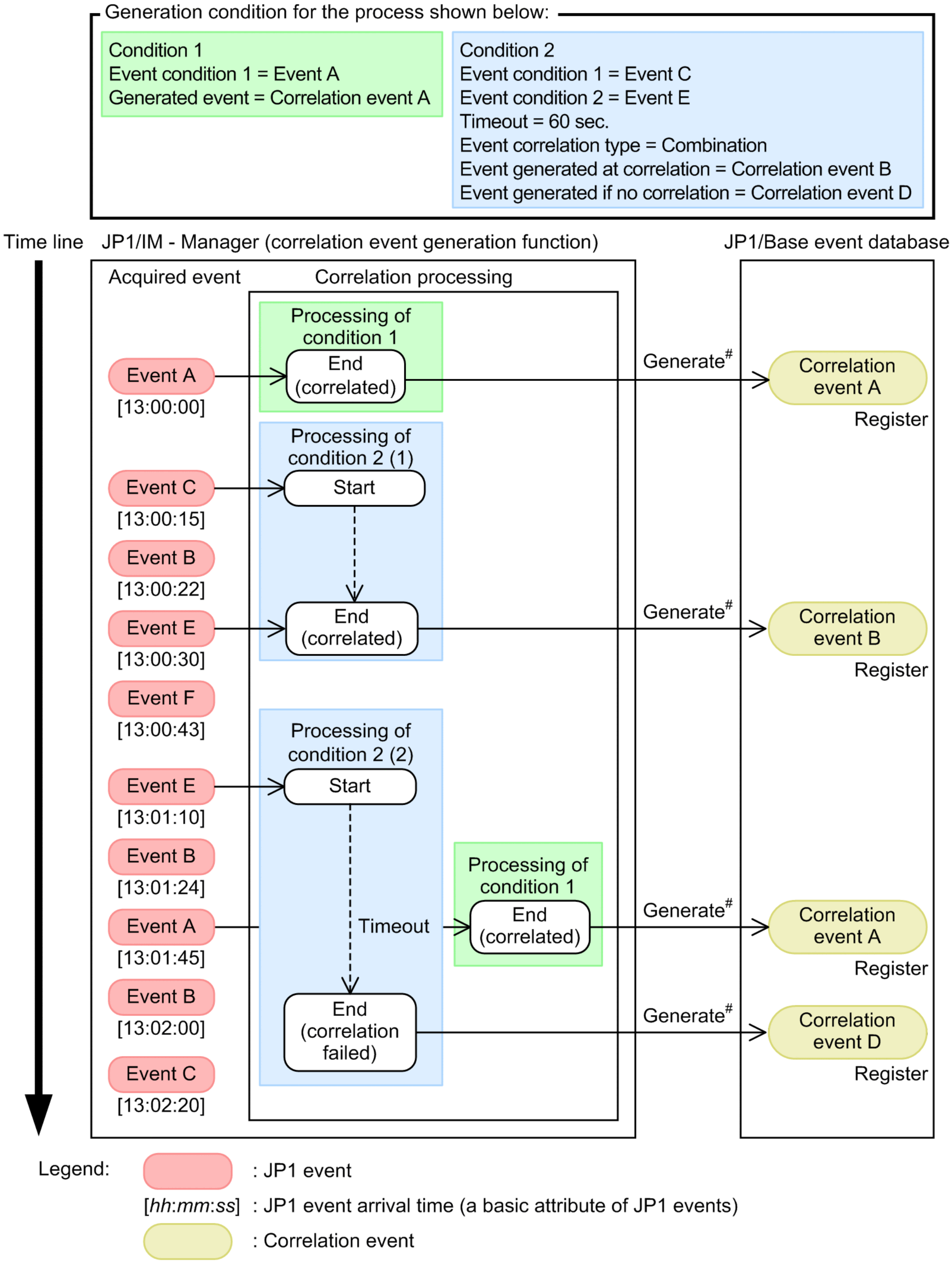
- The service process is forcibly terminated (killed)
- The service process is forcibly terminated by the `jcogencore` command.
- The system is forcibly powered off.

(3) Correlation event issue after JP1 event acquisition

The following figure shows the processing to issue correlation event after JP1 events have been acquired.

Figure 3–26: Correlation event issue after JP1 event acquisition

- Process of correlation event generation



#: When event generation is defined in the correlation event generation definitions for both correlation success and correlation failure for a particular JP1 event, events are generated in both situations.

When only one event condition is defined in a correlation event generation condition, the correlation processing is successful and terminates when a JP1 event matching that event condition is issued.

When multiple event conditions are defined in a correlation event generation condition, the correlation processing is successful and terminates when a JP1 event matching one of the event conditions is issued, and a JP1 event matching another event condition is issued subsequently. If the subsequent match does not occur within the timeout period,# the correlation processing fails and terminates. If you have defined correlation event generation definitions that issue correlation approval events and correlation failure events, both types of correlation events will be issued.

#: A basic attribute of JP1 events. Based on the arrival time.

Note

When you define multiple event conditions, you can select one of three event correlation types: `sequence`, `combination`, or `threshold`.

- `sequence` starts correlation processing based on the order in which the JP1 events are issued. If `sequence` had been set as the event correlation type in generation condition 2 in the above figure, processing of event condition 2 would not start until event condition 1 had been satisfied.
- `combination` is the event correlation type specified in generation condition 2 in the above figure. `combination` starts correlation processing regardless of the order in which event conditions 1 and 2 are satisfied.
- `threshold` issues a correlation event when the number of issued JP1 events matching the defined event condition reaches a threshold.

The processing performed in correlation event issue is output and saved to a correlation event generation history file, and can be referenced as required. For details about this file, see *3.3.4 Contents of a correlation event generation history file*.

(4) Correlation processing when activating or deactivating the integrated monitoring database

The following table describes the event acquisition start location when correlation processing resumes after the integrated monitoring database is activated or deactivated.

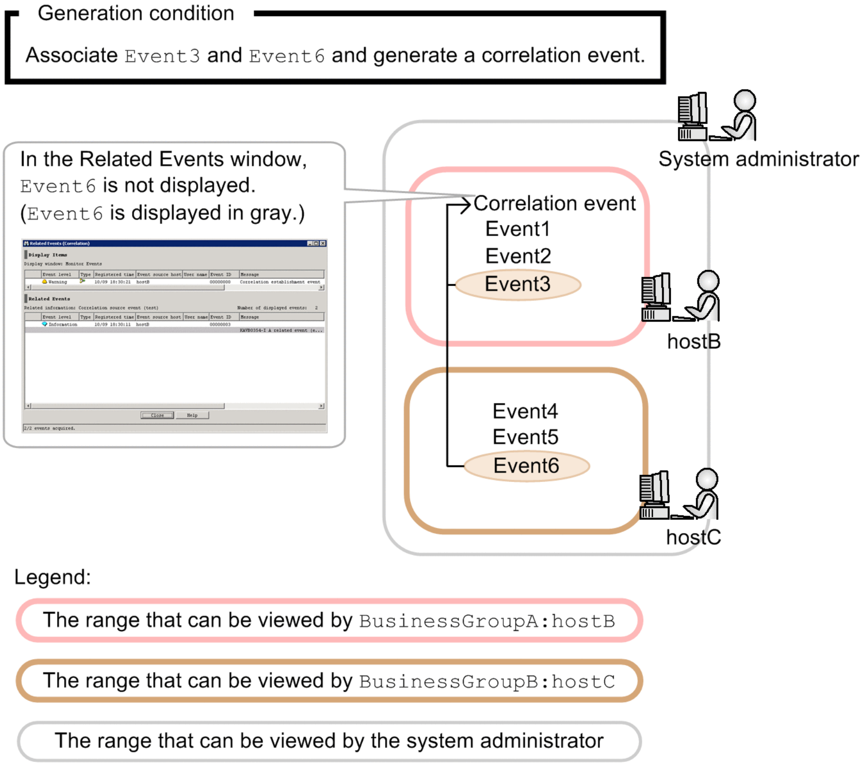
Table 3–10: JP1 event acquisition location of the correlation processing when activating or deactivating the integrated monitoring database

Direction of change	Start option at restart	JP1 event acquisition location when correlation processing resumes
Stop using the integrated monitoring database	`cold`	The point at which the event base service starts
	`warm`	The point at which the event base service stopped at the previous run
Start using the integrated monitoring database	`cold`	According to the value set in the `-b` option of the `jcoimdef` command
	`warm`	

(5) Processing when restriction of viewing and operating business groups is set

When viewing and operating of business groups are restricted, JP1 users cannot define correlation events across the different business groups. Only the system administrator can define correlation events. JP1 users must request the system administrator to set correlation events.

Figure 3–27: Correlation event across different business groups



Generation condition
Associate Event3 and Event6 and generate a correlation event.
In the Related Events window, Event6 is not displayed. (Event6 is displayed in gray.)
System administrator
Correlation event
Event1
Event2
Event3
hostB
Event4
Event5
Event6
hostC
Legend:
The range that can be viewed by BusinessGroupA:hostB
The range that can be viewed by BusinessGroupB:hostC
The range that can be viewed by the system administrator
Related Events (Correlation)
Close
Help

Display Items

Display window: Monitor Events

	Event level	Type	Registered time	Event source host	User name	Event ID	Message
	Warning		10/09 18:30:21	hostB		00000000	Correlation establishment event

Related Events

Related information: Correlation source event (test)   Number of displayed events: 2

	Event level	Type	Registered time	Event source host	User name	Event ID	Message
	Information		10/09 18:30:11	hostB		00000003	
							KAVB0354-I A related event (e...

2/2 events acquired.

If JP1 events generated in different business groups are defined as correlation events, the background colors of those correlation source events are displayed in gray in the Related Events window.

When you define correlation events, define filtering conditions so that only the JP1 events issued in the business system will be displayed as the related events for the correlation events. Also, define variables so that only the JP1 events in the business system will be displayed as issued correlation events.

```
[gyoumuA]

TARGET=E.JP1_SOURCEHOST==/Business system A ...............1

CON=CID:1, E.SEVERITY==Error, E.PRODUCT_NAME>=HITACHI/JP1/AJS2

CON=CID:2, E.SEVERITY==Error, E.PRODUCT_NAME>=HITACHI/JP1/Base

SUCCESS_EVENT=E.SEVERITY:Alert,E.JP1_SOURCEHOST:
$EV1_E.JP1_SOURCEHOST ..........2
```

Description

1. Using a filtering condition (TARGET), filter the events so that only the names of the hosts in the business group (Business system A) are displayed as the event source host names (E.JP1_SOURCEHOST) of the related events. To specify a business group or monitoring group, specify its path by adding a slash (/) before the name.
2. Use a variable ($EV1_E.SOURCEHOST) and let the event source host name (E.JP1_SOURCEHOST) for the correlation event (SUCCESS_EVENT) inherit the name of the event source host whose related event conditions match the event conditions for CID:1.

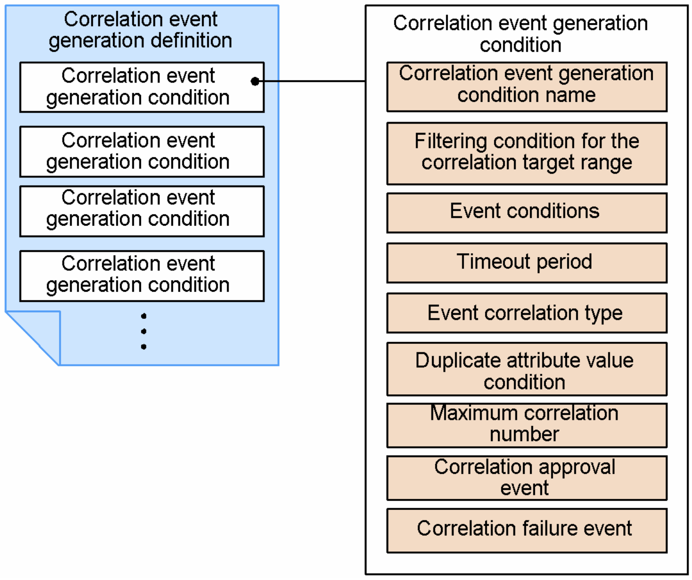
3.3.2 Defining correlation event issue

To issue correlation events, you must prepare a correlation event generation definition.

A correlation event generation definition consists of multiple generation conditions, each of which contains several items.

The following figure shows the structure of a correlation event generation definition.

Figure 3–28: Structure of a correlation event generation definition


Correlation event generation definition
Correlation event generation condition
Correlation event generation condition
Correlation event generation condition
Correlation event generation condition
Correlation event generation condition
Correlation event generation condition name
Filtering condition for the correlation target range
Event conditions
Timeout period
Event correlation type
Duplicate attribute value condition
Maximum correlation number
Correlation approval event
Correlation failure event

Define the above items in a correlation event generation definition file. The items and their meaning are explained next. For details about how to specify each item, and the input rules and restrictions, see *Correlation event generation definition file* in *Chapter 2. Definition Files* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

Note that JP1 users cannot define correlation events. To define correlation events, contact the system administrator.

(1) Correlation event generation condition name

A name identifying the correlation event generation condition.

(2) Filtering condition for the correlation target range

A condition for filtering the range of JP1 events processed according to the correlation event generation condition.

As the filtering condition, specify an attribute value of the target JP1 events. For example, by specifying the name of the event server that issued the event (`B.SOURCESERVER`), you can restrict the processing to issue correlation event to JP1 events issued from a specific agent host.

(3) Event condition

A condition for determining a JP1 event (correlation source event) that triggers a correlation event.

Specify an attribute value of the JP1 events targeted or excluded from the processing to issue correlation event. You can specify multiple event conditions in a generation condition.

When you specify multiple event conditions, those that exclude specific JP1 events (`NOT` specification) are applied first.

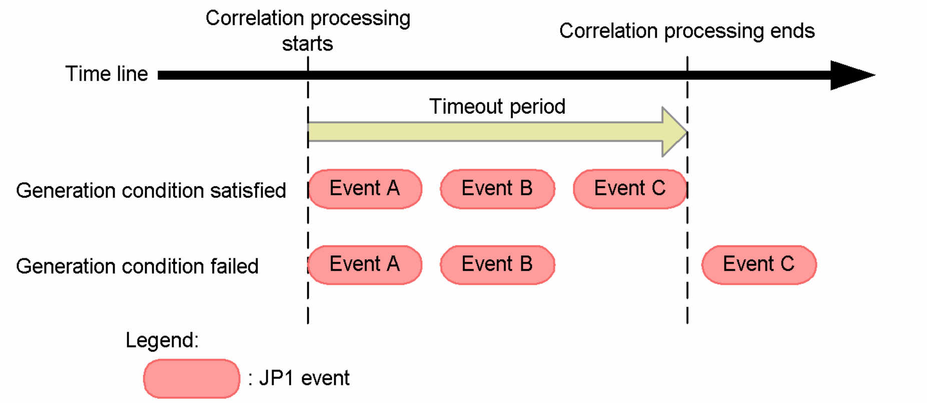
(4) Timeout period

The maximum wait time for a JP1 event matching an event condition.

The timeout period is counted from the arrival time (a basic attribute of JP1 events) of the first JP1 event matching an event condition. If the specified timeout period elapses without the generation condition being met, no correlation event is issued and the correlation processing terminates.

The following example shows when the generation condition is satisfied and when it fails for a succession of events A, B, and C.

Figure 3–29: Timeout period


Correlation processing starts
Correlation processing ends
Time line
Timeout period
Generation condition satisfied
Event A
Event B
Event C
Generation condition failed
Event A
Event B
Event C
Legend:
: JP1 event

(5) Event correlation type

The method by which JP1 events matching an event condition are correlated.

There are three event correlation types:

- Correlation based on event sequence
  The correlation event generation condition is satisfied or fails according to whether JP1 events matching the defined event conditions are issued in a set sequence.
- Correlation based on event combination
  The correlation event generation condition is satisfied or fails according to whether JP1 events matching the defined combination of event conditions are issued, regardless of the order in which they occur.
- Correlation based on thresholds
  The correlation event generation condition is satisfied or fails according to whether the number of issued JP1 events matching a defined event condition reaches a set threshold.

(6) Duplicate attribute value condition

A condition that groups JP1 events matching an event condition on the basis of their attribute value, and issues a correlation event on a group basis. Multiple duplicate attribute value conditions can be specified in a generation condition.

In a duplicate attribute value condition, you can specify a JP1 event attribute name or part of an attribute value. For example, suppose JP1 events indicating an authentication error are associated and issue a correlation event. By specifying the name of the server that issued the event (B.SOURCESERVER), you can issue correlation events on an authentication server basis.

(7) Maximum correlation number

The maximum number of sets of JP1 events that can be processed concurrently by one correlation event generation condition.

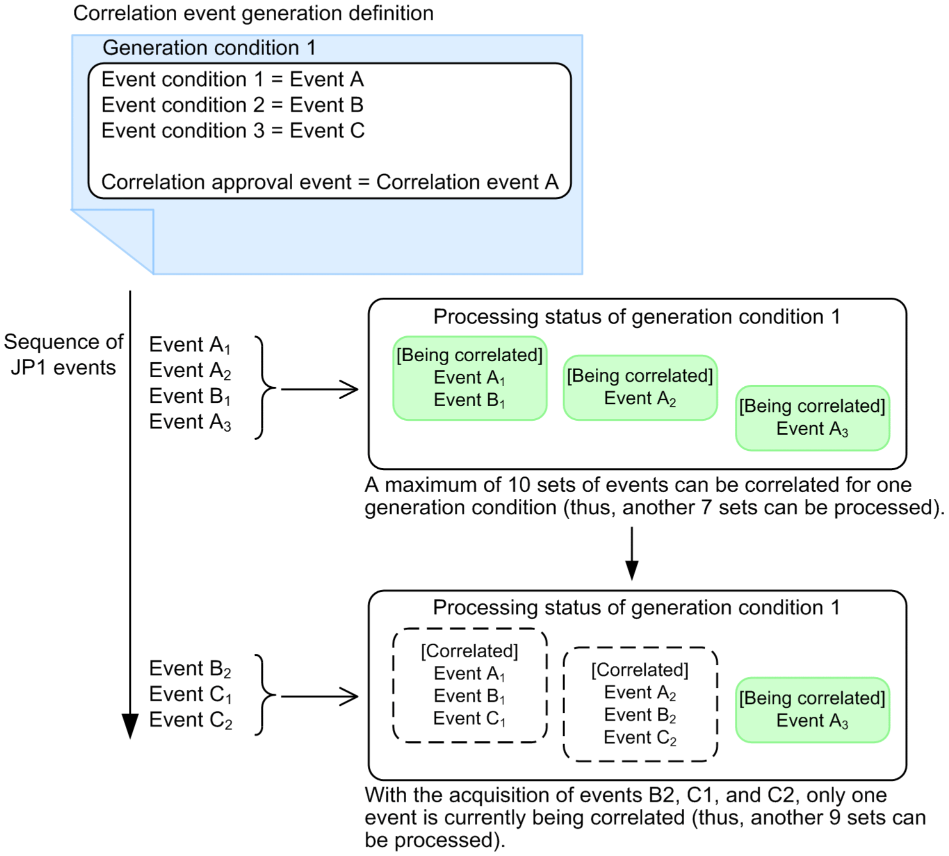
The default when this item is unspecified is 10. When 10 sets of target JP1 events have been acquired for one generation condition, any further target JP1 events that are acquired during correlation processing of that condition will not be processed.

In this case, warning message KAJV2301-W is output to the integrated trace log.

For example, suppose a duplicate attribute value condition is specified, and correlation events are issued by each of the 50 servers in the system. If each server issues a JP1 event at the same time, the first 10 sets of JP1 events can be processed, but the remaining 40 sets cannot. In this type of situation, you would specify 50 sets as the maximum correlation number.

The following figure shows how the correlation processing works when the maximum correction number is the default (10 sets).

Figure 3–30: Correlation processing based on the default maximum correlation number (10 sets)


Correlation event generation definition
Generation condition 1
Event condition 1 = Event A
Event condition 2 = Event B
Event condition 3 = Event C
Correlation approval event = Correlation event A
Sequence of JP1 events
Event A$_1$
Event A$_2$
Event B$_1$
Event A$_3$
Processing status of generation condition 1
[Being correlated] Event A$_1$ Event B$_1$
[Being correlated] Event A$_2$
[Being correlated] Event A$_3$
A maximum of 10 sets of events can be correlated for one generation condition (thus, another 7 sets can be processed).
Event B$_2$
Event C$_1$
Event C$_2$
Processing status of generation condition 1
[Correlated] Event A$_1$ Event B$_1$ Event C$_1$
[Correlated] Event A$_2$ Event B$_2$ Event C$_2$
[Being correlated] Event A$_3$
With the acquisition of events B2, C1, and C2, only one event is currently being correlated (thus, another 9 sets can be processed).

> **Important**
>
> A maximum of 20,000 sets of JP1 events can be correlated concurrently by all the correlation event generation conditions. Avoid specifying a large maximum correlation number in a large number of generation conditions.

When the number of JP1 event sets under correlation reaches 20,000, the KAJV2322-W message is issued and correlation processing stops. Once the number of JP1 event sets under correlation is greater than the maximum value of 20,000, the KAJV2322-W message is not displayed again until the number decreases to 16,000.

(8) Correlation approval event

A JP1 event (*correlation event*) that is issued when a correlation event generation condition is satisfied. You can specify any attribute name and any attribute value for the correlation event. By using a variable to specify an attribute of the correlation source event, you can pass the attribute value to the correlation event.

For details about issued correlation events, see *3.3.8 Issued correlation event*.

(9) Correlation failure event

A JP1 event (*correlation event*) that is issued when a correlation event generation condition is not satisfied. You can specify any attribute name and any attribute value for the correlation event. By using a variable to specify an attribute of the correlation source event, you can pass the attribute value to the correlation event.

For details about issued correlation events, see *3.3.8 Issued correlation event*.

3.3.3 Status transition and operation settings of the correlation event generation function

The correlation event generation function can have any of the statuses shown in the table below.

Table 3–11: Statuses of the correlation event generation function

No.	Status	Description
1	Starting	The correlation event generation function is starting.
2	Running	The correlation event generation function has started and is active.
3	Standby	The correlation event generation function has started but is inactive.
4	Stopping	The correlation event generation function is stopping.
5	Stop	The correlation event generation function has stopped.

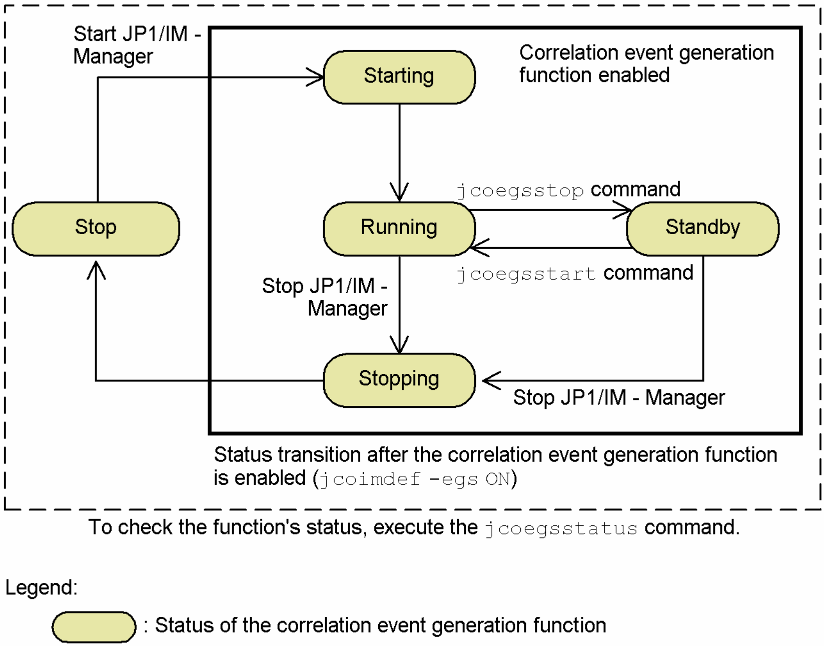
You can check the status of the correlation event generation function using the `jcoegsstatus` command.

To enable the correlation event generation function, after installing JP1/IM - Manager, execute `jcoimdef - egs ON`. After you have performed this setup, the function will start automatically the next time you start JP1/IM - Manager.

When the correlation event generation function has started, you can make it inactive by using the `jcoegsstop` command, and activate it again using the `jcoegsstart` command.

The following figure shows the status transition of the function.

Figure 3–31: Status transition of the correlation event generation function


Start JP1/IM - Manager
Starting
Correlation event generation function enabled
jcoegsstop command
Stop
Running
Standby
jcoegsstart command
Stop JP1/IM - Manager
Stopping
Stop JP1/IM - Manager
Status transition after the correlation event generation function is enabled (jcoimdef -egs ON)
To check the function's status, execute the jcoegsstatus command.
Legend:
: Status of the correlation event generation function

When a large number of unwanted JP1 events have been issued through system maintenance, for example, you can temporarily suspend correlation processing by switching the correlation event generation function to inactive status. The function supports this kind of issued operation.

3.3.4 Contents of a correlation event generation history file

Information about the operating status and correlation processing of the correlation event generation function is logged to a correlation event generation history file. By referencing this file, you can check whether correlation events are being issued according to the defined correlation event generation conditions. For example, if a large number issue failures are being logged for a specific generation condition, it could be that the target JP1 events are an inappropriate combination, or the timeout period might be too short. When periodically reviewing the conditions, look at the correlation event generation history file as a reference. The file can be found in the following location:

In Windows:

console-path`\operation\evgen\egs_discrim{1|2|3}.log`

In UNIX:

```
/var/opt/jp1cons/operation/evgen/egs_discrim{1|2|3}.log
```

You can change the maximum size and number of correlation event generation history files. For details, see *Correlation event generation environment definition file* in *Chapter 2. Definition Files* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

(1) Format of a correlation event generation history file

The format of a correlation event generation history file is as follows:

`{+ | -}`*serial-number time processing-contents*

The serial number is that of the correlation event issue log. The numbers run from 00000001 to 99999999, and then start again from 00000001. When the correlation event generation function is restarted, the serial numbers also start again from 00000001. The time is output in *YYYY*/*MM*/*DD hh*:*mm*:*ss*.*SSS* format (*YYYY*: year, *MM*: month, *DD*: day, *hh*: hour, *mm*: minute, *ss*.*SSS*: second).

Basically, a one-line log entry beginning with a plus sign (+) is output per processing. Where the entry spans multiple lines, the first line begins with a plus sign (+) and the continuation lines begin with a hyphen (-). The contents logged to the file are described next.

(2) Processing results logged to a correlation event generation history file

The following table describes the processing results logged to a correlation event generation history file.

Table 3–12: Processing results logged to a correlation event generation history file

No.	Processing result	Format	Remarks

1	The correlation event generation function is active.	`+Correlation event generation function : RUNNING`
		`-VERSION=`*version-of-correlation event-generation-definition-file*
		`-[`*generation-condition-name*`]`
		`-TARGET=`*filtering-condition-for-correlation-target-range*
		`-CON=`*event-condition*
		`-TIMEOUT=`*timeout-period*
		`-TYPE=`*event-correlation-type*
		`-SAME_ATTRIBUTE=`*duplicate-attribute-value-condition*
		`-CORRELATION_NUM=`*maximum-correlation-number*
		`-SUCCESS_EVENT=`*correlation-approval-event*
		:
			The output items are the contents of the correlation event generation definition file being used.

2	The correlation event generation function is inactive.	`+Correlation event generation function : STANDBY`	--
3	A JP1 event matching the event condition has been issued and correlation processing has started.	`+Generation start` *condition-name* (*correlation-number*) *JP1-event-information* `-SAME_ATTRIBUTE=`*same-attribute-name*:*same-attribute-value* : `-SAME_ATTRIBUTE=`*same-attribute-name*:*same-attribute-value*	*correlation-number* is for identifying the start of processing and the processing result (satisfied or unsatisfied) for each set of JP1 events when multiple sets are being correlated with one generation condition.
4	The generation condition was satisfied.	`+Generation success` *condition-name* (*correlation-number*) -*JP1-event-information-1* -*JP1-event-information-2* : -*JP1-event-information-n* `-SAME_ATTRIBUTE=`*same-attribute-name*:*same-attribute-value* : `-SAME_ATTRIBUTE=`*same-attribute-name*:*same-attribute-value*	--
5	A correlation event has been issued.	`+Correlation event generation succeeded.` *condition-name* (*correlation-number*) *serial-number-in-event-database*	--

No.	Processing result	Format	Remarks

6	The generation condition was not satisfied. (Correlation processing has stopped.)	`+Generation fail` *condition-name* (*correlation-number*) *reason-for-failure*
		–*JP1-event-information-1*
		–*JP1-event-information-2*
		:
		–*JP1-event-information-n*
		`-SAME_ATTRIBUTE=`*same-attribute-name*:*same-attribute-value*
		:
		`-SAME_ATTRIBUTE=`*same-attribute-name*:*same-attribute-value*
			The reason why the generation condition was not satisfied is output as one of the following:
			• The correlation event generation definition has been updated:
			`definition_update`
			• The correlation event generation function was restarted in `cold` start mode:
			`cold_start`
			• The correlation event generation function is inactive.
			`standby`
			• Internal error
			`unknown`

7	The correlation event generation definition has been updated.	`+Correlation event generation definition update`
		`-VERSION=`*version-of-correlation event-generation-definition-file*
		`-[`*generation-condition-name*`]`
		`-TARGET=`*filtering-condition-for-correlation-target-range*
		`-CON=`*event-condition*
		`-TIMEOUT=`*timeout-period*
		`-TYPE=`*event-correlation-type*
		`-SAME_ATTRIBUTE=`*duplicate-attribute-value-condition*
		`-CORRELATION_NUM=`*maximum-correlation-number*
		`-SUCCESS_EVENT=`*correlation-approval-event*
		:
			The output items are the contents of the correlation event generation definition file being used.

8	Output to the header at the following times: • When the correlation event generation function starts • When the correlation event generation history file is switched	`JP1/IM - Central Console/Correlation Event Generation Service`	--
9	A JP1 event matching the event condition has been issued and correlation processing has started, but the JP1 event does not contain the attribute defined in the duplicate attribute value condition.	`+A JP1 event that matches the correlation event generation condition occurred, and the correlation event generation processing started, but the event attribute defined in that attribute value condition does not exist in the JP1 event.` (*condition-name* (*correlation-number*) *serial-number-in-event-database attribute-name*)	The attribute not present in the JP1 event being correlated is output to *attribute-name* at the left.
10	A JP1 event was received after the number of JP1 event sets being correlated had reached the limit of 20,000 sets.	`+Generation fail` *condition-name* (*correlation-number*) `exceeded the threshold (20000)` –*JP1-event-information*	--

Legend:

--: None

The item *JP1-event-information* in the table is output in the following format:

serial-number-in-event-database`,`*event-ID*`,`*source-event-server-name*`,`*arrival-time*`,`*event-level*

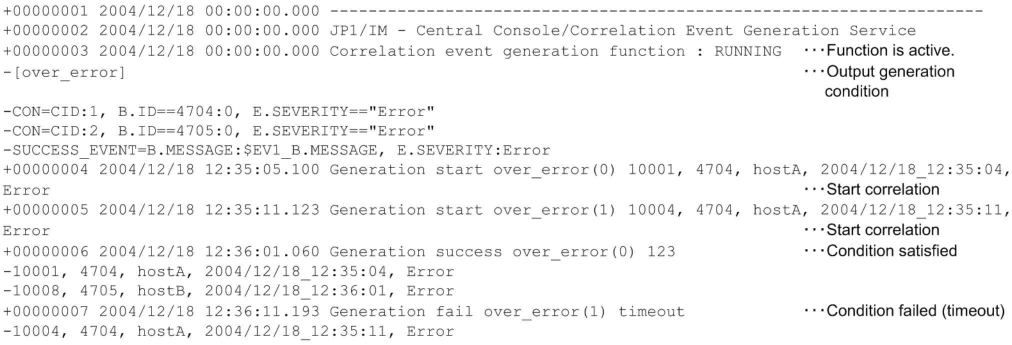
When the correlation event generation function starts or the correlation event generation history file is switched, the header information is output in the following format:

```
-------------------------------------------------------------

JP1/IM - Central Console/Correlation Event Generation Service
```

(3) Example output to a correlation event generation history file

An example of output to a correlation event generation history file is shown below.

Figure 3–32: Example of output to a correlation event generation history file



```
+00000001 2004/12/18 00:00:00.000 --------------------------------------------------------------------
+00000002 2004/12/18 00:00:00.000 JP1/IM - Central Console/Correlation Event Generation Service
+00000003 2004/12/18 00:00:00.000 Correlation event generation function : RUNNING  ···Function is active.
-[over_error]                                                                      ···Output generation
                                                                                      condition
-CON=CID:1, B.ID==4704:0, E.SEVERITY=="Error"
-CON=CID:2, B.ID==4705:0, E.SEVERITY=="Error"
-SUCCESS_EVENT=B.MESSAGE:$EV1_B.MESSAGE, E.SEVERITY:Error
+00000004 2004/12/18 12:35:05.100 Generation start over_error(0) 10001, 4704, hostA, 2004/12/18_12:35:04,
Error                                                                              ···Start correlation
+00000005 2004/12/18 12:35:11.123 Generation start over_error(1) 10004, 4704, hostA, 2004/12/18_12:35:11,
Error                                                                              ···Start correlation
+00000006 2004/12/18 12:36:01.060 Generation success over_error(0) 123             ···Condition satisfied
-10001, 4704, hostA, 2004/12/18_12:35:04, Error
-10008, 4705, hostB, 2004/12/18_12:36:01, Error
+00000007 2004/12/18 12:36:11.193 Generation fail over_error(1) timeout            ···Condition failed (timeout)
-10004, 4704, hostA, 2004/12/18_12:35:11, Error
```

3.3.5 JP1 events subject to correlation processing

The processing performed by the correlation event generation function applies to the following JP1 events.

Target JP1 events

- JP1 events issued by an application program (system events)
- JP1 events issued by a user (user events)

Correlation processing does not apply to the following JP1 events.

Excluded JP1 events

- JP1 events not registered in the JP1/Base event database (events used in JP1/IM - Manager's internal processing and displayed only in JP1/IM - View)
- Correlation events

3.3.6 Situations in which a generation condition is satisfied or fails

The situations in which a generation condition is satisfied or fails are described below. When a JP1 event matches multiple correlation event generation conditions, it is processed by each condition.

(1) Generation condition satisfied

- Only one event condition defined in the generation condition:
  The condition is satisfied when a matching JP1 event is acquired.
- Multiple event conditions defined in the generation condition (combination specified):
  The condition is satisfied when all the matching JP1 events are acquired within the specified time.
- Multiple event conditions defined in the generation condition (sequence specified):
  The condition is satisfied when matching JP1 events are acquired within the specified time and in the specified sequence.
- Threshold defined in the generation condition:
  The condition is satisfied when the number of matching JP1 events acquired within the specified time reaches the defined threshold.

(2) Generation condition fails

- Multiple event conditions defined in the generation condition (combination specified):
  The condition fails if all the matching JP1 events are not acquired within the specified time.
- Multiple event conditions defined in the generation condition (sequence specified):
  The condition fails if the matching JP1 events are not acquired within the specified time and in the specified sequence.
- Threshold defined in the generation condition:
  The condition fails if the number of acquired matching JP1 events does not reach the defined threshold within the specified time.

3.3.7 Situations in which correlation processing fails

Correlation event generation conditions are not satisfied if processing stops. Correlation processing stops in the following cases:

- The correlation event generation function was restarted in `cold` mode while a JP1 event was being processed.
  Correlation fails because information about the JP1 event being processed is discarded as part of the restart processing.
- A JP1 event was being processed when the correlation event generation definition was changed (by the `jcoegschange` command).
  Correlation fails because information about the JP1 event being processed at the time the changed definition was being applied is discarded.
- The correlation event generation function was stopped by the `jcoegsstop` command.
- The event generation service ended abnormally (when not using the integrated monitoring database).
- The event base service ended abnormally (when using the integrated monitoring database).

3.3.8 Issued correlation event

A correlation event is issued when a correlation event generation condition is satisfied or fails. The issued correlation event is registered in the JP1/Base event database.

You can specify any attribute name and any attribute value for the issued event. By using a variable to specify an attribute of the correlation source event, you can pass the attribute value to the correlation event.

The following table describes the contents of an issued correlation event. The table does not cover attributes that can be optionally specified by the user, such as a message (`B.MESSAGE`).

Table 3–13: Contents of correlation events issued by the correlation event generation function

Attribute type		Item	Attribute name	Contents
Basic attribute		Event ID	`ID`	User-defined event ID A value in the range from 0 to 1FFF and from 7FFF8000 to 7FFFFFFF is displayed.
		Message	`MESSAGE`	User-defined message
Extended attribute	Common information	Product name	`PRODUCT_NAME`	`/HITACHI/JP1/IM/GENERATE_EVENT`#
		Object type	`OBJECT_TYPE`	`SERVICE`#
		Object name	`OBJECT_NAME`	`EGS`#
		Occurrence	`OCCURRENCE`	Correlation event type. Either of the following is set: • Generation condition satisfied: `SUCCESS` • Generation condition failed: `FAIL`
	Program-specific information	Relation Event serial number	`JP1_GENERATE_SOURCE_SEQNO`	*serial-number-in-event-databaseΔserial-number-in-event-database*`...`# (serial number of each correlation source event in the event database, separated by spaces)
		Correlation event generation condition name	`JP1_GENERATE_NAME`	Name of the satisfied correlation event generation condition

#: Fixed value, not definable by the user.

To check issued correlation events, you must display **Type** in the Event Console window. Add **Type** to the **Display items & order** box in the Preferences window. With this setting, an icon is displayed in the **Type** field. The icon indicates the generation condition was satisfied; the icon indicates the generation condition failed.

You can perform the same operations and settings on correlation events as on JP1 events. For example, correlation events can trigger an automated action, and can be filtered by an event acquisition filter or event receiver filter. You can also view the correlation source events that resulted in a correlation event in the Related Events (Correlation) window or Related Events (Correlation fails) window.

Note, however, that you cannot make an issued correlation event subject to any further correlation processing.

For details about the Preferences window, see *2.24 Preferences window* in the manual *JP1/Integrated Management - Manager GUI Reference*.

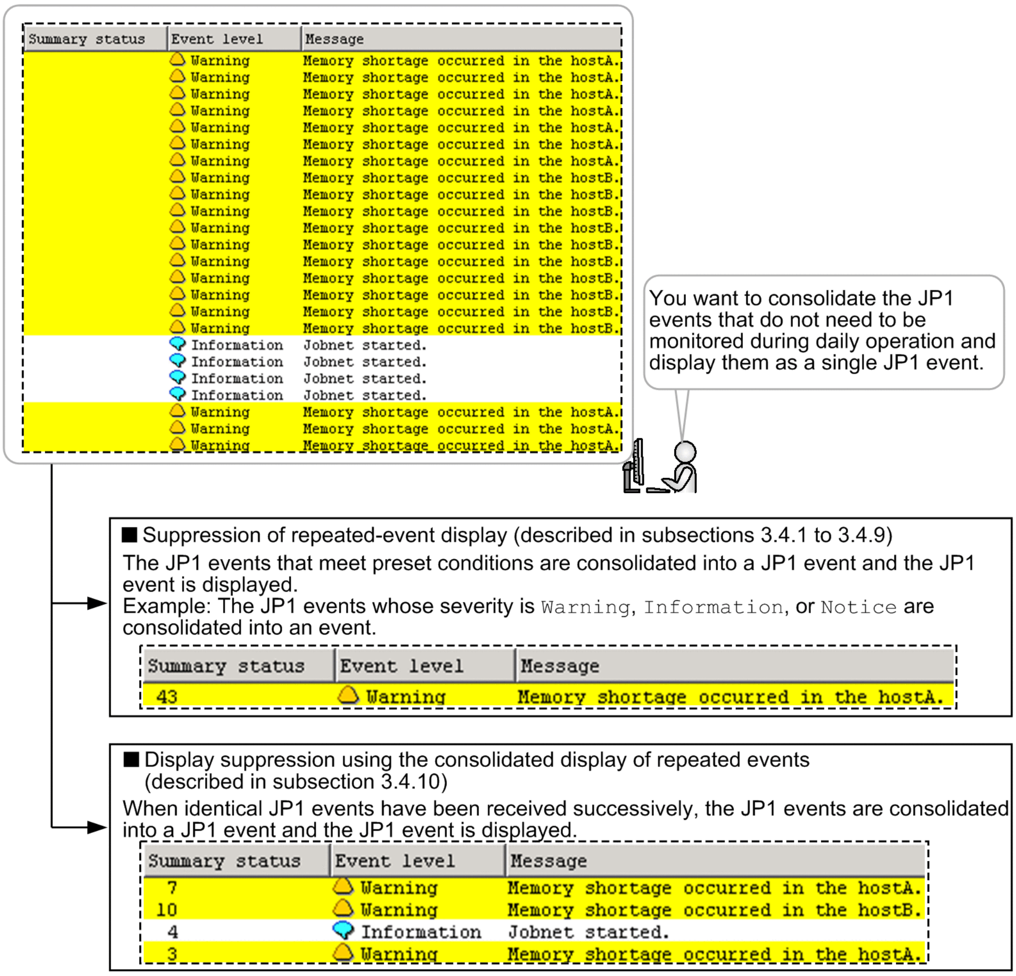
For details about the Related Events (Correlation) and Related Events (Correlation fails) windows, see *2.9 Related Events (Correlation) window* in the manual *JP1/Integrated Management - Manager GUI Reference*.

3.4 Suppressing display of repeated events

JP1/IM - Manager enables you to set JP1 event attributes and comparison keywords as repeated event conditions and consolidate the JP1 events that meet the repeated event conditions into consolidation events in JP1/IM - View. You can thus suppress the display of those individual JP1 events in the event list. This functionality is called the *suppression of repeated-event display*.

The following explanation focuses on an operation, during daily monitoring, to set repeated event conditions for the JP1 events that need not be monitored and display such events as a single consolidated JP1 event.

Figure 3–33: Displaying repeated events as a single consolidated JP1 event



Summary status	Event level	Message
	Warning	Memory shortage occurred in the hostA.
	Warning	Memory shortage occurred in the hostA.
	Warning	Memory shortage occurred in the hostA.
	Warning	Memory shortage occurred in the hostA.
	Warning	Memory shortage occurred in the hostA.
	Warning	Memory shortage occurred in the hostA.
	Warning	Memory shortage occurred in the hostA.
	Warning	Memory shortage occurred in the hostB.
	Warning	Memory shortage occurred in the hostB.
	Warning	Memory shortage occurred in the hostB.
	Warning	Memory shortage occurred in the hostB.
	Warning	Memory shortage occurred in the hostB.
	Warning	Memory shortage occurred in the hostB.
	Warning	Memory shortage occurred in the hostB.
	Warning	Memory shortage occurred in the hostB.
	Warning	Memory shortage occurred in the hostB.
	Warning	Memory shortage occurred in the hostB.
	Information	Jobnet started.
	Information	Jobnet started.
	Information	Jobnet started.
	Information	Jobnet started.
	Warning	Memory shortage occurred in the hostA.
	Warning	Memory shortage occurred in the hostA.
	Warning	Memory shortage occurred in the hostA.

You want to consolidate the JP1 events that do not need to be monitored during daily operation and display them as a single JP1 event.

■ Suppression of repeated-event display (described in subsections 3.4.1 to 3.4.9)
The JP1 events that meet preset conditions are consolidated into a JP1 event and the JP1 event is displayed.
Example: The JP1 events whose severity is `Warning`, `Information`, or `Notice` are consolidated into an event.

Summary status	Event level	Message
43	Warning	Memory shortage occurred in the hostA.

■ Display suppression using the consolidated display of repeated events
(described in subsection 3.4.10)
When identical JP1 events have been received successively, the JP1 events are consolidated into a JP1 event and the JP1 event is displayed.

Summary status	Event level	Message
7	Warning	Memory shortage occurred in the hostA.
10	Warning	Memory shortage occurred in the hostB.
4	Information	Jobnet started.
3	Warning	Memory shortage occurred in the hostA.

Repeated events, here, mean the JP1 events that meet set repeated event conditions, except for the case described in *3.4.10 Suppressing repeated-event display by the consolidated display of repeated events*.

Suppressing the display of repeated events requires the following preconditions to be met:

- The integrated monitoring database has been set up and enabled (by `jcoimdef -db ON`).
- The suppression of repeated-event monitoring has been enabled (by `jcoimdef -storm ON`).
- The repeated event condition to suppress the display of repeated events in the event list has been applied.

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

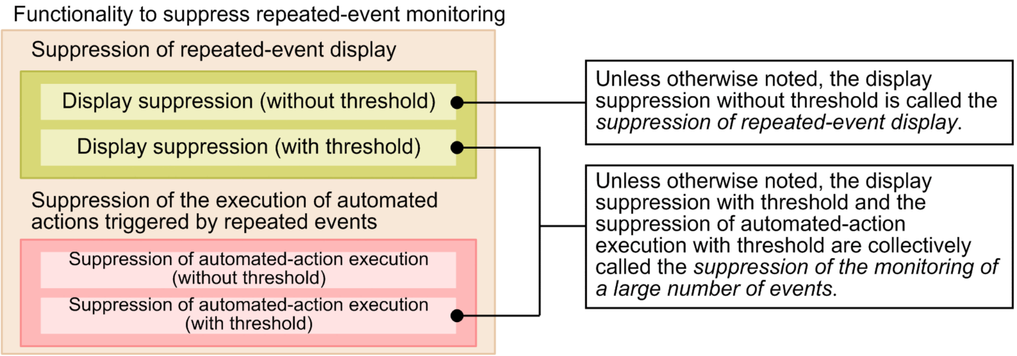
For details about how to apply repeated event conditions, see *2.19 List of Repeated Event Conditions window* in the manual *JP1/Integrated Management - Manager GUI Reference*.

Relationship between the suppression of repeated-event display and the repeated-event monitoring suppression function

The suppression of repeated-event display is part of the repeated-event monitoring suppression function.

The following figure shows the relationship between the repeated-event monitoring suppression function and the suppression of repeated-event display.

Figure 3–34: Relationship between the repeated-event monitoring suppression function and the suppression of repeated-event display


Functionality to suppress repeated-event monitoring
Suppression of repeated-event display
Display suppression (without threshold)
Display suppression (with threshold)
Suppression of the execution of automated actions triggered by repeated events
Suppression of automated-action execution (without threshold)
Suppression of automated-action execution (with threshold)
Unless otherwise noted, the display suppression without threshold is called the *suppression of repeated-event display*.
Unless otherwise noted, the display suppression with threshold and the suppression of automated-action execution with threshold are collectively called the *suppression of the monitoring of a large number of events*.

For details about the repeated-event monitoring suppression function, see *11.1.5 Considerations for suppressing the monitoring of repeated events and a large number of events*.

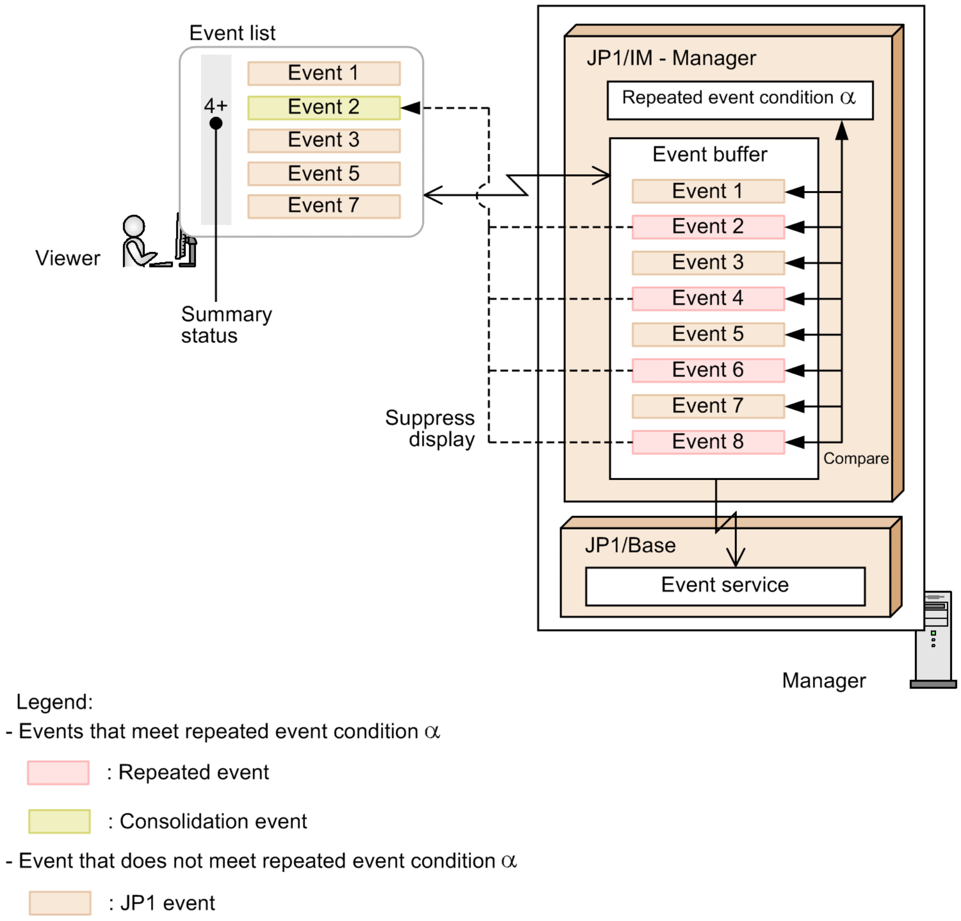
For details about how to enable the suppression of repeated-event monitoring, see *4.3 Setting monitoring of repeated events to be prevented* in the *JP1/Integrated Management - Manager Configuration Guide*.

3.4.1 Mechanism of the suppression of repeated-event display

The suppression of repeated-event display is performed by JP1/IM - Manager and JP1/IM - View. The suppression of repeated-event display enables you to consolidate, on JP1/IM - View, the monitored events that hinder event monitoring in order to suppress the display of those individual events in the event list. Display of dummy events cannot be suppressed.

JP1/IM - Manager acquires monitored events (that have passed through the event acquisition filter) from the event service, and then compares each monitored event with the repeated event condition set by the user. When a monitored event meets the repeated event condition, JP1/IM - Manager determines that *the acquired monitored event is a repeated event*. The events determined to be repeated events are consolidated on JP1/IM - View into a consolidation event, and are not individually displayed in the event list.

Figure 3–35: Mechanism of the suppression of repeated-event display



(1) Relationships among the suppression of repeated-event display, filters, and other functions

After filtering repeated events by a view or severe event filter, JP1/IM - View displays them as consolidation events on the **Monitor Events** or **Severe Events** page of its Event Console window.

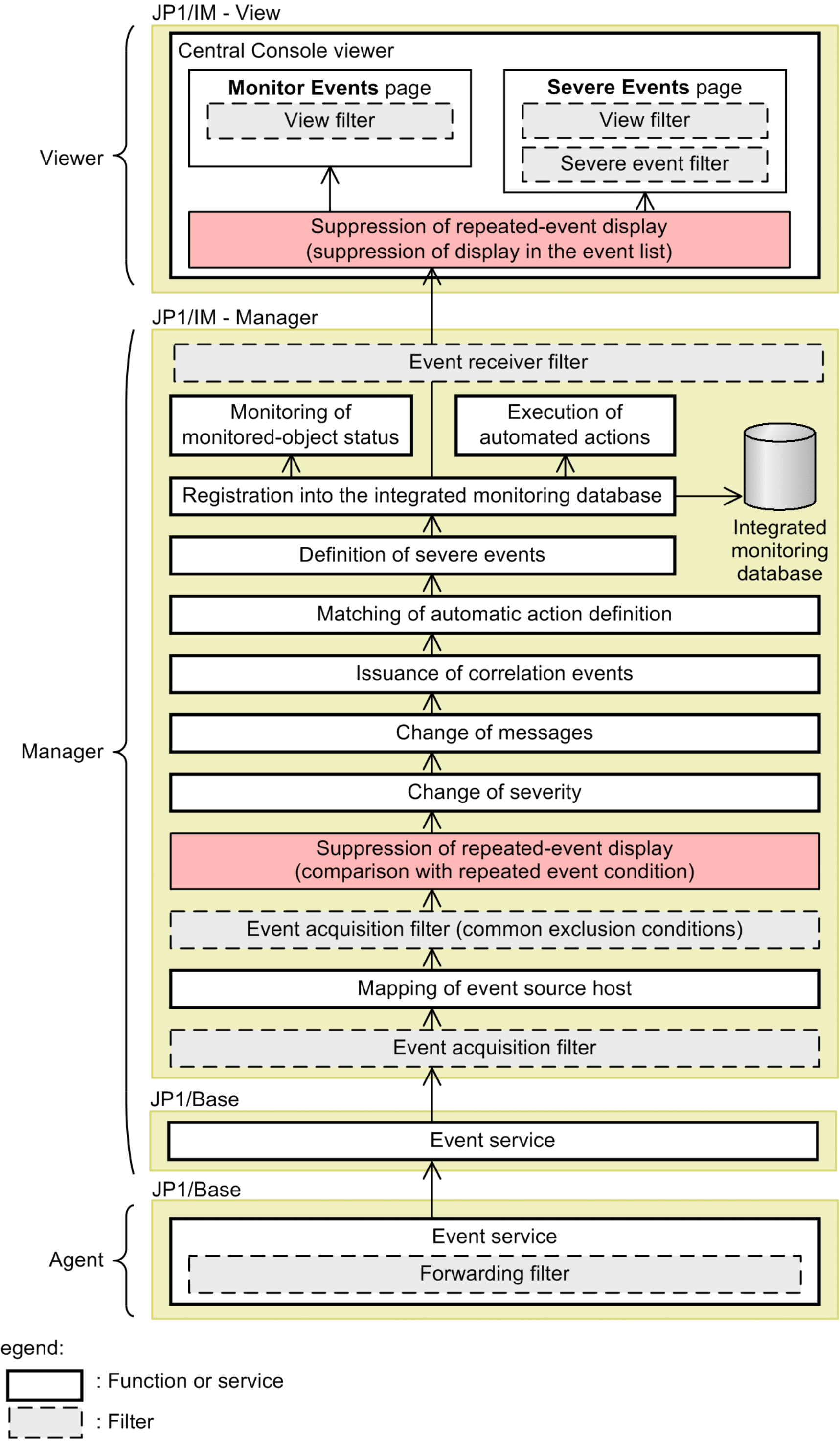
When the view filter is enabled, if the consolidation start event is filtered out by the view filter and not displayed in the Event Console window, no consolidation event is displayed.

When the restrictions on viewing and operating business groups are enabled, if the consolidation start event is not displayed on the Event Console window because of the restrictions, no consolidation event is displayed.

When the specification of event display period is enabled, the repeated events received within the specified period are displayed as consolidation events. When an event being consolidated exists outside the specified period, if JP1/IM - View receives a repeated event within the specified period, the event being consolidated outside the specified period becomes a consolidation completion event. Then, the newly received repeated event becomes a consolidation start event.

The following figure shows the relationships among the suppression of repeated-event display, JP1 event filters, and other functions.

Figure 3‒36: Relationships among the suppression of repeated-event display, filters, and other functions



JP1/IM - View
Viewer
Central Console viewer
Monitor Events page
View filter
Severe Events page
View filter
Severe event filter
Suppression of repeated-event display
(suppression of display in the event list)
JP1/IM - Manager
Manager
Event receiver filter
Monitoring of monitored-object status
Execution of automated actions
Registration into the integrated monitoring database
Integrated monitoring database
Definition of severe events
Matching of automatic action definition
Issuance of correlation events
Change of messages
Change of severity
Suppression of repeated-event display
(comparison with repeated event condition)
Event acquisition filter (common exclusion conditions)
Mapping of event source host
Event acquisition filter
JP1/Base
Event service
JP1/Base
Agent
Event service
Forwarding filter
Legend:
: Function or service
: Filter

3.4.2 Definitions of terms related to the suppression of repeated-event display

This subsection describes main terms, including *repeated start event* and *consolidation start event*, related to the suppression of repeated-event display.

repeated event

A repeated event is a JP1 event that meets a preset condition (repeated event condition). For details about repeated event conditions, see *3.4.3 Repeated event conditions*.

repeated start event

A repeated start event is the first repeated event that triggered the suppression of repeated-event display. For details about the trigger to start the suppression of repeated-event display, see *3.4.4 When suppression of repeated-event display starts*. For details about the trigger to end the suppression of repeated-event display, see *3.4.5 When suppression of repeated-event display ends*.

consolidation start event

A consolidation start event is the oldest repeated event among the events JP1/IM - View displays in the event list.

consolidation event

A consolidation event is a set of a consolidation start event and the events (repeated events meeting the repeated event condition that is met by the consolidation start event) consolidated into the consolidation start event. The event list shows only the information on the consolidation start event.

A *consolidation completion event* means a consolidation event for which the suppression of display has ended already. An *event being consolidated* means a consolidation event for which the suppression of display has not ended yet. The **Summary Status** column of the event list indicates the number of events consolidated into the consolidation event displayed in the event list.

3.4.3 Repeated event conditions

You can specify the event to be a target of display suppression by setting a combination of JP1 event attribute and comparison keyword as a condition. This condition is called a *repeated event condition*. You can set up to 2,500 repeated event conditions.

To set repeated event conditions, use the Repeated Event Condition Settings window and the List of Repeated Event Conditions window. The higher the repeated event condition appears in the List of Repeated Event Conditions window, the higher is its priority.

If you want to add JP1 events as targets of display suppression during system operation, you can add repeated event conditions based on the events displayed in the event list. A repeated event condition that is set based on events displayed in the event list is called an *additional repeated event condition*.

You can use an additional repeated event condition as a normal repeated event condition by changing its type setting in the List of Repeated Event Conditions window.

For details about how to set repeated event conditions and other procedures, see the following documentation:

- For details about how to set a repeated event condition:

  See *5.10.6 Specifying repeated event conditions* in the *JP1/Integrated Management - Manager Administration Guide*.

- For details about how to add a repeated event condition:

  See *5.10.4(1) Adding a repeated event condition based on an event that occurred during system operation* in the *JP1/Integrated Management - Manager Administration Guide*.

- For details about how to convert an added repeated event condition:

  See *5.10.4(3) Converting an added repeated event condition to a regular repeated event condition* in the *JP1/Integrated Management - Manager Administration Guide*.

(1) Setting items of repeated event condition (to suppress repeated-event display)

The following describes the settings for items of a repeated event condition:

- **Event conditions**

  You can specify the JP1 event attributes to be compared when JP1/IM - Manager acquires monitoring-target events.

  For details about the JP1 event attributes that can be specified, see *3.4.3(2) Event comparison attributes that can be specified in repeated event conditions*.

- **Suppression items**

  You can specify what to suppress for the JP1 events that meet the repeated event condition. The operations that can be suppressed are as follows:

  - Consolidated display of repeated events in the Event Console window
  - Execution of the actions that are triggered by repeated events

  To suppress the display of repeated events, you must specify appropriate settings for **Suppression items** so that repeated events will be displayed as consolidation events in the Event Console window. For details about the event list display during the suppression of repeated-event display, see *3.4.6 Event list display during the suppression of repeated-event display*. When you also want to suppress the execution of automated actions, see *3.5.8 Suppressing the execution of automated actions triggered by a large number of events*.

- **Conditions for same attribute values**

  You can specify whether to suppress the display of events that meet a repeated event condition by grouping them by attribute. The condition to suppress events while grouping them by attribute is called a *duplicate attribute value condition*.

  For details about the duplicate attribute value condition, see *3.4.3(3) Grouping repeated events by duplicate attribute value condition*.

- **Threshold**

  You can set a threshold for determining whether a large number of repeated events have occurred. The threshold, however, is not set in a repeated event condition for the normal suppression of repeated-event display because the suppression of display will start only after the set threshold is exceeded.

  For how the threshold is used, see *3.5.4 When the suppression of monitoring of a large number of events starts* and *3.5.5 When the suppression of monitoring of a large number of events ends*.

- **End monitoring period**

  You can set a period by which JP1/IM - Manager determines whether the suppression of repeated-event display can end. The usage of the end monitoring period varies depending on whether the threshold is set.

  The threshold is not set for the suppression of repeated-event display. Therefore, JP1/IM - Manager determines that the suppression of repeated-event display can end when no repeated event has occurred during the end monitoring period. The end monitoring period can be specified in the range from 1 to 86,400 seconds. The default is 300 seconds.

  For how the end monitoring period is used when the threshold is not set (in the case of the suppression of repeated-event display), see *3.4.5 When suppression of repeated-event display ends*.

  For how the end monitoring period is used when a threshold is set (for the suppression of monitoring of a large number of events), see *3.5.5 When the suppression of monitoring of a large number of events ends*.

- **Suppression start event** and **Suppression end event**

  You can specify whether to issue events that separately notify of the start and end of the suppression of repeated-event display. The event to notify of the start of display suppression is called the *suppression start event* (event ID: 00003F58). The event to notify of the end of display suppression is called the *suppression end event* (event ID: 00003F59). By default, neither notification event is issued. For details about the notification events, see *3.4.8 Issuing events associated with the suppression of repeated-event display*.

- **Checks for suppression to continue** and **Processing for when suppression continues**

  You can specify settings to check whether the suppression of repeated-event monitoring continues at intervals of specified time (in seconds) or at every specified number of events. Also, you can specify settings to issue a JP1 event that notifies of continuation or terminates the suppression when the suppression is determined to be continuing. For details, see *3.4.7 Issuing notifications when the suppression of repeated-event display continues*.

(2) Event comparison attributes that can be specified in repeated event conditions

The following table lists the JP1 event attributes and operators that can be specified as a repeated event condition.

Table 3–14: JP1 event attributes and operators

No.	Category	Attribute name	Specification	Operators	Operands
1	Basic attributes	Serial number (`B.SEQNO`)	N	--	--
2		Event ID (`B.ID`)	Y	• Match • Does not match	You can specify a maximum of 100 operands. Specify a hexadecimal value from 0 to 7FFFFFFF. Operands are not case sensitive.
3		Extended event ID (`B.IDEXT`)	N	--	--
4		Type (`B.TYPE`)	N	--	--
5		Registered reason (`B.REASON`)	Y	• Match • Does not match	You can specify a maximum of 100 operands. Specify a decimal value from -2147483648 to 2147483647.
6		Source process ID (`B.PROCESSID`)	Y		
7		Registered time (`B.TIME`)	Y	• Time range	Specify the start date and time and the end date and time of a range, or specify a period. A match occurs when the time value satisfies the condition *range-start-date-and-time* ≤ *time* ≤ *range-end-date-and-time*.
8		Arrived time (`B.ARRIVEDTIME`)	Y		
9		Source user ID (`B.USERID`)	Y	• Match • Does not match	You can specify a maximum of 100 operands. Specify a decimal value from -2147483648 to 2147483647.
10		Source group ID (`B.GROUPID`)	Y		
11		Source user name (`B.USERNAME`)	Y	• Match • First characters • Does not match • Is contained • Is not contained • Regular expression	You can specify a maximum of 100 operands. However, only a single operand can be specified when the operator is regular expression. Specify a string that does not contain control characters. Operands are case sensitive.
12		Source group name (`B.GROUPNAME`)	Y		

No.	Category	Attribute name	Specification	Operators	Operands
13		Event source server name (B.SOURCESERVER)	Y	• Match • First characters • Does not match • Is contained • Is not contained • Regular expression	You can specify a maximum of 100 operands. However, only a single operand can be specified when the operator is regular expression. Specify a string that does not contain control characters. If ON is specified in the -ignorecasehost option of the jcoimdef command, operands are not case sensitive. You can specify a business group.
14		Destination event server name (B.DESTSERVER)	N	--	--
15		Source IP address (B.SOURCEIPADDR)	Y	• Match • First characters • Does not match • Is contained • Is not contained • Regular expression	You can specify a maximum of 100 operands. However, only a single operand can be specified when the operator is regular expression. Specify a string that does not contain control characters. Operands are case sensitive. If the address is an IPv6 address, use lower-case alphabetic characters for the specification.
16		Destination IP address (B.DESTIPADDR)	N	--	--
17		Source serial number (B.SOURCESEQNO)	N	--	--
18		Code set (B.CODESET)	N	--	--
19		Message (B.MESSAGE)	Y	• Match • First characters • Does not match • Is contained • Is not contained • Regular expression	You can specify a maximum of 100 operands. However, only a single operand can be specified when the operator is regular expression. Specify a string that does not contain control characters. Operands are case sensitive.
20		Event details (B.DETAIL)	N	--	--
21	Extended attributes (common information)	Original severity level (E.SEVERITY)	Y	• Match • Attribute value specified • Attribute value not specified	You can specify multiple operands from among emergency, alert, critical, error, warning, notice, information, and debug.
22		User name (E.USER_NAME)	Y	• Match • First characters • Does not match • Is contained • Is not contained • Regular expression	You can specify a maximum of 100 operands. However, only a single operand can be specified when the operator is regular expression. Specify a string that does not contain control characters. Operands are case sensitive.
23		Product name (E.PRODUCT_NAME)	Y		
24		Object type (E.OBJECT_TYPE)	Y		

No.	Category	Attribute name	Specification	Operators	Operands
25		Object name (`E.OBJECT_NAME`)	Y		
26		Root object type (`E.ROOT_OBJECT_TYPE`)	Y		
27		Root object name (`E.ROOT_OBJECT_NAME`)	Y		
28		Object ID (`E.OBJECT_ID`)	Y		
29		Occurrence (`E.OCCURRENCE`)	Y		
30		Start time (`E.START_TIME`)	Y	• Time range • Match • First characters • Does not match • Is contained • Is not contained • Regular expression	• When the operator is time range: Specify the start date and time and the end date and time of a range, or specify a period. A match occurs when the time value satisfies the condition *range-start-date-and-time* ≤ *time* ≤ *range-end-date-and-time*. The attribute value is converted to a number of seconds (0 to 2,147,483,647) for the comparison. If the attribute value is outside this range, the condition does not match. • When the operator is not time range: You can specify a maximum of 100 operands. However, only a single operand can be specified when the operator is regular expression. Specify a string that does not contain control characters. Operands are case sensitive.
31		End time (`E.END_TIME`)	Y		
32		Result code (`E.RESULT_CODE`)	Y	• Match • First characters • Does not match • Is contained • Is not contained • Regular expression	You can specify a maximum of 100 operands. However, only a single operand can be specified when the operator is regular expression. Specify a string that does not contain control characters. Operands are case sensitive.
33		Event source host name (`E.JP1_SOURCEHOST`)	Y	• Match • First characters • Does not match • Is contained • Is not contained • Regular expression	You can specify a maximum of 100 operands. However, only a single operand can be specified when the operator is regular expression. Specify a string that does not contain control characters. Operands are case sensitive. You can specify a business group.
34	Extended attribute (user-specific information)	`E.`*xxxxxxx*	Y	• Match • First characters • Does not match • Is contained	You can specify a maximum of 100 operands. However, only a single operand can be specified when the operator is regular expression.

No.	Category	Attribute name	Specification	Operators	Operands
				- Is not contained - Regular expression	Specify a string that does not contain control characters. Operands are case sensitive. As the attribute name (XXXXXXX), you can specify a string of 32 or fewer bytes that begins with an upper-case alphabetic character and consists of upper-case alphabetic characters, numeric characters, and underbars (_).

Legend:

Y: Can be specified.

N: Cannot be specified.

--: None

(3) Grouping repeated events by duplicate attribute value condition

When you suppress repeated-event monitoring, you can suppress the events that match a repeated event condition by grouping the events according to attribute. This type of condition is called a *duplicate attribute value condition*.

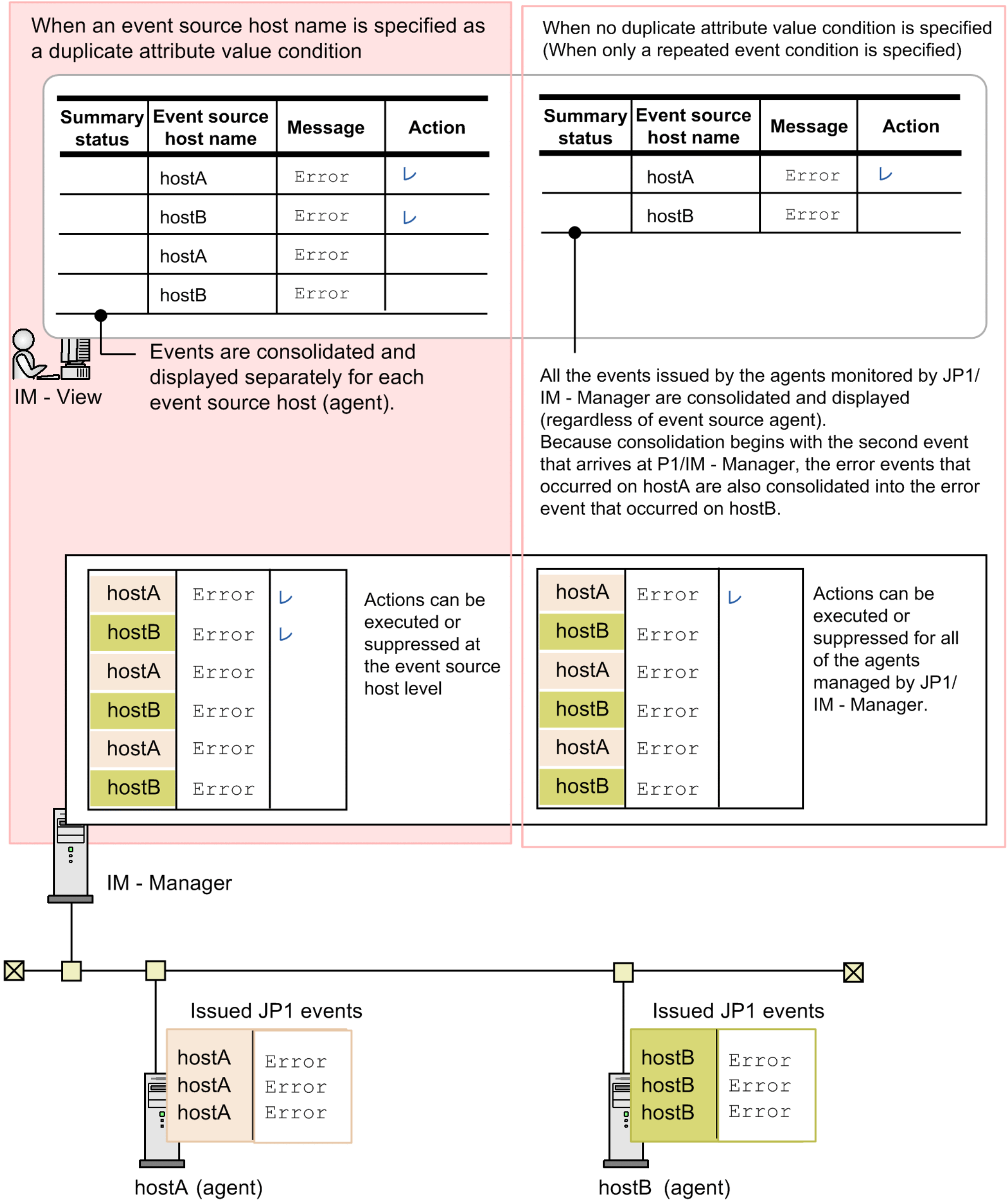
You can specify duplicate attribute value conditions for each repeated event condition on the **Options** page of the Repeated Event Condition Settings window. The maximum number of duplicate attribute value conditions you can specify for a repeated event is 3.

The following are the names of the attributes that can be specified in duplicate attribute value conditions: event source server name (`B.SOURCESERVER`), destination event server name (`B.DESTSERVER`), message (`B.MESSAGE`), event ID (`B.ID`), registered reason (`B.REASON`), source user ID (`B.USERID`), source group ID (`B.GROUPID`), source user name (`B.USERNAME`), source group name (`B.GROUPNAME`), event source host name (`E.JP1_SOURCEHOST`), and `E.`*xxxxxxx* (extended attribute, which relates to common or user-specific information). These attributes are case sensitive. However, if `ON` is specified in the `-ignorecasehost` option of the `jcoimdef` command, the event source server name (`B.SOURCESERVER`), destination event server name (`B.DESTSERVER`), and event source host name (`E.JP1_SOURCEHOST`) are not case sensitive.

Attribute values are compared for full matching. If repeated events do not have any attributes (that is, the attribute values are empty strings), the repeated events are grouped together as repeated events without attributes, and their monitoring is suppressed accordingly. If a repeated event does not have an attribute that is specified in a duplicate attribute value condition, the repeated event is treated as a repeated event without attributes.

Suppose, for example, that the repeated event condition is the "event whose **Message** value is `Error`." The following figure shows the difference in operation depending on whether an event source host name is specified as a duplicate attribute value condition.

Figure 3–37: Difference depending on whether a duplicate attribute value condition is specified



When an event source host name is specified as a duplicate attribute value condition
Summary status
Event source host name
Message
Action
hostA
Error
hostB
Error
hostA
Error
hostB
Error
Events are consolidated and displayed separately for each event source host (agent).
IM - View
When no duplicate attribute value condition is specified (When only a repeated event condition is specified)
All the events issued by the agents monitored by JP1/IM - Manager are consolidated and displayed (regardless of event source agent).
Because consolidation begins with the second event that arrives at P1/IM - Manager, the error events that occurred on hostA are also consolidated into the error event that occurred on hostB.
Actions can be executed or suppressed at the event source host level
Actions can be executed or suppressed for all of the agents managed by JP1/IM - Manager.
IM - Manager
Issued JP1 events
hostA (agent)
hostB (agent)

- When an event source host name is specified as a duplicate attribute value condition:

  When a duplicate attribute condition is specified, events can be monitored for each agent.

  First, the JP1 events issued by agents arrive at JP1/IM - Manager.

  When the execution of actions is suppressed, JP1/IM - Manager suppresses actions for the event whose **Message** value is `Error` (repeated event condition) and for the event source host name (duplicate attribute value condition). In the example shown in the above figure, an action is executed for the first error event that arrives from hostA and that arrives from hostB. For subsequent events that arrive, actions are suppressed.

  JP1/IM - View consolidates events at the event level for an event whose **Message** value is `Error` (repeated event condition) and at the event source host name level (duplicate attribute value condition), and displays consolidated events. In the example shown in the above figure, the first error event that arrives from hostA and that arrives from hostB is displayed. Subsequent events that arrive are consolidated separate into the error event on hostA and into the error event on hostB, and displayed.

- When no duplicate attribute value condition is specified:

  JP1/IM - Manager can monitor all of the events issued by the agents it monitors regardless of the event source agent.

First, the JP1 events issued by agents arrive at JP1/IM - Manager.

When the execution of actions is suppressed, JP1/IM - Manager suppresses actions for an event whose **Message** value is `Error` (repeated event condition). In the example shown in the above figure, an action is executed for the first error event that arrives. For subsequent events that arrive, actions are suppressed regardless of event source agent.

JP1/IM - View consolidates events at the event level for events whose **Message** value is `Error` (repeated event condition). In the example shown in the above figure, the first error event that arrives is displayed. Subsequent events that arrive are consolidated into the error event and displayed as consolidated events regardless of the event source agent.

3.4.4 When suppression of repeated-event display starts

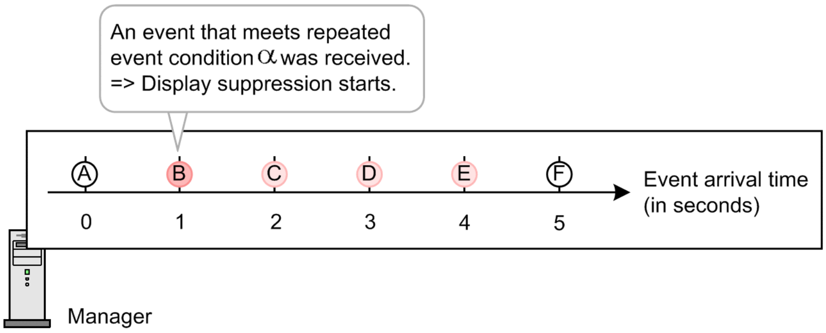
This subsection describes when JP1/IM - Manager starts suppressing the display of repeated events. The descriptions in this subsection apply to all types of suppression (including the suppression of automated-action execution) imposed on the repeated events that meet a repeated event condition specified without any threshold value set.

JP1/IM - Manager determines whether to start suppressing repeated-event display when it receives an event from the event service.

JP1/IM - Manager determines whether to start suppressing repeated-event display according to each repeated event condition.

The repeated event condition set for repeated-event display excludes threshold value setting. Therefore, after JP1/IM - Manager has started, JP1/IM - Manager starts suppressing repeated-event display when it receives, from the event service, an event that meets a repeated event condition. A maximum of 2,500 types of repeated events can be targets of display suppression.

Figure 3–38: Starting the suppression of repeated-event display


An event that meets repeated event condition α was received.
=> Display suppression starts.
A
B
C
D
E
F
0
1
2
3
4
5
Event arrival time (in seconds)
Manager

Legend:

- JP1 events that meet repeated event condition α

  ● : Repeated start event

  ○ : Repeated event

- JP1 event that does not meet repeated event condition α

  ○ : JP1 event

For the information that is displayed by JP1/IM - View when the suppression of repeated-event display starts, see *3.4.6 Event list display during the suppression of repeated-event display*.

3.4.5 When suppression of repeated-event display ends

This subsection describes when JP1/IM - Manager ends suppressing the display of repeated events. The descriptions in this subsection apply to all types of suppression (including the suppression of automated-action execution) imposed on the repeated events that meet a repeated event condition specified without any threshold value set.

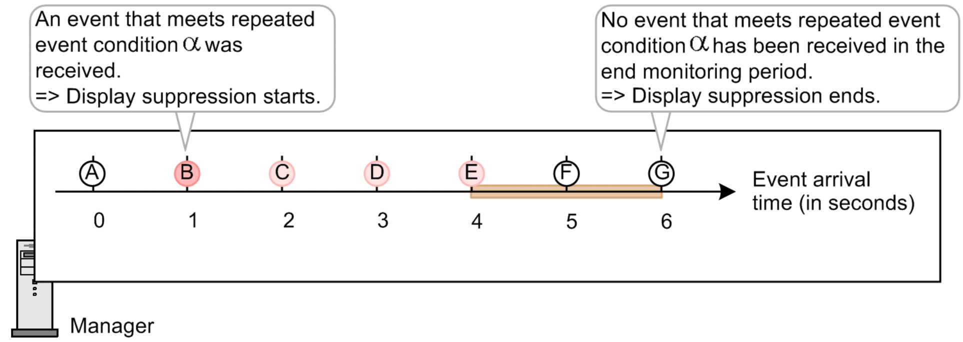
After a repeated event was determined as a target of display suppression, JP1/IM - Manager ends suppressing repeated-event display if it receives, from the event service, no suppression-target repeated event for a specified period (end monitoring period). The end monitoring period is specified on the **Options** page of the Repeated Event Condition Settings window.

JP1/IM - Manager determines whether to end suppressing repeated-event display when it receives an event from the event service.

JP1/IM - Manager determines whether to end suppressing repeated-event display according to each repeated event condition.

The following describes the operation in which JP1/IM - Manager does not receive any repeated event subject to display suppression from the event service for a specified period (end monitoring period) that is assumed to be 2 seconds.

Figure 3–39: Ending the suppression of repeated-event display


An event that meets repeated event condition α was received.
=> Display suppression starts.
No event that meets repeated event condition α has been received in the end monitoring period.
=> Display suppression ends.
A
B
C
D
E
F
G
0
1
2
3
4
5
6
Event arrival time (in seconds)
Manager

Legend:

🟧 : End monitoring period (2 seconds)

- JP1 events that meet repeated event condition α

● : Repeated start event

◌ : Repeated event

- JP1 event that does not meet repeated event condition α

○ : JP1 event

JP1/IM - Manager determines whether to end suppressing repeated-event display on the basis of the arrival time (`B.ARRIVEDTIME`) of the events acquired from the event service. JP1/IM - Manager ends display suppression when the arrival time of the latest event acquired from the event service satisfies the condition shown below.

- Condition for ending the suppression of repeated-event display

  Arrived-time-of-the-newly-acquired-event - *arrival-time-of-the-latest-repeated-event* ≥ *end-monitoring-time*

In the example shown in Figure 3-39, the above condition for ending the suppression of repeated-event display is satisfied first when event G is acquired.

- Condition for ending the suppression of repeated-event display (with reference to event G)

  Arrived time of event G (second 6) - arrival time of event E (second 4) ≥ 2 seconds

Therefore, JP1/IM - Manager ends suppressing repeated-event display when it receives event G.

For the information that is displayed by JP1/IM - View when the suppression of repeated-event display ends, see *3.4.6 Event list display during the suppression of repeated-event display*.

Other cases of ending display suppression than those in which no repeated event subject to display suppression has been acquired from the event service for a specified period (end monitoring period)

The suppression of repeated-event display ends also in the following cases:

- When JP1/IM - Manager stops

  If the suppression of repeated-event display ends because JP1/IM - Manager stops, no suppression end event is issued even when issuance of the notification of the end of display suppression has been set. For details about the suppression end event, see *3.4.8 Issuing events associated with the suppression of repeated-event display*.
- When a repeated event condition is changed or deleted

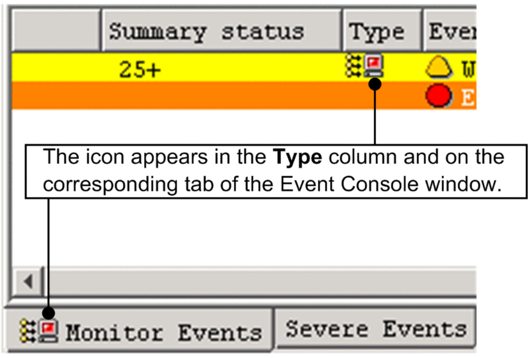
  In this case, JP1/IM - Manager ends suppressing the display of only the consolidation events that meet specific repeated event conditions. The specific repeated event conditions are those that were marked with the editing icon when they were updated in the List of Repeated Event Conditions window or those that have been deleted.

3.4.6 Event list display during the suppression of repeated-event display

When repeated-event display is suppressed, the repeated events that meet the same repeated event condition are displayed as a consolidation event in the event list of the Event Console window.

The number of repeated events that are consolidated into a consolidation event is indicated in the **Summary Status** column. When the event list includes at least a consolidation event, the icon indicating a large number of events have occurred, appears in the **Type** column and on the corresponding tab of the Event Console window.

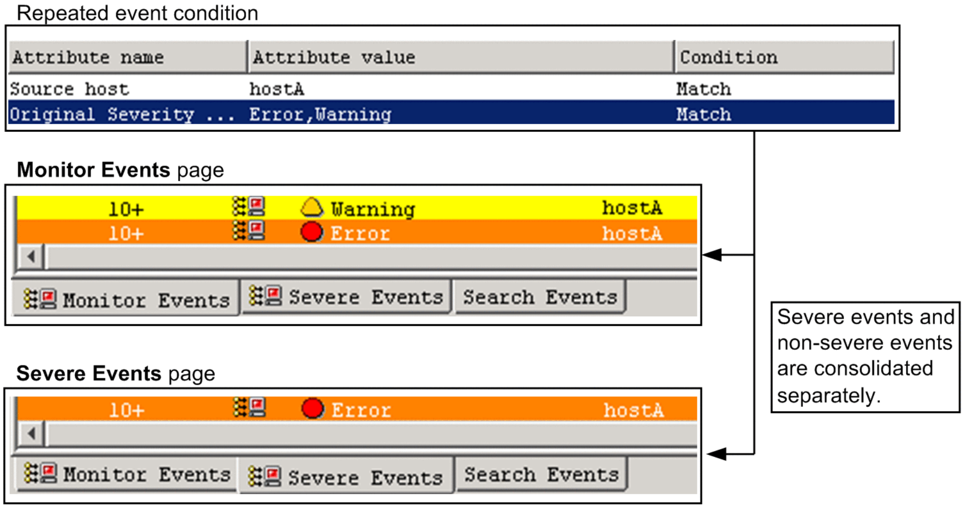
Figure 3–40: Icon display in the Type column and on the corresponding tab of the Event Console window



The icon appears in the **Type** column and on the corresponding tab of the Event Console window.

If the repeated events whose display is suppressed under the same repeated event condition include both severe events and non-severe events, the severe events and non-severe events are displayed as separate consolidation events.

Figure 3–41: Displaying consolidation events when repeated events include both severe events and non-severe events



Repeated event condition

Attribute name	Attribute value	Condition
Source host	hostA	Match
Original Severity ...	Error,Warning	Match

Monitor Events page

```
10+   Warning   hostA
10+   Error     hostA
```

Severe Events page

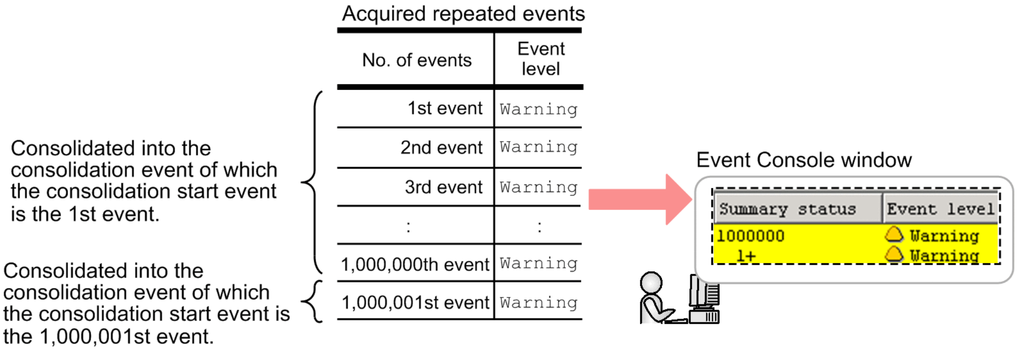
```
10+   Error     hostA
```

Severe events and non-severe events are consolidated separately.

(1) Maximum number of repeated events that can be consolidated into a consolidation event

A maximum of 1,000,000 repeated events can be consolidated into a single consolidation event. When the 1,000,001st repeated event arrives, the 1,000,001st repeated event is treated as a consolidation start event, and a new consolidation event appears in the event list.

Figure 3–42: Displaying a new consolidation event when the 1,000,001st repeated event arrives



Acquired repeated events

No. of events	Event level
1st event	Warning
2nd event	Warning
3rd event	Warning
:	:
1,000,000th event	Warning
1,000,001st event	Warning

Consolidated into the consolidation event of which the consolidation start event is the 1st event.

Consolidated into the consolidation event of which the consolidation start event is the 1,000,001st event.

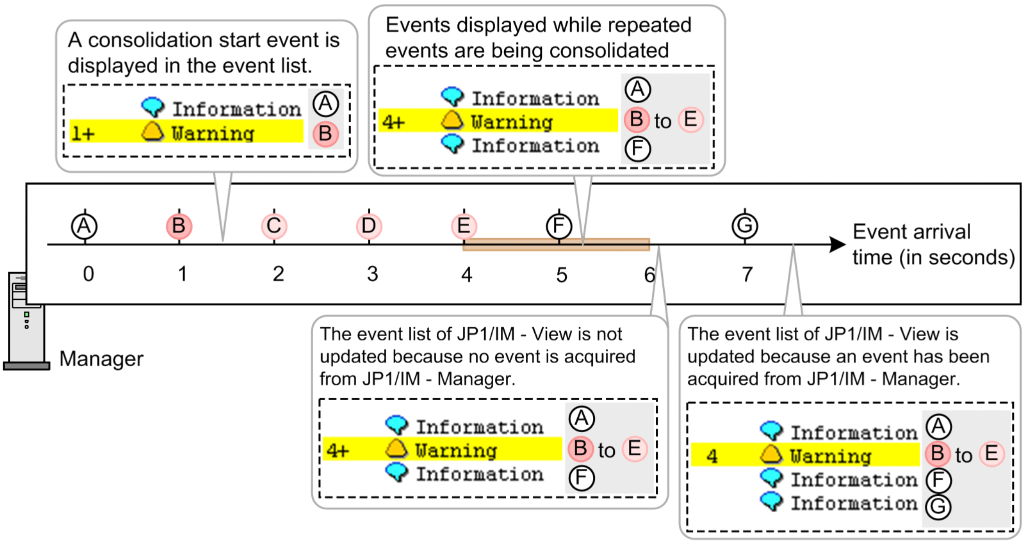
Event Console window

Summary status	Event level
1000000	Warning
1+	Warning

(2) When the number of events and the indication of + sign (shown or hidden) are updated in the Summary Status column

The **Summary Status** column for an event being consolidated displays the number of repeated events consolidated into the event and the + sign indicates that the suppression of repeated-event displays continues. These indications are updated when JP1/IM - View acquires an event from JP1/IM - Manager.

Figure 3–43: When the number of events and the indication of + sign (shown or hidden) are updated


A consolidation start event is displayed in the event list.
Information Ⓐ
1+ Warning Ⓑ
Events displayed while repeated events are being consolidated
Information Ⓐ
4+ Warning Ⓑ to Ⓔ
Information Ⓕ
Ⓐ Ⓑ Ⓒ Ⓓ Ⓔ Ⓕ Ⓖ
0 1 2 3 4 5 6 7
Event arrival time (in seconds)
Manager
The event list of JP1/IM - View is not updated because no event is acquired from JP1/IM - Manager.
Information Ⓐ
4+ Warning Ⓑ to Ⓔ
Information Ⓕ
The event list of JP1/IM - View is updated because an event has been acquired from JP1/IM - Manager.
Information Ⓐ
4 Warning Ⓑ to Ⓔ
Information Ⓕ
Information Ⓖ

Legend:

▨ : End monitoring period (2 seconds)

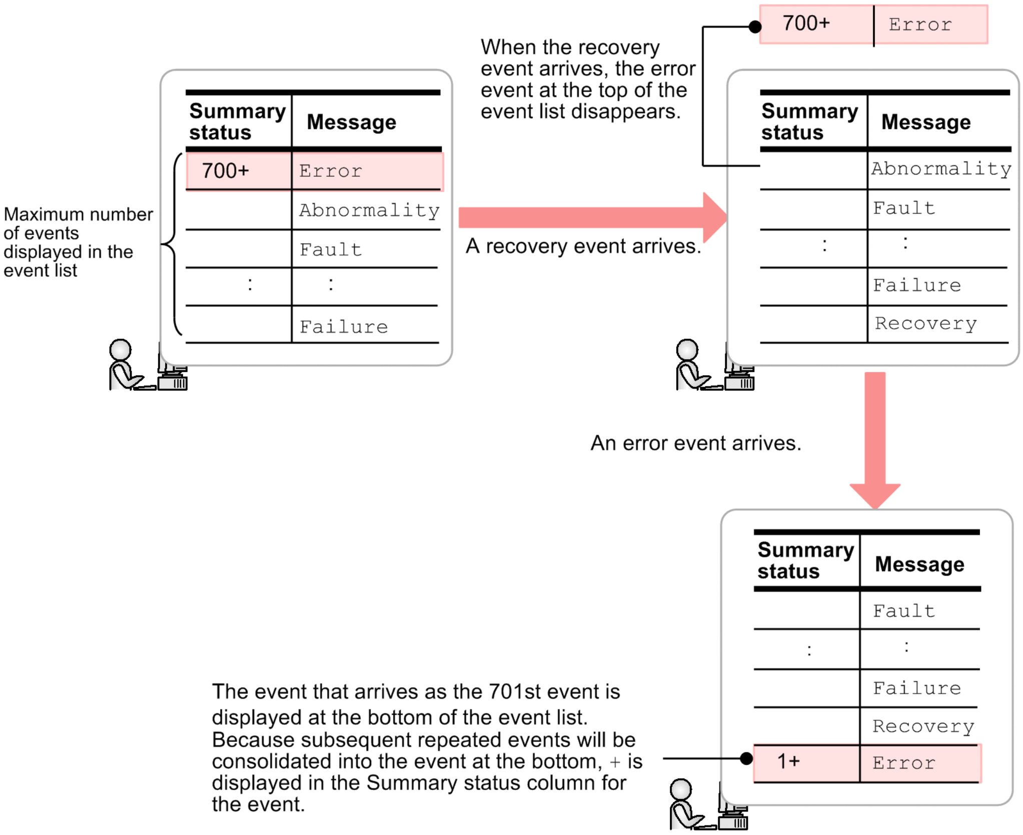
- JP1 events that meet repeated event condition α
  - ● : Repeated start event
  - ○ : Repeated event
- JP1 event that does not meet repeated event condition α
  - ○ : JP1 event

(3) How events are displayed when an event being consolidated disappears from the event list

The event list of the Event Console window can display a maximum of 2,000 events (maximum number of events stored in the scroll buffer). After the maximum number of events stored in the scroll buffer has been reached, the oldest event disappears from the event list each time a new event to be displayed in the event list arrives. The following describes how events are displayed after an event being consolidated disappears from the event list.

Assume that JP1/IM - View acquires a new event meeting the same repeated event condition applying to the event being consolidated that disappeared. JP1/IM - View treats the newly acquired event as a consolidation start event, and displays a new event being consolidated at the bottom of the event list.

Figure 3–44: How events are displayed when acquiring a new event meeting the same repeated event condition applying to the event being consolidated that disappeared


700+
Error
When the recovery event arrives, the error event at the top of the event list disappears.
Summary status
Message
700+
Error
Abnormality
Fault
:
:
Failure
Maximum number of events displayed in the event list
A recovery event arrives.
Summary status
Message
Abnormality
Fault
:
:
Failure
Recovery
An error event arrives.
Summary status
Message
Fault
:
:
Failure
Recovery
1+
Error
The event that arrives as the 701st event is displayed at the bottom of the event list. Because subsequent repeated events will be consolidated into the event at the bottom, + is displayed in the Summary status column for the event.

When a severe event is an event being consolidated

While repeated-event display is suppressed, severe events disappear from the **Severe Events** page of the Event Console window in the following order of priority:

1. The event among the following events that is displayed at the top of the event list on the **Severe Events** page of the Event Console window:

   - Processed events

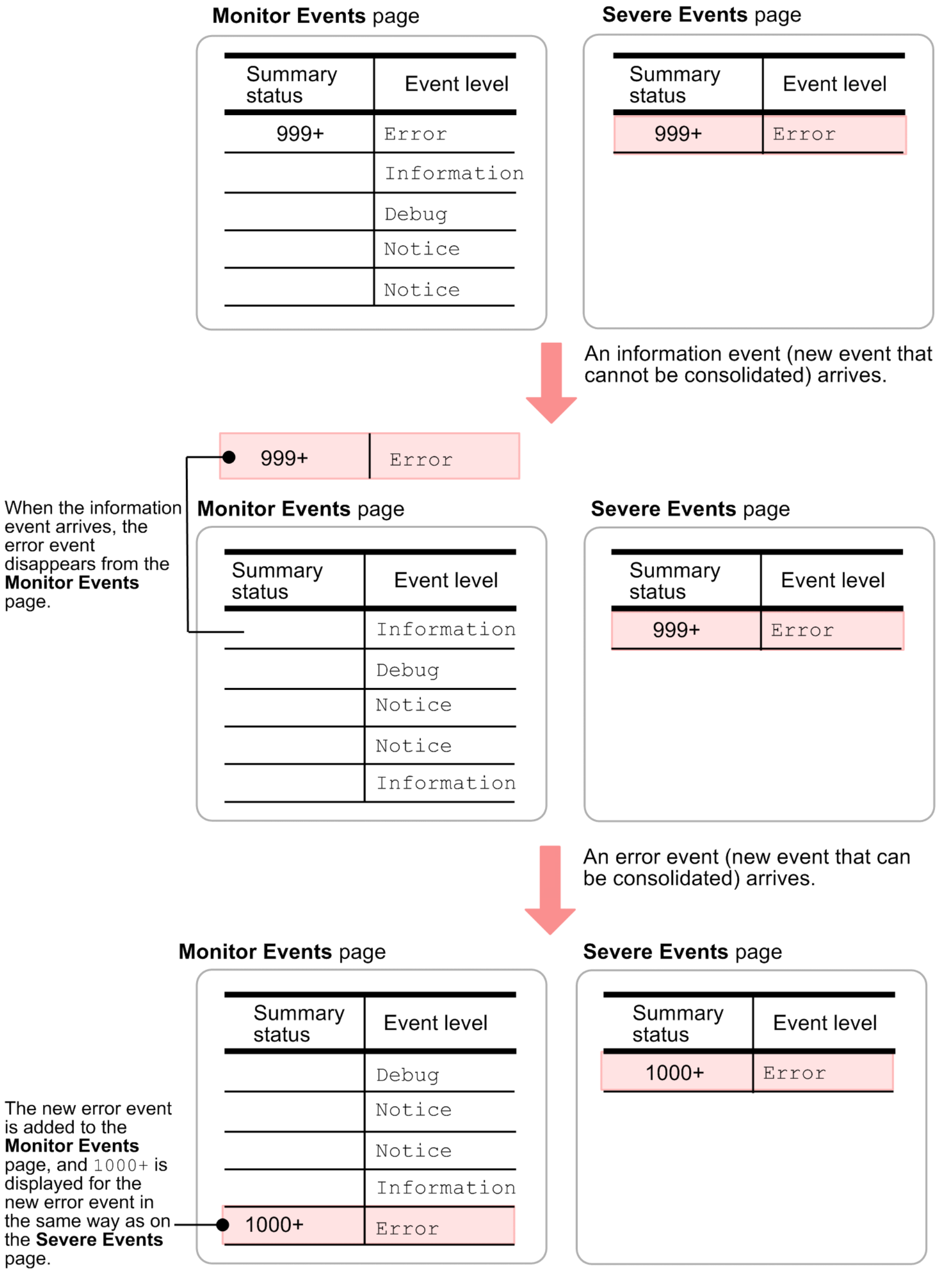
   - Consolidation events and consolidated repeated events among which the 1st (oldest) to 100th repeated events have all been processed (! is not displayed as the response status icon)

2. The event displayed at the top of the event list on the **Severe Events** page of the Event Console

When the same event being consolidated is displayed on both the **Monitor Events** and **Severe Events** pages, the **Summary status** indication for the event is the same on both pages.

Assume that a severe event being consolidated disappears from the **Monitor Events** page, and a new severe event meeting the same repeated event condition applying to the severe event being consolidated is acquired. The following figure shows how events are displayed on the **Monitor Events** and **Severe Events** pages in that case.

Figure 3–45: Display on the Monitor Events and Severe Events pages



Monitor Events page

Summary status	Event level
999+	Error
	Information
	Debug
	Notice
	Notice

Severe Events page

Summary status	Event level
999+	Error

An information event (new event that cannot be consolidated) arrives.

999+	Error

When the information event arrives, the error event disappears from the **Monitor Events** page.

Monitor Events page

Summary status	Event level
	Information
	Debug
	Notice
	Notice
	Information

Severe Events page

Summary status	Event level
999+	Error

An error event (new event that can be consolidated) arrives.

Monitor Events page

Summary status	Event level
	Debug
	Notice
	Notice
	Information
1000+	Error

Severe Events page

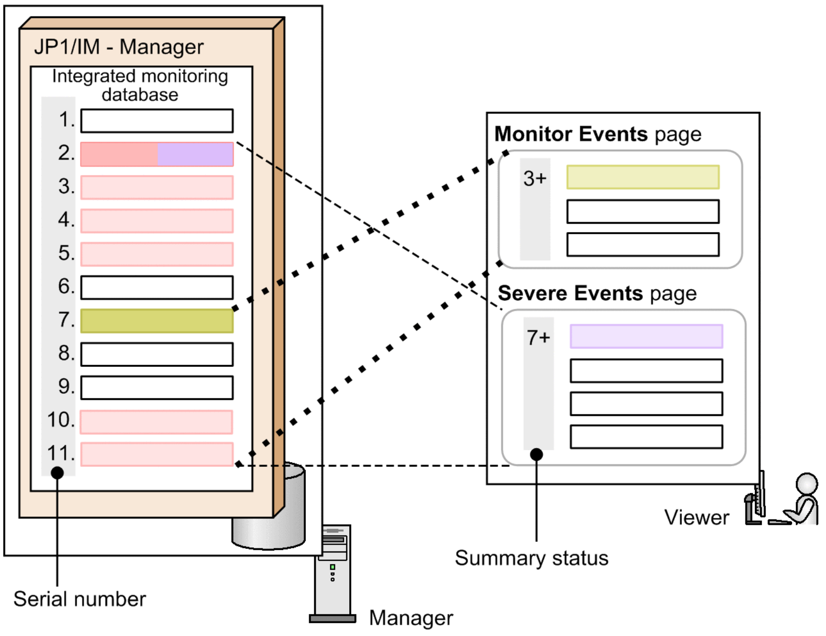
Summary status	Event level
1000+	Error

The new error event is added to the **Monitor Events** page, and `1000+` is displayed for the new error event in the same way as on the **Severe Events** page.

(4) How events are displayed if the information in the Summary Status column is different between the Monitor Events and Severe Events pages when the range of events to be collected at login is specified

When repeated-event display is suppressed, the same information is displayed, in principle, in the **Summary Status** column on the **Monitor Events** and **Severe Events** pages. When, however, the range of events to be collected at login is specified, the number of repeated events within the range might differ between the **Monitor Events** and **Severe Events** pages. If the number of repeated events within the range differs, the information in the **Summary Status** column is different between the **Monitor Events** and **Severe Events** pages.

Figure 3–46: Display on the Monitor Events and Severe Events pages (at login)



Legend:

- Events that meet repeated event condition α

🟥 : Repeated start event

▨ : Repeated event

🟩 : Consolidation start event (on the **Monitor Events** page)

🟨 : Consolidation event (on the **Monitor Events** page)

🟪 : Consolidation start event (on the **Severe Events** page)

▧ : Consolidation event (on the **Severe Events** page)

🟥🟪 : Event that is a repeated start event and also a consolidation start event (on the **Severe Events** page)

- Event that does not meet repeated event condition α

□ : JP1 event

In the example shown in the above figure, the range of events to be collected at login differs between the **Monitor Events** and **Severe Events** pages, and, therefore, different numbers are displayed in their **Summary Status** columns. Also the Related Events (Summary) window displays different information for the consolidation events displayed on the **Monitor Events** and **Severe Events** pages.

(5) How to check consolidated repeated events other than the consolidation start event

You can check individual repeated events consolidated into a consolidation event in the Related Events (Summary) window. You can check the repeated events that have disappeared from the event list of the Event Console window by using the event search function. You can check those repeated events also among past events that can be displayed by moving the slider in the **event display start-time specification area** of the Event Console window.

Checking the repeated events consolidated in a consolidation event

To open the Related Events (Summary) window, select a consolidation event on the **Monitor Events** or **Severe Events** page, right-click to open a pop-up menu, and then, from the pop-up menu, select **Display Related Event List**. The Related Events (Summary) window displays a maximum of 100 repeated events. The window does not display the 101st and subsequent repeated events.

To check the repeated events that are not displayed, search for those events and then check the **Search Events** page of the Event Console window. You can search for repeated events consolidated in a consolidation event by specifying the suppressed event ID (assigned to each consolidation event) as a search condition.

Note that, if the repeated events whose display is suppressed are correlation events and corresponding correlation source events are to be displayed, you need to open the Related Events (Correlation) window from the Related Events (Summary) window.

For details about how to check repeated events and consolidation events and change the response status, see *5.4.1 Checking detailed information about repeated events and changing the response status* in the *JP1/Integrated Management - Manager Administration Guide*.

Note

The Related Events window is available in the following two types:

- Window to display consolidation events: Related Events (Summary) window
- Window to display correlation source events: Related Events (Correlation) window

You can open either window by selecting an event in the Event Console window, and then, from the View menu or the pop-up menu that is displayed by right-clicking, select **Display Related Event List**. If, however, correlation events are consolidated for display, you can open only the Related Events (Summary) window from the Event Console window.

Checking the repeated events that have disappeared from the event list of the Event Console window

If you move the slider in the **event display start-time specification area** of the Event Console window, event consolidation is canceled.

Also, if you click the **Previous Event** button in the **event display start-time specification area** of the Event Console window, the event list displays the event that precedes the oldest event other than dummy events displayed in the event list. When the event list displays the preceding event, the consolidation events displayed in the event list are released from consolidation.

3.4.7 Issuing notifications when the suppression of repeated-event display continues

You can specify settings for **Notifications for when suppression continues** so as to check whether the suppression of repeated-event display continues at intervals of a specified time (number of seconds) or a specified number of events. When display suppression continues, a JP1 event can be issued to notify of the continuation of display suppression or display suppression can be terminated.

Notifications for when suppression continues is a setting item for repeated event conditions, which must be set for individual repeated event conditions. This subsection describes when to check whether display suppression continues.

Note that, if checking whether display suppression occurs concurrently with ending display suppression, ending display suppression takes priority.

Important

For illustrative purposes, given here is an example of checking whether the suppression of repeated-event display continues at short intervals. Note that, if you specify the checking (of whether the suppression of repeated-event display continues) at short intervals during actual system operation, a large number of notification events might be issued as a result of checking. Therefore, specify an appropriate interval of checking according to the system environment.

You can select time (number of seconds) or number of events as the unit of checking interval. The following describes the checking operations with respective units of interval selected:

- Checking at intervals of specified time (number of seconds)

  The first checking is performed when the condition shown below is satisfied by two repeated events that meet the same repeated event condition:

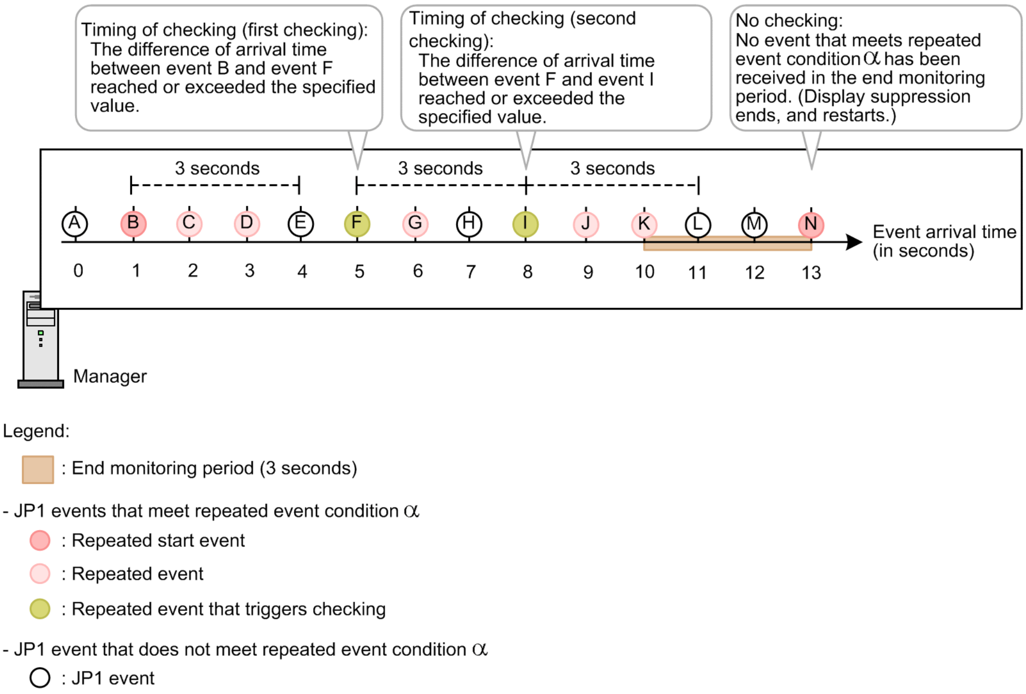
  Arrived-time-of-the-latest-repeated-event - *arrival-time-of-the-repeated-start-event* ≥ *specified-number-of-seconds*

  For the second and subsequent checkings, in the above condition, the reference event (*repeated start event*) is substituted by the event that triggered the preceding checking.

  The specifiable number of seconds ranges from 1 to 86,400 seconds.

  When you specify settings to check whether the suppression of repeated event continues at intervals of 3 seconds, the checking is performed as shown in the figure below. Note that, in this example, the end monitoring period is set to 3 seconds.

Figure 3–47: Checking whether suppression continues at intervals of specified time (number of seconds)



Timing of checking (first checking): The difference of arrival time between event B and event F reached or exceeded the specified value.
Timing of checking (second checking): The difference of arrival time between event F and event I reached or exceeded the specified value.
No checking: No event that meets repeated event condition α has been received in the end monitoring period. (Display suppression ends, and restarts.)
3 seconds
3 seconds
3 seconds
A B C D E F G H I J K L M N
0 1 2 3 4 5 6 7 8 9 10 11 12 13
Event arrival time (in seconds)
Manager
Legend:
: End monitoring period (3 seconds)
- JP1 events that meet repeated event condition α
: Repeated start event
: Repeated event
: Repeated event that triggers checking
- JP1 event that does not meet repeated event condition α
: JP1 event

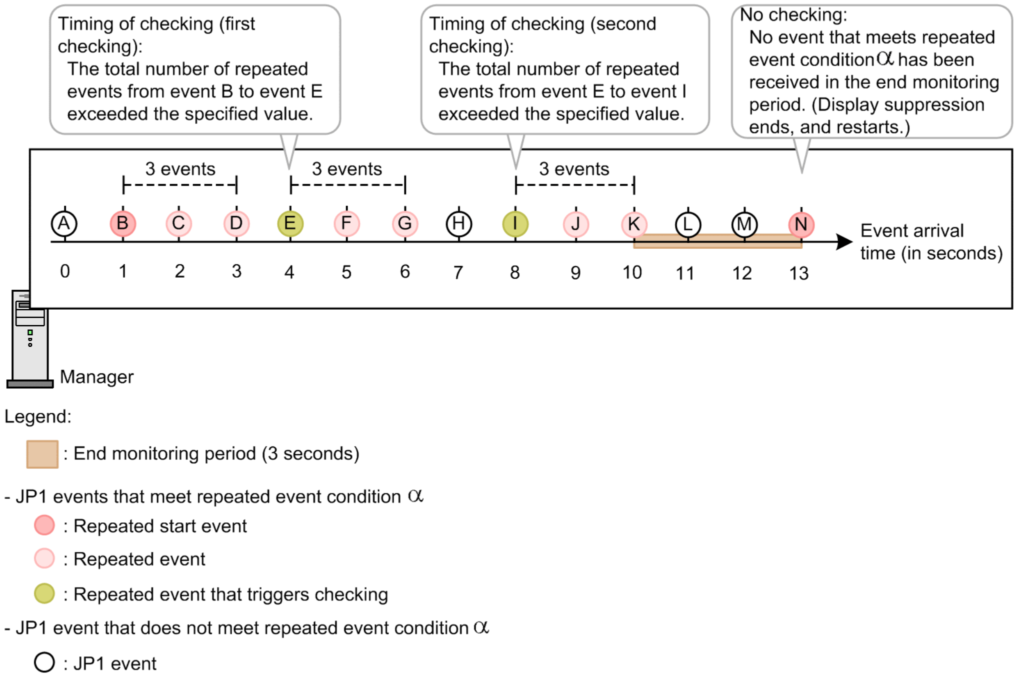
- Checking at intervals of a specified number of events

  The first checking is performed when the specified number of events is exceeded by the total number of the repeated events meeting the same repeated event condition. The repeated events are counted from the repeated start event up to the latest repeated event. For the second and subsequent checkings, in the above condition, the reference event (repeated start event) is substituted by the event that triggered the preceding checking.

  The specifiable number of events ranges from 1 to 1,000,000.

  When you specify settings to check whether the suppression of repeated event continues at intervals of 3 events, the checking is performed as shown in the figure below. Note that, in this example, the end monitoring period is set to 3 seconds.

Figure 3–48: Checking whether suppression continues at intervals of specified number of events


Timing of checking (first checking):
The total number of repeated events from event B to event E exceeded the specified value.
Timing of checking (second checking):
The total number of repeated events from event E to event I exceeded the specified value.
No checking:
No event that meets repeated event condition α has been received in the end monitoring period. (Display suppression ends, and restarts.)
3 events
3 events
3 events
A B C D E F G H I J K L M N
0 1 2 3 4 5 6 7 8 9 10 11 12 13
Event arrival time (in seconds)
Manager
Legend:
: End monitoring period (3 seconds)
- JP1 events that meet repeated event condition α
: Repeated start event
: Repeated event
: Repeated event that triggers checking
- JP1 event that does not meet repeated event condition α
: JP1 event

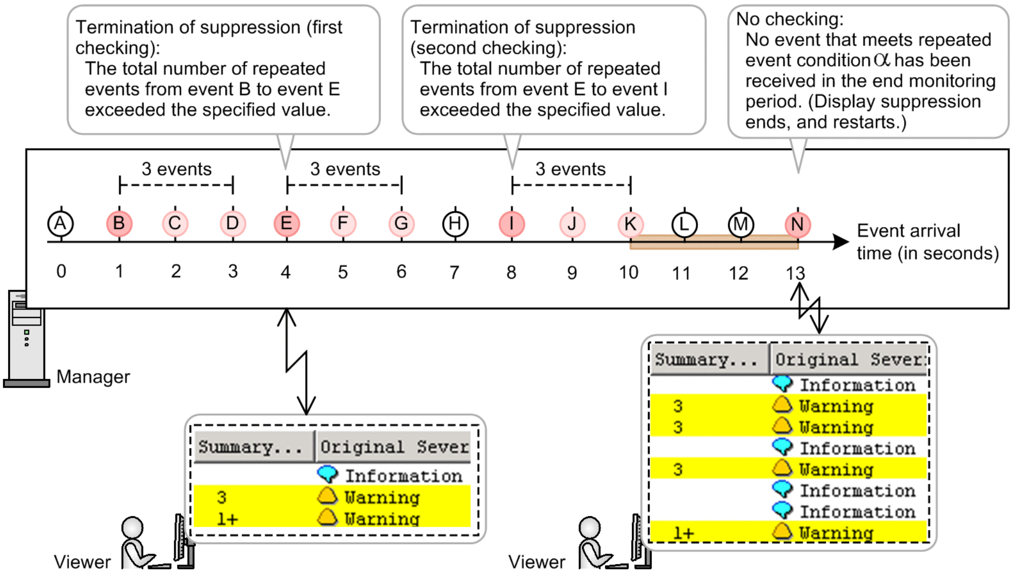
(1) Terminating suppression of repeated-event display

You can terminate the suppression of repeated-event display that has continued. Terminating display suppression enables you to consolidate repeated events in appropriate groups. Terminating display suppression also prevents the events being consolidated from being hidden among other events because, after display suppression is terminated, the event list periodically displays the events being consolidated. You cannot specify *terminating display suppression* and *issuing an event to notify of the continuation of display suppression* together in a repeated event condition.

After display suppression is terminated, the suppression of repeated-event display starts newly, assuming that the repeated start event is the event that triggered the preceding checking on whether display suppression continues.

When you specify settings to check whether the suppression of repeated event continues at intervals of 3 events and terminate the suppression if it continues, the checking is performed as shown in the figure below.

Figure 3–49: Terminating the suppression of repeated-event display


Termination of suppression (first checking):
The total number of repeated events from event B to event E exceeded the specified value.
Termination of suppression (second checking):
The total number of repeated events from event E to event I exceeded the specified value.
No checking:
No event that meets repeated event condition α has been received in the end monitoring period. (Display suppression ends, and restarts.)
3 events
3 events
3 events
A
B
C
D
E
F
G
H
I
J
K
L
M
N
0
1
2
3
4
5
6
7
8
9
10
11
12
13
Event arrival time (in seconds)
Manager
Summary...
Original Sever
Information
3
Warning
1+
Warning
Viewer
Summary...
Original Sever
Information
3
Warning
3
Warning
Information
3
Warning
Information
Information
1+
Warning
Viewer

Legend:

▨ : End monitoring period (3 seconds)

- JP1 events that meet repeated event condition α

● : Repeated start event

◌ : Repeated event

- JP1 event that does not meet repeated event condition α

○ : JP1 event

Note that an event to notify that suppression will be terminated (event ID: 00003F60) can be issued to notify that display suppression is terminated. For details, see *3.4.8 Issuing events associated with the suppression of repeated-event display*.

Note

When you specify *repeated events other than repeated start events* as action-suppressed events for a suppression item in the repeated event condition, an automated action will be executed only once every time display suppression is terminated. For details about the suppression of the execution of automated actions, see *3.5.8 Suppressing the execution of automated actions triggered by a large number of events*.

(2) Notifying of the continuation of the suppression of repeated-event display

An event to notify that suppression will continue (event ID: 00003F65) can be issued to notify that the suppression of repeated-event display continues. You cannot specify *terminating display suppression* and *issuing an event to notify of the continuation of display suppression* together in a repeated event condition. For details, see *3.4.8 Issuing events associated with the suppression of repeated-event display*.

3.4.8 Issuing events associated with the suppression of repeated-event display

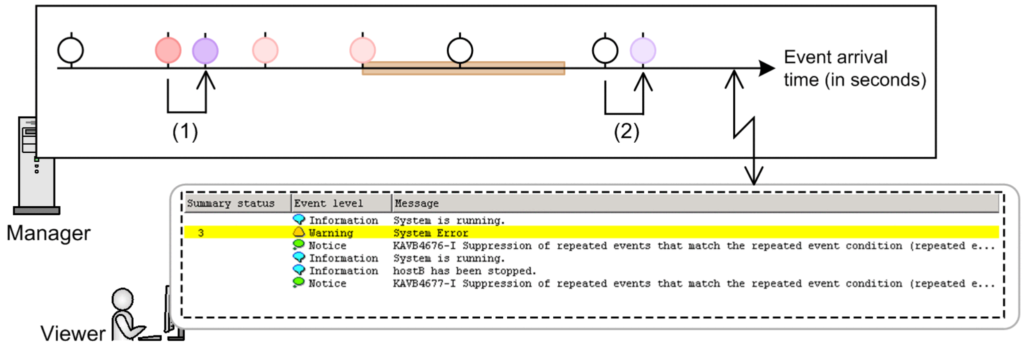
When the suppression of repeated-event display is used, various notifications can be issued. A suppression start event (event ID: 00003F58) can be issued to notify of the start of suppression, and a suppression end event (event ID:

00003F59) can be issued to notify of the end of suppression. After the check for whether the suppression of repeated-event display continues, an event to notify that suppression will continue (event ID: 00003F65) can be issued when display suppression continues. Also, an event to notify that suppression will be terminated (event ID: 00003F60) can be issued when display is terminated.

Specify whether to issue the individual events associated with the suppression of repeated-event display on the **Options** page of the Repeated Event Condition Settings window.

Figure 3-50 shows how the suppression start and suppression end events are issued. Figure 3-51 shows how the event to notify that suppression will continue and the event to notify that suppression will be terminated are issued. Note that the event to notify that suppression will continue and the event to notify that suppression will be terminated are issued in the same timing.

Figure 3–50: Issuing events (suppression start and suppression end events) associated with the suppression of repeated-event display



Summary status	Event level	Message
	Information	System is running.
3	Warning	System Error
	Notice	KAVB4676-I Suppression of repeated events that match the repeated event condition (repeated e...
	Information	System is running.
	Information	hostB has been stopped.
	Notice	KAVB4677-I Suppression of repeated events that match the repeated event condition (repeated e...

Legend:

▨ : End monitoring period

- JP1 events that meet repeated event condition α

● : Repeated start event

○ : Repeated event

- JP1 events that do not meet repeated event condition α

● : Suppression start event

○ : Suppression end event

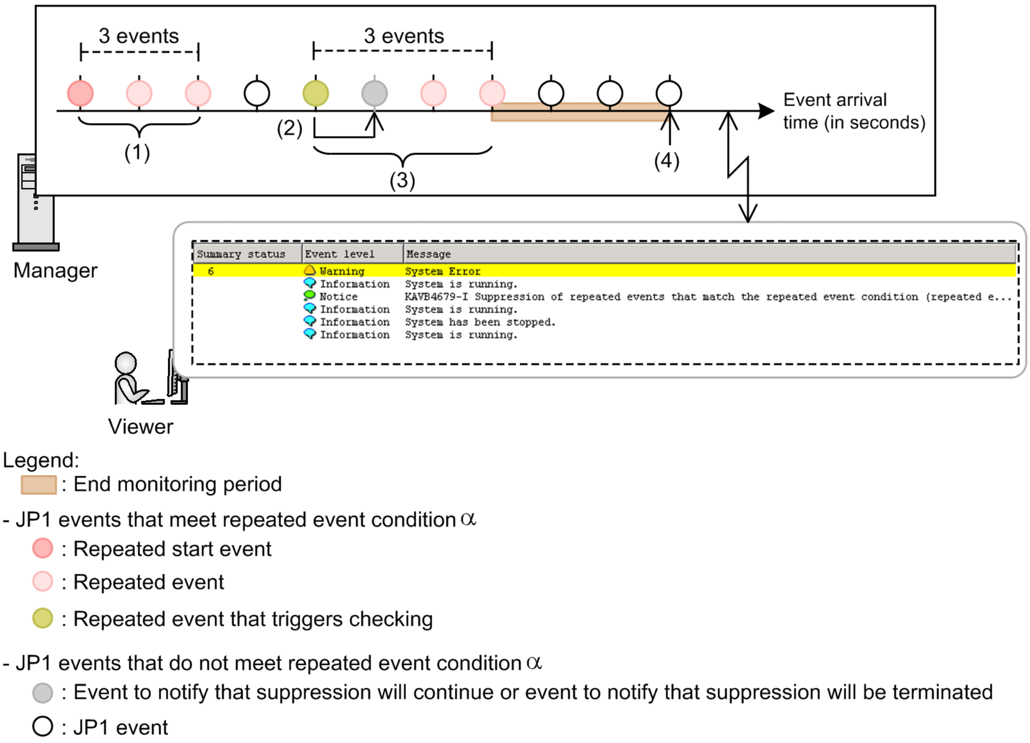
○ : JP1 event

The following describes how the suppression start and suppression end events are issued in sequence of the numbers in the figure (the numbers in the figure correspond to the numbers below).

1. The suppression start event is issued to notify of the start of suppression at the same time as the reception of a repeated start event from the event service.
2. The suppression end event is issued at the same time as the reception of an event (from the event service) whose arrival time exceeds the arrival time of the latest repeated event by at least the end monitoring period. The suppression end event notifies the end of suppression.

No suppression end event is issued when display suppression ends because JP1/IM - Manager is stopped or restarted.

Figure 3–51: Issuing events (to notify that suppression will continue and to notify that suppression will be terminated) associated with the suppression of repeated-event display


3 events
3 events
(1)
(2)
(3)
(4)
Event arrival time (in seconds)
Manager
Viewer
Legend:
: End monitoring period
- JP1 events that meet repeated event condition α
: Repeated start event
: Repeated event
: Repeated event that triggers checking
- JP1 events that do not meet repeated event condition α
: Event to notify that suppression will continue or event to notify that suppression will be terminated
: JP1 event

Summary status	Event level	Message
6	Warning	System Error
	Information	System is running.
	Notice	KAVB4679-I Suppression of repeated events that match the repeated event condition (repeated e...
	Information	System is running.
	Information	System has been stopped.
	Information	System is running.

The following describes how the event to notify that suppression will continue and the event to notify that suppression will be terminated are issued. The description follows the numbers in the figure (the numbers in the figure correspond to the numbers below). Assume that repeated event condition α specifying whether display suppression continues is to be checked at intervals of three events.

1. The manager has acquired three repeated events that meet repeated event condition α. Therefore, the manager determines that display suppression should continue when it acquires the next repeated event that meets repeated event condition α.
2. Because display suppression was determined to continue, the event to notify that suppression will continue or the event to notify that suppression will be terminated is issued according to the settings for **Processing for when suppression continues**.
3. The manager has acquired three repeated events (counted from the event that triggered the checking of the continuation of display suppression) that meet repeated event condition α. Therefore, the manager determines display suppression should continue when it acquires the next repeated event that meets repeated event condition α.
4. The manager has not acquired any repeated event that meets repeated event condition α within the end monitoring period. Therefore, neither suppression of the event to notify that suppression will continue, nor the event to notify that suppression will be terminated is issued.

3.4.9 Notes on suppression of repeated-event display

This subsection describes notes on the suppression of repeated-event display. The notes apply also to the suppression of monitoring of a large number of events.

- Suppression of repeated-event monitoring continues until an event satisfies the condition for determining that the occurrence of repeated events has ended. Accordingly, if no events have occurred since the start of suppression, the event list continues its consolidated display (the + mark indicates that events are being consolidated) even though a period of time greater that the end monitoring period has passed. Also, no suppression end event is issued even though a period of time greater than the end monitoring period has passed. For details, see *3.4.5 When suppression of repeated-event display ends*.

- When the setting for a repeated event condition is either changed or toggled between enable and disable, suppression of monitoring of corresponding repeated events terminates. If you want to forcibly terminate suppression of monitoring of specific repeated events, open the List of Repeated Event Conditions window, clear the **Apply** check box for the repeated event condition whose monitoring suppression is to be terminated, and then click the **Apply** button. If you want to forcibly terminate suppression of monitoring of specific repeated events and then suppress the monitoring again, clear the **Apply** check box for the repeated event condition, select the **Apply** check box again, and then click the **Apply** button.

  You can check the event condition corresponding to specific repeated events in the Related Events (Summary) window or Event Details window.

- When you specify the issuance of a suppression start or suppression end event, the suppression start or suppression end events will be issued in large numbers if many suppression-starting or suppression-ending operations are detected at a time. Specify the issuance of suppression start or suppression end event only for the repeated event conditions that require the specification.

3.4.10 Suppressing repeated-event display by the consolidated display of repeated events

JP1/IM - View has a function to display the successively received JP1 events that have identical content in a consolidated form. This function is called *consolidated display of repeated events*. You cannot use this function when the suppression of repeated-event monitoring is enabled.

The consolidated display of repeated events can be set up by individual users.

Definitions of terms related to the consolidated display of repeated events

Some of the terms related to the consolidated display of repeated events are defined below. Note that, although the terms defined below include those used for the suppression of repeated-event display, their meanings might be different.

consolidation start event

A consolidation start event is the first JP1 event JP1/IM - View receives among the JP1 events that have the same content.

repeated event

A repeated event is a JP1 event that is received in succession after a consolidation start event and has the same content as the consolidation start event.

consolidation event

A consolidation event is a consolidated group of a consolidation start event and repeated events. The consolidation event is classified into two types: *event being consolidated*, for which consolidation is being done, and *consolidation completion event*, for which consolidation has ended.

non-consolidation event

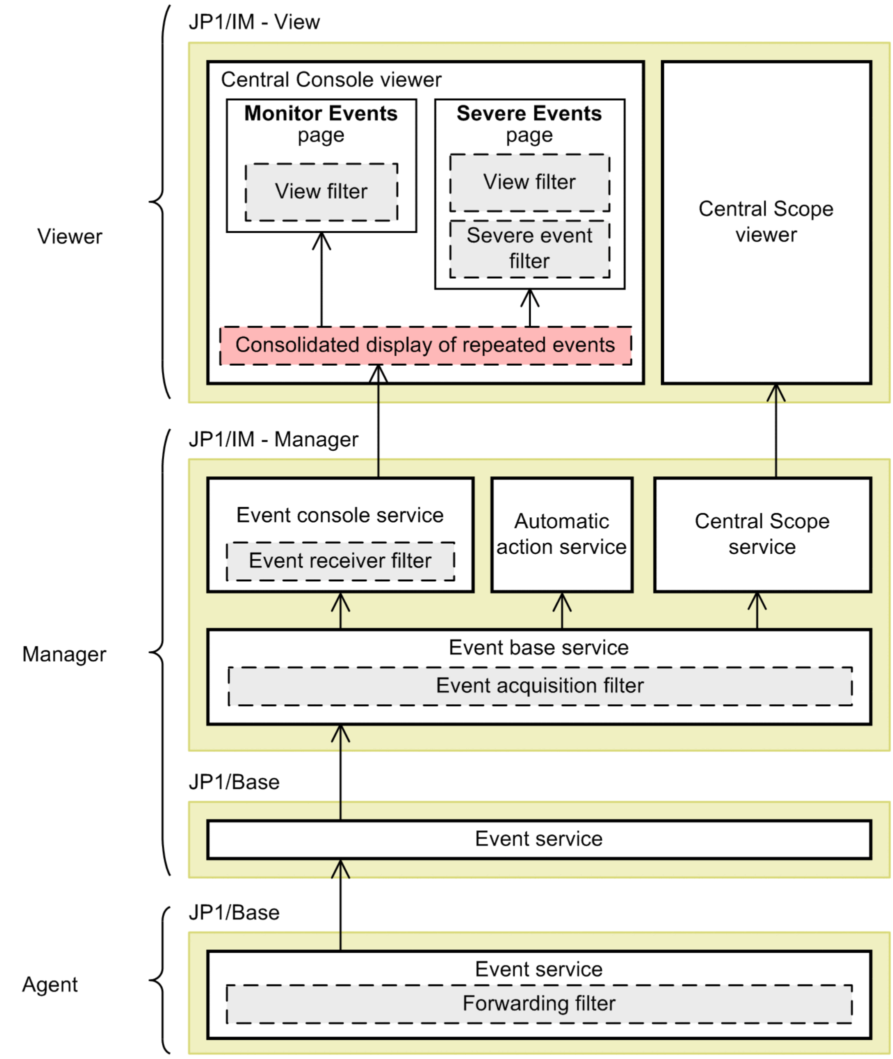
A non-consolidation event is an event into which no events are consolidated because it has no corresponding repeated events.

Relationships among consolidated display of repeated events, filters, and other functions

The consolidation event resulting from the repeated events passes through the view filter or severe events filter in JP1/IM - View and appears on the **Monitor Events** page or **Severe Events** page of the Event Console window.

The following figure shows the relationships between consolidated display of repeated events and each of the JP1 event filters.

Figure 3–52: Relationships between consolidated display of repeated events and JP1 event filters



Legend:

▭ : Service

▨ : Filter

(1) Differences between the consolidated display of repeated events and the suppression of repeated-event display

At one time, you can only enable either the consolidated display of repeated events or the suppression of repeated-event display. The following table lists the differences between the consolidated display of repeated events and the suppression of repeated-event display.

Table 3–15: Differences between the consolidated display of repeated events and the suppression of repeated-event display

Item	Consolidated display of repeated events	Suppression of repeated-event display
Consolidation target	JP1 events that have the same content as the latest event	JP1 events that meet the repeated event condition set by the user

Item	Consolidated display of repeated events	Suppression of repeated-event display
Suppression of automated action	Unsupported	Supported
Consolidation of non-successive JP1 events	Unsupported	Supported

(2) Conditions for starting event consolidation and ending event consolidation

JP1/IM - View performs event consolidation. The following describes the conditions for starting event consolidation and those for ending event consolidation:

Conditions for starting event consolidation

Before starting event consolidation, JP1/IM - View regards the latest JP1 event received from JP1/IM - Manager as a temporary consolidation event. If the next JP1 event received has the same content as the temporary consolidation start event, JP1/IM - View determines the next JP1 event as a repeated event to be consolidated into a consolidation event, and starts consolidation.

Conditions for ending event consolidation

Event consolidation ends when any of the following conditions is satisfied:

- The contents of the received JP1 event do not match the consolidation start event.
- The difference between the arrival times of the consolidation start event and received JP1 event exceeds the set timeout value.
- The number of repeated events exceeds the maximum repeat count (100).
- The user clicks the **OK** button in the Preferences window.
- The event being consolidated was not defined as a severe event, but becomes so due to a change in the severe event definition.
- The event being consolidated was defined as a severe event, but is no longer so due to a change in the severe event definition.

For details about the conditions for completing event consolidation, see *11.1.6 Considerations for consolidated display of repeated events*.

(3) Event comparison attributes

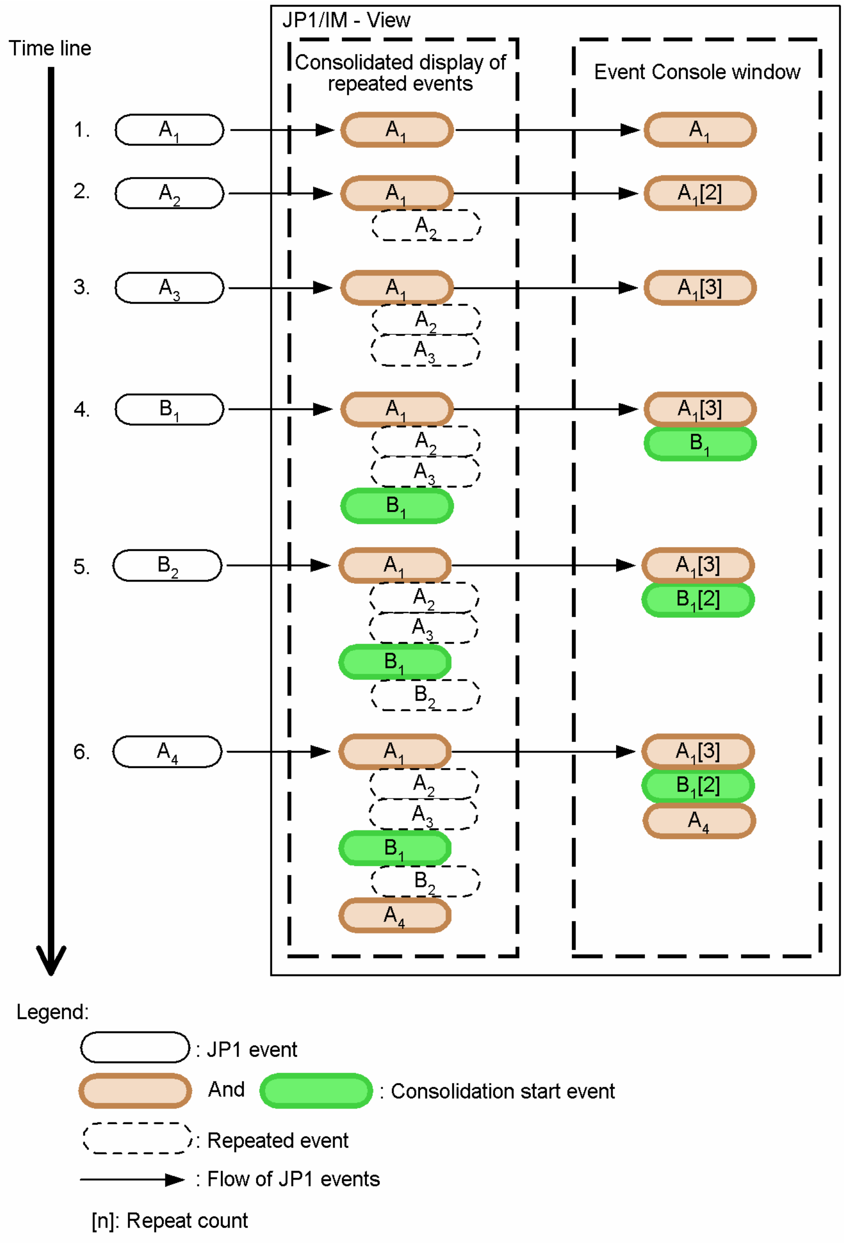
On receipt of a new JP1 event, JP1/IM - View compares its contents with the consolidation start event, based on the attribute values of the JP1 event. If all attribute values match, the new JP1 event is judged to have the same contents as the consolidation start event.

JP1 event attributes consist of the following detailed information: Source host, event level, object type, object name, root object type, root object name, occurrence, user name, message, product name, action, type, and event ID. You cannot compare event contents based on specific JP1 event attributes only. If mapping of the event source hosts is enabled, the event source host name is added as an attribute. If you changed the event level of a JP1 event using the function for changing the severity level, the new event level applies when the JP1 event contents are compared.

(4) Example of processing to consolidate repeated events

The following figure shows an example of consolidation processing of repeated events.

Figure 3–53: Consolidation processing of repeated events



The flow of processing described below, following the numbers in the figure:

1. JP1/IM - View receives JP1 event A_1 and begins consolidation. JP1 event A_1 becomes a consolidation start event. Information about consolidation start event A_1 appears in the Event Console window.
2. JP1/IM - View receives JP1 event A_2 and compares its contents with the consolidation start event A_1. Because A_2 and A_1 have identical contents, JP1 event A_2 is judged to be a repeated event and is aggregated into A_1. Information about consolidation start event A_1 and the repeat count (2) appears as A_1[2] in the Event Console window.
3. JP1/IM - View receives JP1 event A_3 and compares its contents with the consolidation start event A_1. Because A_3 and A_1 have identical contents, JP1 event A_3 is judged to be a repeated event and is aggregated into A_1. Information about consolidation start event A_1 and the repeat count (3) appears as A_1[3] in the Event Console window.

4. JP1/IM - View receives JP1 event B_1 and compares its contents with the consolidation start event A_1. Because B_1 and A_1 do not have identical contents, aggregation into consolidation start event A_1 ends and aggregation into JP1 event B_1 begins. Thus, B_1 becomes the current consolidation start event.

   Information about B_1 and the previous consolidation event A_1 appears in the Event Console window.

5. JP1/IM - View receives JP1 event B_2 and compares its contents with the consolidation start event B_1. Because B_2 and B_1 have identical contents, JP1 event B_2 is judged to be a repeated event and is aggregated into B_1.

   Information about B_1 and its repeat count (2), and about the previous consolidation event A_1, appears in the Event Console window. (The former appears as `B`$_1$`[2]`.)

6. JP1/IM - View receives JP1 event A_4 and compares its contents with the consolidation start event B_1. Because A_4 and B_1 do not have identical contents, aggregation into consolidation start event B_1 ends and aggregation into JP1 event A_4 begins. Aggregation into the earlier consolidation start event A_1 has already ended; therefore JP1 event A_4 cannot be aggregated into A_1. Thus, A_4 becomes the new consolidation start event.

   Information about the earlier event A_1, previous event B_1, and current consolidation event A_4 appears in the Event Console window.

3.5 Suppressing monitoring of a large number of events

If a large number of JP1 events occur and hinder normal monitoring of JP1 events, you can use the suppression of repeated-event monitoring by JP1/IM - Manager and the suppression of event forwarding by JP1/Base to resolve the problem.

If an event triggers occurrence of a large number of JP1 events, the JP1 events might fill the relevant event list and cause excessive commands (that are automatically executed as automated actions) to be executed. This would disable normal monitoring of JP1 events. The suppression of repeated-event monitoring provided by JP1/IM - Manager enables you to suppress the display of a large number of JP1 events in the event list and the execution of automated actions. The suppression of event forwarding provided by JP1/Base enables you to suppress event forwarding by executing a command on the host where a large number of events are occurring. This functionality is called the *suppression of monitoring of a large number of events*.

Suppressing the monitoring of a large number of events requires the following preconditions to be met:

- The integrated monitoring database has been set up and enabled (by `jcoimdef -db ON`).
- The suppression of repeated-event monitoring has been enabled (by `jcoimdef -storm ON`).
- The repeated event conditions to suppress the display of repeated events in the event list and the execution of automated actions have been applied.

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

For details about how to apply repeated event conditions, see *2.19 List of Repeated Event Conditions window* in the manual *JP1/Integrated Management - Manager GUI Reference*.

Suppressing the monitoring of a large number of events enables you to normally monitor the system even when a large number of JP1 events occur.

Repeated events, herein, means the JP1 events that meet a repeated event condition.

3.5.1 Mechanism of the suppression of monitoring of a large number of events

The suppression of monitoring of a large number of events is performed by JP1/IM - Manager, JP1/IM - View, and JP1/Base. The suppression of monitoring of a large number of events enables you to consolidate, on JP1/IM - View, the monitored events that hinder event monitoring in order to suppress the display of those individual events in the event list. The suppression of monitoring of a large number of events enables you also to suppress the execution of the automated actions that are triggered by those events. Monitoring of dummy events cannot be suppressed.

The following table describes the roles of JP1/IM - Manager, JP1/IM - View, and JP1/Base in the suppression of monitoring of a large number of events.

Table 3–16: Roles of individual products in the suppression of monitoring of a large number of events

Product name	Role of product
JP1/IM - Manager	• Determines whether the events acquired from the event service are the events that occur in large numbers. (Registration of a large

Product name	Role of product
	number of events in the event database of the manager cannot be prevented.) • Suppresses the execution of the automated actions that are triggered by a large number of events.
JP1/IM - View	• Suppresses the display of a large number of events.
JP1/Base	• Prevents a large number of events from being registered in the event database of the manager.

The following separately illustrates the roles of JP1/IM - Manager and JP1/Base in the mechanism of suppressing the monitoring of a large number of events:

Mechanism of suppressing the monitoring of a large number of events (JP1/IM - Manager)

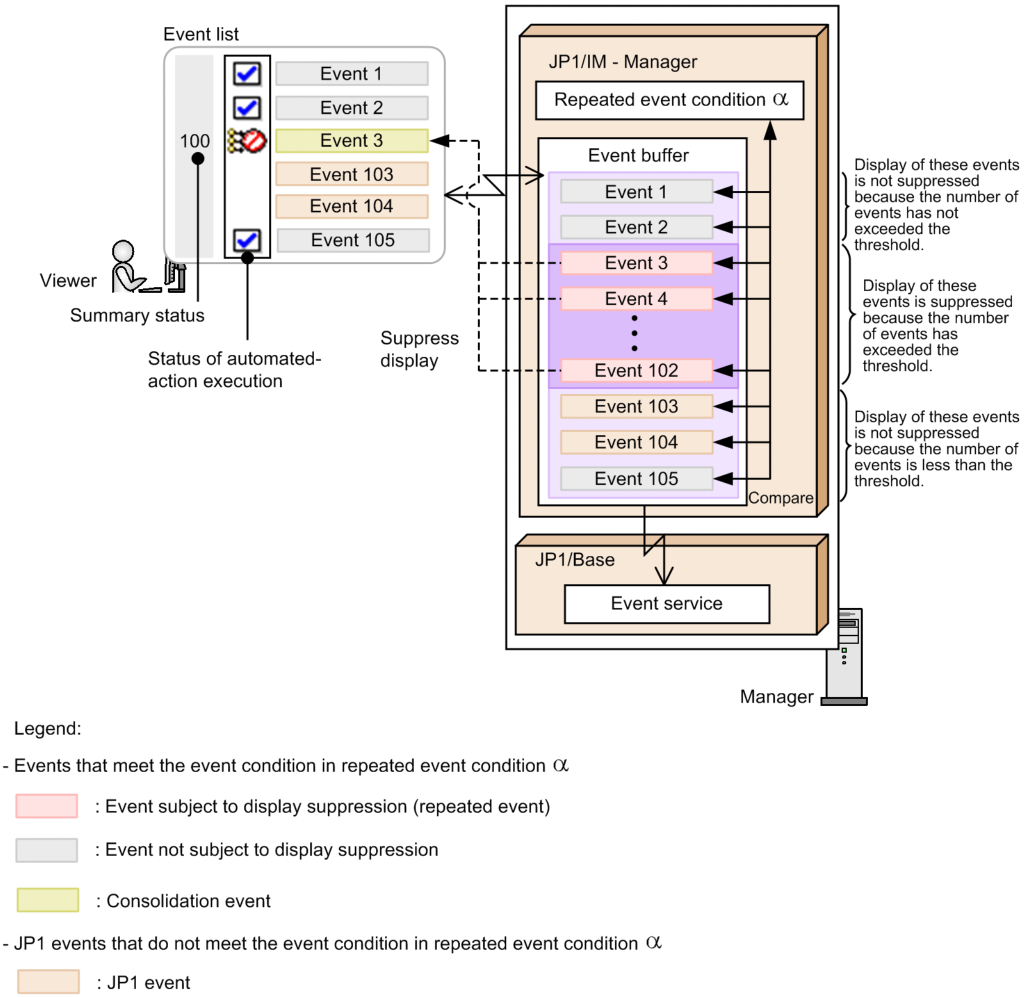
JP1/IM - Manager suppresses the monitoring of a large number of events by treating them as repeated events.

JP1/IM - Manager acquires monitoring-target events (that have passed through the event acquisition filter) from the event service, and then compares them with a repeated event condition set by the user. In the repeated event condition, the user must set the event condition to determine *whether to suppress events when they occur in large numbers* and the threshold for determining *whether the events have occurred in large numbers*.

When a monitoring-target event meets the following conditions, JP1/IM - Manager determines that the acquired monitoring-target event is *one of the events that have occurred in large numbers*, and suppresses its monitoring.

- The monitoring-target event meets the event condition set in the repeated event condition.
- The number of monitoring-targets that have occurred exceeds the set threshold.

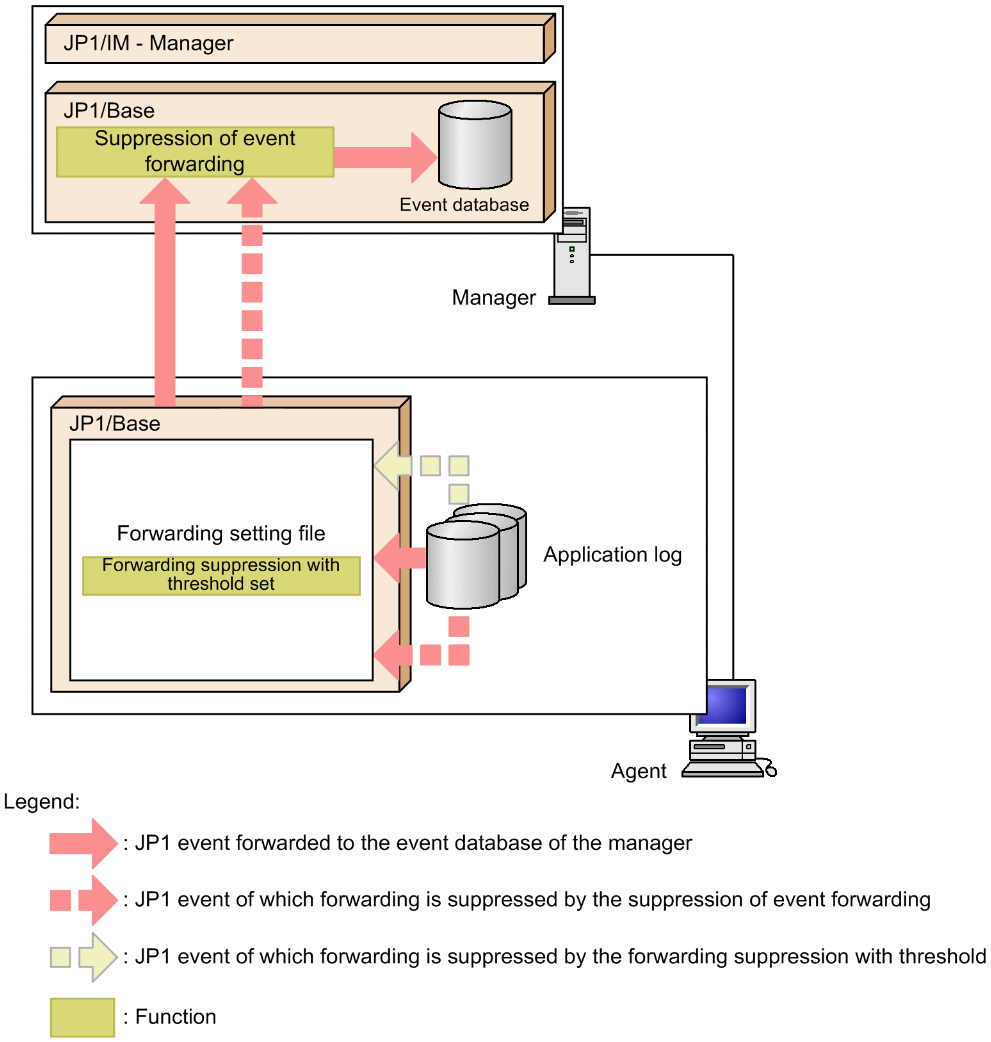
Figure 3–54: Mechanism of suppressing the monitoring of a large number of events (JP1/IM - Manager)


Event list
100
Event 1
Event 2
Event 3
Event 103
Event 104
Event 105
Viewer
Summary status
Status of automated-action execution
Suppress display
JP1/IM - Manager
Repeated event condition α
Event buffer
Event 1
Event 2
Event 3
Event 4
Event 102
Event 103
Event 104
Event 105
Compare
Display of these events is not suppressed because the number of events has not exceeded the threshold.
Display of these events is suppressed because the number of events has exceeded the threshold.
Display of these events is not suppressed because the number of events is less than the threshold.
JP1/Base
Event service
Manager
Legend:
- Events that meet the event condition in repeated event condition α
: Event subject to display suppression (repeated event)
: Event not subject to display suppression
: Consolidation event
- JP1 events that do not meet the event condition in repeated event condition α
: JP1 event

Mechanism of suppressing the monitoring of a large number of events (JP1/Base)

When a large number of JP1 events have occurred, JP1/Base suppresses the forwarding of the JP1 events to the manager by using the forwarding setting file (forwarding filter) for the relevant agent.

Figure 3–55: Mechanism of suppressing the monitoring of a large number of events (JP1/Base)


JP1/IM - Manager
JP1/Base
Suppression of event forwarding
Event database
Manager
JP1/Base
Forwarding setting file
Forwarding suppression with threshold set
Application log
Agent
Legend:
: JP1 event forwarded to the event database of the manager
: JP1 event of which forwarding is suppressed by the suppression of event forwarding
: JP1 event of which forwarding is suppressed by the forwarding suppression with threshold
: Function

The following table explains the differences between JP1/IM - Manager's repeated event monitoring suppression function and JP1/Base's event forwarding suppression function when a large number of JP1 events occur.

Table 3–17: Differences between the repeated event monitoring suppression function and the event forwarding suppression function

Comparison item	JP1/IM - Manager's repeated event monitoring suppression function	JP1/Base's event forwarding suppression function#
Handling of events	Events are consolidated by the manager.	Forwarding of events to the manager is suppressed.
Monitoring of events	Monitoring of events can be continued.	Events for an agent whose event forwarding was suppressed can no longer be monitored.
Suppressing monitoring of events that have occurred in large number (suppressing display of the events in the event list and suppressing execution of automated actions)	Monitoring can be suppressed.	Monitoring is not needed.
Load on network traffic and manager hosts	There are loads because events continue to be forwarded from agents.	There is no load because event forwarding from agents is suppressed.
Adding events to the manager host's event database	Added	Not added

#: When forwarding of JP1 events is suppressed, the manager can no longer check important events that are issued by a corresponding agent and that might need to be monitored. To check events that occurred while forwarding was suppressed, you must use JP1/IM - View to search the corresponding agent's event database. For details, see *3.6 Searching for events*.

Also, consider the settings for the JP1 events that will be transferred from JP1/Base to the manager and the manager's JP1 event filtering settings. For details about settings for the JP1 events that are transferred by JP1/Base, see *11.1.2 Considerations for forwarding JP1 events to managers*. For details about the filtering settings on a manager, see *11.1.3 Considerations for filtering JP1 events*.

(1) Relationships among the suppression of monitoring of a large number of events, filters, and other functions

After receiving a large number of events, JP1/IM - View filters them by its view or severe events filter, and then displays them as consolidation events on the **Monitor Events** or **Severe Events** page of its Event Console window. When the large number of events JP1/IM - Manager received are to trigger automated actions, JP1/IM - Manager suppress the execution of the automated actions according to the corresponding repeated event condition.

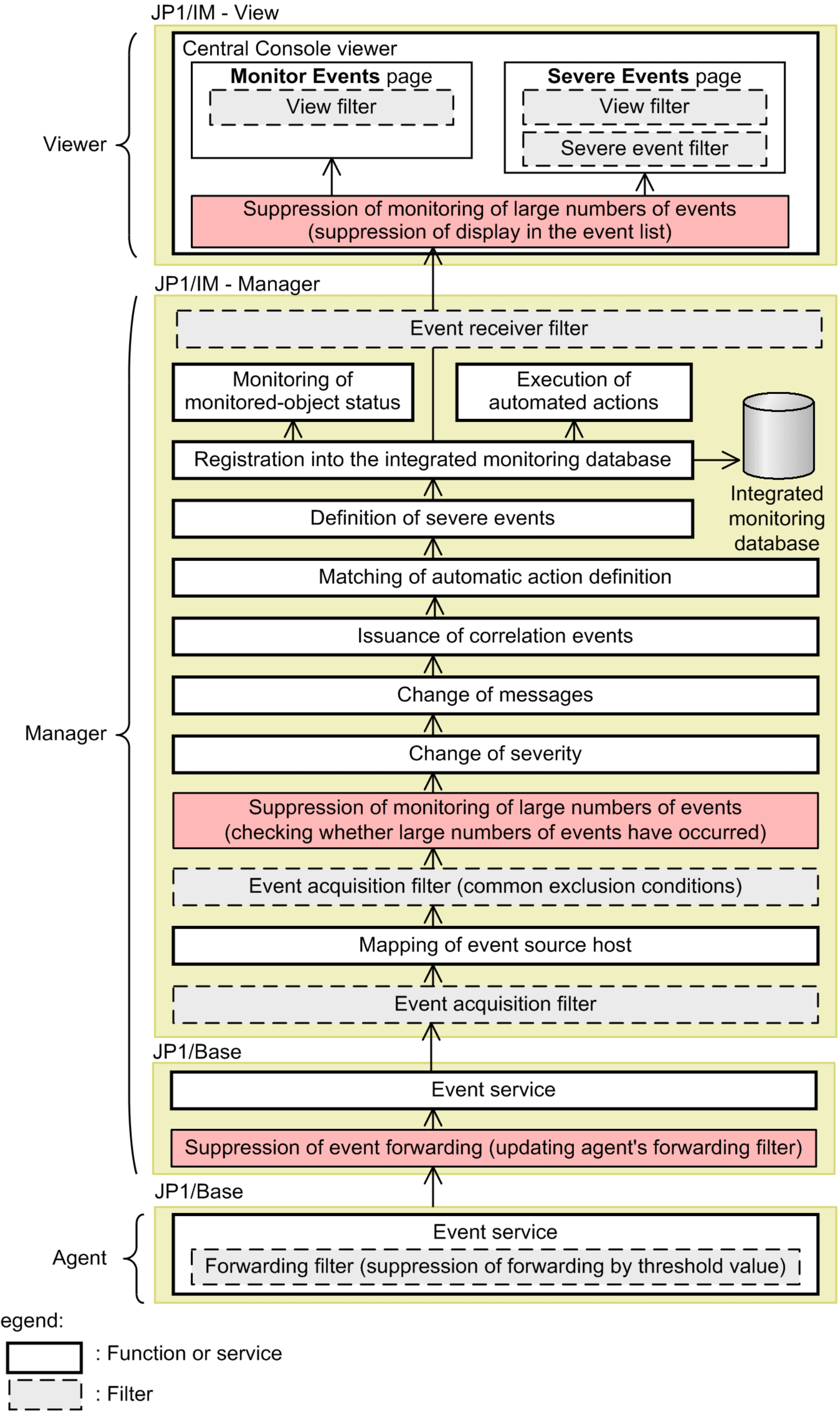
When the view filter is enabled, if the consolidation start event is filtered out by the view filter and not displayed in the Event Console window, no consolidation event is displayed.

When the restrictions on viewing and operating business groups are enabled, if the consolidation start event is not displayed on the Event Console window because of the restrictions, no consolidation event is displayed.

When the specification of event display period is enabled, the repeated events received within the specified period are displayed as consolidation events. If JP1/IM - View retains an event being consolidated outside the specified period and receives a repeated event within the specified period, the event being consolidated outside the specified period becomes a consolidation completion event. Then, the newly received repeated event becomes a consolidation start event.

The following figure shows the relationships among the suppression of monitoring of a large number of events, JP1 event filters, and other functions.

Figure 3–56: Relationships among the suppression of monitoring of a large number of events, JP1 event filters, and other functions


JP1/IM - View
Viewer
Central Console viewer
Monitor Events page
View filter
Severe Events page
View filter
Severe event filter
Suppression of monitoring of large numbers of events (suppression of display in the event list)
JP1/IM - Manager
Event receiver filter
Monitoring of monitored-object status
Execution of automated actions
Registration into the integrated monitoring database
Integrated monitoring database
Definition of severe events
Matching of automatic action definition
Issuance of correlation events
Change of messages
Manager
Change of severity
Suppression of monitoring of large numbers of events (checking whether large numbers of events have occurred)
Event acquisition filter (common exclusion conditions)
Mapping of event source host
Event acquisition filter
JP1/Base
Event service
Suppression of event forwarding (updating agent's forwarding filter)
JP1/Base
Agent
Event service
Forwarding filter (suppression of forwarding by threshold value)
Legend:
: Function or service
: Filter

3.5.2 Definitions of terms related to the suppression of monitoring of a large number of events

This subsection describes the main terms, including *repeated start event* and *suppression of event forwarding*, related to the suppression of monitoring of a large number of events.

Terms related to JP1/IM - Manager:

large number of events

A large number of events are those events among the JP1 events that meet a preset condition (repeated event condition) which occurred in large numbers, exceeding the preset threshold. For details about the repeated event condition, see *3.5.3 Repeated event condition for the suppression of monitoring of a large number of events*.

repeated start event

A repeated start event is that event received first among a large number of events that triggered the suppression of monitoring of that large number of events. For details about the trigger to start the suppression of monitoring of a large number of events, see *3.5.4 When the suppression of monitoring of a large number of events starts*. For details about the trigger to end the suppression of monitoring of a large number of events, see *3.5.5 When the suppression of monitoring of a large number of events ends*.

consolidation start event

A consolidation start event is the oldest one of the large number of events JP1/IM - View displays in the event list.

consolidation event

A consolidation event is a set of a consolidation start event and the events (large number of events meeting the repeated event condition that is met by the consolidation start event) consolidated into the consolidation start event. The event list shows only the information on the consolidation start event.

A *consolidation completion event* means a consolidation event for which suppression has already ended. An *event being consolidated* means a consolidation event for which suppression has not ended yet. The **Summary Status** column of the event list indicates the number of events consolidated into the consolidation event displayed in the event list.

Terms related to JP1/Base

suppression of event forwarding

The suppression of event forwarding is to suppress event forwarding from an agent to the manager, when the agent attempts to forward a large number of events to the manager. For this purpose, the manager executes a command on the agent.

forwarding suppression by threshold

The forwarding suppression by threshold is to preset a threshold for the amount of event forwarding in the forwarding setting file in preparation for occurrence of a large number of JP1 events.

3.5.3 Repeated event condition for the suppression of monitoring of a large number of events

The concept of repeated event condition, specifiable comparison attributes, and the concept of duplicate attribute value condition are the same as those described for the suppression of repeated event display. For details, see *3.4.3 Repeated event conditions*. This subsection describes the settings items of repeated event condition the suppression of monitoring of a large number of events

(1) Setting items of repeated event condition (to suppress monitoring of a large number of events)

The following describes the settings items of a repeated event condition:

- **Event conditions**

  You can specify the JP1 event attributes to be compared when JP1/IM - Manager acquires monitoring-target events.

For details about the JP1 event attributes that can be specified, see *3.4.3(2) Event comparison attributes that can be specified in repeated event conditions*.

- **Suppression items**

  You can specify what to suppress for the JP1 events that meet the repeated event condition. The operations that can be suppressed are as follows:

  - Consolidated display of repeated events in the Event Console window
  - Execution of the actions that are triggered by repeated events

  To suppress the monitoring of a large number of events, you must specify both of the above items as suppression items. For details about the display in the event, see *3.4.6 Event list display during the suppression of repeated-event display*. For details about the automated actions subject to the suppression of execution, see *3.5.8 Suppressing the execution of automated actions triggered by a large number of events*.

- **Conditions for same attribute values**

  You can specify whether to suppress the display of events that meet a repeated event condition by grouping them by attribute. The condition to suppress events while grouping them by attribute is called a *duplicate attribute value condition*.

  For details about the duplicate attribute value condition, see *3.4.3(3) Grouping repeated events by duplicate attribute value condition*.

- **Threshold**

  You can set a threshold for determining whether the JP1 events meeting an event condition have occurred in large numbers. The threshold can be set by specifying the *occurrence monitoring period* and *number of occurring events*.

  For the suppression of monitoring of a large number of events, set the threshold in the repeated event condition. The occurrence monitoring period can be specified in the range from 1 to 60 seconds. The number of occurring events can be specified in the range from 1 to 200 events.

  For how the threshold is used, see *3.5.4 When the suppression of monitoring of a large number of events starts* and *3.5.5 When the suppression of monitoring of a large number of events ends*.

- **End monitoring period**

  You can set a period by which JP1/IM - Manager determines whether the occurrence of a large number of JP1 events has ended. The usage of the end monitoring period varies depending on whether the threshold is set.

  The threshold is set for the suppression of monitoring of a large number of events. Therefore, JP1/IM - Manager determines that the occurrence of a large number of JP1 events has ended when the number of relevant JP1 events that occurred during the end monitoring period did not exceed the threshold. The end monitoring period can be specified in the range from 1 to 86,400 seconds. The default is 300 seconds.

  For how the end monitoring period is used when the threshold is not set (in the case of the suppression of repeated-event display), see *3.4.5 When suppression of repeated-event display ends*.

  For how the end monitoring period is used when the threshold is set (in the case of the suppression of monitoring of a large number of events), see *3.5.5 When the suppression of monitoring of a large number of events ends*.

- **Suppression start event** and **Suppression end event**

  You can specify whether to issue events that separately notify of the start and end of the suppression of monitoring of a large number of events. The event to notify of the start of monitoring suppression is called the *suppression start event* (event ID: 00003F58). The event to notify of the end of monitoring suppression is called the *suppression end event* (event ID: 00003F59). By default, neither notification event is issued. For details, see *3.5.10 Issuing events associated with the suppression of monitoring of a large number of events*.

- **Checks for suppression to continue** and **Processing for when suppression continues**

  You can specify settings to check whether the suppression of monitoring of a large number of events continues at intervals of specified time (in seconds) or at every specified number of events. Also, you can specify settings to issue a JP1 event that notifies of continuation or terminates the suppression when the suppression is determined to be continuing. If, however, the suppression of monitoring of a large number of events is terminated, the number of occurring events per occurrence monitoring period is set to 1. As a result, a large number of events subject to monitoring suppression will be displayed in the event list, and unnecessary automated actions will be executed until the number of occurring events per occurrence monitoring period exceeds the threshold. Therefore, for the normal suppression of monitoring of a large number of events, the termination of monitoring suppression is not specified. If you want to terminate monitoring suppression when monitoring suppression is determined to be continuing, consider whether the termination of monitoring suppression causes problems before specifying settings for **Processing for when suppression continues**.

For the mechanism of issuing JP1 events as notifications when monitoring suppression is determined to be continuing, see *3.5.10 Issuing events associated with the suppression of monitoring of a large number of events*.

3.5.4 When the suppression of monitoring of a large number of events starts

For the suppression of monitoring of a large number of events, JP1/IM - Manager, after it started, suppresses the large number of events acquired from the event service by using the repeated-event monitoring suppression function. JP1/IM - Manager determines that events have occurred in large numbers when the conditions below are all met, and then starts the suppression of monitoring of the large number of events by using the repeated-event monitoring suppression function.

- The events meet the event conditions in the repeated event condition.
- The number of repeated events that have occurred is not less than the specified threshold.
- Less than 2,500 types of repeated events are being suppressed.

JP1/IM - Manager determines whether to start suppressing the monitoring of a large number of events when it receives, from the event service, an event that meets the event conditions in a repeated event condition.

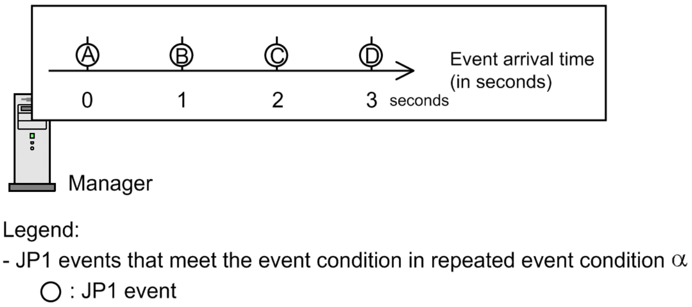
JP1/IM - Manager determines whether to start suppressing the monitoring of a large number of events according to each repeated event condition.

You can set the threshold for determining whether a large number of events have occurred by specifying the occurrence monitoring period and the number of occurring events. Specify the threshold (occurrence monitoring period and the number of occurring events) on the **Options** page of the Repeated Event Condition Settings window.

The following describes when the events that meet the event conditions in repeated event condition α are determined to be targets of monitoring suppression. Assume that the occurrence monitoring period is 2 seconds and the number of occurring events is 5.

First, assume that a large number of events that meet the repeated event condition α have occurred as shown in the following figure.

Figure 3–57: Occurrence of repeated event (1)


A
B
C
D
Event arrival time
(in seconds)
0
1
2
3
seconds
Manager
Legend:
- JP1 events that meet the event condition in repeated event condition α
○ : JP1 event

Whether an event that meets the event conditions in a repeated event condition occurred within the occurrence monitoring period is determined by the arrival time (`B.ARRIVEDTIME`) of the event. When the condition described below is satisfied by two events that meet the event conditions in a repeated event condition, the events are determined to have occurred within the occurrence monitoring period.

- Condition for determining events to be within the occurrence monitoring period

  Arrival time of the latest event ≥ *arrival time of an event* ≥ *arrival time of the latest event* - *occurrence-monitoring-period*

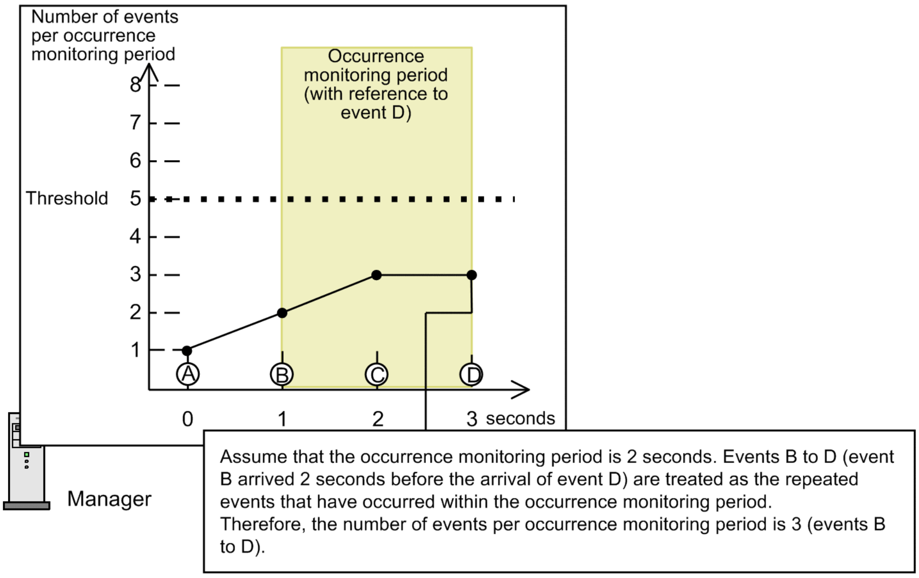
Among the events that have occurred as shown in Figure 3-57, event D is the latest event that meets the event conditions in repeated event condition α. The arrival time of event D is 3 seconds. The occurrence monitoring period is 2 seconds. Therefore, the events that meet the event conditions in repeated event condition α and for which the arrival time is in the range specified below are treated as the repeated events that have occurred within the occurrence monitoring period.

- Condition for determining events to be within the occurrence monitoring period (with reference to event D)

  Arrival time of event D (3 seconds) ≥ *arrival time of the event meeting the event conditions in the repeated event condition* α (1 to 3 seconds) ≥ *arrival time of event D* (3 seconds) - *occurrence monitoring time* (2 seconds)

The following figure shows a graph of the number of events per occurrence monitoring period calculated as described above.

Figure 3–58: Graph of the number of events per occurrence monitoring period (1)



Assume that the occurrence monitoring period is 2 seconds. Events B to D (event B arrived 2 seconds before the arrival of event D) are treated as the repeated events that have occurred within the occurrence monitoring period. Therefore, the number of events per occurrence monitoring period is 3 (events B to D).

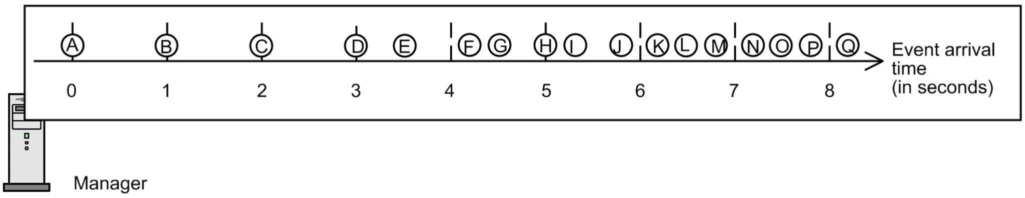
Legend:
- JP1 events that meet the event condition in repeated event condition α
  ○ : JP1 event

As shown in *Figure 3-58 Graph of the number of events per occurrence monitoring period (1)*, events B to D within the occurrence monitoring period (from second 1 to second 3) are treated as the repeated events that have occurred within the occurrence monitoring period. Therefore, the number of events per occurrence monitoring period is 3 at the time of event D.

At this point, the system is not in the status in which *a large number of events have occurred* because the number of events per occurrence monitoring period is less than the threshold.

Assume that the events that meet the event conditions in repeated event condition α have occurred as shown in the following figure after events had occurred as shown in *Figure 3-57 Occurrence of repeated event (1)*.

Figure 3–59: Occurrence of repeated events (2)



Legend:

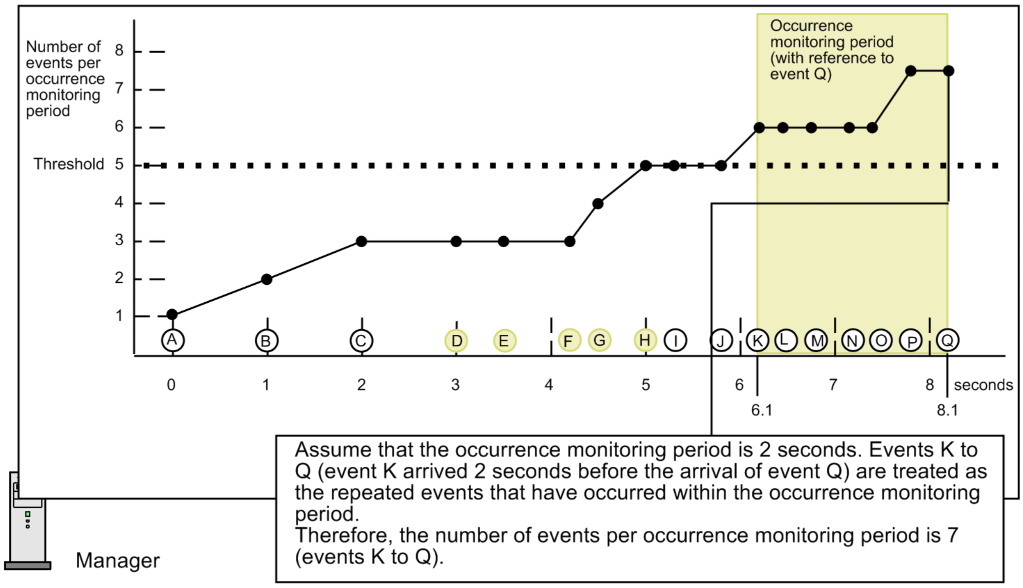
- JP1 events that meet the event condition in repeated event condition α

○ : JP1 event

Here, event Q is the latest event that meets the event conditions in repeated event condition α. Events are treated in a similar way to the above case. Seven events, events K to Q, within the occurrence monitoring period (from second 6.1 to second 8.1) shown in Figure 3-60 are treated as the repeated events that have occurred within the occurrence monitoring period with reference to event Q.

The following figure shows a graph of the number of events per occurrence monitoring period obtained after all events are checked in a similar way.

Figure 3–60: Graph of the number of events per occurrence monitoring period (2)



Assume that the occurrence monitoring period is 2 seconds. Events K to Q (event K arrived 2 seconds before the arrival of event Q) are treated as the repeated events that have occurred within the occurrence monitoring period.
Therefore, the number of events per occurrence monitoring period is 7 (events K to Q).

Legend:

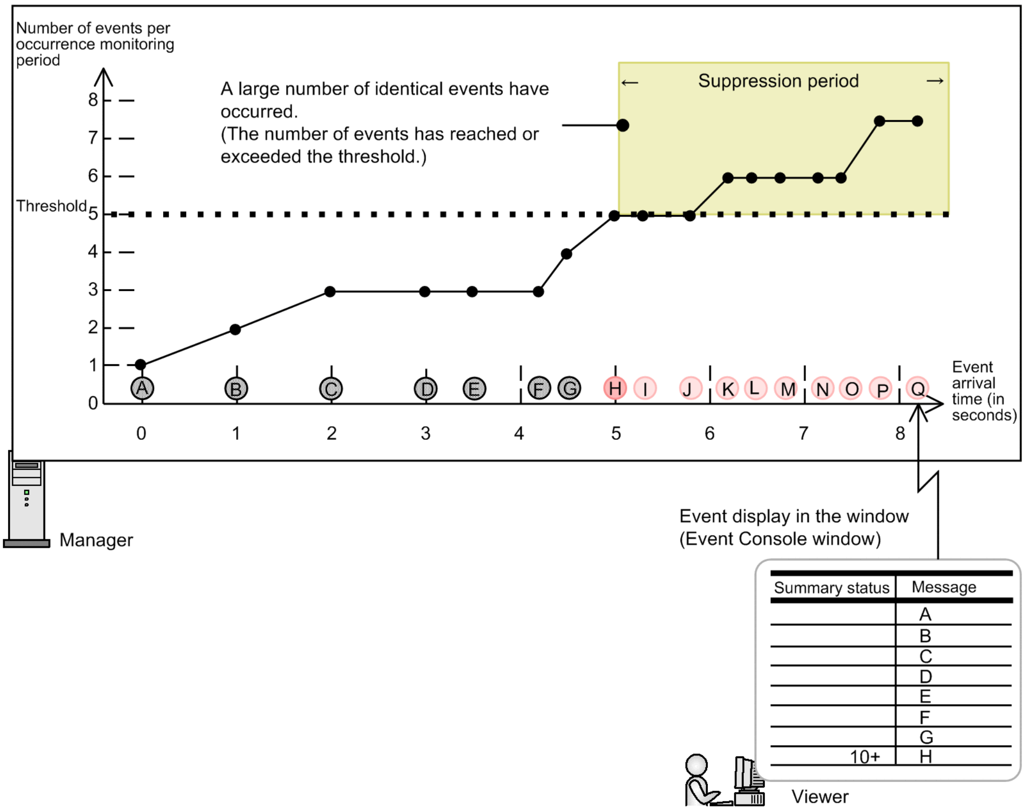
- JP1 events that meet the event condition in repeated event condition α

○ : JP1 event

● : Events that caused the number of events per occurrence monitoring period to reach or exceed the threshold at the time of event H

Focus attention on event H in Figure 3-60. Because five events, D to H, have occurred during 2 seconds (occurrence monitoring period) from second 3 to second 5, the number of events per occurrence monitoring period reaches the threshold at the time of event H. Accordingly, the system enters the status in which *a large number of events have occurred*, and the suppression of monitoring of a large number of events starts with event H.

Figure 3–61: When monitoring of repeated events are suppressed



Summary status	Message
	A
	B
	C
	D
	E
	F
	G
10+	H

Legend:

- JP1 events that meet the event condition in repeated event condition α

🔴 : Event occurring in large numbers that is subject to display suppression (repeated event)

○ : Event occurring in large numbers that is subject to display suppression

● : JP1 event that is not subject to display suppression

In the suppression period (second 5 and after) shown in the above figure, monitoring of the events occurring in large numbers are suppressed because JP1/IM - Manager determines that *a large number of events have occurred*. Monitoring of the events after event H is suppressed until the number of relevant events occurring is kept lower than the threshold for a specified period (end monitoring period).

As a larger number of occurring events is specified as a threshold value, a larger number of JP1 events are displayed in the event list of the Event Console window. For example, when 200 is specified as the number of occurring events, 200 repeated events are displayed in the event list of the Event Console window before monitoring suppression starts.

For the information that is displayed by JP1/IM - View when the suppression of monitoring of a large number of events, see *3.4.6 Event list display during the suppression of repeated-event display*.

3.5.5 When the suppression of monitoring of a large number of events ends

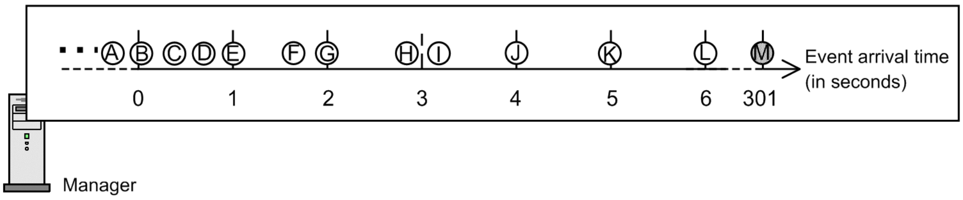
After having started the suppression of monitoring of a large number of events, JP1/IM - Manager ends monitoring suppression when the number of suppression-target events acquired is kept lower than the threshold for a specified period (end monitoring period). The end monitoring period and threshold are specified on the **Options** page of the Repeated Event Condition Settings window.

JP1/IM - Manager determines whether to end suppression of monitoring of a large number of events when it receives an event from the event service.

JP1/IM - Manager determines whether to end suppressing repeated-event display according to each repeated event condition.

The following describes when the suppression of monitoring of a large number of events that meet repeated event condition α ends if the number of occurring events is kept lower than the threshold for an end monitoring period. Assume that, in repeated event condition α, the occurrence monitoring period is 2 seconds, the number of occurring events is 5, and the end monitoring period is 300 seconds (5 minutes).

Figure 3–62: Occurrence of a large number of events (1)



Legend:

- JP1 events that meet the event condition in repeated event condition α

○ : Event occurring in large numbers that is subject to display suppression

● : Latest JP1 event acquired from the event service

Assume that a large number of events that meet repeated event condition α have occurred as shown in Figure 3-62.

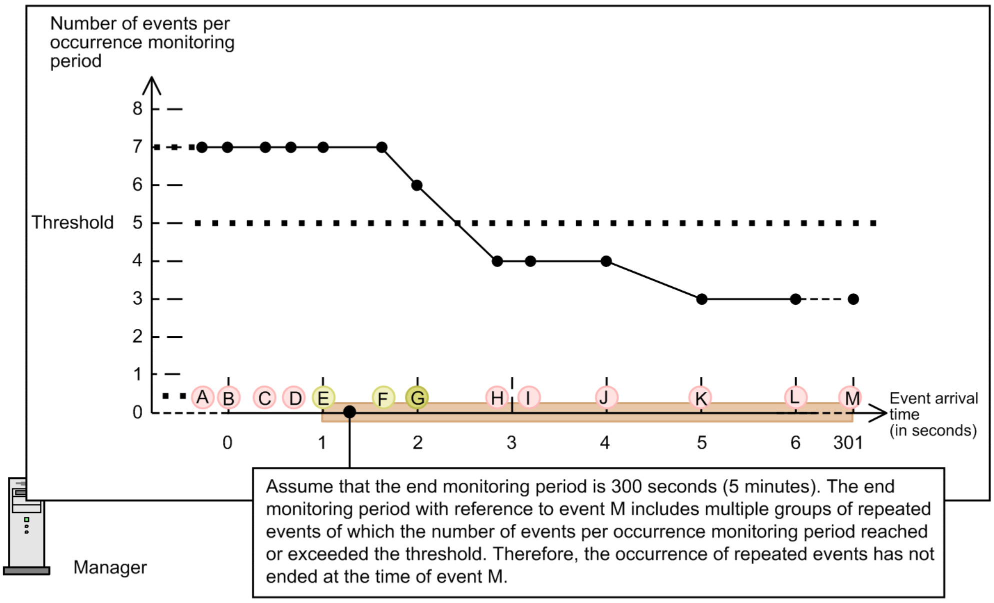
JP1/IM - Manager determines whether the occurrence of a large number of events has ended on the basis of the arrival time (`B.ARRIVEDTIME`) of the events occurring in large numbers. JP1/IM - Manager determines that the occurrence of a large number of events has ended when the following condition is satisfied:

- Condition for determining whether the occurrence of a large number of events has ended

  Arrival-time-of-the-event-acquired-from-the-event-service - *last-one-of-the-events-occurring-in-large-numbers-that-caused-the-number-of-occurring-events-to-reach-or-exceed-the-threshold* ≥ *end-monitoring-period*

Among the events that have occurred as shown in Figure 3-62, the latest event acquired from the event service is event M, which arrived at second 301. The figure below graphically shows the number of occurring events per occurrence monitoring period and threshold. For details about how to read the graph of the number of occurring events per occurrence monitoring period and threshold, see *3.5.4 When the suppression of monitoring of a large number of events starts*.

Figure 3–63: Graph of the number of events per occurrence monitoring period (3)



Assume that the end monitoring period is 300 seconds (5 minutes). The end monitoring period with reference to event M includes multiple groups of repeated events of which the number of events per occurrence monitoring period reached or exceeded the threshold. Therefore, the occurrence of repeated events has not ended at the time of event M.

Legend:

▨ : End monitoring period (300 seconds)

- Events that meet the event condition in repeated event condition α

○ : Event occurring in large numbers that is subject to display suppression

○ : Group of a large number of events of which the number of events reached or exceeded the threshold in the end monitoring period

● : Group of a large number of events, subject to display suppression, of which the number of events reached or exceeded the threshold most recently

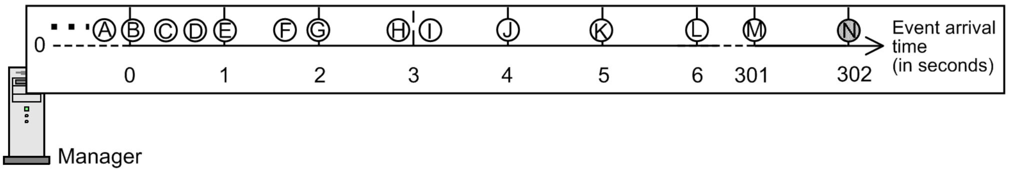
This graph shows that event G is the last one of the events occurring in large numbers that caused the number of occurring events to reach or exceed the threshold, and its arrival time is second 2. The end monitoring period is from second 1 to second 301 as shown in Figure 3-63. The following expression represents the relationships among the arrival time of event G, arrival time of event M, and the end monitoring time specified in repeated event condition α:

Arrival time of event M (second 301) - arrival time of event G (second 2) < end monitoring time specified in repeated event condition α (300 seconds)

The difference between the arrival time of event M and that of event G is less than the length of end monitoring period. Therefore, the suppression of monitoring of a large number of events does not end when event M is acquired.

Assume that JP1 events have occurred as shown in the following figure after a large number of events that meet repeated event condition α had occurred as shown in Figure 3-62.

Figure 3–64: Occurrence of a large number of events (2)



Legend:

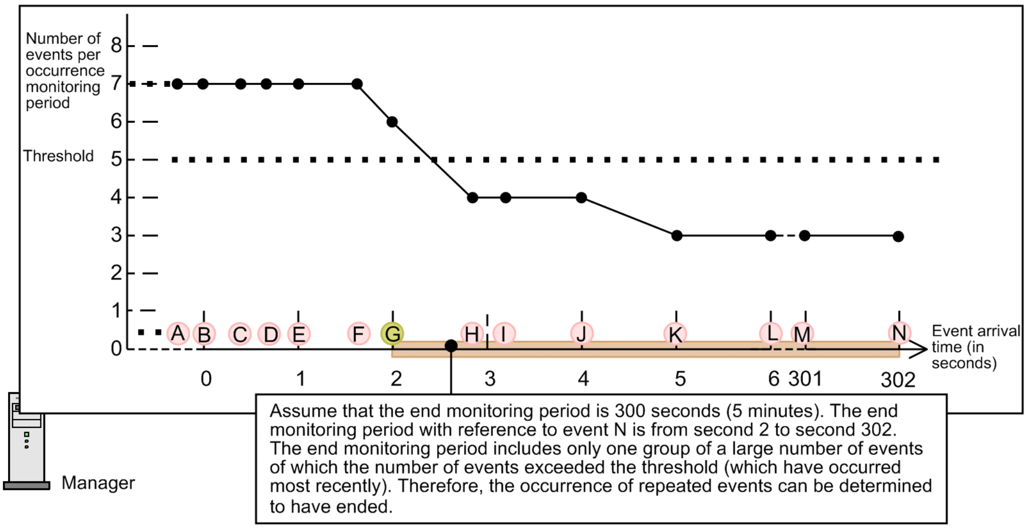
- JP1 events that meet the event condition in repeated event condition α

○ : Event occurring in large numbers that is subject to display suppression

● : Latest JP1 event acquired from the event service

When events have occurred as shown in Figure 3-64, event N, arriving at second 302, is the latest event acquired from the event service. The following figure graphically shows the number of occurring events per occurrence monitoring period and threshold at the time of event N.

Figure 3–65: Graph of the number of events per occurrence monitoring period (4)



Assume that the end monitoring period is 300 seconds (5 minutes). The end monitoring period with reference to event N is from second 2 to second 302. The end monitoring period includes only one group of a large number of events of which the number of events exceeded the threshold (which have occurred most recently). Therefore, the occurrence of repeated events can be determined to have ended.

Legend:

▨ : End monitoring period (300 seconds)

- Events that meet the event condition in repeated event condition α

○ : Event occurring in large numbers that is subject to display suppression

● : Group of a large number of events, subject to display suppression, of which the number of events reached or exceeded the threshold most recently

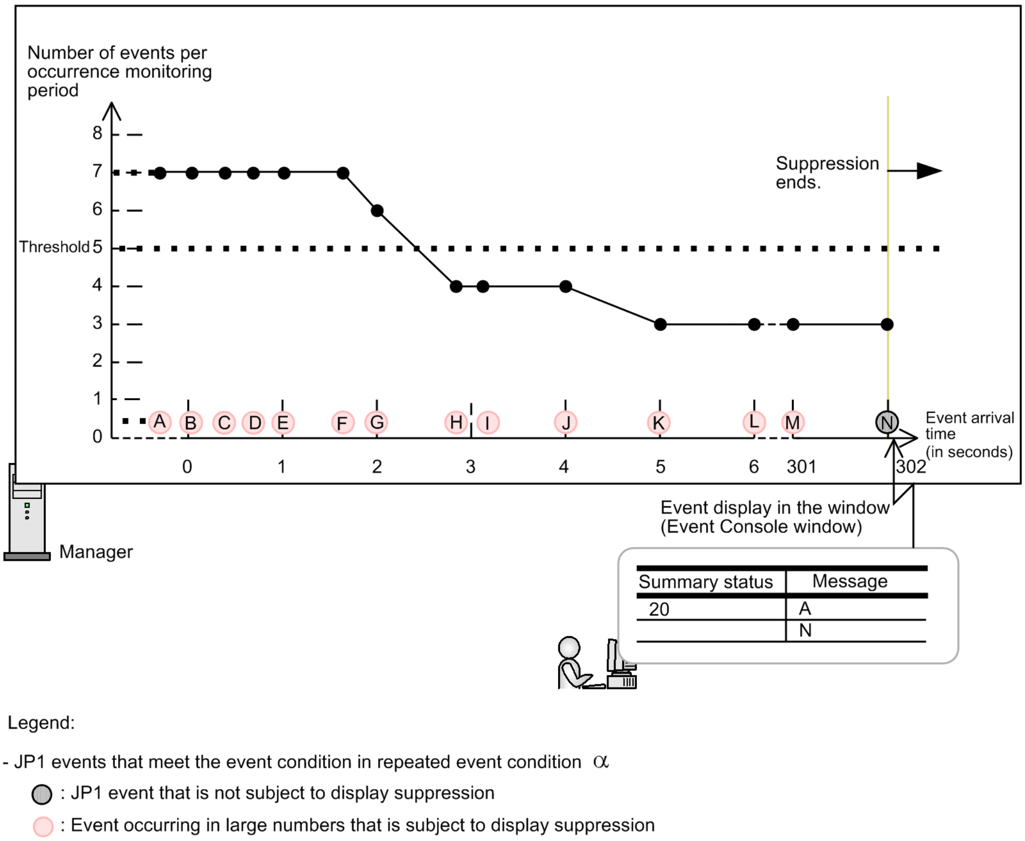
This graph shows that event G is the last one of the events occurring in large numbers that caused the number of occurring events to reach or exceed the threshold, and its arrival time is second 2. The end monitoring period is from second 2 to second 302 as shown in Figure 3-65. The following expression represents the relationships among the arrival time of event G, arrival time of event N, and the end monitoring time specified in repeated event condition α:

Arrival time of event N (second 302) - arrival time of event G (second 2) ≥ end monitoring time specified in repeated event condition α (300 seconds)

Because the difference between the arrival time of event N and that of event G is more than the length of end monitoring period, the suppression of monitoring of a large number of events ends.

The following figure shows the events occurring in large numbers whose monitoring is suppressed and those whose monitoring is not suppressed when events have occurred as shown in Figure 3-65.

Figure 3–66: Events occurring in large numbers whose monitoring is suppressed and those whose monitoring is not suppressed



Summary status	Message
20	A
	N

The suppression of monitoring ends at second 302. Therefore, monitoring suppression does not apply to event N and subsequently occurring events that meet the event conditions in repeated event condition α.

For the information that is displayed by JP1/IM - View when the suppression of monitoring of a large number of events, see *3.4.6 Event list display during the suppression of repeated-event display*.

Ending monitoring suppression except when the number of acquired events occurring in large numbers is kept lower than the threshold for a specified period (end monitoring period)

The suppression of monitoring of a large number of events ends also in the following cases:

- When JP1/IM - Manager stops

  If the suppression of monitoring of a large number of events ends because JP1/IM - Manager stops, no suppression end event is issued even when issuance of the notification of the end of monitoring suppression has been set. For details about the suppression end event, see *3.5.10 Issuing events associated with the suppression of monitoring of a large number of events*.

- When a repeated event condition is changed or deleted

  In this case, JP1/IM - Manager ends suppressing the monitoring of only the consolidation events that meet specific repeated event conditions. The specific repeated event conditions are those which were marked with the editing icon when they were updated in the List of Repeated Event Conditions window or those which have been deleted.

3.5.6 Event list display during the suppression of monitoring of a large number of events

The event list display during the suppression of monitoring of a large number of events is the same as the event list display during the suppression of repeated-event display. For details, see *3.4.6 Event list display during the suppression of repeated-event display*.

3.5.7 Issuing notifications when the suppression of monitoring of a large number of events continues

You can specify settings for **Notifications for when suppression continues** to check whether the suppression of monitoring of a large number of events continues at intervals of specified time (number of seconds) or a specified number of events. When monitoring suppression continues, a JP1 event can be issued to notify of the continuation of monitoring suppression.

Notifications for when suppression continues is a setting item of repeated event condition, which must be set for individual repeated event conditions. This subsection describes when to check whether monitoring suppression continues.

Note that, if checking whether monitoring suppression occurs concurrently with ending monitoring suppression, ending monitoring suppression takes priority.

> **Important**
>
> For illustrative purposes, given here is an example of checking whether the suppression of monitoring of a large number of events continues at short intervals. Note that, if you specify the checking (of whether monitoring suppression continues) at short intervals during actual system operation, a large number of notification events might be issued as a result of checking. Therefore, specify an appropriate interval of checking according to the system environment.

You can select time (number of seconds) or number of events as the unit of checking interval. The following describes the checking operations with respective units of interval selected:

- Checking at intervals of specified time (number of seconds)

  The first checking is performed when the condition shown below is satisfied by the two repeated events that meet the same repeated event condition:

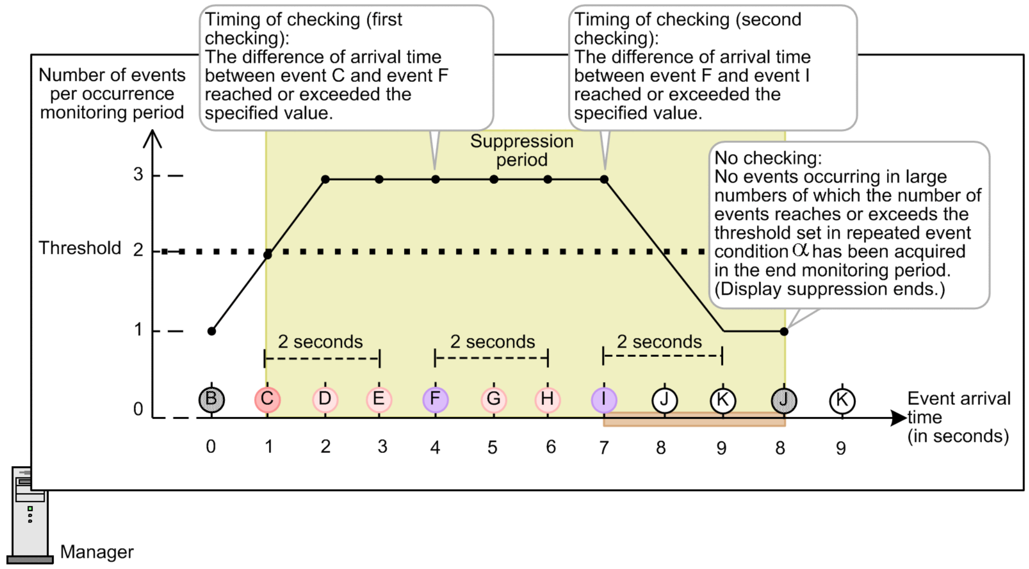
  Arrived-time-of-the-latest-repeated-event - *arrival-time-of-the-repeated-start-event* ≥ *specified-number-of-seconds*

  For the second and subsequent checkings, in the above condition, the reference event (*repeated start event*) is substituted by the event that triggered the preceding checking.

  The specifiable number of seconds ranges from 1 to 86,400 seconds.

  The figure below shows an example of checking whether the suppression of monitoring of a large number of events at intervals of 2 seconds. Note that, in this example, the end monitoring period is set to 3 seconds.

Figure 3–67: Checking whether suppression continues at intervals of specified time (number of seconds)



Timing of checking (first checking):
The difference of arrival time between event C and event F reached or exceeded the specified value.
Timing of checking (second checking):
The difference of arrival time between event F and event I reached or exceeded the specified value.
Number of events per occurrence monitoring period
Suppression period
No checking:
No events occurring in large numbers of which the number of events reaches or exceeds the threshold set in repeated event condition α has been acquired in the end monitoring period.
(Display suppression ends.)
3
Threshold 2
1
0
2 seconds
2 seconds
2 seconds
B
C
D
E
F
G
H
I
J
K
J
K
0
1
2
3
4
5
6
7
8
9
8
9
Event arrival time (in seconds)
Manager

Legend:

▨ : End monitoring period (3 seconds)

- JP1 events that meet the event condition in repeated event condition α

● : Event occurring in large numbers that is subject to display suppression (repeated event)

● : Event occurring in large numbers that is subject to display suppression

● : Event occurring in large numbers that triggers checking

● : JP1 event (not subject to display suppression)

- JP1 events that do not meet repeated event condition α

○ : JP1 event

- Checking at intervals of a specified number of events

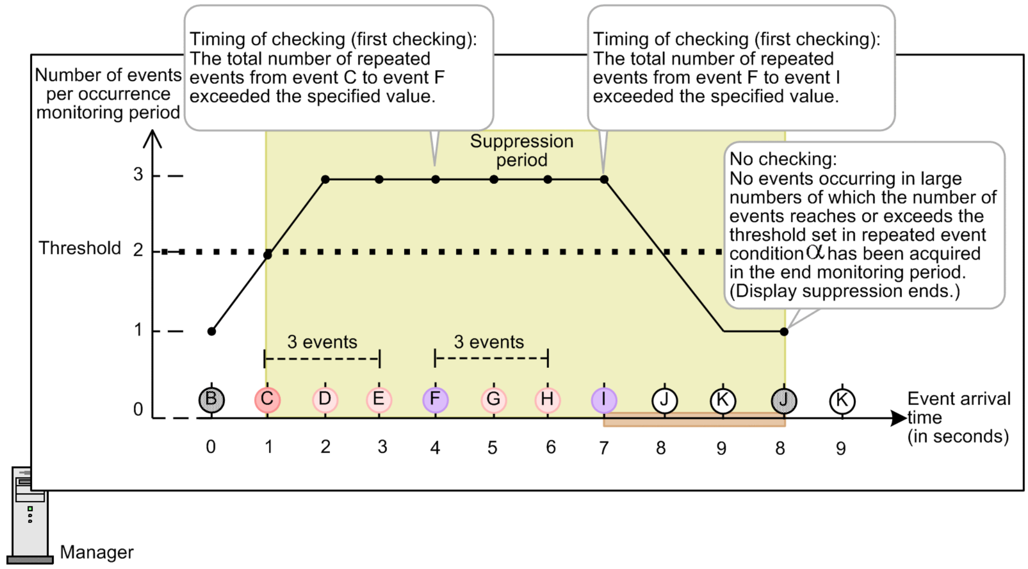
  The first checking is performed when the specified number of events is exceeded by the total number of the repeated events meeting the same repeated event condition. The repeated events are counted from the repeated start event up to the latest repeated event.

  For the second and subsequent checkings, in the above condition, the reference event (*repeated start event*) is substituted by the event that triggered the preceding checking.

  The specifiable number of events ranges from 1 to 1,000,000.

  The figure below shows an example of checking whether the suppression of monitoring of a large number of events at intervals of three events. Note that, in this example, the end monitoring period is set to 3 seconds.

Figure 3–68: Checking whether suppression continues at intervals of specified number of events


Timing of checking (first checking): The total number of repeated events from event C to event F exceeded the specified value.
Timing of checking (first checking): The total number of repeated events from event F to event I exceeded the specified value.
Number of events per occurrence monitoring period
Suppression period
No checking: No events occurring in large numbers of which the number of events reaches or exceeds the threshold set in repeated event condition α has been acquired in the end monitoring period. (Display suppression ends.)
3
Threshold 2
1
0
3 events
3 events
B
C
D
E
F
G
H
I
J
K
J
K
0
1
2
3
4
5
6
7
8
9
8
9
Event arrival time (in seconds)
Manager

Legend:

🟧 : End monitoring period (3 seconds)

- JP1 events that meet the event condition in repeated event condition α
  - ● : Event occurring in large numbers that is subject to display suppression (repeated event)
  - ○ : Event occurring in large numbers that is subject to display suppression
  - ● : Event occurring in large numbers that triggers checking
  - ● : JP1 event (not subject to display suppression)
- JP1 events that do not meet repeated event condition α
  - ○ : JP1 event

Note

You can specify terminating monitoring suppression or issuing a notification event as the action to be taken when monitoring suppression is determined to be continuing. If, however, the monitoring suppression using a repeated event condition with a threshold set is terminated, the events subject to monitoring suppression will be displayed in the event list and unnecessary automated actions will be executed. This situation begins immediately after monitoring suppression is terminated and continues until the number of occurring events exceeds the threshold again. Therefore, for the normal suppression of monitoring of a large number of events, the termination of monitoring suppression is not specified. If you want to terminate monitoring suppression when monitoring suppression is determined to be continuing, consider whether the termination of monitoring suppression causes problems before specify settings for **Processing for when suppression continues**.

(1) Notifying of the continuation of the suppression of monitoring of a large number of events

When the suppression of monitoring of a large number of events is determined to be continuing, you can issue an event (event ID: 00003F65) to notify that suppression will continue.

For details, see *3.5.10 Issuing events associated with the suppression of monitoring of a large number of events*.

3.5.8 Suppressing the execution of automated actions triggered by a large number of events

When setting a repeated event condition in the Repeated Event Condition Settings window, you can specify suppression of automated actions as a suppression item to prevent unnecessary automated actions from being triggered by a large number of events.

The suppression of execution of automated actions is applied for the same period as the period for which the suppression of event display using a repeated event condition is applied.

The repeated events that meet a repeated event condition specifying the suppression of execution of automated actions are not compared with action conditions. Also, the repeated events for which automated-action execution is suppressed can be searched as the events not subject to actions in the Event Search Conditions, Settings for View Filter, and Detailed Settings for Event Receiver Filter windows.

The following table shows the differences in the suppression of actions between the suppression of repeated-event monitoring and the suppression of automated-action execution.

Table 3–18: Differences in the suppression of actions

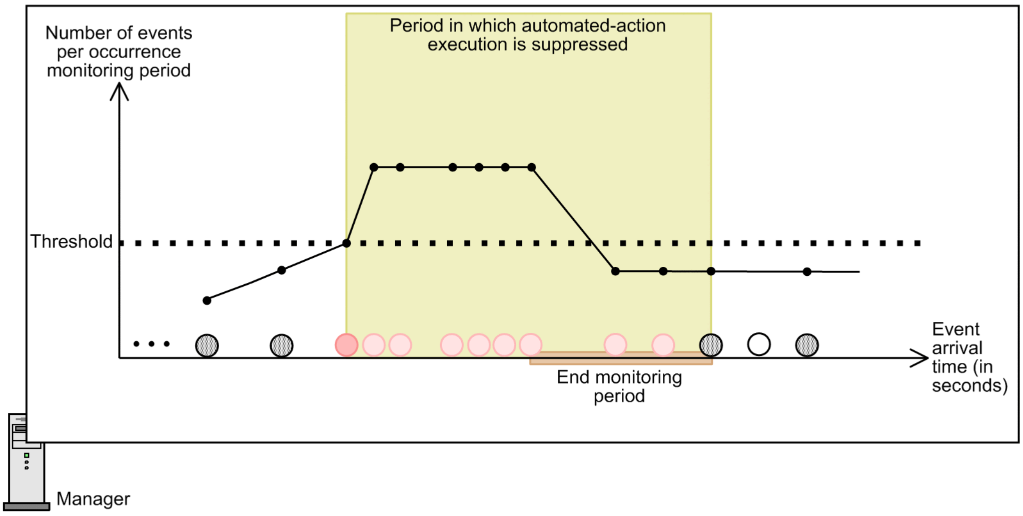
Item	Suppressing actions by the suppression of repeated-event monitoring	Suppressing actions by the suppression of automated-action execution
Unit of suppression	Repeated event	Action definition
Suppression time	Suppression continues as long as a large number of repeated events occur.	1 to 3,600 seconds
Reference to action logs	Action logs cannot be referenced.	Action logs can be referenced by clicking the **Action Log** button in the Event Details window.
Re-execution of action	Actions cannot be re-executed.	An action can be re-executed by clicking the **Re-execute** button in the List of Action Results, Action Log, or Action Log Details window.
Display in the **Action** field of the Event Console window	🚫	🚫

For details about the suppression of actions by the suppression of automated action, see *5.4.4 Suppressing identical actions*.

(1) Range of automated actions subject to execution suppression (when suppressing the execution of actions for all repeated events)

The following describes the range of automated actions subject to execution suppression. Assume that the suppression of automated-action execution is specified in the repeated event condition and **All repeated events** is selected as the range of execution suppression.

Figure 3–69: Range of automated actions subject to execution suppression (all repeated events)



Legend:

- JP1 events that meet the event condition in repeated event condition α

  🔴 : JP1 event subject to suppression of automated-action execution (repeated start event)

  ◌ : JP1 event subject to suppression of automated-action execution

  ● : JP1 event not subject to suppression of automated-action execution

- JP1 events that do not meet the event condition in repeated event condition α

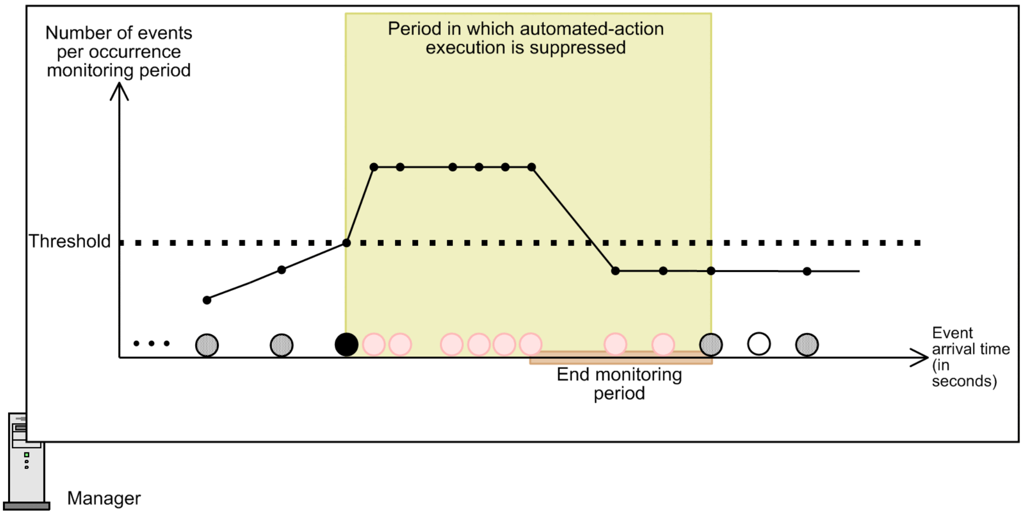
  ○ : JP1 event

As shown in the above figure, when **All repeated events** is selected, the execution of automated actions is suppressed for all suppression-target events, including repeated start events.

(2) Range of automated actions subject to the suppression of execution (when suppressing the execution of actions for the repeated events other than repeated start events)

The following describes the range of automated actions subject to execution suppression. Assume that the suppression of automated-action execution is specified in the repeated event condition and **Repeated events other than repeated start events** is selected as the range of execution suppression.

Figure 3–70: Range of automated actions subject to execution suppression (repeated events other than repeated start events)


Number of events per occurrence monitoring period
Period in which automated-action execution is suppressed
Threshold
Event arrival time (in seconds)
End monitoring period
Manager

Legend:

- JP1 events that meet the event condition in repeated event condition α

○ : JP1 event subject to suppression of automated-action execution

● : JP1 event not subject to suppression of automated-action execution (repeated start event)

◉ : JP1 event not subject to suppression of automated-action execution

- JP1 events that do not meet the event condition in repeated event condition α

○ : JP1 event

As shown in the above figure, when **Repeated events other than repeated start events** is selected, the execution of automated actions is suppressed for the suppression-target events other than repeated start events.

3.5.9 Suppressing the forwarding of a large number of events

You can suppress the event forwarding from an agent as a measure to be taken when a large number of events occur on the agent. Suppressing the forwarding of a large number of events can reduce the load on the manager.

The following describes how to suppress the forwarding of a large number of events:

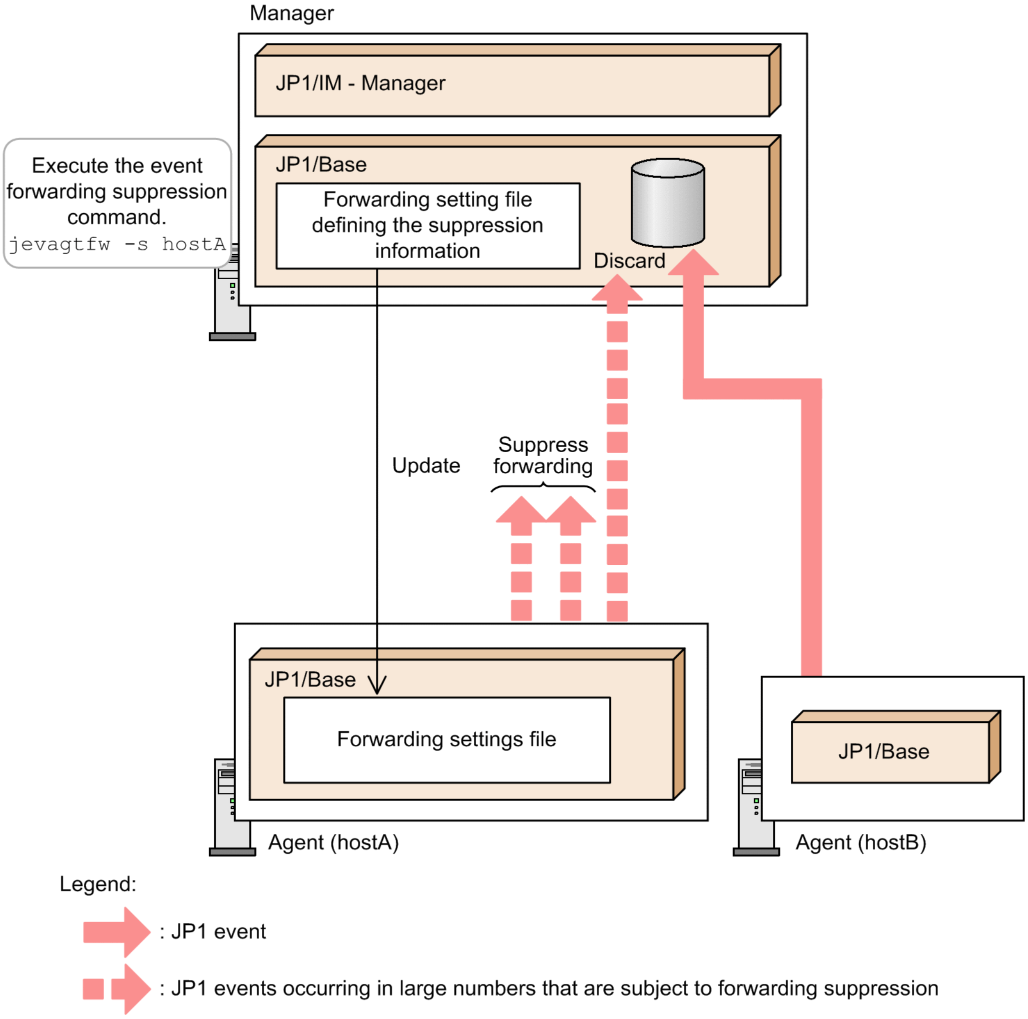
- Suppressing the event forwarding from agents by an operation from the manager
- Stopping the log file traps that output a large number of events by an operation from the manager
- Setting a threshold for automatically suppressing the event forwarding from agents

(1) Suppressing the event forwarding from agents by an operation from the manager

You can suppress the event forwarding from an agent where a large number of events have occurred by an operation from the manager. To achieve this, use the event forwarding suppression command (`jevagtfw` command) of JP1/Base. Specify the host name of the suppression-target agent in a parameter of the `jevagtfw` command, and execute the command from the manager. You can thus suppress the event forwarding from the suppression-target agent. Also, the JP1 events that are forwarded from the suppression-target agent can be discarded by the event server of the manager.

This functionality enables the manager to control the event forwarding from agents. Therefore, you can quickly take a measure, from the manager, against the occurrence of a large number of events on an agent.

Figure 3–71: Overview of the operation of the jevagtfw command


Manager
JP1/IM - Manager
JP1/Base
Execute the event forwarding suppression command.
jevagtfw -s hostA
Forwarding setting file defining the suppression information
Discard
Update
Suppress forwarding
JP1/Base
Forwarding settings file
Agent (hostA)
JP1/Base
Agent (hostB)
Legend:
: JP1 event
: JP1 events occurring in large numbers that are subject to forwarding suppression

To use this functionality, the JP1/Base on the manager host must be version 10-50 or later. Also the JP1/Base on the suppression-target agent host must be version 08-00 or later.

For details about the event transfer suppression command (`jevagtfw` command), see the chapter for commands and the chapter describing the suppression of event forwarding by the `jevagtfw` command in the *JP1/Base User's Guide*.

(2) Stopping the log file traps that output a large number of events by an operation from the manager

When a log file trap has issued a large number of JP1 events, you can stop the log file trap by an operation from the manager. You can use IM Configuration Management to stop individual log file traps on an agent from the manager. By using IM Configuration Management, you can stop the process of the suppression-target log file trap by an operation in the Display/Edit Profiles window for the relevant host.

ID and log file trap name of a log file trap

When JP1/Base on the agent host is version 10-50 or later, the ID number and log file trap name of a log file trap are added to the attributes of the JP1 events issued by that log file trap. (The log file trap name is added only if it was set when the log file trap was started.)

When JP1/Base of the manager is version 10-50 or later, the ID number and log file trap name of the log file trap are added to the attributes of the JP1 events issued by the remote-monitoring log file trap.

The added ID number and log file trap name of the log file trap are displayed as event attributes in the Event Details window when JP1/IM - Manager on the manager host is version 10-50 or later. Because you can identify the log file trap that is the source of a JP1 event with the attribute information of the JP1 event, you can quickly know the log file trap to be stopped.

> **Note**
>
> You can stop a log file trap on an agent from the manager also by executing the `jevlogstop` command with the ID number or log file trap name of the log file trap specified in the Execute Command window. For details about the `jevlogstop` command, see the chapter for commands in the *JP1/Base User's Guide*.
>
> In the case of the remote-monitoring log file trap, to stop a log file trap, execute the `jcfallogstop` command with the monitored host name and the log file trap name of the log file trap specified. For details about the `jcfallogstop` command, see *jcfallogstop* in *1. Commands* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

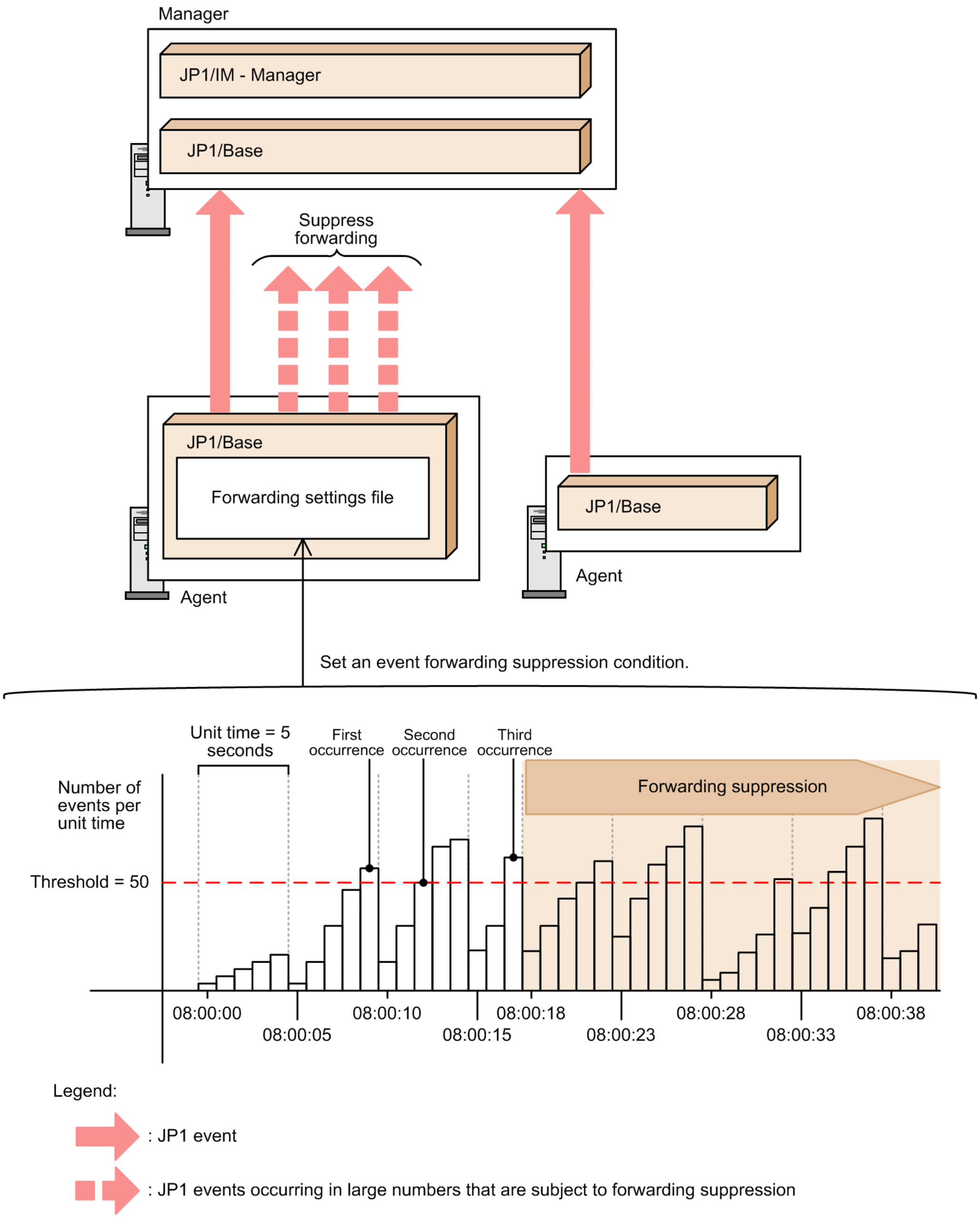
(3) Setting a threshold for automatically suppressing the event forwarding from agents

When you set, in advance, a threshold for determining whether a large number of events occur, event forwarding can be suppressed automatically if a large number of events occur on an agent.

For the event server of agents, set an event forwarding suppression condition, which corresponds to the threshold for the suppression of monitoring of a large number of events. The event forwarding suppression condition specifies, for example, that event forwarding must be suppressed if issuance of at least 50 events within 5 seconds has occurred three times successively.

Setting an expected condition for the occurrence of a large number of events as the event forwarding suppression condition prevents the forwarding of a large number of events from agents.

Figure 3–72: Overview of event forwarding suppression using a threshold



To use this functionality, JP1/Base on the suppression-target agent host must be version 10-50 or later.

For details about the event forwarding suppression using a threshold, see the chapter describing the event forwarding suppression using a threshold in the *JP1/Base User's Guide*.

3.5.10 Issuing events associated with the suppression of monitoring of a large number of events

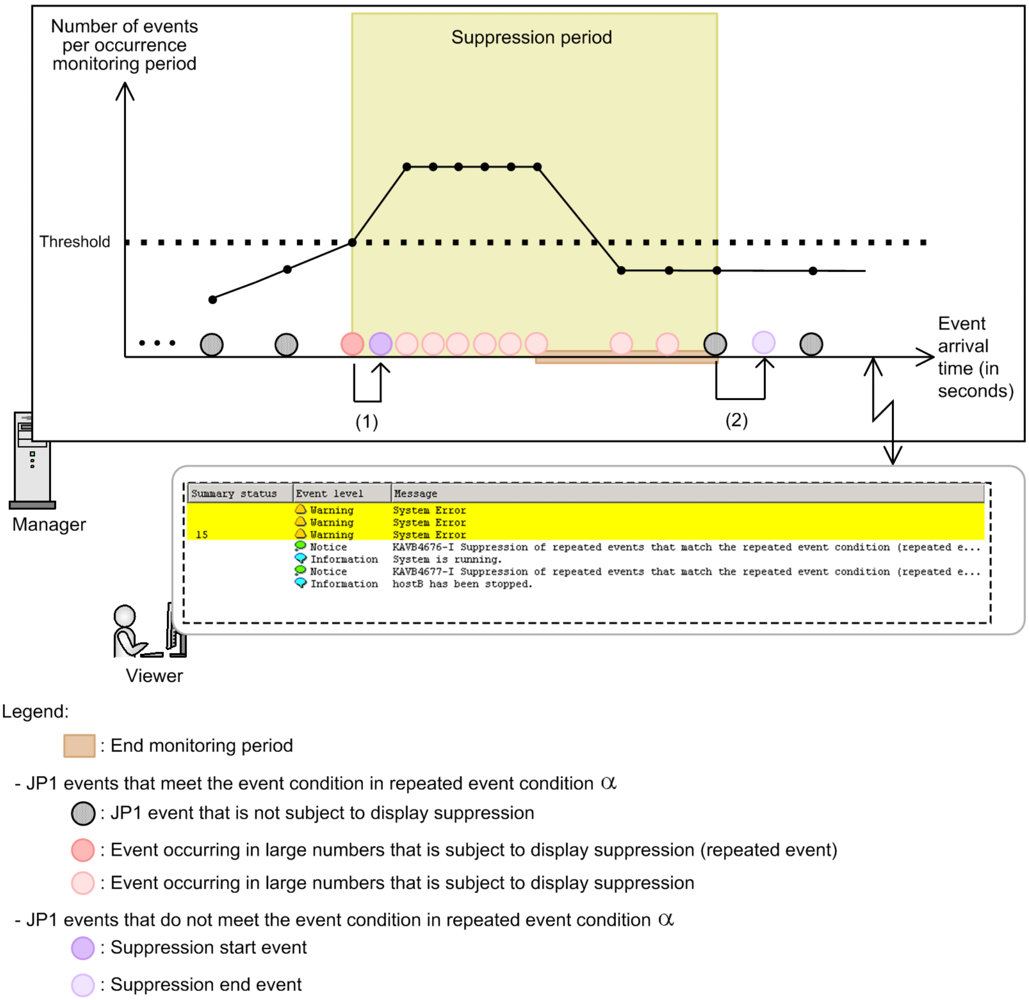
When the suppression of monitoring of a large number of events is used, various notifications can be issued. A suppression start event (event ID: 00003F58) can be issued to notify of the start of suppression, and a suppression end event (event ID: 00003F59) can be issued to notify of the end of suppression. After whether monitoring suppression continues is checked, an event to notify that suppression will continue (event ID: 00003F65) can be issued when display suppression continues.

Whether to issue the individual events associated with the suppression of monitoring of a large number of events is specified as items of repeated event condition on the **Options** page of the Repeated Event Condition Settings window.

Figure 3-73 shows how the suppression start and suppression end events are issued. Figure 3-74 shows how the event to notify that suppression will continue is issued.

> **Important**
>
> When you intend to issue the suppression start event, suppression end event, and event to notify that suppression will continue, specify the timings of their issuance appropriately according to the system environment. Consideration is required to prevent these events from occurring in large numbers.

Figure 3–73: Issuing events (suppression start and suppression end events) associated with the suppression of monitoring of a large number of events


Number of events per occurrence monitoring period
Suppression period
Threshold
Event arrival time (in seconds)
(1)
(2)
Manager
Viewer
Legend:
▨ : End monitoring period
- JP1 events that meet the event condition in repeated event condition α
● : JP1 event that is not subject to display suppression
● : Event occurring in large numbers that is subject to display suppression (repeated event)
○ : Event occurring in large numbers that is subject to display suppression
- JP1 events that do not meet the event condition in repeated event condition α
● : Suppression start event
○ : Suppression end event

Summary status	Event level	Message
	Warning	System Error
	Warning	System Error
15	Warning	System Error
	Notice	KAVB4676-I Suppression of repeated events that match the repeated event condition (repeated e...
	Information	System is running.
	Notice	KAVB4677-I Suppression of repeated events that match the repeated event condition (repeated e...
	Information	hostB has been stopped.

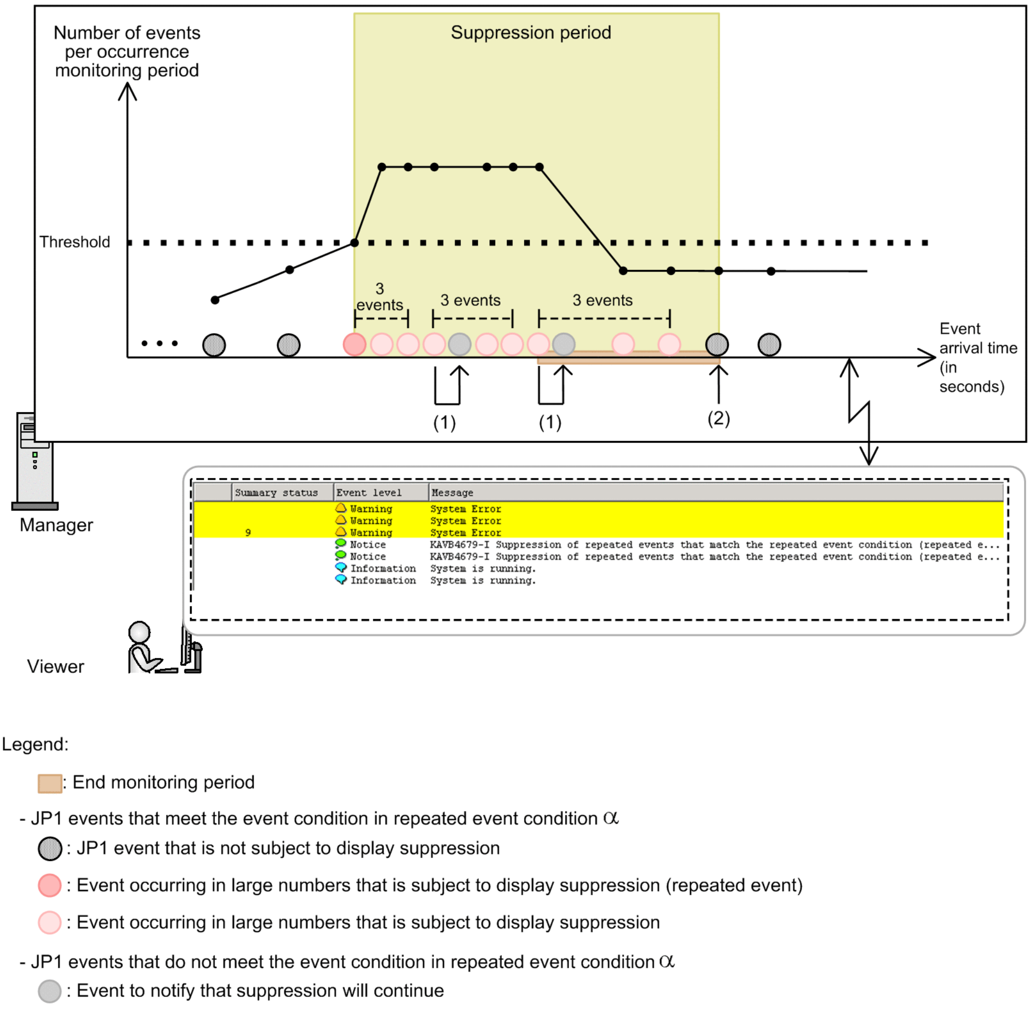
The following describes how the suppression start and suppression end events are issued in sequence of the numbers in the figure (the numbers in the figure correspond to the numbers below).

1. JP1/IM - Manager starts the suppression of monitoring of a large number of events when the number of acquired events meeting repeated event condition α reaches or exceeds the threshold. The suppression start event is issued to notify of the start of suppression at the same time as the start of monitoring suppression.
2. JP1/IM - Manager ends the suppression of monitoring of a large number of events when it receives (from the event service) a specific event. The specific event is the event whose arrival time exceeds the arrival time of the last event (among those occurring in large numbers) that is not less than the threshold by at least the end monitoring period.

The suppression end event to notify of the end of suppression is issued at the same time as the end of monitoring suppression.

No suppression end event is issued when monitoring suppression ends because JP1/IM - Manager is stopped or restarted.

Figure 3–74: Issuing the event (to notify that suppression will continue) associated with the suppression of monitoring of a large number of events


Number of events per occurrence monitoring period
Suppression period
Threshold
3 events
3 events
3 events
Event arrival time (in seconds)
(1)
(1)
(2)
Manager
Viewer
Legend:
: End monitoring period
- JP1 events that meet the event condition in repeated event condition α
: JP1 event that is not subject to display suppression
: Event occurring in large numbers that is subject to display suppression (repeated event)
: Event occurring in large numbers that is subject to display suppression
- JP1 events that do not meet the event condition in repeated event condition α
: Event to notify that suppression will continue

Summary status	Event level	Message
	Warning	System Error
	Warning	System Error
9	Warning	System Error
	Notice	KAVB4679-I Suppression of repeated events that match the repeated event condition (repeated e...
	Notice	KAVB4679-I Suppression of repeated events that match the repeated event condition (repeated e...
	Information	System is running.
	Information	System is running.

The following describes how the event to notify that suppression will continue and the event to notify that suppression will be terminated are issued. The description follows the numbers in the figure (the numbers in the figure correspond to the numbers below). Assume that repeated event condition α specifies that whether monitoring suppression continues is to be checked at intervals of three events.

1. The event to notify that suppression will continue is issued because JP1/IM - Manager determines that the suppression of monitoring of a large number of events meeting repeated event condition α continues.
2. The event to notify that suppression will continue is not issued because the suppression of monitoring of a large number of events meeting repeated event condition α ended.

3.5.11 Notes on the suppression of monitoring of a large number of events

The notes on the suppression of monitoring of a large number of events are the same as those on the suppression of repeated-event display. For details, see *3.4.9 Notes on suppression of repeated-event display*.

3.6 Searching for events

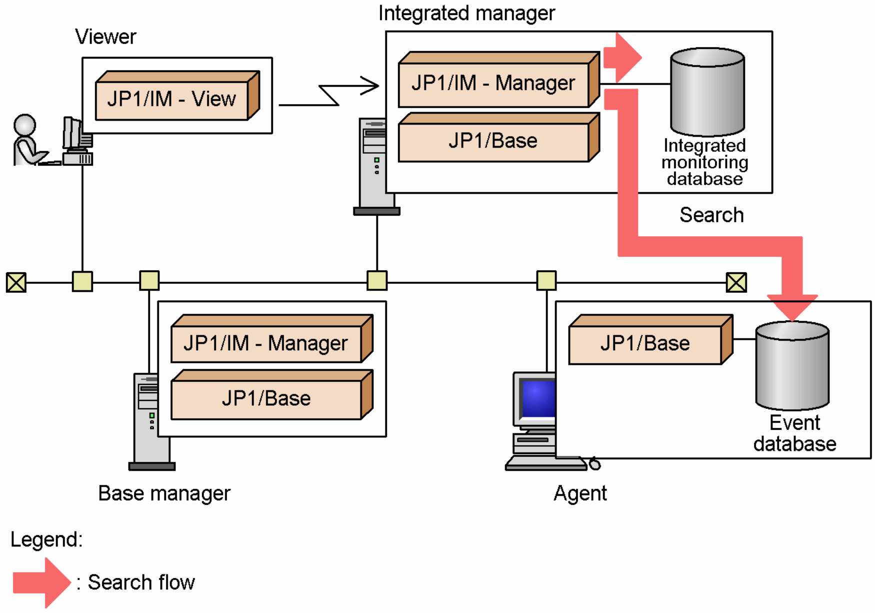
In JP1/IM, you can search for JP1 events registered with JP1/Base using various search conditions, and display them on the **Search Events** page of the Event Console window. When you use the integrated monitoring database, you can search for JP1 events registered with the event service or integrated monitoring database, and display them on the **Search Events** page. As well as JP1 event attributes, the search conditions might include the response status of severe events and whether an automated action has been executed. You can also use regular expressions for some types of searches.

As the host on which to search, you can specify not only the manager that you are logged in to, but also a remote host on which JP1/Base is installed.

If restrictions are set on viewing and operating business groups, the event server in the monitored business group will be searched.

When you use the integrated monitoring database, you can specify which database to search. You can specify either the integrated monitoring database or the JP1/Base event database.

Figure 3–75: Overview of event searching



The following describes JP1 event searches and search conditions, followed by a description of the flow of processing when searching for events.

3.6.1 Searching for JP1 events

JP1 events that need to be managed appear on the **Monitor Events** page of the Event Console window, but you can also use the event search function to display the following JP1 events:

- Past JP1 events that have disappeared from the **Monitor Events** page because the number of JP1 events has exceeded the maximum number of viewable events (JP1/IM - View's scroll buffer size)
- JP1 events erased from the **Severe Events** page by the **Delete** button
- JP1 events without the event level extended attribute (only JP1 events for which an event level is specified are displayed in JP1/IM - View)
- JP1 events filtered out by the forwarding filter and not sent to a JP1/IM manager (normal events, for example)

- JP1 events filtered out by the event acquisition filter and not acquired by JP1/IM (normal events, for example)
- JP1 events stored in the integrated monitoring database, if being used

You can check the contents of the events displayed as the search result on the **Search Events** page using the **Event Details** button and **Monitor** button in the same way as on the **Monitor Events** page.

Search conditions

The event search conditions are saved in JP1/IM - Manager for each user and for each of the following JP1/IM - View versions:

- The search conditions set in JP1/IM - View 07-00
- The search conditions set in JP1/IM - View 07-10 to 07-51
- The search conditions set in JP1/IM - View 08-00 to 08-10
- The search conditions set in JP1/IM - View 08-50
- The search conditions set in JP1/IM - View 09-00 to 09-10
- The search conditions set in JP1/IM - View 09-50 to 10-50
- The search conditions set in JP1/IM - View 11-00

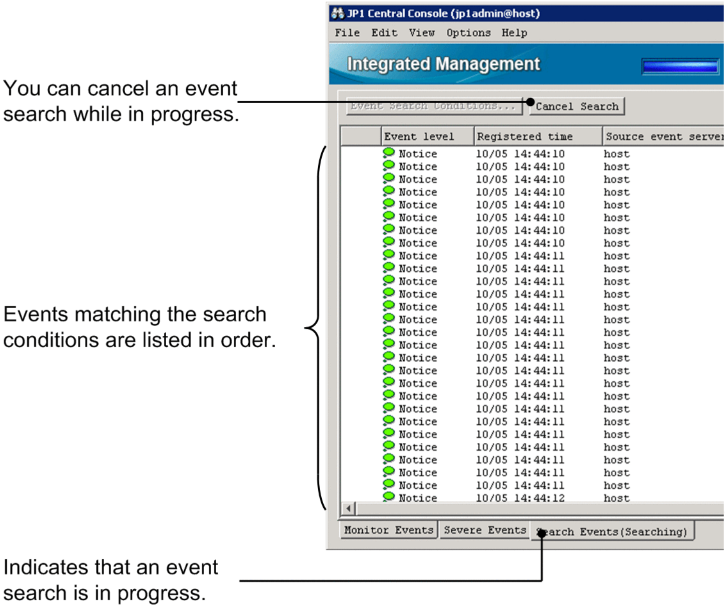
If the manager does not have a search condition whose version corresponds to the connected JP1/IM - View, the search conditions one version earlier than the version of the connected JP1/IM - View are acquired.

Progress display

While an event search is in progress, **(Searching)** appears on the tab of the **Search Events** page. When the search is completed, a dialog box reports that the search has ended and **(Searching)** disappears. This is a way of telling whether a search is still in progress when there are a large number of events to be searched or the search is taking a long time.

Events found to match the search conditions are listed in order on the **Search Events** page. The following figure shows the **Search Events** page while a search is in progress.

Figure 3–76: Search Events page during an event search



Event level	Registered time	Source event server
Notice	10/05 14:44:10	host
Notice	10/05 14:44:10	host
Notice	10/05 14:44:10	host
Notice	10/05 14:44:10	host
Notice	10/05 14:44:10	host
Notice	10/05 14:44:10	host
Notice	10/05 14:44:10	host
Notice	10/05 14:44:10	host
Notice	10/05 14:44:11	host
Notice	10/05 14:44:11	host
Notice	10/05 14:44:11	host
Notice	10/05 14:44:11	host
Notice	10/05 14:44:11	host
Notice	10/05 14:44:11	host
Notice	10/05 14:44:11	host
Notice	10/05 14:44:11	host
Notice	10/05 14:44:11	host
Notice	10/05 14:44:11	host
Notice	10/05 14:44:11	host
Notice	10/05 14:44:11	host
Notice	10/05 14:44:11	host
Notice	10/05 14:44:11	host
Notice	10/05 14:44:11	host
Notice	10/05 14:44:11	host
Notice	10/05 14:44:11	host
Notice	10/05 14:44:11	host
Notice	10/05 14:44:11	host
Notice	10/05 14:44:12	host

You can cancel an event search while in progress.

Events matching the search conditions are listed in order.

Indicates that an event search is in progress.

Canceling a search

You can cancel an event search already in progress if you have set the wrong search conditions, for example, or if you have just found the events you were looking for.

To cancel an event search, click the **Cancel Search** button on the **Search Events** page, or choose **View** and then **Cancel Search**.

When you cancel an event search, the JP1 events found up to that point are listed in the window.

> **Note**
>
> You can perform other tasks during an event search. For example, you can perform event monitoring in parallel with an event search. The menu commands for other tasks that you can perform remain selectable.
>
> Some selectable menu commands cannot be used while a search is in progress. If you attempt to use them, an error message appears.

3.6.2 Event search conditions

The following conditions apply to event searches:

- JP1/Base must be installed and the event service must be active on the host to be searched. (But the host does not need to be managed within a hierarchical system configuration.)
- The host to be searched must be directly reachable from the JP1/IM manager.

  To perform an event search, the JP1/IM - Manager (Central Console) to which you are logged in from JP1/IM - View connects directly to the host to be searched. The host must have a resolvable host name and be able to communicate. In particular, take care when searching for events in a firewall environment or when the host is connected to multiple LANs.

  Sometimes a JP1 event might arrive from a host that cannot be searched (because it is not directly reachable). This occurs because events are not transferred directly from agent to manager, but are forwarded in stages from agent to base manager, and from base manager to integrated manager. Event transfer and event searches use different communication paths. An event search can only be conducted on a host that the manager can communicate with directly.
- The JP1 events to be searched must still reside in the event database or integrated monitoring database.

  If you specify the event database in the search conditions, JP1 events in the event database are searched. If you specify the integrated monitoring database in the search conditions, JP1 events in the integrated monitoring database are searched.

  Each instance of JP1/Base has two event databases. When the maximum capacity (default 10 MB) of one event database is reached, the other event database is swapped in. At this point, the contents of the swapped-in event database are erased, and the erased JP1 events cannot be searched.

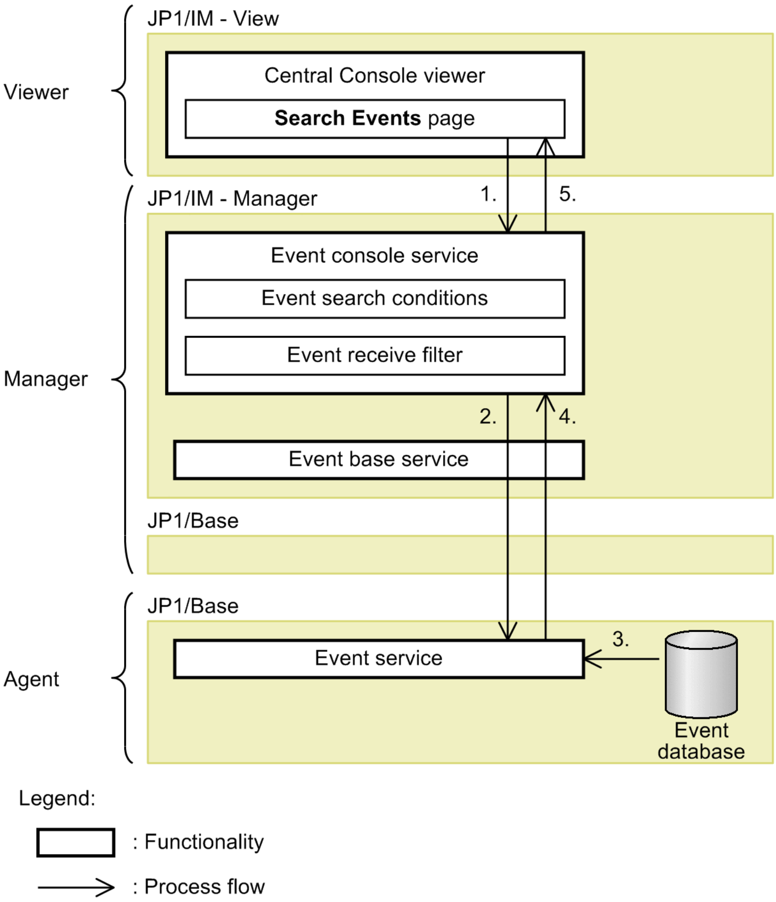
  The information in the event database and integrated monitoring database takes the form of files that are overwritten in a wrap-around cycle. Old JP1 events that have been overwritten cannot be retrieved.

3.6.3 Flow of processing of event searching

The flow of processing when searching for events differs according to the database you specify.

The following describes the flow of processing when searching the event database and when searching the integrated monitoring database.

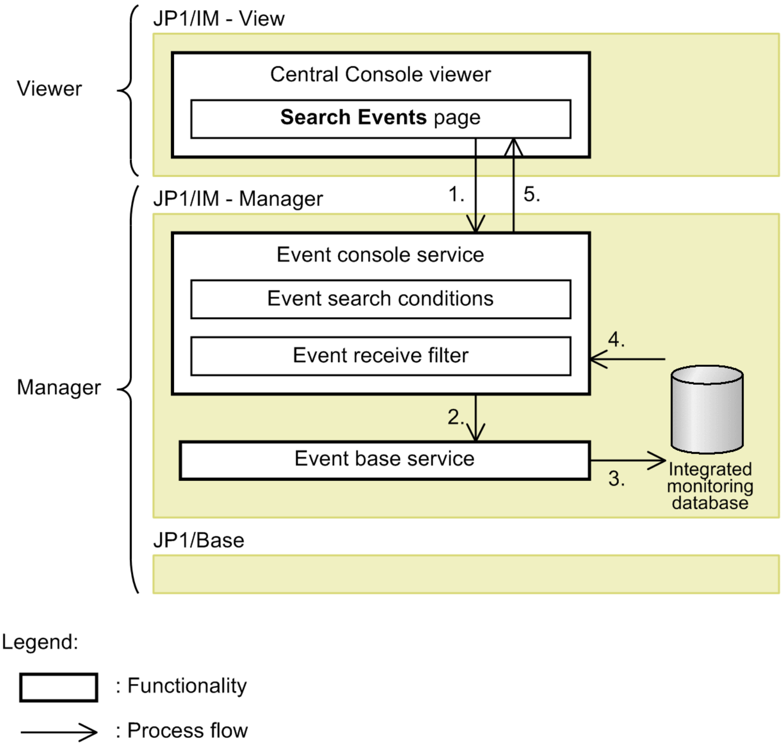
Figure 3–77: Flow of processing of event searching (event database specified)



The flow of processing when searching the event database is described below, following the numbers in the figure:

1. On the **Search Events** page of the Event Console window, specify conditions about the host to search and the JP1 events to retrieve, and then execute the search.
2. On receiving the search request from JP1/IM - View, the event console service of JP1/IM - Manager issues a search request to the event service of JP1/Base on the target host.
3. The event service of JP1/Base acquires JP1 events matching the search conditions from the event database.
4. The event service of JP1/Base sends back information about the JP1 events matching the search conditions to the event console service of JP1/IM - Manager.
5. The event console service of JP1/IM - Manager sends the received information back to JP1/IM - View, and the information is displayed on the **Search Events** page of the Event Console window.

Figure 3–78: Flow of processing event searching (integrated monitoring database specified)



The flow of processing when searching the integrated monitoring database is described below, following the numbers in the figure:

1. On the **Search Events** page of the Event Console window, specify conditions about the host to search and the JP1 events to retrieve, and then execute the search.
2. On receiving the search request from JP1/IM - View, the event console service of JP1/IM - Manager issues a search request to the event base service of JP1/IM - Manager on the target host.
3. The event base service of JP1/IM - Manager acquires JP1 events in memory and saves them to the integrated monitoring database.
4. The event console service of JP1/IM - Manager acquires JP1 events matching the search conditions from the integrated monitoring database.
5. The event console service of JP1/IM - Manager sends the received information back to JP1/IM - View, and the information is displayed on the **Search Events** page of the Event Console window.

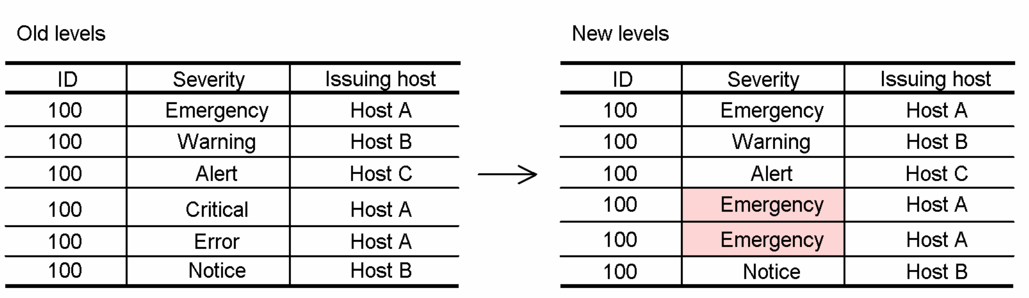
3.7 Changing the event level (severity) of JP1 events

When the integrated monitoring database is used, you can use the severity changing function, which changes the event level (severity) of a JP1 event to a predefined event level. By using this function, you can manage JP1 events depending on the system operations. You can change the event level of a JP1 event to `Emergency`, `Alert`, `Critical`, `Error`, `Warning`, `Information`, `Notice`, or `Debug`. After changing an event level, you can specify the new event level, or monitor events by using the new event level while using the following functions:

- JP1 event filtering (event receiver filter, severe event filter, and view filter)
- Correlation event
- Event search (when the search object is the integrated monitoring database)
- Event guide
- Automated action
- Output of event report
- Central Scope

By using these functions, for example, you can change the different event levels of JP1 events issued from various hosts to one event level for each host, or change different event levels of JP1 events to one event level for JP1 events.

Figure 3–79: Changing the event levels of JP1 events issued on Host A to Emergency



Old levels

ID	Severity	Issuing host
100	Emergency	Host A
100	Warning	Host B
100	Alert	Host C
100	Critical	Host A
100	Error	Host A
100	Notice	Host B

New levels

ID	Severity	Issuing host
100	Emergency	Host A
100	Warning	Host B
100	Alert	Host C
100	Emergency	Host A
100	Emergency	Host A
100	Notice	Host B

If you use the severity changing function, execute the `jcoimdef` command to enable this function. To enable this function, see *4.13 Setting the severity changing function* in the *JP1/Integrated Management - Manager Configuration Guide*.

You can specify the severity changing function in the Severity Change Definition Settings window or in the severity changing definition file. For details about the Severity Change Definition Settings window, see *2.21 Severity Change Definition Settings window (Add Severity Change Definition Settings window)* in the manual *JP1/Integrated Management - Manager GUI Reference*.

For details about the severity changing definition file, see *Severity changing definition file (jcochsev.conf)* (*Chapter 2. Definition Files*) in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

3.8 Changing the message display format

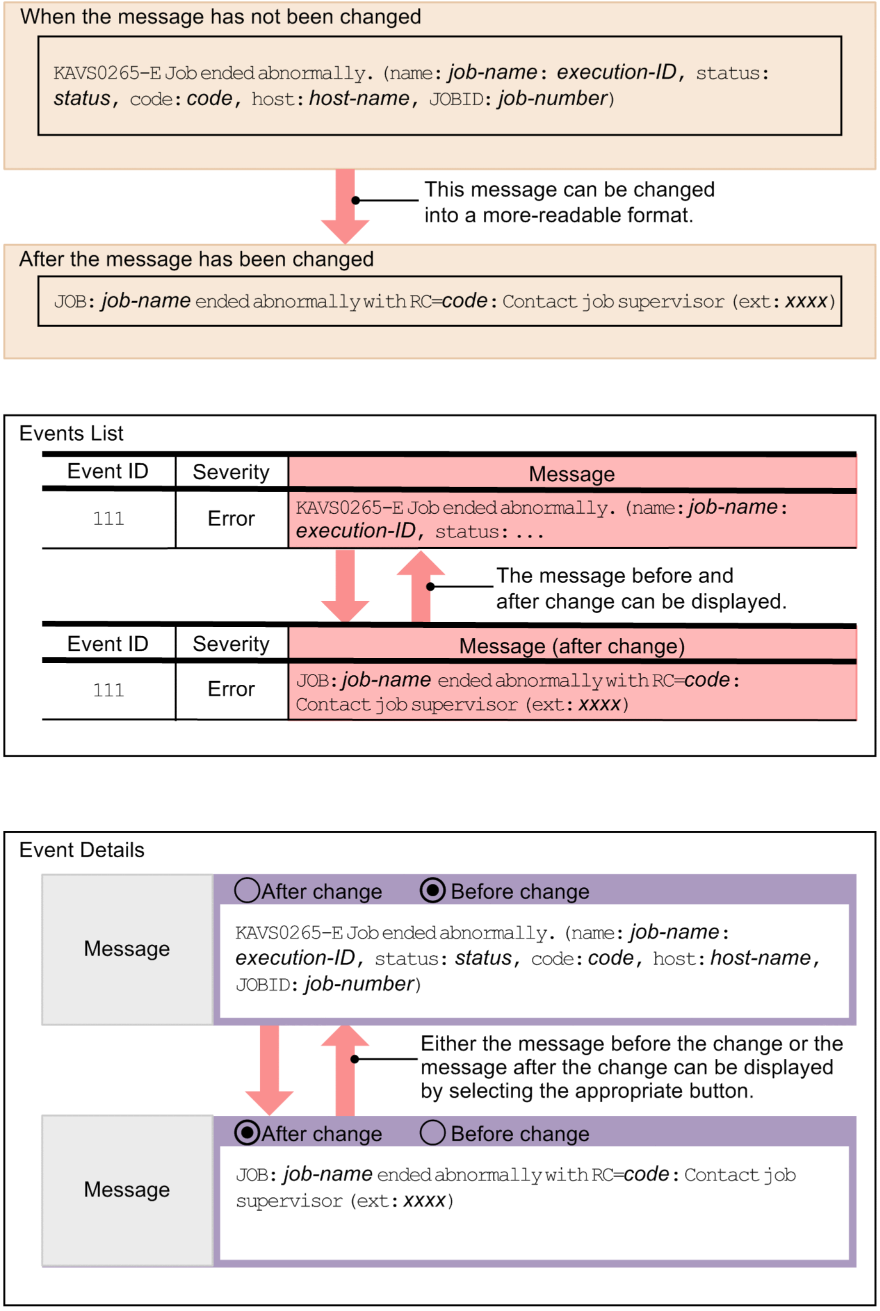
If you use the integrated monitoring database, you can use the display message change function. This function changes JP1 event messages to a predefined message display format. The function enables you to change JP1 event messages into a more readable format when they are displayed in JP1/IM - View's event list and the Event Details window. After you have changed messages, you can use the following functions to specify and monitor those messages:

- Inheritance to actions
- View filter
- Event search (when the search object is the integrated monitoring database)
- Event details
- Output of event report

For example, the operator can view and filter messages displayed in JP1/IM - View or, when using the email notification function to send email, insert the message text into the subject line or body of an email message.

The event inheritance information conversion function enables you to acquire readable event inheritance information by converting the lengths of message texts and numeric values to specified formats.

Figure 3–80: Overview of changing display messages



When the message has not been changed

KAVS0265-E Job ended abnormally. (name: *job-name*: *execution-ID*, status: *status*, code: *code*, host: *host-name*, JOBID: *job-number*)

This message can be changed into a more-readable format.

After the message has been changed

JOB: *job-name* ended abnormally with RC=*code*: Contact job supervisor (ext: *xxxx*)

Events List

Event ID	Severity	Message
111	Error	KAVS0265-E Job ended abnormally. (name: *job-name*: *execution-ID*, status: ...

The message before and after change can be displayed.

Event ID	Severity	Message (after change)
111	Error	JOB: *job-name* ended abnormally with RC=*code*: Contact job supervisor (ext: *xxxx*)

Event Details

Message

○After change ● Before change

KAVS0265-E Job ended abnormally. (name: *job-name*: *execution-ID*, status: *status*, code: *code*, host: *host-name*, JOBID: *job-number*)

Either the message before the change or the message after the change can be displayed by selecting the appropriate button.

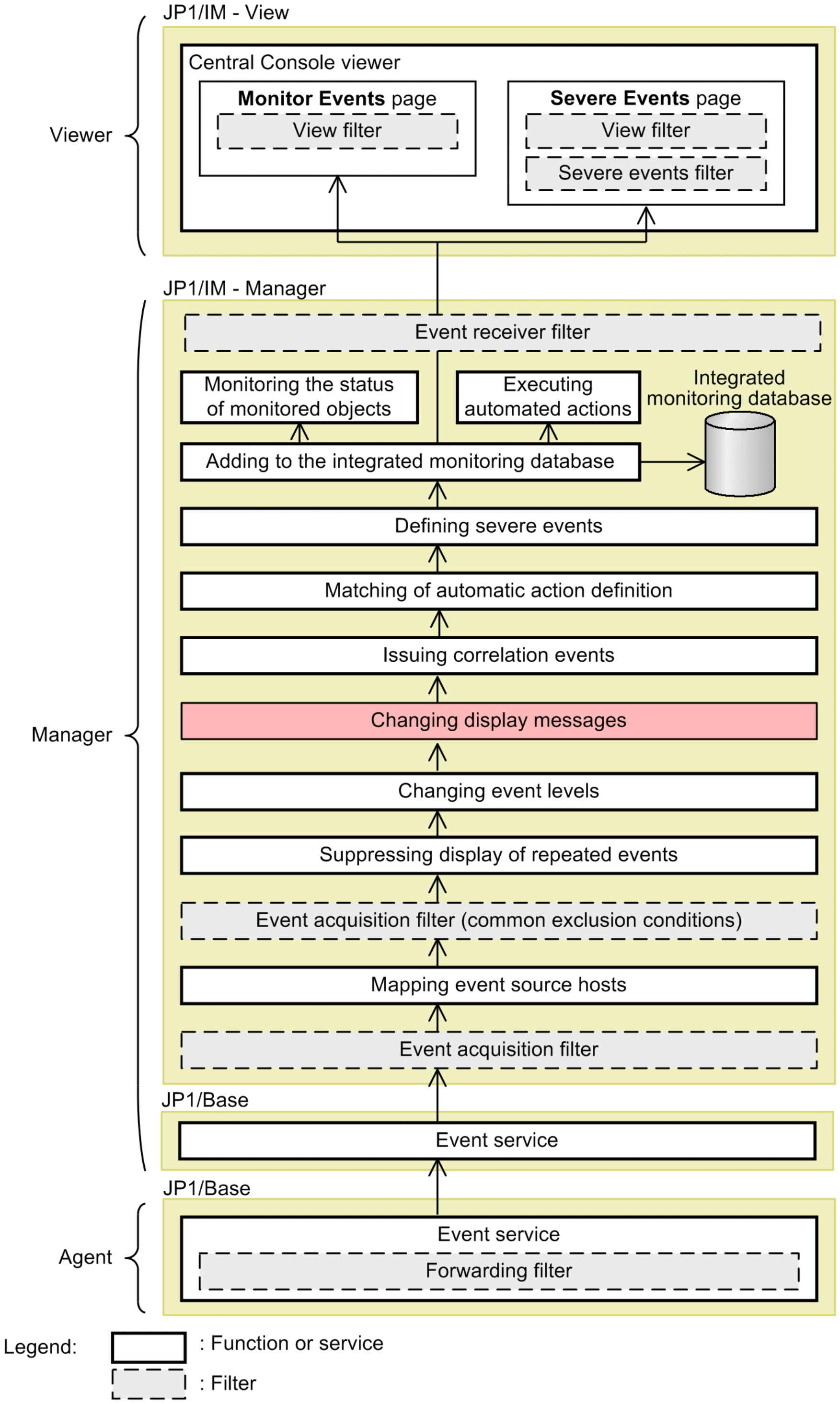
Message

●After change ○ Before change

JOB: *job-name* ended abnormally with RC=*code*: Contact job supervisor (ext: *xxxx*)

The following figure shows the relationship between the display message change function and the JP1 event filters and functions.

Figure 3–81: Relationship between the display message change function and the filters and functions


JP1/IM - View
Viewer
Central Console viewer
Monitor Events page
View filter
Severe Events page
View filter
Severe events filter
JP1/IM - Manager
Event receiver filter
Monitoring the status of monitored objects
Executing automated actions
Integrated monitoring database
Adding to the integrated monitoring database
Defining severe events
Matching of automatic action definition
Issuing correlation events
Changing display messages
Manager
Changing event levels
Suppressing display of repeated events
Event acquisition filter (common exclusion conditions)
Mapping event source hosts
Event acquisition filter
JP1/Base
Event service
JP1/Base
Agent
Event service
Forwarding filter
Legend:
: Function or service
: Filter

The display messages cannot be changed for events that occur after display messages have been changed or for JP1 events (event ID is `00006400`) that have been converted by JP1/IM - MO.

You must enable the integrated monitoring database to use the display message change function. Note that the display message change function cannot be used if the IM database has not been updated after upgrading a version 10-50 or earlier. For details, see *4.14 Setting the display message change function* in the *JP1/Integrated Management - Manager Configuration Guide*.

You can use the display message change function in the Display Message Change Definitions window. For details about the Display Message Change Definitions window, see *2.23 Display Message Change Definition Settings window (Add Display Message Change Definition Settings window)* in the manual *JP1/Integrated Management - Manager GUI Reference*.

You can also use the display message change definition file (`jcochmsg.conf`) to configure the display message change function. The display message change definition file (`jcochmsg.conf`) defines conditions for changing the messages to be displayed for JP1 events and the new messages that are to be displayed. For details, see *Display message change definition file (jcochmsg.conf)* in *Chapter 2. Definition Files* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

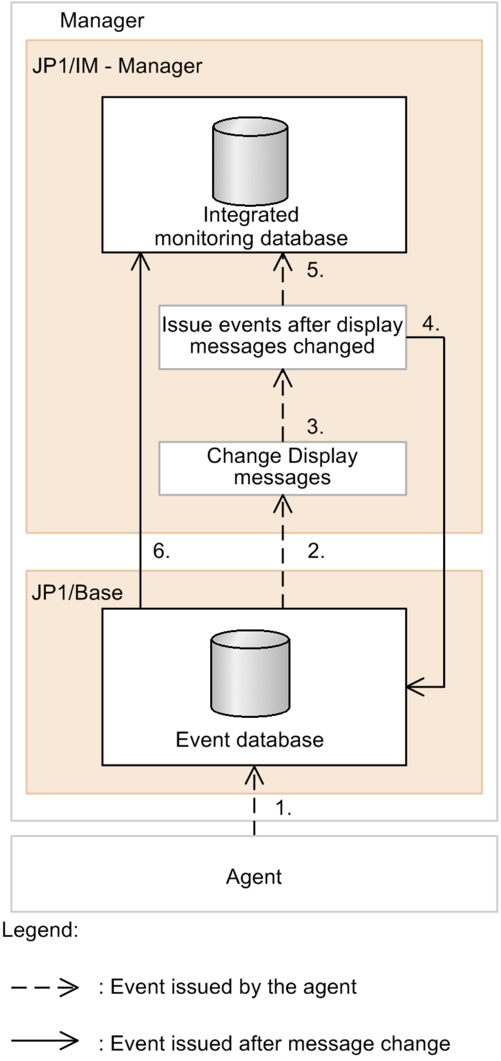
3.8.1 Using the display message change function to change messages and then issuing JP1 events

You can issue JP1 events so the user program can view the messages that have been changed by using the display message change function.

This is a compatibility function for user programs that view the JP1 events issued by JP1/IM - MO (events after a display message change) in an environment in which JP1/IM - MO is used with a version 10-50 or earlier.

The JP1 events equivalent to JP1/IM - MO (events after display message change) are issued only for those events whose display message has been changed.

Figure 3–82: Flow of event issuance after display message change


Manager
JP1/IM - Manager
Integrated monitoring database
5.
Issue events after display messages changed
4.
3.
Change Display messages
6.
2.
JP1/Base
Event database
1.
Agent
Legend:
: Event issued by the agent
: Event issued after message change

The flow of processing is described below, following the numbers in the figure. (The numbers in the figure correspond to the numbers below.)

1. Events issued by the agent are forwarded to JP1/Base on the manager host.
2. JP1/IM - Manager obtains the above events.
3. The display messages for the events in step 2 are changed.
4. Events after display message change are issued.
5. The events in step 3 are registered in the integrated monitoring database.
6. JP1/IM - Manager obtains the events in step 4, and then registers them in the integrated monitoring database.

If you will be issuing events after display message change, enable the function in the environment definition file for events after the display message is changed. For details, see *Environment definition file for events after the display message is changed (chmsgevent.conf)* (*Chapter 2. Definition Files*) in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

3.9 Mapping of the event source hosts

The management of host information in JP1 events has been a troublesome task for the system administrator when those events are issued from other monitoring systems. For example, the system administrator needs to check the host information displayed in messages and in the Event Details window.

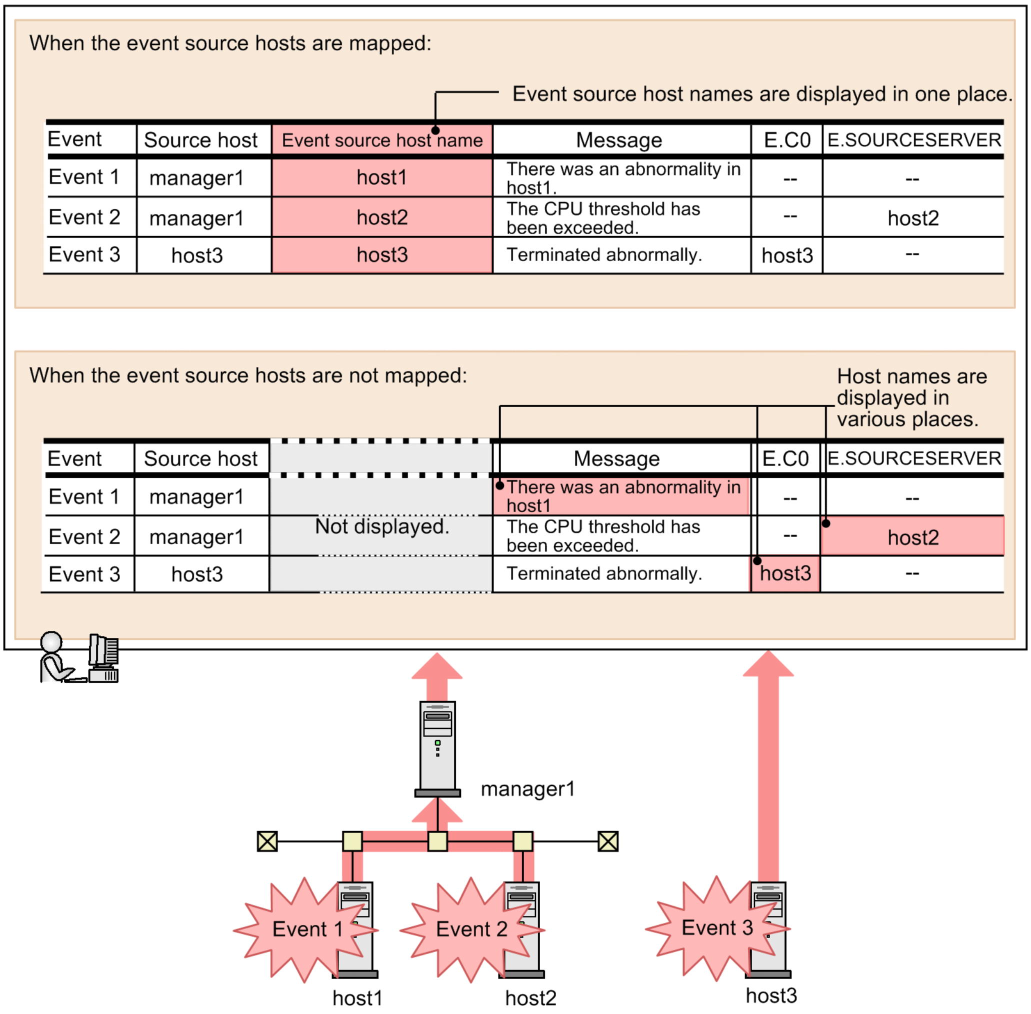
When you use mapping of the event source hosts, you can display and define the events that caused JP1 events as the *event source hosts*.

The mapping function of the event source host compares a JP1 event received from the event service on the manager host with the event condition. If the JP1 event satisfies the event condition, the function maps information about the host on which the event set in the JP1 event has occurred to the **Event source host name** attribute (which is an extended attribute of the JP1 event), and then adds the information to the integrated monitoring database. If the JP1 event does not satisfy the event condition, the function maps the information about that host to **Source host** (event-issuing server) and then adds the information to the integrated monitoring database.

By using this function, the system administrator can display **Event source host name** as an item in the Event Console window, and then use an event source host to search for events or define actions.

This function can be used when the integrated monitoring database is used.

Figure 3–83: Example display in the Event Console window



When the event source hosts are mapped:

Event source host names are displayed in one place.

Event	Source host	Event source host name	Message	E.C0	E.SOURCESERVER
Event 1	manager1	host1	There was an abnormality in host1.	--	--
Event 2	manager1	host2	The CPU threshold has been exceeded.	--	host2
Event 3	host3	host3	Terminated abnormally.	host3	--

When the event source hosts are not mapped:

Host names are displayed in various places.

Event	Source host		Message	E.C0	E.SOURCESERVER
Event 1	manager1	Not displayed.	There was an abnormality in host1	--	--
Event 2	manager1		The CPU threshold has been exceeded.	--	host2
Event 3	host3		Terminated abnormally.	host3	--

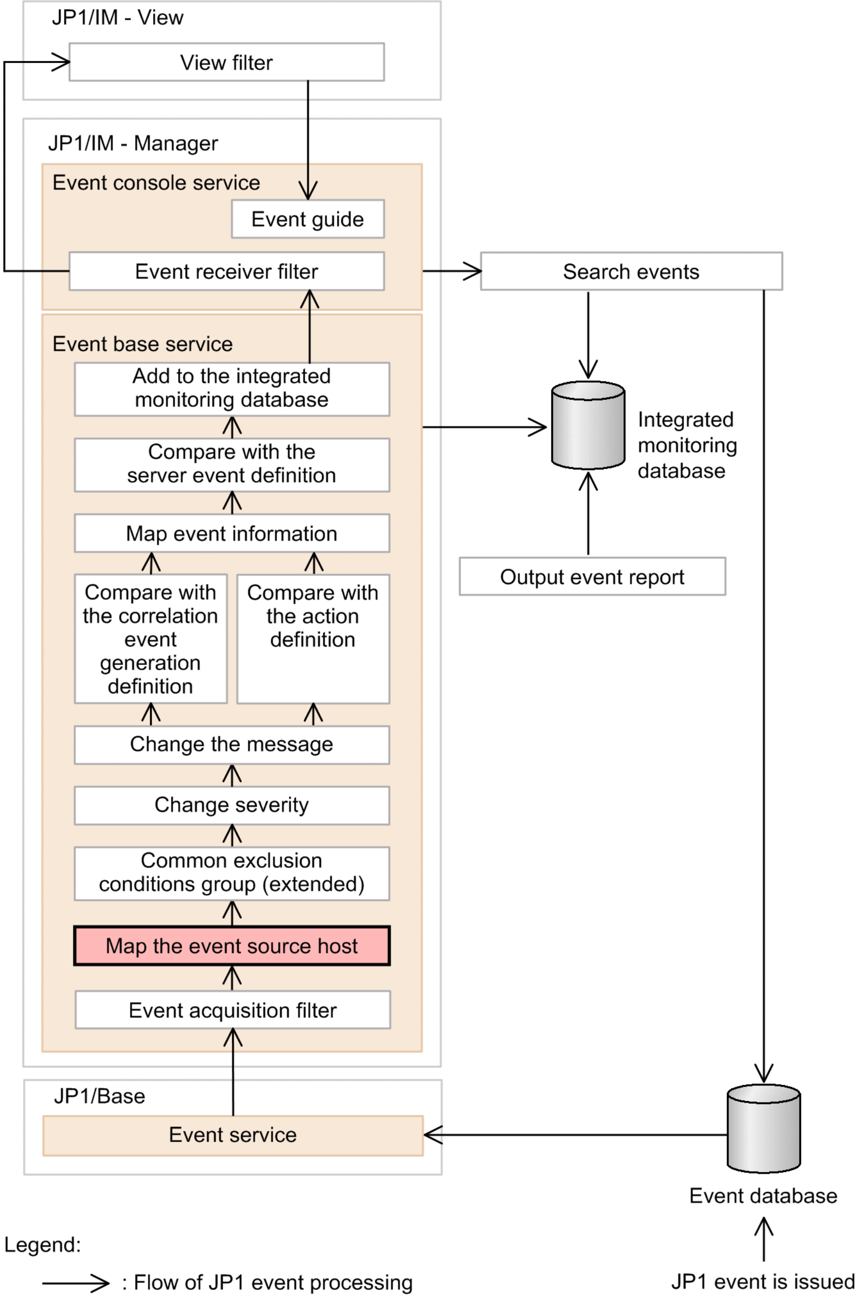
Execute the `jcoimdef` command to enable mapping of the event source hosts. To do this, see *4.15 Setting event source host mapping* in the *JP1/Integrated Management - Manager Configuration Guide*.

Event source hosts are not displayed in the event list by default. To display the event source hosts in the event list, from the Preferences window, set the event source host item in **Available items**. For details about the Preferences window, see *2.24 Preferences window* in the manual *JP1/Integrated Management - Manager GUI Reference*.

3.9.1 Overview of mapping

Mapping of event source hosts is provided by the event base service. The following shows the relationship between the processing of main functions and event-source-host mapping.

Figure 3–84: Relationship between the processing of main functions and event-source-host mapping


JP1/IM - View
View filter
JP1/IM - Manager
Event console service
Event guide
Event receiver filter
Search events
Event base service
Add to the integrated monitoring database
Compare with the server event definition
Map event information
Compare with the correlation event generation definition
Compare with the action definition
Change the message
Change severity
Common exclusion conditions group (extended)
Map the event source host
Event acquisition filter
Integrated monitoring database
Output event report
JP1/Base
Event service
Event database
JP1 event is issued
Legend:
: Flow of JP1 event processing

After JP1 events are acquired from the JP1/Base event service, host information is mapped with JP1 event extended attribute **Event source host name** (`E.JP1_SOURCEHOST`). The JP1 events to be mapped here are the JP1 events that are automatically mapped and any JP1 events that match the conditions defined in the event-source-host mapping definition file.

For details about the JP1 events that are automatically mapped, see *4.15 Setting event source host mapping* in the manual *JP1/Integrated Management - Manager Configuration Guide*. For details about the event-source-host mapping definition file, see *Event-source-host mapping definition file (user_hostmap.conf)* in *Chapter 2. Definition Files* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

If an acquired event does not match any of the conditions in the event-source-host mapping definition file, the value of **Source host** (`B.SOURCESERVER`) is mapped. If a value has already been set for the extended attribute for acquired JP1 event **Event source host name** (`E.JP1_SOURCEHOST`), the event source host is not mapped even if the event matches the conditions in the event-source-host mapping definition file.

Event source hosts are not mapped in the following cases:

- There is no attribute subject to mapping.
  The error message ID `KAVB4666-W` is set for **Event source host name** (`E.JP1_SOURCEHOST`).
- The value of the attribute subject to mapping is the null character.
  The value of **Source host** (`B.SOURCESERVER`) is mapped.
- The event source host name for the received JP1 event exceeds 255 bytes.
  The error message ID `KAVB4666-W` is set for **Event source host name** (`E.JP1_SOURCEHOST`).
- The number of program-specific extended attributes exceeds 100 as a result of mapping.
  Event source host name (`E.JP1_SOURCEHOST`) is not set.
- The size of the JP1 event exceeds 10,000 bytes, the permitted maximum size, as a result of mapping.
  Event source host name (`E.JP1_SOURCEHOST`) is not set.

If overwrite installation is performed for JP1/IM - Manager, the definitions set in the event-source-host mapping definition file are inherited. Also, the setting as to whether to enable or disable the mapping function of the event source hosts is inherited.

3.10 Event guide function

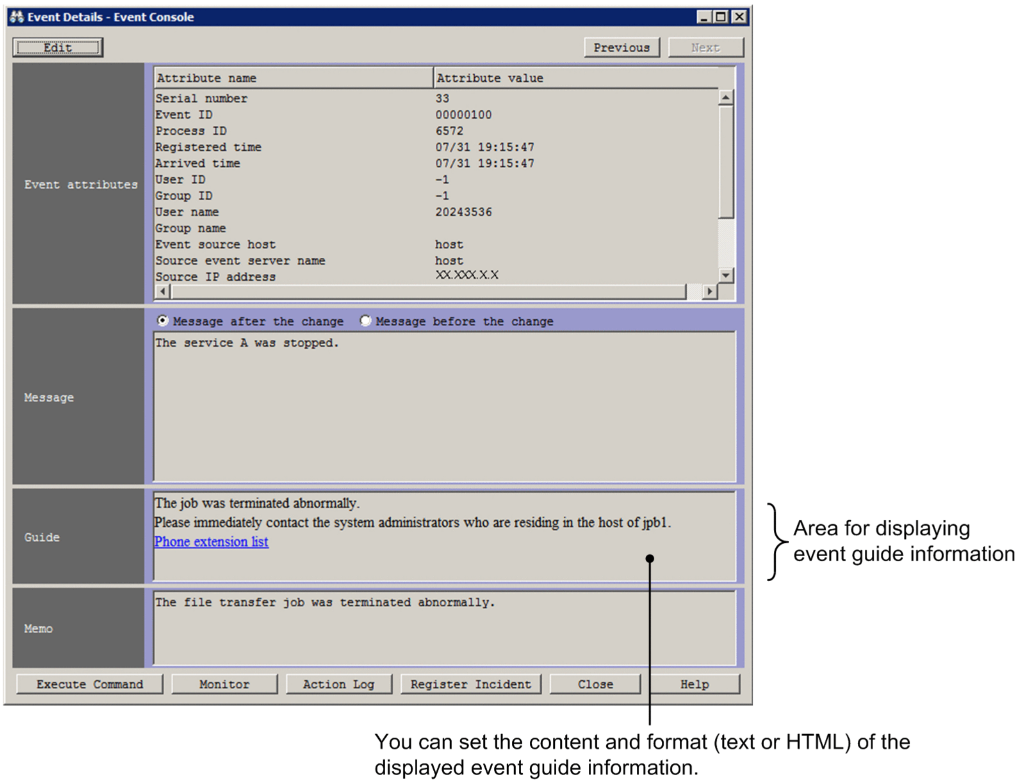
The event guide function displays guidance on handling JP1 events displayed in the Event Console window.

The system administrator carries out error investigation and resolution based on JP1 events, but it is difficult to learn all the tracking and troubleshooting procedures for the numerous JP1 events that might be issued from a linked JP1 product or user application.

By using the event guide function, you can register and accumulate know-how (such as past cases and how to investigate or handle errors) which you can refer to when an error occurs.

The information displayed by the event guide function is known as *event guide information*. You can specify the contents and format (text or HTML) of this information. Event guide information appears in the Event Details window as part of the JP1 event details. The following figure shows a display example.

Figure 3–85: Example of event guide information displayed in the Event Details window



Attribute name	Attribute value
Serial number	33
Event ID	00000100
Process ID	6572
Registered time	07/31 19:15:47
Arrived time	07/31 19:15:47
User ID	-1
Group ID	-1
User name	20243536
Group name	
Event source host	host
Source event server name	host
Source IP address	XX.XXX.X.X

● Message after the change ○ Message before the change

The service A was stopped.

The job was terminated abnormally.
Please immediately contact the system administrators who are residing in the host of jpb1.
Phone extension list

The file transfer job was terminated abnormally.

Area for displaying event guide information

You can set the content and format (text or HTML) of the displayed event guide information.

By default, the **Guide** area does not appear in the Event Details window.

The event guide information file is referenced when you log in to JP1/IM - View. If one or more applicable conditions are found, the **Guide** area is displayed. The file and its settings are described next.

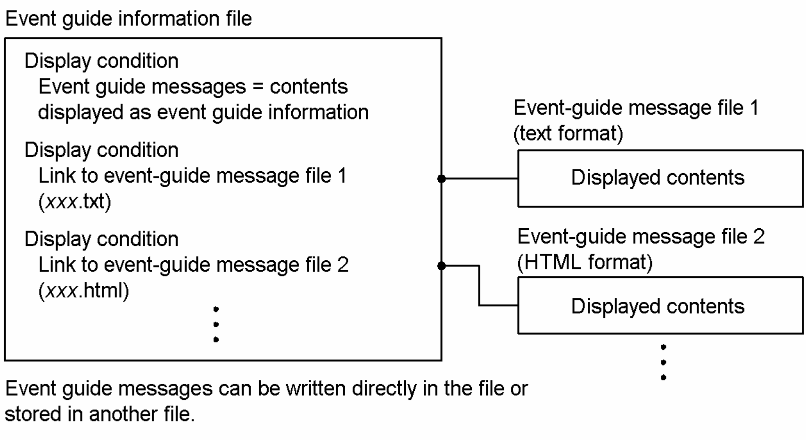
3.10.1 Settings for event guide information

Event guide information is set in an event guide information file managed by JP1/IM - Manager.

In this file, you can enter settings about the contents to be displayed as event guide information, conditions about the target JP1 events, and other definitions.

The contents displayed as event guide information are called *event guide messages*. Messages can be stored and managed in individual files known as *event-guide message files*. The relationship between the two types of files is shown below.

Figure 3–86: Relationship between the event guide information file and event-guide message files


Event guide information file
Display condition
Event guide messages = contents displayed as event guide information
Display condition
Link to event-guide message file 1 (*xxx*.txt)
Display condition
Link to event-guide message file 2 (*xxx*.html)
Event-guide message file 1 (text format)
Displayed contents
Event-guide message file 2 (HTML format)
Displayed contents
Event guide messages can be written directly in the file or stored in another file.

The update timing after you edit an event guide message differs for the event guide information file and event-guide message files, as follows:

- Event guide information file

  To apply the changes (edited message or condition definition) in the event guide information file, you must execute the `jco_spmd_reload` command or restart JP1/IM - Manager.

  After the changes have been applied, the **Guide** area, if not currently displayed, appears in the Event Details window the next time a user logs in to JP1/IM - View.

- Event-guide message file

  After you edit an event-guide message file, the changes appear when you simply refresh the Event Details window.

We recommend that you use an event-guide message file if you periodically edit messages.

3.10.2 Conditions for displaying event guide information

Using a condition (`EV_COMP`), you can specify which of the issued JP1 events to target in displaying event guide information. When you specify multiple conditions, an AND condition is assumed and the guide information is displayed when all the conditions are satisfied.

`EV_COMP` is a JP1 event comparison condition in the format *attribute-name*`:`*attribute-value*. You can set a maximum of 100 such conditions.

- *attribute-name*

  Specify the name of a JP1 event attribute (basic or extended attribute).

  For example, you can specify the event ID (`B.ID`), event level (`E.SEVERITY`), or other attribute name. If you changed the event level of a JP1 event using the function for changing the severity level, the new event level applies when the JP1 event contents are compared.

  You can also specify program-specific information (provided as an extended attribute of JP1 events) for a particular JP1 product.

  For example, you can specify the host that executes JP1/AJS jobs (`E.C0`).

Note that you cannot use a business group name for the source event server name (B.SOURCESERVER), destination event server name (B.DESTSERVER), and event source host name (E.JP1_SOURCEHOST). If you specify a business group name, it will be treated as a host name.

When specifying IPv6 addresses for the source IP address (B.SOURCEIPADDR) and destination IP address (B.DESTIPADDR), use lower case characters as follows:

```
0011:2233:4455:6677:8899:aabb:ccdd:eeff
```

You cannot use the abbreviated format of an IP address as follows:

```
2012:7:8::a:b
```

- *attribute-value*

  Specify the attribute value corresponding to the attribute name.

  For example, to specify JP1 events whose event level (E.SEVERITY) is Error, specify E.SEVERITY:Error. To specify an event whose event ID (B.ID) is 00000111, specify B.ID: 00000111:00000000.

When event guide information is displayed in JP1/IM - View, the contents of the event guide information file are referenced from the top. When an item matching the conditions is found, referencing stops and the applicable information appears in the Event Details window.

Because the Event Details window displays only the first of possibly multiple items in the event guide information file that match the conditions, bear the following in mind when setting display conditions:

- Make sure that the comparison condition does not duplicate a comparison condition set for a different event guide item.

  For example, by setting multiple conditions in a comparison condition, such as an event level or message in addition to the event ID, you can differentiate the comparison condition from that set for another event guide item.

  A regular expression can be written as an attribute value, but it must require a complete match.
- Set no more than one event guide item for one JP1 event.

  To set multiple items for one JP1 event, consider writing multiple action procedures in HTML format in an event-guide message file.

3.10.3 Contents displayed as event guide information

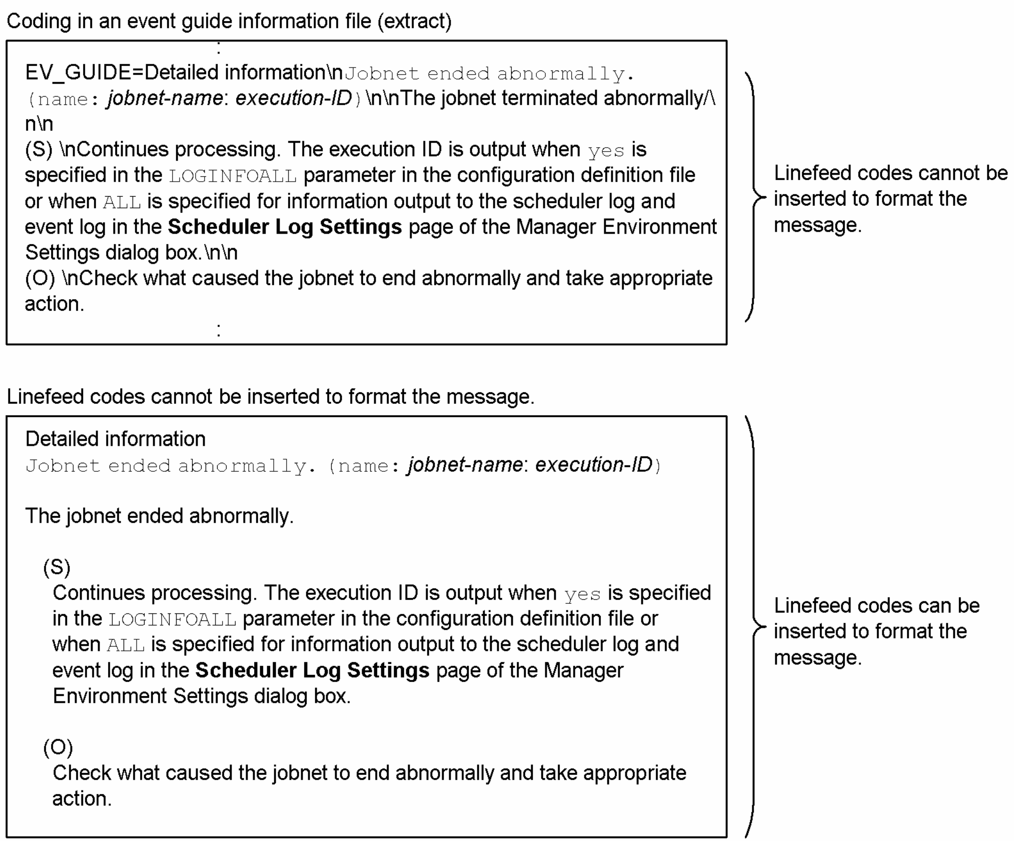
To write event guide messages directly in an event guide information file, specify EV_GUIDE. To use event-guide message files, specify EV_FILE instead of EV_GUIDE and write the file locations.

Messages can be written in text format or HTML format. The attribute values of JP1 events can also be used as variables in messages (by prefixing the attribute value with $). For example, if you write $B.MESSAGEΔ (where Δ represents a space), JP1 event messages (B.MESSAGE) will be handled as variables, and the attribute value of the JP1 event will be displayed in the event guide message.

Event-guide message file as a useful tool when editing

When event guide messages are written directly in an event guide information file (EV_GUIDE specified), each message is a single line. You cannot format the message layout by inserting linefeed codes. However, you can do so in an event-guide message file (EV_FILE specified). This is illustrated in the figure below.

Figure 3–87: Examples of writing event guide information



Coding in an event guide information file (extract)

```
                              :
EV_GUIDE=Detailed information\nJobnet ended abnormally.
(name: jobnet-name: execution-ID) \n\nThe jobnet terminated abnormally/\
n\n
(S) \nContinues processing. The execution ID is output when yes is
specified in the LOGINFOALL parameter in the configuration definition file
or when ALL is specified for information output to the scheduler log and
event log in the Scheduler Log Settings page of the Manager Environment
Settings dialog box.\n\n
(O) \nCheck what caused the jobnet to end abnormally and take appropriate
action.
                              :
```

Linefeed codes cannot be inserted to format the message.

Linefeed codes cannot be inserted to format the message.

Detailed information
`Jobnet ended abnormally. (name:` *jobnet-name*: *execution-ID*`)`

The jobnet ended abnormally.

(S)
Continues processing. The execution ID is output when `yes` is specified in the `LOGINFOALL` parameter in the configuration definition file or when `ALL` is specified for information output to the scheduler log and event log in the **Scheduler Log Settings** page of the Manager Environment Settings dialog box.

(O)
Check what caused the jobnet to end abnormally and take appropriate action.

Linefeed codes can be inserted to format the message.

Because you can apply formatting in this way, an event-guide message file is useful when you are preparing messages in HTML format, and there is a large amount of information or you need to periodically review the message contents.

About event guide information files:

See *Event guide information file (jco_guide.txt)* in *Chapter 2. Definition Files* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

3.11 Setting memo entries

You can set additional information about a JP1 event displayed in the Event Console window. This functionality is available for JP1 events registered in the integrated monitoring database when you use the integrated monitoring database.

When an issue is encountered during investigation of a JP1 event, the system administrator will need to record what steps were taken or report the issue to other users. By entering a memo to accompany the particular JP1 event, the system administrator can summarize what steps were taken and write notes to other users. Users can then find out the state of investigation and what precautions to take, simply by referencing the JP1 event in the Event Console window.

Memo entries are subject to content comparisons in the following:

- View filter conditions
- Event search conditions

The contents of a memo entry can be included in an event report output by the `jcoevtreport` command.

To use the memo functionality, enable memo entry in the `jcoimdef` command.

3.12 Adding program-specific attributes

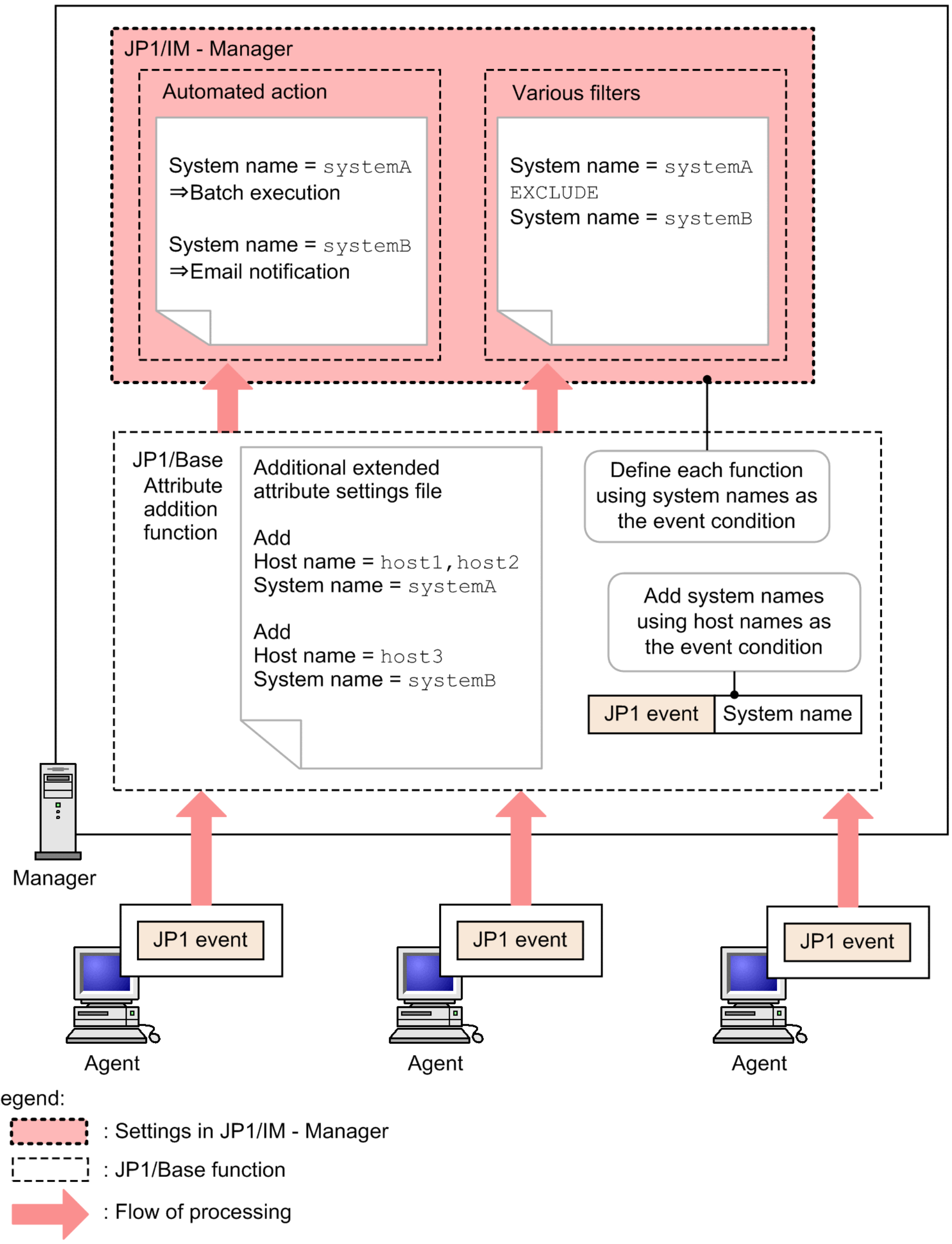
If the number of events that might occur increases due to addition of monitored applications and hosts, the system administrator must set similar event conditions for each function, which constitutes an added burden on the management tasks.

Addition of program-specific attributes is a function for adding program-specific attributes to JP1 events. This function enables the system administrator to define actions and filtering for a set of events with a common attribute (grouping). When the number of events increases after program-specific attributes have been defined, the system administrator only needs to modify the attribute addition function definition. There is no need to change the definitions of automated actions or various filters. In addition, the definition of each function becomes simple.

This function enables the system administrator to display events with the added information, such as system names, business names, and system status. This saves time in checking multiple attribute values and system configuration information, which makes the handling of events easier.

The following figure provides an overview of the procedure for adding attributes to JP1 events and defining them in individual functions.

Figure 3–88: Overview of adding program-specific attributes



Addition of attributes to JP1 events is specified when the corresponding events are registered into or forwarded and received in the event database.

Normally, you can centrally set and manage attribute addition conditions for JP1 events that are transferred from monitored hosts by setting the attribute addition conditions on the manager host.

Note that event registration performance is adversely affected in proportion to the product of the number of attribute addition conditions and the number of registered events. If you run JP1/IM - Manager in a system hierarchy, we strongly recommend that you use a base manager or a relay manager to set attribute addition conditions.

Added attributes are maintained even when the corresponding JP1 events are forwarded to other hosts. Therefore, the attribute information added by a base manager or a relay manager can be used as is, even if the attribute addition conditions are not set in the top JP1/IM - Manager.

Conditions for specifying JP1 events to which attributes are to be added and the attribute names to be added are defined in the additional extended attribute settings block (from `add` to `end-add [exit]`) in the additional extended attribute settings file. You can define a maximum of 1,024 additional extended attribute settings blocks.

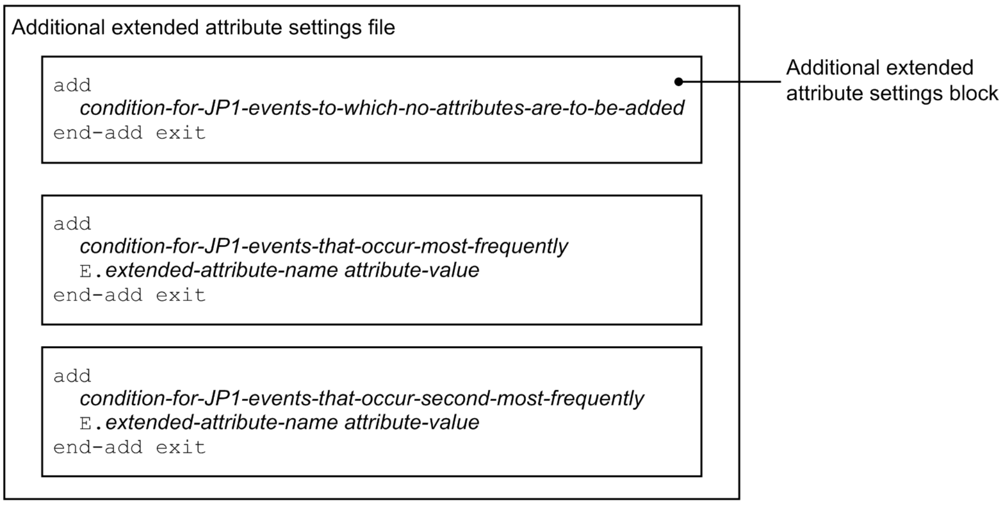
Individual conditions are checked sequentially from the top of the additional extended attribute settings block for each JP1 event that is registered or is forwarded and received. If a condition is satisfied, the specified attribute name and value are added. If `exit` is specified in an additional extended attribute settings block, the additional extended attribute settings block processing is skipped for the corresponding JP1 event and the next JP1 event is processed.

To minimize the effects of attribute addition on the registration and forwarding of JP1 events, we recommend that you define the additional extended attribute settings file as follows:

- Do not specify `exit` in additional extended attribute settings blocks except when multiple conditions are used for a single JP1 event to add different attributes. This saves time in processing subsequent additional extended attribute settings blocks.
- In the first additional extended attribute settings block, specify the condition for JP1 events to which no attributes are to be added. This saves time in processing subsequent additional extended attribute settings blocks.
- Define the conditions for JP1 events that occur frequently early in the additional extended attribute settings file.

See the following figure for details.

Figure 3–89: How to specify the additional extended attribute settings file


Additional extended attribute settings file
Additional extended attribute settings block

```
add
   condition-for-JP1-events-to-which-no-attributes-are-to-be-added
end-add exit

add
   condition-for-JP1-events-that-occur-most-frequently
   E.extended-attribute-name attribute-value
end-add exit

add
   condition-for-JP1-events-that-occur-second-most-frequently
   E.extended-attribute-name attribute-value
end-add exit
```

For details about adding program-specific attributes, see *4.10 Adding program-specific attributes* in the *JP1/Integrated Management - Manager Configuration Guide*.

For details about the additional extended attribute settings file, see the *JP1/Base User's Guide*.

3.13 Displaying program-specific extended attributes and specifying them in event conditions

If you specify a definition file for extended event attributes (extended file), you can display desired item names for program-specific extended attributes in the events list in the Event Console window. You can also specify desired item names for program-specific extended attributes in event conditions, such as view filters and event receiver filters.

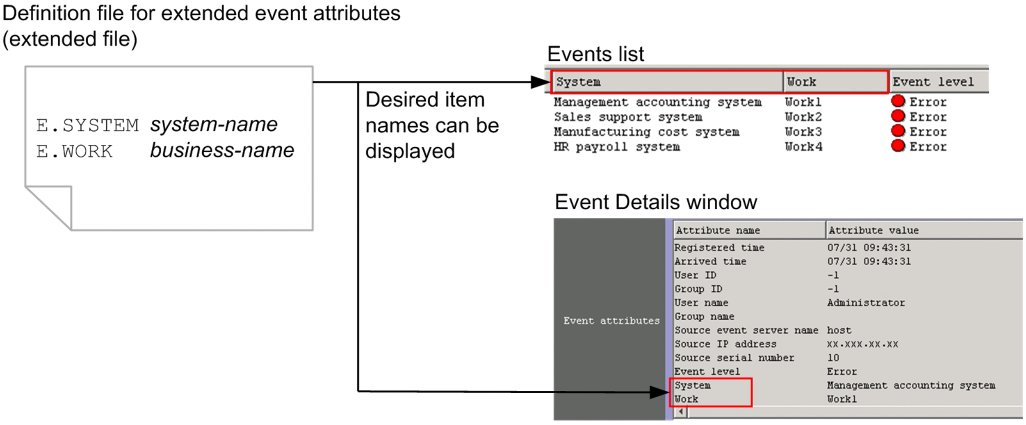
3.13.1 Displaying and outputting program-specific extended attributes

You can display in the events list and the Event Details window and output in event reports desired item names for program-specific extended attributes that are defined in the definition file for extended event attributes (extended file). This functionality is called the program-specific extended attribute display function.

You use the definition file for extended event attributes (extended file) to specify the program-specific extended attribute display function for each system (JP1/IM - Manager). When you use JP1/IM - View to connect to the JP1/IM - Manager on which the definition file for extended event attributes (extended file) has been set, the defined item names are displayed for extended attributes in the events list and the Event Details window. You can use the Preferences window to set the program-specific extended attribute items to be displayed or hidden in the events list for each user.

Note that in the Web-based JP1/IM - View, the item names defined in the definition file for extended event attributes (extended file) cannot be displayed in the events list. In the Web-based JP1/IM - View, only the Event Details window and the Edit Event Details window can display item names that are defined in the definition file for extended event attributes (extended file).

Figure 3–90: Displaying program-specific extended attributes in JP1/IM - View



System	Work	Event level
Management accounting system	Work1	● Error
Sales support system	Work2	● Error
Manufacturing cost system	Work3	● Error
HR payroll system	Work4	● Error

Attribute name	Attribute value
Registered time	07/31 09:43:31
Arrived time	07/31 09:43:31
User ID	-1
Group ID	-1
User name	Administrator
Group name	
Source event server name	host
Source IP address	xx.xxx.xx.xx
Source serial number	10
Event level	Error
System	Management accounting system
Work	Work1

If you set a definition file for extended event attributes (extended file), the program-specific extended attributes that are displayed in the windows for specifying event conditions, such as view filters and event receiver filters, are displayed as item names (such as system name and server's role), not as attribute names (such as `E.SYSTEM` and `E.ROLE`). For details, see *3.13.2 Specifying program-specific extended attributes in event conditions*.

You can also output these item names, not the attribute names, to CSV-format event reports in the same manner as for basic attributes and shared extended attributes on the JP1/IM - Manager in which the definition file for extended event attributes (extended file) has been set. For details, see *3.15 CSV output of information displayed in JP1/IM - View*.

Table 3–19: Functions that can display or output program-specific extended attributes

Component	Function#1, #2	Window or command
Central Console	Display of events list (including CSV output)	Event Console window
		Related Events (Summary) window
		Related Events (Correlation) window
		Execute Command window
	Display of event details	Event Details window
		Edit Event Details window
	Output of event report	`jcoevtreport` command
	Window for setting event conditions	Action Parameter Detailed Definitions window#3
		Common Exclusion-Condition Settings (Extended) window
		Severity Change Definition Settings window (Add Severity Change Definition Settings window)
		Repeated Event Condition Settings window
		Event Search Conditions (Program-Specific Information in Extended Attribute) window
		Severe Event Definitions window#4
		Event Acquisition Settings window#4
		Common Exclusion-Conditions Settings window#4
		Event Search Conditions window#4
		Settings for View Filter window#4
		Detailed Settings for Event Receiver Filter window#4
		Event-Information Mapping Definitions window
		Display Message Change Definition Settings window (Add Display Message Change Definition Settings window)

#1: In the Web-based JP1/IM - View, functions other than the function for displaying event details cannot display program-specific extended attributes.

#2: To enable functions other than the function for displaying event details to display program-specific extended attributes, JP1/IM - Manager 11-00 or later and JP1/IM - View 11-00 or later must be connected. To enable the function for displaying event details to display program-specific extended attributes, JP1/IM - Manager 11-00 or later must be connected (with no restriction on the version of JP1/IM - View).

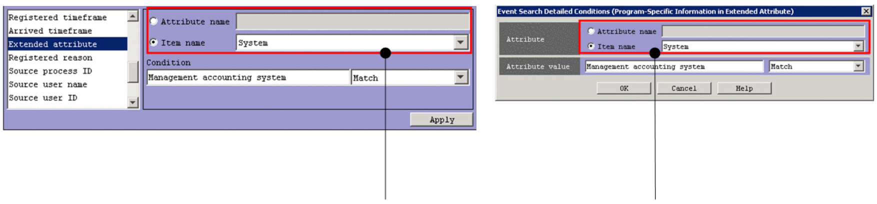
#3: The Action Parameter Detailed Definitions (for compatibility) window is excluded.

#4: The Event Search Conditions (Program-Specific Information in Extended Attribute) window is opened from this window to specify settings.

3.13.2 Specifying program-specific extended attributes in event conditions

If you set a definition file for extended event attributes (extended file), you can specify item names (such as system name and server's role) instead of attribute names (such as `E.SYSTEM` and `E.ROLE`) as program-specific extended attributes in event conditions, such as view filters and event receiver filters. This functionality is called the program-specific extended attribute specification function.

Figure 3–91: Program-specific extended attributes that are displayed in the windows for specifying event conditions



In windows such as the Action Parameter Detailed Definitions window

Registered timeframe
Arrived timeframe
Extended attribute
Registered reason
Source process ID
Source user name
Source user ID

○ Attribute name
● Item name: System

Condition: Management accounting system — Match

In the Event Search Detailed Conditions (Program-Specific Information in Extended Attribute) window

Event Search Detailed Conditions (Program-Specific Information in Extended Attribute)

Attribute: ○ Attribute name / ● Item name: System

Attribute value: Management accounting system — Match

You can select an item name defined in the definition file for extended event attributes (extended file).

You can specify item names as program-specific extended attributes in the following functions (windows):

- Action Parameter Detailed Definitions window#
- Event-Information Mapping Detailed Definitions window
- Severe Event Definitions window
- Event Acquisition Settings window
- Common Exclusion-Conditions Settings window
- Common Exclusion-Condition Settings (Extended) window
- Settings for View Filter window
- Detailed Settings for Event Receiver Filter window
- Event Search Conditions window
- Severity Change Definition Settings window (Add Severity Change Definition Settings window)
- Repeated Event Condition Settings window
- Display Message Change Definition Settings window (Add Display Message Change Definition Settings window)

#: The Action Parameter Detailed Definitions (for compatibility) window is excluded.

3.14 Displaying user-defined event attributes

By customizing the JP1/IM definition files, you can extend the functionality available when another application is linked with JP1/IM. With the extended functions, you can perform the following operations.

3.14.1 Displaying the attributes of user-defined events

User applications can issue JP1 events by calling a JP1/Base function. You can add user-defined event attributes (extended attributes specific to the issuing program) to the issued JP1 event. A JP1 event that has a user-defined event attribute is known as a *user-defined event*.

Event attributes (program-specific extended attributes) are not normally displayed in the Event Details window in JP1/IM - View, but you can display them if you create a definition file that defines the event attributes. For details about how to display user-defined events using a definition file, see *4.12 How to display user-specific event attributes* in the *JP1/Integrated Management - Manager Configuration Guide*.

3.14.2 Displaying a monitor window from a JP1 event

By creating a definition file of user-defined events, from the JP1 event listing in JP1/IM - View you can launch and operate the GUI of the application that issued a particular JP1 event. For details about how to launch a monitor window from a JP1 event based on a definition file, see *4.17.1 How to open monitor windows* in the *JP1/Integrated Management - Manager Configuration Guide*.

3.14.3 Adding items to the Tool Launcher window

You can add items to the function tree displayed in the Tool Launcher window of JP1/IM - View. This allows you to launch the GUI of a system management program or application management program.

To add an item to the Tool Launcher window, use a definition file.

For details about how to add items to the Tool Launcher window using a definition file, see *4.18.2 How to add new menus* in the *JP1/Integrated Management - Manager Configuration Guide*.

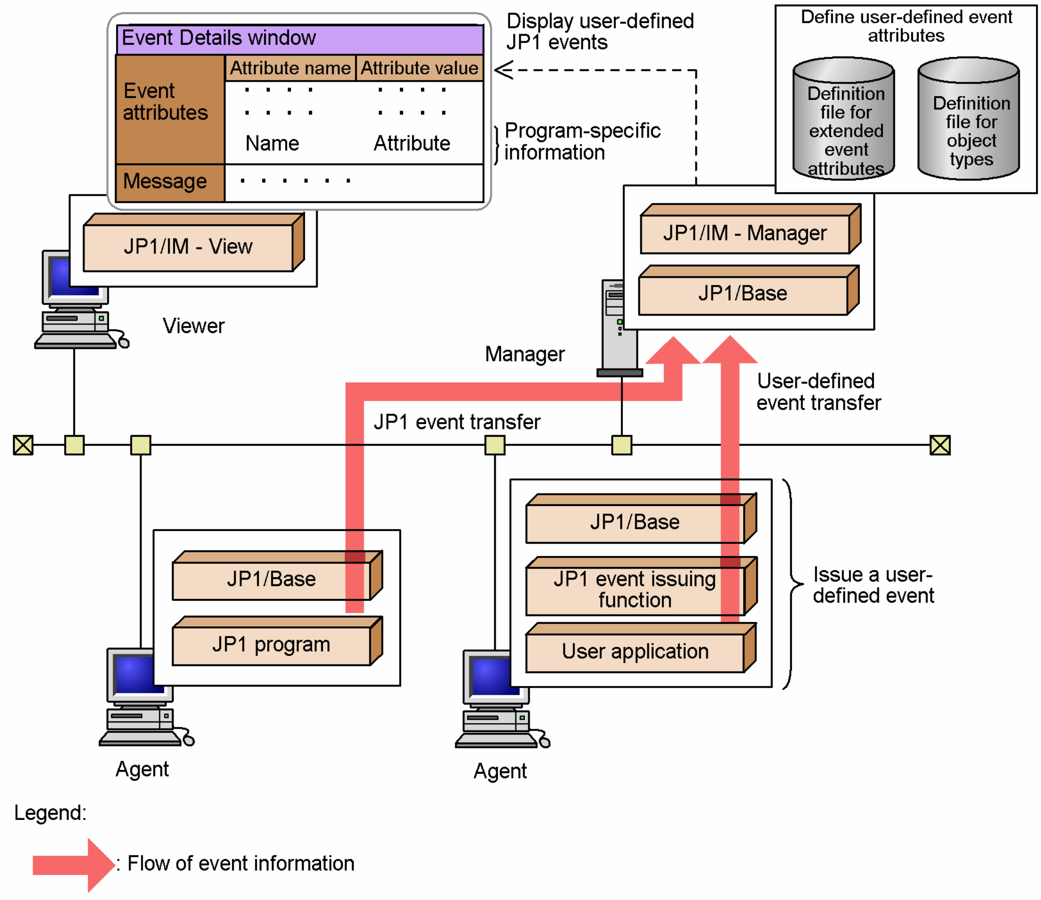
3.14.4 Flow of event information

Using the JP1 event issuing function provided by JP1/Base, you can execute user-defined events that have user-defined event attributes (program-specific extended attributes) directly from a user application.

In JP1/IM, you can create a definition file and display these user-defined event attributes in the Event Details window.

The following figure provides an overview of the flow of processing from issuing a user-defined event to displaying its user-defined event attributes.

Figure 3–92: Flow of processing from issuing a user-defined event to displaying its attributes


Event Details window
Attribute name
Attribute value
Event attributes
Name
Attribute
Message
Display user-defined JP1 events
Program-specific information
Define user-defined event attributes
Definition file for extended event attributes
Definition file for object types
JP1/IM - View
Viewer
JP1/IM - Manager
JP1/Base
Manager
User-defined event transfer
JP1 event transfer
JP1/Base
JP1 program
Agent
JP1/Base
JP1 event issuing function
User application
Issue a user-defined event
Agent
Legend:
: Flow of event information

3.15 CSV output of information displayed in JP1/IM - View

In JP1/IM, you can output the information displayed in JP1/IM - View in CSV format. The following functions support CSV output:

- Saving event listings to a file
- Saving event information in the integrated monitoring database to a file
- Copying JP1 event information and action execution results to the clipboard

These functions are described next.

3.15.1 Saving event listings (CSV snapshot)

In JP1/IM, you can take a CSV snapshot# of the event information displayed in JP1/IM - View. Based on this information, you can keep a history of day-to-day monitoring and actions. You can also use your CSV snapshots when reviewing the system during maintenance, for example.

The following describes the types of information you can export as a CSV snapshot, and the output format, items, and timing.

#: *Snapshot* refers to extracting information at a particular point in time.

(1) Information that can be exported as a snapshot

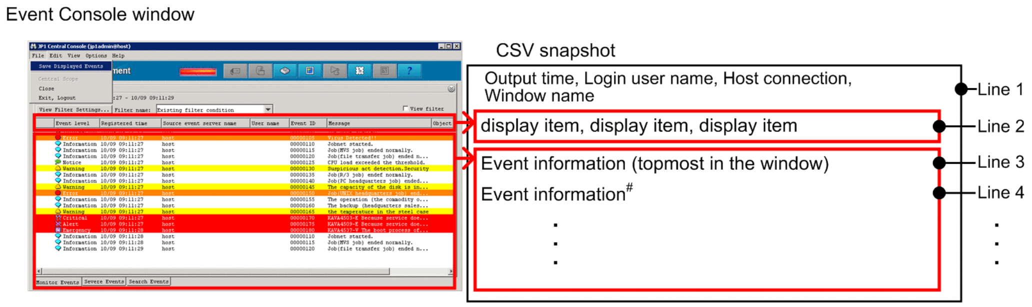
You can take a CSV snapshot of the event lists in following pages:

- **Monitor Events** page of the Event Console window
- **Severe Events** page of the Event Console window
- **Search Events** page of the Event Console window
- **Response-Waiting Events** page of the Event Console window

(2) Snapshot image and format

The following figure shows a CSV snapshot.

Figure 3–93: CSV snapshot image of events list information


Event Console window
CSV snapshot
Output time, Login user name, Host connection, Window name
display item, display item, display item
Event information (topmost in the window)
Event information#
Line 1
Line 2
Line 3
Line 4

#: Output on each line in the same order as displayed in the window.

Line 1 is the CSV header information, separated by commas.

Line 2 is the display items set in JP1/IM - View, separated by commas and output in order of display from left to right. You can set the display items of JP1/IM - View on the **Event Attributes** page of the Preferences window.

Line 3 is the event information listed first in the window, separated by commas in the same way as the display items (line 2).

Line 4 and subsequent lines are event information output in the same format as line 3, following the window display items.

The CSV output format is as follows:

- Items are separated by commas (`,`).
  item1`,`*item2*`,`*item3*`,`*item4*`,`*item5*`, . . .`
- Any item containing a comma (`,`) is enclosed with double quotation marks (`"`).
  item1`,"`*item,2*`",`*item3*`,`*item4*`,`*item5*`, . . .`
- Any item containing a control character (0x00 to 0x1F, and 0x7F to 0x9F) is enclosed with double quotation marks (`"`).
  item1`,"`*item(*`0x00`*)2*`",`*item3*`,`*item4*`,`*item5*`, . . .`
- When an item contains a double quotation mark (`"`), another double quotation mark is inserted before it, and the whole is enclosed with double quotation marks (`"`).
  item1`,"`*item*`""`*2*`",`*item3*`,`*item4*`,`*item5*`, . . .`
- Empty items are shown as blank (nothing is entered).
  item1`,,`*item3*`,`*item4*`,`*item5*`, . . .`

(3) Snapshot output items

The following table describes the header information output to line 1 of a CSV snapshot.

Table 3–20: Output header information

Header item	Output contents
Output time	The time at which the snapshot was taken is output in the following format (year/month/day hour:minute:second): • When the attribute value is the cumulative number of seconds from 1970/01/01 00:00:00 (GMT): The attribute value is converted for the time zone set for JP1/IM - View in the *YYYY*/*MM*/*DD* *hh*:*mm*:*ss* format and output. • When the attribute value is other than the above: The character string set as the attribute value is output.
Login user name	The name of the JP1 user who took the CSV snapshot
Host connection	The name of the manager host to which the JP1 user was logged in when the snapshot was taken
Window name	The name of the page (**Monitor Events**, **Severe Events**, or **Search Events**) displayed in the Event Console window when the snapshot was taken

The contents (display items) output to line 2 of the snapshot differs according to the settings in the JP1/IM - View Preferences window. The contents (event information) output to line 3 and subsequent lines also differs according to the contents in line 2.

The following table describes the contents output to line 2 and subsequent lines.

Table 3–21: Contents output to the body of a snapshot

Display item (contents in line 2)	Event information (contents in line 3 onward)	Output conditions
Response status	The icons in the window are converted into character strings and output as follows: 🏁 -> `Processed` ▶ -> `Processing` ⏸ -> `Held` (no icon) -> `Unprocessed` When the response status differs among the JP1 events in a consolidation event, the icon is followed by an exclamation mark (!). In the snapshot, the exclamation mark appears to the right of the string. When a JP1 event has a memo entry, the icon and exclamation mark are followed by a comma and then `Memo`.	--
Summary status	The character strings displayed in the window are output as is.	Output when **Enable** is selected for **Display most significant status** in the Preferences window (that is, when the consolidated display of repeated events is used) and the repeated-event monitoring suppression function is enabled.
Event level	The character strings displayed in the window are output as is. The severity color coding and icons are not output.	Output when this item is set in the **Display items & order** list box in the Preferences window.
Original severity level		
New severity level	The icon in the window is converted into a character string and output as follows: ☑ New severity level flag -> `Changed` (no icon) -> (blank)	
Start time	Output in the following format: • When the attribute value is the cumulative number of seconds from 1970/01/01 00:00:00 (GMT): The attribute value is converted for the time zone set for JP1/IM - View in the *YYYY*/*MM*/*DD* *hh*:*mm*:*ss* format, and then output. • When the attribute value is other than the above: The character string set as the attribute value is output.	
End time		
Arrived time		
Registered time		
Source host	The character strings displayed in the window are output.	
User name		
Message		
Event ID		
Product name		
Object type		
Object name		
Root object type		
Root object name		
Occurrence		

Display item (contents in line 2)	Event information (contents in line 3 onward)	Output conditions
Serial number		
Source process ID		
Source user ID		
Source group ID		
Source user name		
Source group name		
Source serial number		
Event source host name		
Action	The icons in the window are converted into character strings and output as follows: ☑ -> `Execute` ☑🚫 -> `Partially suppress` 🚫 -> `Suppress` 🚫 -> `Repeated event` 🚫 -> `Action-excluded event` (no icon) -> (blank) When the action status differs among the JP1 events in a consolidation event, the icon is followed by an exclamation mark (!). In the snapshot, the exclamation mark appears to the right of the string.	
Type	The icons in the window are converted into character strings and output as follows: -> `Complete-correlations event` -> `Incomplete-correlations event` -> `Repeated event` -> `Repeated event, complete-correlations event` -> `Repeated event, incomplete-correlations event` (no icon) -> (blank)	
Action type	The icons in the window are converted into character strings and output as follows: -> `Command` R -> `Rule` R -> `Command,Rule` (no icon) -> (blank)	
Message (after change)	The character strings displayed in the window are output as is.	
Display message change	The icons in the window are converted into character strings and output as follows: ☑ Display message change flag -> Changed (no icon) -> (blank)	
Display message change definition	The character strings displayed in the window are output as is.	

Display item (contents in line 2)	Event information (contents in line 3 onward)	Output conditions
Program-specific extended attribute	The character strings displayed in the window are output as is.	Output if the attribute is defined in the definition file for extended event attributes (extended file) and this item is set in **Display items & order** in the Preferences window.

Legend:

--: None.

When a program-specific extended attribute is mapped to a display item in the event-information mapping definitions, the attribute value is output to the snapshot in the same format as displayed in the Event Console window (value prefixed with `#` followed by a space).

If there are no events displayed in the window, only the header information (line 1) and the display items (line 2) will appear in the snapshot. If there is no information for a particular display item, that field is blank.

If the character string is a control character, it is converted into a space when displayed in the window, but appears as is when output to a CSV snapshot.

(4) Snapshot timing

To take a CSV snapshot, choose **File** and then **Save Displayed Events** in the Event Console window. The currently displayed event information is captured in the snapshot.

> **Important**
>
> - By default, the event information displayed in the **Monitor Events** page and **Severe Events** page of the Event Console window is automatically refreshed at 5-second intervals.
>
>   To stop the event information from being refreshed automatically when taking a snapshot, in the Preferences window change **Automatic refresh** from **Apply** to **Do not apply**.
> - You cannot export CSV snapshot files to a removable medium.

3.15.2 Saving event information in the integrated monitoring database (CSV report)

The functionality for outputting event information from the integrated monitoring database is referred to as *output of an event report*.

Using this feature in JP1/IM, you can save information about the JP1 events registered in the integrated monitoring database as a CSV-formatted report. To output an event report, execute the `jcoevtreport` command. As a command option, you can specify what event information to output.

For the command syntax, see *jcoevtreport* in *Chapter 1. Commands* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

The following describes the range of information you can output in an event report, and the output format, items, and command options.

(1) Information that can be output to an event report

You can output the following event information to an event report:

- Time-specified event information
  You can specify the arrival time of the JP1 events to be output.
- Program-specific event information
  You can specify particular items of program-specific information. If you do not specify any items, all items are output.
- Information about events that match a filter condition
  You can limit the JP1 events to be output using pass conditions or exclusion-conditions in a filter. For the items you can specify in a filter condition, see *Table 3-22 Contents output to an event report*.
  You can specify a maximum of 50 filter conditions in one pass condition group or one exclusion-condition group. In a filter for extended attributes (program-specific information), however, you can specify a maximum of five filter conditions in one pass condition group or one exclusion-condition group.

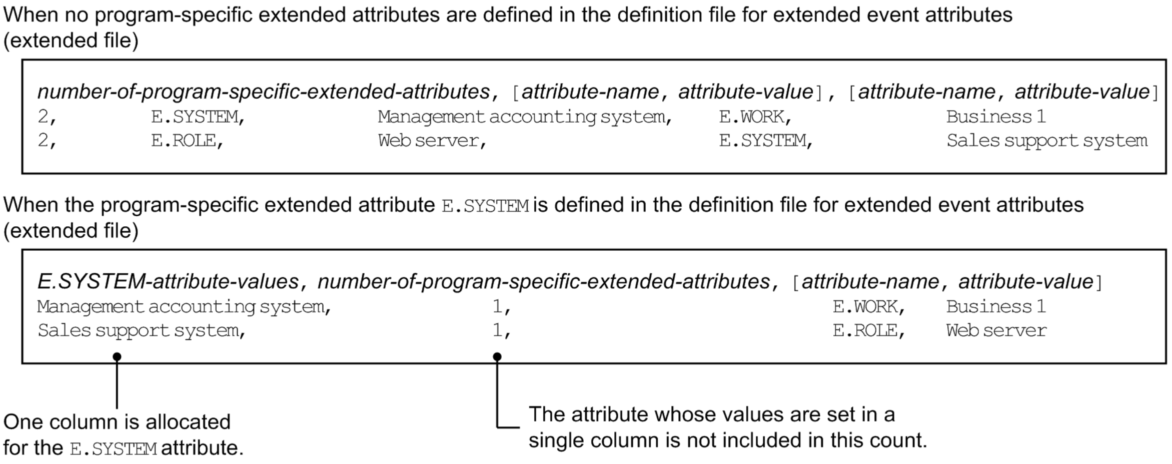
(2) Image and format of an event report

If you specify the header option during CSV output, CSV header items are output to line 1, separated by commas.

In line 2 and subsequent lines, event information is output in the following order, separated by commas:

basic-attribute, *extended-attributes-(common-information)*, *IM-attributes*, *extended-attribute (program-specific-information)*

For the extended attributes (program-specific information), the output format depends on whether program-specific extended attributes are defined in the definition file for extended event attributes (extended file).



When no program-specific extended attributes are defined in the definition file for extended event attributes (extended file)

```
number-of-program-specific-extended-attributes, [attribute-name, attribute-value], [attribute-name, attribute-value]
2,        E.SYSTEM,          Management accounting system,     E.WORK,            Business 1
2,        E.ROLE,            Web server,                       E.SYSTEM,          Sales support system
```

When the program-specific extended attribute E.SYSTEM is defined in the definition file for extended event attributes (extended file)

```
E.SYSTEM-attribute-values, number-of-program-specific-extended-attributes, [attribute-name, attribute-value]
Management accounting system,           1,                                  E.WORK,    Business 1
Sales support system,                   1,                                  E.ROLE,    Web server
```

One column is allocated for the E.SYSTEM attribute.
The attribute whose values are set in a single column is not included in this count.

If some of the program-specific extended attributes are defined in the definition file for extended event attributes (extended file) and some are not, the defined program-specific extended attributes are output first, and then the undefined program-specific extended attributes are output.

When multiple program-specific extended attributes are defined in the definition file for extended event attributes (extended file), the attributes are output in the order they are defined.

If you specify program-specific extended attributes in the environment definition file for event report output (`evtreport.conf`), the program-specific extended attributes defined in the definition file for extended event attributes (extended file) are output in the same format as for the program-specific extended attributes that are not defined in the definition file for extended event attributes (extended file).

If you do not specify program-specific extended attributes for items that are to be output to event reports, the number of program-specific extended attributes appears as `0`, and the attribute name and value are blank (nothing is entered).

(3) Items output to an event report

When you specify the header option, header information for the attribute name or item name is output to line 1 of the CSV file. For the extended attributes (program-specific information) defined in the definition file for extended event attributes (extended file), the defined item names are output as headers.

By default, no headers are output.

Table 3–22: Contents output to an event report

Attribute type	Item	Header information
Basic attribute	Serial number	The character string displayed in the window is output.
	Event ID	The character string displayed in the window is output.
	Source process ID	The character string displayed in the window is output.
	Registered time	Output in the following format: • When the attribute value is the cumulative number of seconds from 1970/01/01 00:00:00 (GMT): The time is output in one of the following two formats according to the specification of the `-t` option of the `jcoevtreport` command: - When `ON` is specified in the `-t` option: Format *YYYYMMDDhhmmss* in the time zone of the `jcoevtreport` command. - When `OFF` is specified in the `-t` option: Cumulative number of seconds from 1970/01/01 00:00:00 (GMT) • When the attribute value is other than the above: The character string set as the attribute value is output.
	Arrived time	
	Registered reason	Output in decimal format.
	Source user ID	
	Source group ID	
	Source user name	Output as a character string.
	Source group name	
	Source host	
	Destination event server name	
	Source IP address	The IP address is output as a character string.
	Destination IP address	
	Source serial number	The character string displayed in the window is output.
	Code set	Output as a character string.
	Message	The character strings displayed in the window are output.
Extended attribute	Event level	The character string is converted and output as follows: ☒ Emergency -> `Emergency`

Attribute type	Item	Header information
(common information)		✖ Alert -> `Alert` ‼ Critical -> `Critical` ● Error -> `Error` ▲ Warning -> `Warning` ● Normal -> `Normal` ● Information -> `Information` D Debug -> `Debug` For all other event levels, the character string displayed in the window is output as is. The severity color coding and icons are not output.
	User name	The character string displayed in the window is output.
	Product name	
	Object type	
	Object name	
	Root object type	
	Root object name	
	Object ID	Output as a character string.
	Occurrence	The character string displayed in the window is output.
	Start time	Output in either of the following formats: • *YYYYMMDDhhmmss* • Cumulative seconds from 1970/01/01 00:00:00 (GMT)
	End time	
	Result code	Output as a character string.
	Event source host name	
IM attributes	Action type	The icons in the window are converted into character strings and output as follows: ⬡ -> `Command` R -> `Rule` ⬡ R -> `Command,Rule` (no icon) -> (blank)
	Action suppression	The icons in the window are converted into character strings and output as follows: ☑ -> `Execute` ☑⊘ -> `Partially suppress` ⊘ -> `Suppress` ⊘ -> `Repeated event` (no icon) -> (blank)
	Severe event	Either of the following is output: If the JP1 event is not severe: Blank If the JP1 event is severe: `Severe Event`
	Correlation event	The icons in the window are converted into character strings and output as follows: ✓ -> `Complete-correlations event` ✗ -> `Incomplete-correlations event` (no icon) -> (blank)
	Original severity level	The icon is converted and output as follows:

Attribute type	Item	Header information
		☒ Emergency -> `Emergency` ✖ Alert -> `Alert` ‼ Critical -> `Critical` ● Error -> `Error` ▲ Warning -> `Warning` ● Normal -> `Normal` ● Information -> `Information` D Debug -> `Debug` For all other event levels, the character string displayed in the window is output as is. The severity color coding and icons are not output.
	New severity level	The icon in the window is converted and output as follows: ☑ -> `Changed` (no icon) -> (blank)
	Response status	The icons in the window are converted into character strings and output as follows: 🏁 -> `Processed` ▶ -> `Processing` ⏸ -> `Held` (no icon) -> `Unprocessed`
	Summary status	The character strings displayed in the window are output.
	Severe event release	The following character string is output: If the severe event has not been released: Blank If the severe event has been released: `Released`
	Severe event deletion	The following character string is output: If the severe event has not been deleted: Blank If the severe event has been deleted: `Delete`
	Memo	The character strings displayed in the window are output.
	Message (after change)	The character strings displayed in the window are output as is.
	Display message change	The icons in the window are converted into character strings and output as follows: ☑ `->` Changed (no icon) `->` (blank)
	Display message change definition	The character strings displayed in the window are output as is.
Extended attribute reserved by the system (program-specific information)	Relation Event serial number (`E.JP1_GENERATE_SOURCE_SEQNO`)	The serial numbers of relation events are listed in the following format, separated with spaces (Δ): *serial-number-1*Δ*serial-number-2*Δ...Δ*serial-number-n* (*n* is a number between 1 and 100)
	Correlation event generation condition name (`E.JP1_GENERATE_NAME`)	Output as a character string. This item is the name of a correlation event generation condition that is satisfied.
	Suppressed event ID (`E.JP1_IMSUPPRESS_ID`)	Output as a character string. This item is output when the repeated-event monitoring suppression function is used. This item is the serial number (unique number in the event database) of a repeated event that occurs more frequently than the threshold.

Attribute type	Item	Header information
	Repeated event condition name (E.JP1_IMSUPPRESS_NAME)	Output as a character string. This item is output when the repeated-event monitoring suppression function is used. This item is the name of a repeated event condition that determined that the event was a repeated-event.
	Monitoring ID (E.JP1_TRAP_ID)	Output as a character string. This item is the log file trap ID.
	Monitoring target name (E.JP1_TRAP_NAME)	Output as a character string. This item is the log file trap name.
	Common exclude conditions group ID (E.JP1_IMCOMEXCLUDE_ID)	Output as a character string. This item is the ID of the common exclusion-conditions group that caused the exclusion.
	Common exclude conditions group name (E.JP1_IMCOMEXCLUDE_NAME)	Output as a character string. This item is the condition name of the common exclusion-conditions group that caused the exclusion.
	Common exclude conditions group target-for-exclusion (E.JP1_IMCOMEXCLUDE_TARGET)	Output the following character string indicating the exclusion target of common exclusion-conditions: When an event is excluded from automated-action execution -> action
Extended attribute (program-specific information)	E.*xxxxxxx*	Output as a character string.

(4) Command options

You can specify the following options in the jcoevtreport command to output maintenance information and to save the event report:

- Export maintenance information
  jcoevtreport -sys -s 20090101000000 -e 20090103000000 (This example outputs JP1 events that were registered in the integrated monitoring database between 2009/01/01 00:00:00 and 2009/01/03 00:00:00.)
- Save events before deletion
  jcoevtreport -save

These two options are explained next.

(a) Export maintenance information

When an error occurs in the integrated monitoring database, this option outputs information about all JP1 events registered between the output start time and end time to the event report.

The attribute name appears in the header part.

Because the purpose is to collect data for investigating a database error, you cannot specify what items to output or any filtering conditions.

(b) Save events before deletion

This option outputs an event report about JP1 events due for deletion to free up space in the integrated monitoring database.

With this option specified, the command outputs in CSV format all the JP1 events registered in the integrated monitoring database that have not previously been saved to an event report.

■ Warning before deletion of unsaved JP1 events

You can issue a deletion warning event (event ID: 3F52) when the ratio of JP1 events in the integrated monitoring database that have not been output to an event report (relative to the maximum number of entries in the database) exceeds a set threshold for issuing a deletion warning event (by default, when the unsaved data exceeds 80% of the database capacity).

Specify the ratio of unsaved JP1 events in the `-dbntcpos` option of the `jcoimdef` command.

Specify the threshold for issuing a deletion warning event in the `-dbntc` option of the `jcoimdef` command.

For details, see *jcoimdef* in *Chapter 1. Commands* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

■ Display information about saving events before deletion in the standard output

You can specify an option to display information about saving events due for deletion. Set the `-showsv` option of the `jcoevtreport` command to display this information in the standard output.

This option lets you see how much free space will be required to save the events, and helps you adjust the timing for outputting an event report before the target events are deleted.

With this option specified, the following items can be displayed in the standard output:

- Ratio of JP1 events that have not been output to an event report (relative to the maximum number of entries in the integrated monitoring database)
  The ratio of JP1 events in the integrated monitoring database that have not been output to an event report is shown as a percentage.
- Data size of the JP1 events that have not been output to an event report
  The data size of the JP1 events in the integrated monitoring database that have not been output to an event report is shown in megabytes.
- Threshold for issuing a deletion warning event
  If issue of a deletion warning event is specified, the threshold is shown as a percentage. If you specify `OFF` in the `jcoimdef` command's `-dbntc` option, a hyphen (`-`) is shown.

3.15.3 Copying JP1 event information and action execution results to the clipboard

In JP1/IM, you can copy selected JP1 event information and action execution results to the clipboard in CSV format. You can then make temporary use of the information. For example, you can copy information about a JP1 event triggered by a major error into a text editor or the body of an email.

The clipboard feature is enabled by default. For the procedure to enable or disable copying to the clipboard, see *1.19.2 Customizing operation of JP1/IM - View (Central Console viewer and Central Scope viewer) (for Windows)* in the *JP1/Integrated Management - Manager Configuration Guide*.

The following describes the windows and types of information that you can copy to the clipboard, and the output format and output items.

(1) Target windows and types of information

You can copy the following types of information to the clipboard:

- JP1 event information
- Action log
- Command log

The clipboard feature can be used in all windows in which these types of information are displayed. The following table lists the applicable windows and display items.

Table 3–23: Applicable windows and display items when copying to the clipboard

Window name	Display item	Information
Event Console window • **Monitor Events** page • **Severe Events** page • **Search Events** page	List of events	JP1 event information
Event Details window	**Event attributes**	JP1 event information (detailed information)
Related Events (Summary) window	• **Display Items** • **Related Events**	JP1 event information
Related Events (Correlation) window	• **Display Items** • **Related Events**	JP1 event information
Action Log window	**Log**	Action log
Action Log Details window	**Log**	Action log (detailed information)
List of Action Results window	**Log**	Action log
Execute Command window	**Log**	Command log

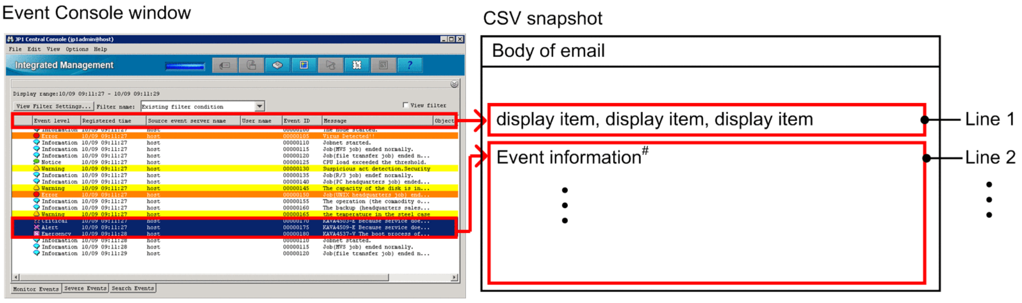
In the Event Console window, you can copy information to the clipboard by choosing **Edit** and then **Copy**, or by pressing the **Ctrl+C** keys. In all other windows, press the **Ctrl+C** keys to copy selected information to the clipboard.

(2) CSV image and format

Information copied to the clipboard can be output in CSV format, in the same order as displayed in JP1/IM - View. The display item names are added as header information to identify the items.

The following figure shows the CSV output.

Figure 3–94: CSV snapshot image of the information copied to the clipboard



#: Only the selected event information is output in the same order as displayed in the window.

Line 1 is the display item names corresponding to the information selected in JP1/IM - View, separated by commas.

Line 2 and subsequent lines are the selected information, separated by commas and following the order of the display item names in line 1.

The CSV output format is as follows:

- Items are separated by commas (`,`).

  item1`,`*item2*`,`*item3*`,`*item4*`,`*item5*`, . . .`

- Lines are separated by linefeed codes (`CRLF`).

  item1`,`*item2*`,`*item3*`,`*item4*`,`*item5*`, . . .`(`CRLF`)

  item1`,`*item2*`,`*item3*`,`*item4*`,`*item5*`, . . .`(`CRLF`)

- Any item containing a comma (`,`) is enclosed with double quotation marks (`"`).

  item1`,"`*item,2*`",`*item3*`,`*item4*`,`*item5*`, . . .`

- Any item containing a control character (0x00 to 0x1F, and 0x7F to 0x9F) is enclosed with double quotation marks (`"`).

  item1`,"`*item(*`0x00`*)2*`",`*item3*`,`*item4*`,`*item5*`, . . .`

- When an item contains a double quotation mark (`"`), another double quotation mark is inserted before it, and the whole is enclosed with double quotation marks (`"`).

  item1`,"`*item*`""`*2*`",`*item3*`,`*item4*`,`*item5*`, . . .`

- Empty items are shown as blank (nothing is entered).

  item1`,,`*item3*`,`*item4*`,`*item5*`, . . .`

(3) CSV output items

The following describes the items and contents that are copied to the clipboard.

JP1 event information

The contents output when copying JP1 event information to the clipboard are the same as the contents output to line 2 and subsequent lines when saving an event listing as a CSV snapshot. For details, see *Table 3-21 Contents output to the body of a snapshot*. As there is no header information, the display item names are output to line 1, and the event information is output to line 2 onward.

Action log

The following table describes the contents output as an action log.

Table 3–24: Contents output as an action log

Display item name	Output contents
Type[#]	The icons in the window are converted into character strings and output as follows: ⚙ -> `Command` R -> `Rule`
Action serial number	The character string displayed in the window is output.
Action	The character string displayed in the window is output.
Host	The character string displayed in the window is output.
Status	The character string displayed in the window is output.
Delay	The character string displayed in the window is output.
Registered time	Output in the following format: • When the attribute value is the cumulative number of seconds from 1970/01/01 00:00:00 (GMT): The attribute value is converted for the time zone set for JP1/IM - View in the *YYYY*/*MM*/*DD* *hh*:*mm*:*ss* format, and then output. • When the attribute value is other than the above: The character string set as the attribute value is output.
Event arrival time	
End time	
Return code	The character string displayed in the window is output.

#: Output only when linked with JP1/IM - Rule Operation.

Command log

The following table describes the contents output as a command log.

Table 3–25: Contents output as a command log

Display item name	Output contents
Time	Output in the following format:. • When the attribute value is the cumulative seconds from 1970/01/01 00:00:00 (GMT): The attribute value is converted for the time zone set for JP1/IM - View in the *YYYY*/*MM*/*DD* *hh*:*mm*:*ss* format, and then output. • When the attribute value is other than the above: The character string set as the attribute value is output.
Host	The character string displayed in the window is output.
Message	The character strings displayed in the window are output.

JP1 event information (details) or action log (details)

The following table describes the contents output as detailed information about a JP1 event or an action log entry.

Table 3–26: Contents output as detailed information

Display item name	Output contents
Attribute name	The character string displayed in the window is output.
Attribute value	The character string displayed in the window is output. However, when time is displayed as the attribute value, the attribute value is output in the following format: • When the attribute value is the cumulative number of seconds from 1970/01/01 00:00:00 (GMT):

Display item name	Output contents
	The attribute value is converted for the time zone set for JP1/IM - View in the *YYYY*/*MM*/*DD hh*:*mm*:*ss* format, and then output. • When the attribute value is other than the above: The character string set as the attribute value is output.

(4) Notes

Note the following when copying displayed information to the clipboard:

- The functionality is not supported in the Web-based JP1/IM - View.
- If you want to copy information to the clipboard by pressing the **Ctrl+C** keys, make sure that the functionality is enabled. It is enabled by default.
- The information copied to the clipboard is the item selected in the window that has the focus when you perform a copy operation by choosing a command or by pressing the shortcut keys. The selected information is not copied if it was changed to an unselected state as the result of an auto-refresh action that scrolled the item out of view before it was copied.
- When the amount of information to be copied to the clipboard exceeds the maximum memory usage, the copy processing is canceled and the information is not copied.

3.16 Specifying the event display start-time

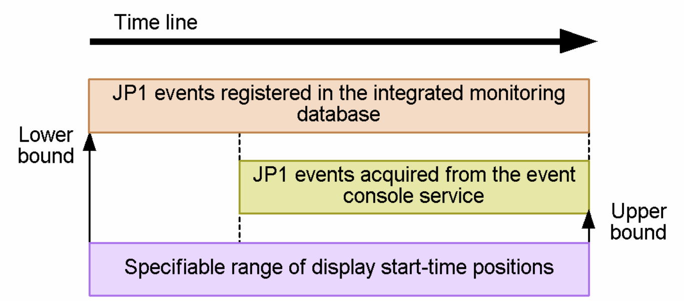
In the event display start-time specification area of the Event Console window, you can specify the start-time position for listing JP1 events.

To specify the display start-time position, you must first activate the integrated monitoring database. This enables JP1/IM to reference information about the JP1 events that have been acquired from JP1/Base and registered in the integrated monitoring database.

3.16.1 Range of date and time that can be specified as event display start-time

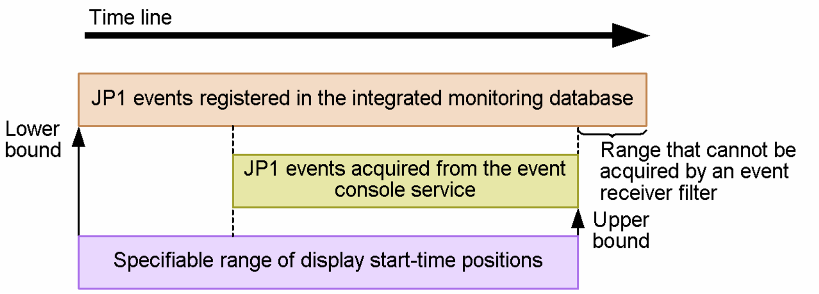
Specify date and time (year, month, day, hour, minute, and second) as an event display start-time position. The date and time that can be specified ranges from the arrival time of the oldest JP1 event registered in the integrated monitoring database to the arrival time of the JP1 event most recently acquired from the event console service.

Figure 3–95: Specifiable range of display start-time positions when the integrated monitoring database contains JP1 events acquired from the event console service


Time line
JP1 events registered in the integrated monitoring database
Lower bound
JP1 events acquired from the event console service
Upper bound
Specifiable range of display start-time positions

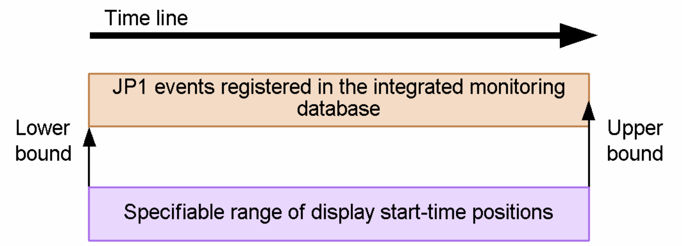
JP1 events that cannot be acquired from the event console service (by using an event receiver filter) cannot be displayed.

Figure 3–96: Specifiable range of display start-time positions when the integrated monitoring database contains some JP1 events that cannot be acquired from the event console service


Time line
JP1 events registered in the integrated monitoring database
Lower bound
JP1 events acquired from the event console service
Range that cannot be acquired by an event receiver filter
Upper bound
Specifiable range of display start-time positions

When the integrated monitoring database contains only JP1 events that are not acquired from the event console service, the lower bound of the specifiable range is the arrival time of the oldest JP1 event, and the upper bound is the arrival time of the most recent JP1 event.

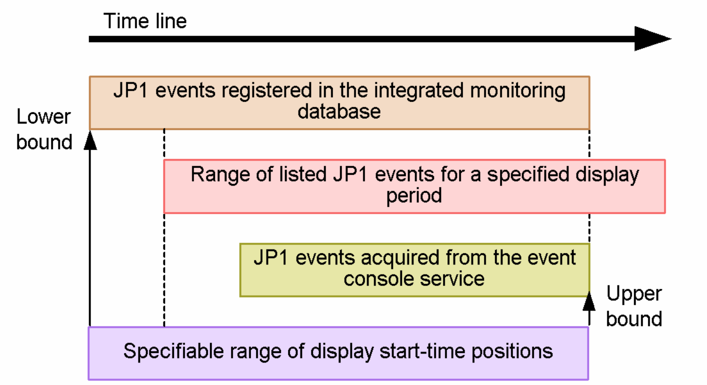
Figure 3–97: Specifiable range of display start-time positions when the integrated monitoring database contains only JP1 events not acquired from the event console service


Time line
JP1 events registered in the integrated monitoring database
Lower bound
Upper bound
Specifiable range of display start-time positions

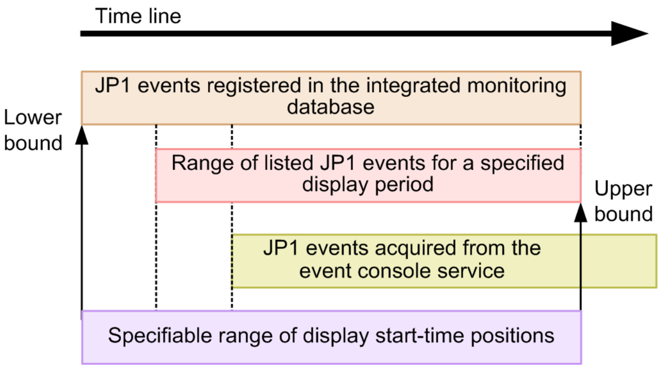
When JP1 events are listed by display period specification, the lower bound of the specifiable start-time positions is the arrival time of the oldest JP1 event in the specified period or the arrival time of the oldest JP1 event registered in the integrated monitoring database, whichever is later. The upper bound is the arrival time of the most recent JP1 event in the specified display period or the arrival time of the most recent JP1 event acquired from the event console service, whichever is earlier.

The figures below show the range of date and time that can be specified as event display start-time positions in respective cases.

- In the following figure, the oldest JP1 event registered in the integrated monitoring database has an earlier arrival time than the oldest JP1 event in the specified display period, and the most recent JP1 event in the specified display period has a later arrival time than the most recent JP1 event acquired from the event console service.


Time line
JP1 events registered in the integrated monitoring database
Lower bound
Range of listed JP1 events for a specified display period
JP1 events acquired from the event console service
Upper bound
Specifiable range of display start-time positions

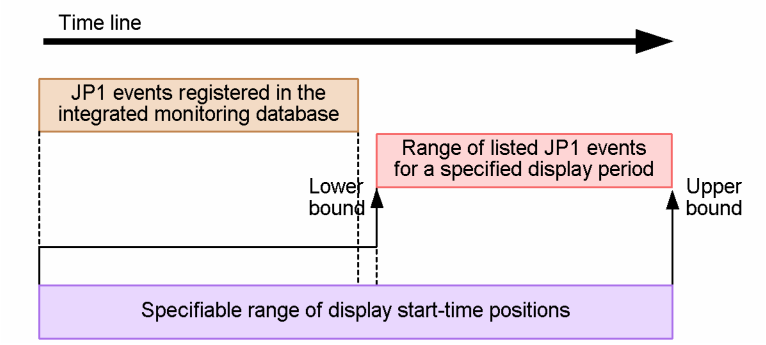
- In the following figure, the oldest JP1 event registered in the integrated monitoring database has an earlier arrival time than the oldest JP1 event in the specified display period, and the most recent JP1 event in the specified display period has an earlier arrival time than the most recent JP1 event acquired from the event console service.


Time line
JP1 events registered in the integrated monitoring database
Lower bound
Range of listed JP1 events for a specified display period
Upper bound
JP1 events acquired from the event console service
Specifiable range of display start-time positions

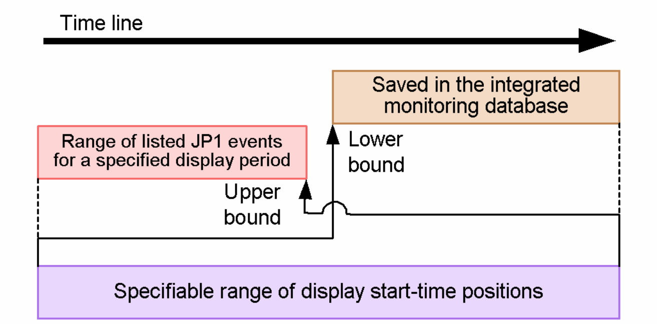
Note that the event display start-time specification area is unavailable when:

- No JP1 events have been registered in the integrated monitoring database.

- JP1 events are listed by display period specification, and no JP1 events were registered in the integrated monitoring database during the specified period, as illustrated below:


Time line
JP1 events registered in the integrated monitoring database
Range of listed JP1 events for a specified display period
Lower bound
Upper bound
Specifiable range of display start-time positions

- JP1 events are listed by display period specification, and a time discrepancy between JP1/IM - Manager and JP1/IM - View means that the most recent JP1 event than can be displayed in the specified period is registered after the oldest event registered in the integrated monitoring database (that is, the lower and upper bounds of the specifiable range of display start-time positions are reversed):


Time line
Saved in the integrated monitoring database
Range of listed JP1 events for a specified display period
Lower bound
Upper bound
Specifiable range of display start-time positions

When JP1 events are listed by display period specification, the time at which the JP1 event arrived at JP1/IM - Manager is compared with the current time of the JP1/IM - View host. Any discrepancy between the times of JP1/IM - Manager and JP1/IM - View could result in a JP1 event outside the specified display period being included in the listing. We recommend that you synchronize the time settings of JP1/IM - Manager and JP1/IM - View.

The event display start-time specification area appears in the window only if you are using the integrated monitoring database.

For details about specifying a display period, see *3.18 Specifying the event display period*.

3.16.2 Specifying the event display start-time position using the slider

You can easily specify the start-time position for listing JP1 events using the slider in the event display start-time specification area.

The slider is at the far right when the most recent events are displayed. As you move the slider to the left, events saved in the integrated monitoring database are listed from the start-time position indicated by the slider, up to the maximum number of viewable events (scroll buffer size). The listed events are those that have passed through an event receiver filter or view filter.

When you move the slider to the far left, the oldest event is displayed.

If auto-scroll is enabled, after a new JP1 event is registered, the slider position returns to the latest status position. To change the setting so that the slider does not return to the latest position, disable the auto-scroll function.

3.16.3 Specifying the event display start-time position by date and time

You can specify a precise start-time position by specifying the arrival time of the events you want to view. Set the desired arrival time in the event display start-time text boxes in the event display start-time specification area.

When you enter an arrival time, events saved in the integrated monitoring database are listed from the specified time up to the maximum number of viewable events (scroll buffer size). The slider in the event display start-time specification area moves to the time position that you entered in the start-time text boxes.

The defaults for the start-time text boxes depends on the time at which you were logged in to JP1/IM - Manager.

If you log in to JP1/IM - Manager later than the base time on a particular day, the base time of that day is displayed in the text boxes by default.

Example: The base time is 09:00, and you log in at 2008/07/08 10:00.
The default date and time shown in the event display start-time text boxes is 2008/07/08 09:00.

If you log in to JP1/IM - Manager earlier than the base time on a particular day, the base time of the previous day is displayed in the text boxes by default.

Example: The base time is 09:00, and you log in at 2008/07/08 08:00.
The default date and time shown in the event display start-time text boxes is 2008/07/07 09:00.

3.16.4 Specifying the event display start-time position using the buttons

The event display start-time specification area has the following buttons: **Oldest Event**, **Previous Event**, **Next Event**, and **Most Recent Event**.

Click the **Oldest Event** button to list the maximum number of viewable events (scroll buffer size) stored in the integrated monitoring database, starting from the oldest event.

Click the **Previous Event** button or **Next Event** button to move the viewable events up or down one event.

Click the **Most Recent Event** button to return the event listing to the state before you set the start-time position.

3.16.5 Processing after event display start-time specification

When you specify an event display start-time position, JP1/IM retrieves the maximum number of viewable events (scroll buffer size) stored in the integrated monitoring database that match the specified search condition.

At completion of the search, the retrieved events are listed in the Event Console window.

The **Status** display, and whether the **Cancel** button is available, change according to the search progress and result.

For details, see *2.2 Monitor Events page* in the manual *JP1/Integrated Management - Manager GUI Reference*.

3.17 Range of events to be collected at login

A function is provided to set the range of events to be collected at login. This function enables you to specify a point of time from which JP1/IM - View starts acquiring old events from JP1/IM - Manager when you log in to JP1/IM - Manager.

Note that the function to set the range of events to be collected at login is not available in Web-based JP1/IM - View. Even if the function is enabled, the system behaves in the same way as when the function is disabled as long as you are logged in with Web-based JP1/IM - View.

The following table compares when the function for setting the range of events to be collected at login is used and when the function is not used.

Table 3–27: Comparison between when the function for setting the range of events to be collected at login is used and when the function is not used.

Item	When the function is used	When the function is not used
Severe Events page at login	The severe events in the target period are displayed. This period begins a set amount of time before the login time on the host where the Central Console is operating.	Events in the range from the most recent to event 2,000 in the event buffer are displayed. The number of events to be displayed depends on the count in the event buffer and the count in the global buffer.
Monitor Events page at login	The events ranging from the most recent event to a previous event that occurred at specified date and time are displayed.	
Range of events to be collected at login	The events to be displayed are inherited during re-login because the display start point matches the display status at the time of logout.	The events that are not inherited are displayed because the display start point does not match the display status at the time of logout.

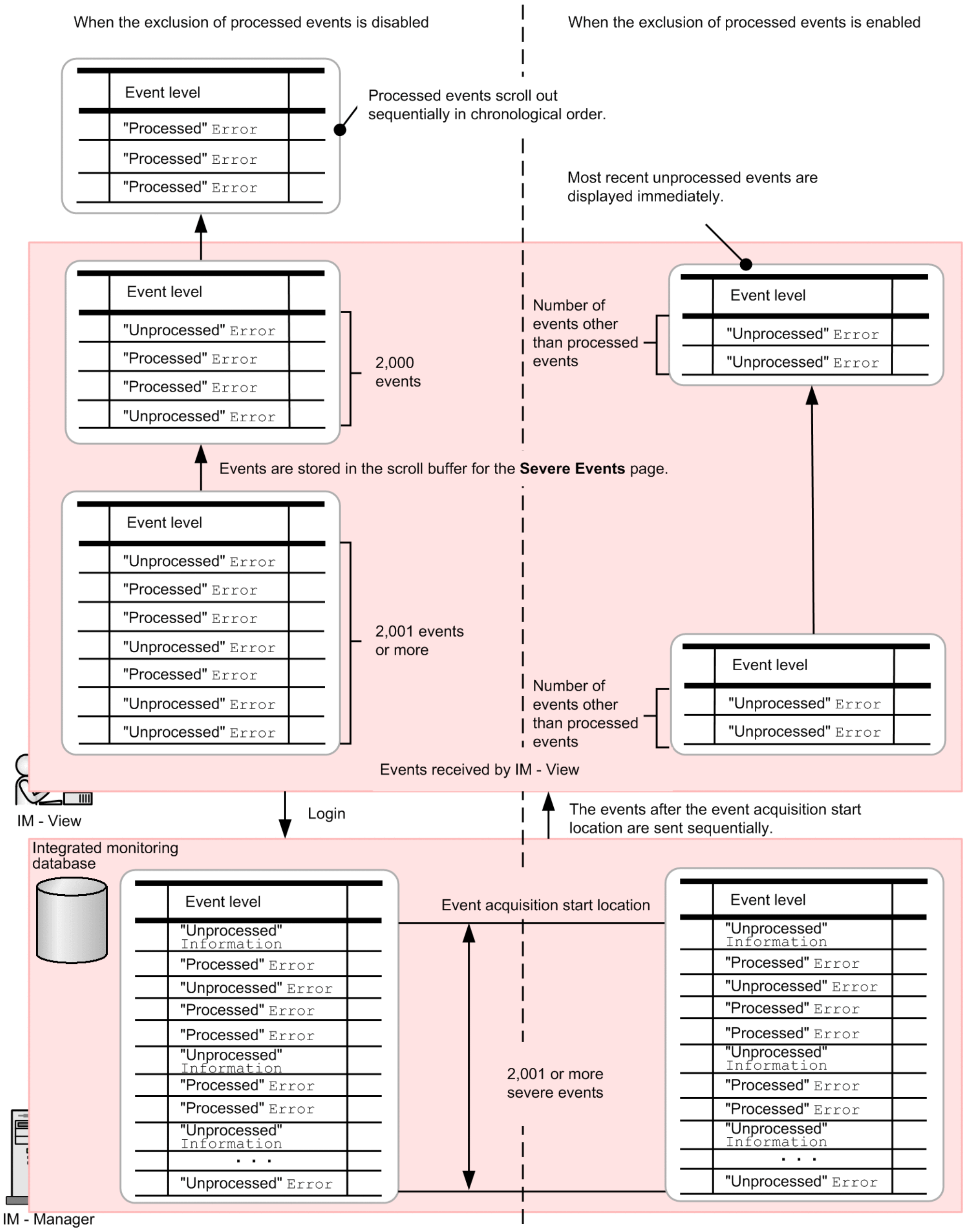
As described above, the **Monitor Events** and **Severe Events** pages are used in different ways, and you can specify the range of events to be collected at login differently for individual pages. The range of events to be collected at login can be specified by time in number of days.

At login, the Central Console calculates the point of time to begin event acquisition based on the number of days or time set in the system and the login time on the host where the Central Console is operating. Then, the Central Console acquires the events that have occurred since the calculated point of time up to the most recent event from the integrated monitoring database.

When you use this functionality, the integrated monitoring database must be enabled.

When the range of events to be collected at login is set, you can specify settings, on the **Severe Events** page, to exclude already processed severe events from event collection at login from the integrated monitoring database. This function is called the *exclusion of processed events*. If, before a severe event is *processed*, 2001 or more *processed* severe events are collected during system operation, said severe event cannot be displayed immediately at login. The exclusion of processed events enables you to immediately display most recent events other than processed events at login. Set the exclusion of processed events in the System Environment Settings window. For details, see *2.11 System Environment Settings window* in the manual *JP1/Integrated Management - Manager GUI Reference*.

Figure 3–98: Exclusion of processed events



When the exclusion of processed events is disabled
When the exclusion of processed events is enabled
Event level
"Processed" Error
"Processed" Error
"Processed" Error
Processed events scroll out sequentially in chronological order.
Most recent unprocessed events are displayed immediately.
Event level
"Unprocessed" Error
"Processed" Error
"Processed" Error
"Unprocessed" Error
2,000 events
Number of events other than processed events
Event level
"Unprocessed" Error
"Unprocessed" Error
Events are stored in the scroll buffer for the Severe Events page.
Event level
"Unprocessed" Error
"Processed" Error
"Processed" Error
"Unprocessed" Error
"Processed" Error
"Unprocessed" Error
"Unprocessed" Error
2,001 events or more
Number of events other than processed events
Event level
"Unprocessed" Error
"Unprocessed" Error
Events received by IM - View
IM - View
Login
The events after the event acquisition start location are sent sequentially.
Integrated monitoring database
Event level
"Unprocessed" Information
"Processed" Error
"Unprocessed" Error
"Processed" Error
"Processed" Error
"Unprocessed" Information
"Processed" Error
"Processed" Error
"Unprocessed" Information
. . .
"Unprocessed" Error
Event acquisition start location
2,001 or more severe events
Event level
"Unprocessed" Information
"Processed" Error
"Unprocessed" Error
"Processed" Error
"Processed" Error
"Unprocessed" Information
"Processed" Error
"Processed" Error
"Unprocessed" Information
. . .
"Unprocessed" Error
IM - Manager

Important

The number of events that have occurred during the period from the specified point of time to begin collection to the most recent time might exceed the maximum number of events that can be displayed by the viewer. If this occurs, excessive events scroll out. Therefore, the system administrator must specify the point of time to begin collection so that the number of events collected at login does not exceed the maximum number of events that can be displayed by the viewer. If a large number of events have been issued in the range of events to be collected at login, it might take time to display the most recent events at login. If that occurs, temporarily change the range of events to be collected at login, and restore the range when the issued repeated events grow out of the monitoring range. Event collection cannot be canceled functionally. In such cases, you must log out, change the range setting, and then log in again. Besides, if multiple users login at the same time, it might take additional time to display and update events. If this occurs, wait a while, and then re-execute processing.

- Events to be collected
  - Like the events stored in the event buffer, the events to be collected are all the events except the dummy events, which are not stored in the integrated monitoring database.
  - The events to be collected for the **Severe Events** page are as shown in the following table according to the setting of the exclusion of processed events.

Table 3–28: Types of events to be collected according to the setting of the exclusion of processed events

Event processing status	Setting of the exclusion of processed events	
	Enabled	Disabled
Processed	N	Y
Processing	Y	Y
Held	Y	Y
Unprocessed	Y	Y

Legend:

Y: The event is to be collected.

N: The event is not to be collected.

- Applicable filters

  The filters applicable to the events that are collected from the integrated monitoring database at login are the same as those applicable to the events that are acquired from the event console service. Also, the events that are displayed are the same as those acquired from the event console service.

  For details about filters, see *3.2 Filtering of JP1 events*.

- Number of events that are sent to JP1/IM - View at a time

  The number of events that are sent to JP1/IM - View at a time is the number of events specified in the **Num. of events to acquire at update** field of the Preferences window.

- Determination of event acquisition start location

  The following gives examples of calculating the range of event collection:

Figure 3–99: When the login time is later than the base time and the range of event collection is set to 3 days

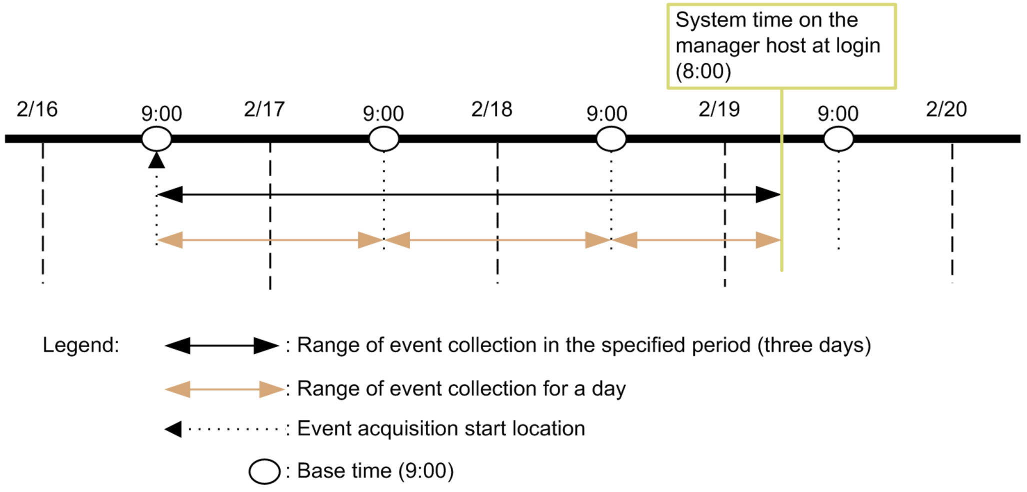
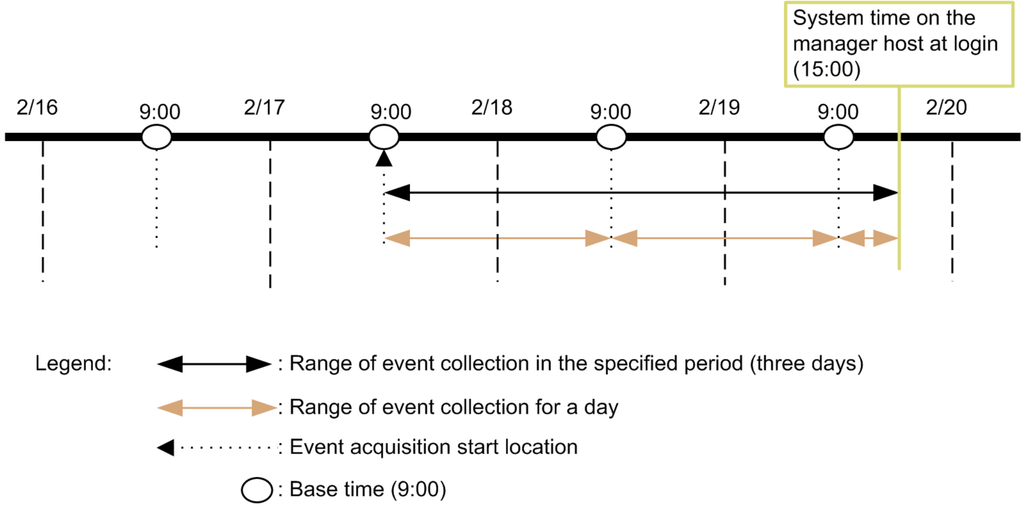

System time on the manager host at login (8:00)
2/16
9:00
2/17
9:00
2/18
9:00
2/19
9:00
2/20
Legend:
: Range of event collection in the specified period (three days)
: Range of event collection for a day
: Event acquisition start location
: Base time (9:00)

Figure 3–100: When the login time is earlier than the base time and the range of event collection is set to 3 days

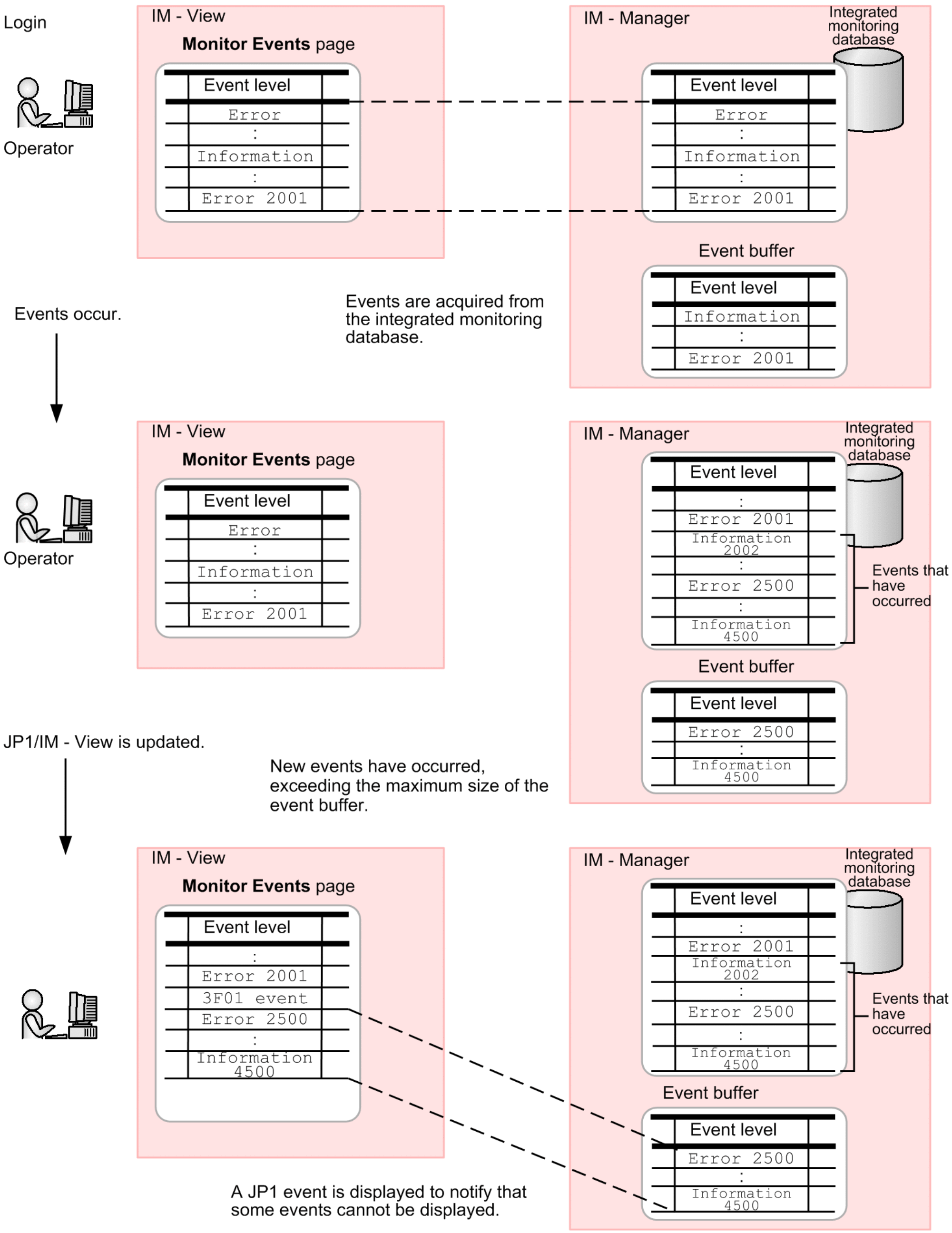

System time on the manager host at login (15:00)
2/16
9:00
2/17
9:00
2/18
9:00
2/19
9:00
2/20
Legend:
: Range of event collection in the specified period (three days)
: Range of event collection for a day
: Event acquisition start location
: Base time (9:00)

Even when the function to set the range of events to be collected at login is used, the existing event buffer remains the same.

If the event buffer retains uncollected events when the display of collected events is updated after events have been collected from the integrated monitoring database, the uncollected events are acquired from the event buffer.

If the event buffer does not retain any uncollected event, a dummy event with event ID 3F01 is displayed in JP1/IM - View as always. This functionality can be set separately for the **Monitor Events** and **Severe Events** pages. Therefore, at login, events might be acquired from the event buffer for only one of these pages. If events can be displayed on only one of the pages, a dummy event with event ID 3F02 is displayed on the page that cannot display any events. When the dummy event with event ID 3F02 is displayed on the **Severe Events** page, the event is forcibly treated as a severe event. The following figure shows the flow when updating the display of collected events.

Figure 3–101: Updating the display of collected events when the event buffer has overflowed



If you change the setting of the range of events to be collected at login, the new setting will be applied at the next login.

For details about the range of events to be collected at login, see *4.1.1 Displaying events by specifying the event acquisition range at login* in the *JP1/Integrated Management - Manager Configuration Guide*.

3.18 Specifying the event display period

You can change the JP1 events listed in the Event Console window, restricting the listing to a specified period.

To restrict the listing, set a base time and a duration.

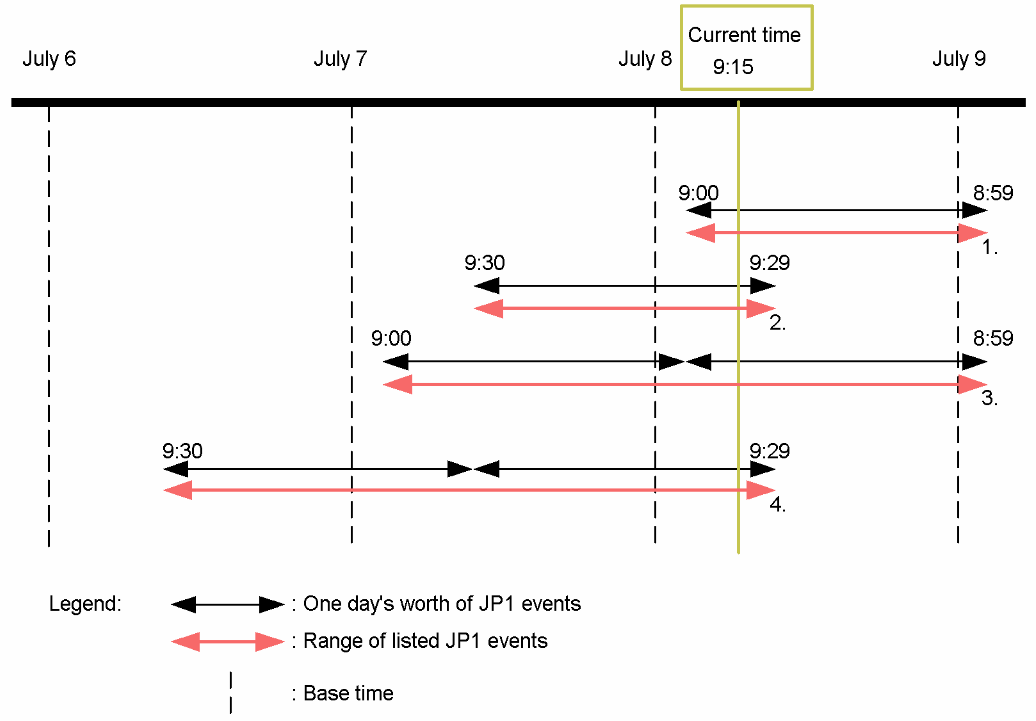
3.18.1 Range of listed JP1 events for a specified display period

The display period specification applies to JP1 events that have passed through an event acquisition filter, event receiver filter, severe events filter, or view filter.

To determine whether a specific JP1 event occurred during the specified display period, its arrival time at JP1/IM - Manager is compared with the current time of the JP1/IM - View host. Any discrepancy between the times of JP1/IM - Manager and JP1/IM - View could result in a JP1 event outside the specified display period being included in the listing. We recommend that you synchronize the time settings of JP1/IM - Manager and JP1/IM - View.

The following figures illustrate the range of JP1 events that are listed when you specify a display period.

Figure 3–102: Range of listed events when the current time is 9:15 am on July 8



The numbers below correspond to the numbers in the figure.

1. Range of listed JP1 events when the display period is one day and the base time is 9:00.
2. Range of listed JP1 events when the display period is one day and the base time is 9:30.
3. Range of listed JP1 events when the display period is two days and the base time is 9:00.
4. Range of listed JP1 events when the display period is two days and the base time is 9:30.

When you use the integrated monitoring database, the listing specification applies to JP1 events saved in the database.

If you specify a start-time position for listing JP1 events with the integrated monitoring database, the range of JP1 events that are listed changes as follows:

Figure 3–103: Range of listed events when the display period is two days and the current time is earlier than the base time

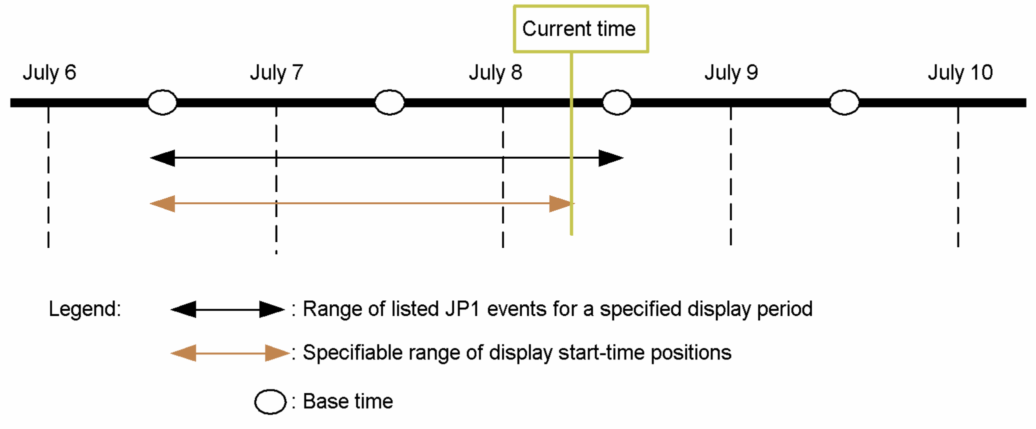
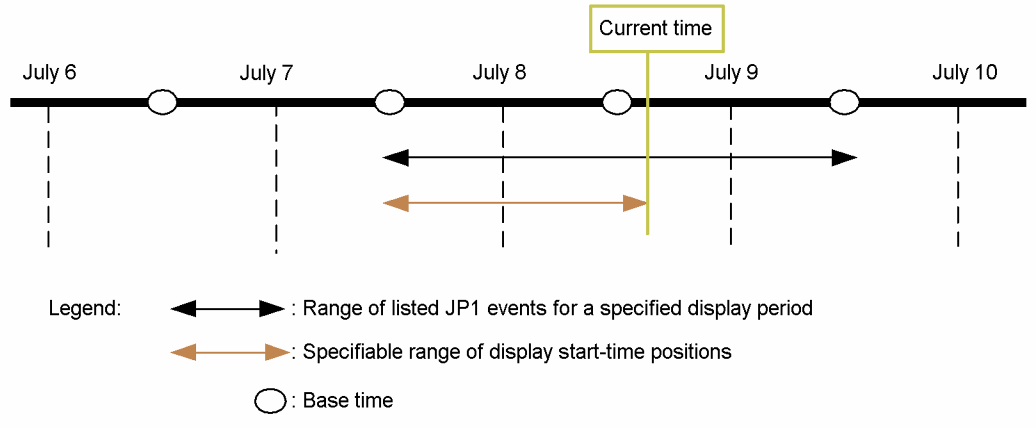

Current time
July 6
July 7
July 8
July 9
July 10
Legend:
: Range of listed JP1 events for a specified display period
: Specifiable range of display start-time positions
: Base time

Figure 3–104: Display range when the display period is two days and the current time is later than the base time


Current time
July 6
July 7
July 8
July 9
July 10
Legend:
: Range of listed JP1 events for a specified display period
: Specifiable range of display start-time positions
: Base time

For details about the event display period specification, see *5.7 Narrowing the JP1 events to be displayed by specifying a time period* in the *JP1/Integrated Management - Manager Administration Guide*.

For details about the event display start-time specification, see *3.16 Specifying the event display start-time*.

3.19 Performing system operations from JP1/IM

When a problem is detected during system monitoring, you can investigate using the following JP1/IM operations:

- Launch linked applications by monitor startup
- Tool Launcher
- Command execution from JP1/IM - View

This section describes these JP1/IM operations.

To launch a linked application by monitor startup or from the Tool Launcher, the OS user who started JP1/IM - View must have execution rights for that application.

3.19.1 Launching a linked product by monitor startup

In JP1/IM, you can select a JP1 event in the Event Console window and launch the GUI of the relevant application. This is known as *monitor startup*.

Depending on the application, by invoking the monitor startup you can directly launch a window related to the selected JP1 event. For example, if you select a job execution event issued by JP1/AJS and invoke the monitor startup, you will be taken directly to the window for managing the execution status of that job without having to navigate from a higher-level jobnet window.

Because you can launch an application window directly from a JP1 event that you want to investigate, you can quickly get on with the task by intuitive operation.

To use this functionality, the application that issued the JP1 event must support linkage with the monitor startup. For details about monitor startup support in a particular product, see the relevant manual listed below. For example, the JP1/AJS and JP1/PFM documentation describes the setup required to invoke the monitor startup from the Event Console window.

- JP1/AJS: See the description about monitoring jobnets using JP1/IM in the *JP1/Automatic Job Management System 3 Linkage Guide*.
- JP1/PFM: See the description of JP1/IM linkage in the *JP1/Performance Management Planning and Configuration Guide*.

You can add and change the applications that can be launched using the monitor startup by customizing a JP1/IM definition file. For an overview and description of how to customize the settings, see *4.17 Setting monitor startup for linked products* in the *JP1/Integrated Management - Manager Configuration Guide*.

Important

The authentication information in JP1/IM - View is accessed when a user opens a window of any of the following linked products using the monitor startup functionality:

- JP1/IM - Rule Operation
- JP1/AJS - View
- JP1/AJS - Web Console
- JP1/PFM - Web Console

Note that JP1/IM - View authentication information is invalidated in the following cases:

- The authentication server that the user is logged in to is restarted.
- The information is reloaded by the `jbs_spmd_reload` command on the authentication server that the user is logged in to.
- The primary authentication server that the user is logged in to is switched to the secondary authentication server.

When the authentication information in JP1/IM - View is invalid, the operations that can be performed depend on the product versions, as follows:

- When JP1/IM - Manager and JP1/IM - View are both version 08-10 or later, the JP1/IM - View user is automatically re-authenticated and authentication information is re-acquired.
- When either JP1/IM - Manager or JP1/IM - View is version 08-01 or earlier, authentication fails on the linked product side.

In 64-bit editions of Windows, if you execute a command in the `%WINDIR%\System32` folder, the WOW64 redirection function redirects the command to a command in the `%WINDIR%\SysWow64` folder. If the command is not found in the destination folder, command execution might fail. Be careful when you specify a command in the `%WINDIR%\System32` folder as the execution command.

(1) Overview of opening user-specified monitor windows

The functionality provided by JP1/IM - View lets you open a monitor window for a listed JP1 event. In the monitor window, you can view details about the job or application that issued the event, and directly operate on that job or application. Note that this functionality is not available with the Web-based JP1/IM - View.

By customizing a JP1/IM definition file, in addition to the windows you can open by default#, you can open the user-specified windows listed below (only one application can be launched for a JP1 event):

- User-specified application window
  Specify the executable file of the application.
- Web page
  Specify the URL of the Web page you want to open.

You can also pass information about the particular JP1 event to the launched application.

#

By default, you can open any of the following:

- JP1/AJS (application window)
- A submap window (Web page) of HP NNM version 7.5 or earlier

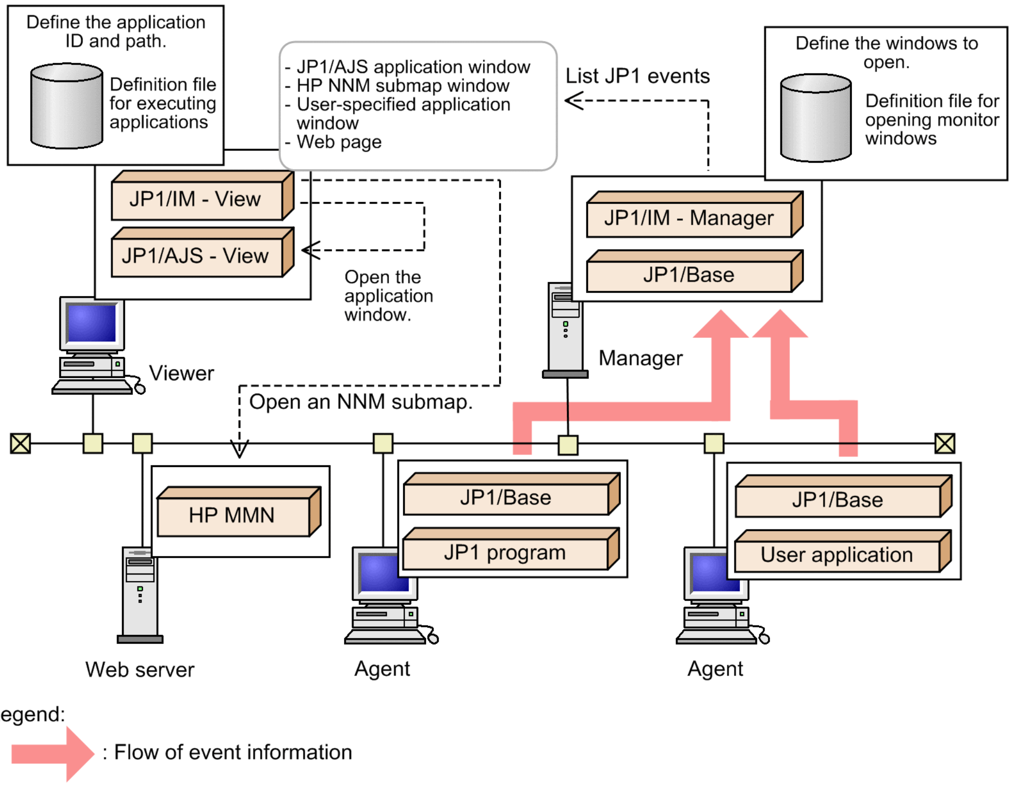
Some settings might have been added to the above products to enhance linkage with JP1/IM. Refer to the documentation of the application you want to use with JP1/IM.

For details about launching a monitor window for HP NNMi, see the manual *Job Management Partner 1/Integrated Management - Event Gateway for Network Node Manager i Description, User's Guide and Reference*.

Note that monitor windows are controlled by the OS user who launched JP1/IM - View.

The following figure provides an overview of opening monitor windows.

Figure 3–105: Opening monitor windows from JP1 events listed in JP1/IM - View


Define the application ID and path.
Definition file for executing applications
- JP1/AJS application window
- HP NNM submap window
- User-specified application window
- Web page
List JP1 events
Define the windows to open.
Definition file for opening monitor windows
JP1/IM - View
JP1/AJS - View
Open the application window.
JP1/IM - Manager
JP1/Base
Manager
Viewer
Open an NNM submap.
HP MMN
JP1/Base
JP1 program
JP1/Base
User application
Web server
Agent
Agent
Legend:
: Flow of event information

(2) Prerequisites

- To open an application program window, the executable file for that window must be placed on the machine on which JP1/IM - View is installed.
- To open a Web page, a Web server is required for the supported Web browser to connect to.

3.19.2 Tool Launcher

From the Tool Launcher window in JP1/IM - View, you can launch windows of products in the JP1 series and many other applications. The Tool Launcher window lists the application functions that are linked with JP1/IM, allowing the windows of the appropriate application to be launched directly from the listing.

You can launch the following two types of windows from JP1/IM - View:

Windows of applications on the viewer

You can launch and view the windows of any linked application installed on the same machine as JP1/IM - View.

Web pages

You can view the Web pages provided by any linked application in the system. Your Web browser starts with the required Web page. To view a Web page from the Tool Launcher, you must set the Web page's Uniform Resource Locator (URL) in advance.

A number of applications linked with JP1/IM are pre-registered in the Tool Launcher. For details, see *7.3.2 Functions that can be operated from the Tool Launcher window* in the *JP1/Integrated Management - Manager Administration Guide*.

If the application you want to register in the Tool Launcher is not mentioned in the above manual, see the documentation for that product. For example, the JP1/PFM manual explains how to register JP1/PFM functionality in the Tool Launcher.

- JP1/PFM: See the description of JP1/IM linkage in the *JP1/Performance Management User's Guide*.

You can add and change the applications that can be displayed in the Tool Launcher window by customizing a JP1/IM definition file. For an overview and detailed description of how to customize the settings, see *4.18 Setting the Tool Launcher window* in the *JP1/Integrated Management - Manager Configuration Guide*.

Important

When you call the window of a linked product by using the Tool Launcher, the product might require you to use the authentication information in JP1/IM - View. The following shows examples of the linked products that require you to use the authentication information in JP1/IM - View:

- JP1/IM - Rule Operation
- JP1/AJS3 - View
- JP1/AJS - Web Console
- JP1/PFM - Web Console

Note that JP1/IM - View authentication information is invalidated in the following cases:

- The authentication server that the user is logged in to is restarted.
- The information is reloaded by the `jbs_spmd_reload` command on the authentication server that the user is logged in to.
- The primary authentication server that the user is logged in to is switched to the secondary authentication server.

When the authentication information in JP1/IM - View is invalid, the operations that can be performed depend on the product versions, as follows:

- When JP1/IM - Manager and JP1/IM - View are both version 08-10 or later, the JP1/IM - View user is automatically re-authenticated and authentication information is re-acquired.
- When either JP1/IM - Manager or JP1/IM - View is version 08-01 or earlier, authentication fails on the linked product side.

In 64-bit editions of Windows, if you execute a command in the `%WINDIR%\System32` folder, the WOW64 redirection function redirects the command to a command in the `%WINDIR%\SysWow64` folder. If the command is not found in the destination folder, command execution might fail. Be careful when you specify a command in the `%WINDIR%\System32` folder as the execution command.

(1) Mechanism of calling other applications from the Tool Launcher window

The Tool Launcher window of JP1/IM - View lists the programs linked with JP1/IM. From the Tool Launcher, you can launch another management application program or open a Web page.

By customizing a JP1/IM - View definition file, you can add a new item to the Tool Launcher window. As the window to open from the new item, you can specify the following:

- User-specified application window

Specify the executable file of the application.

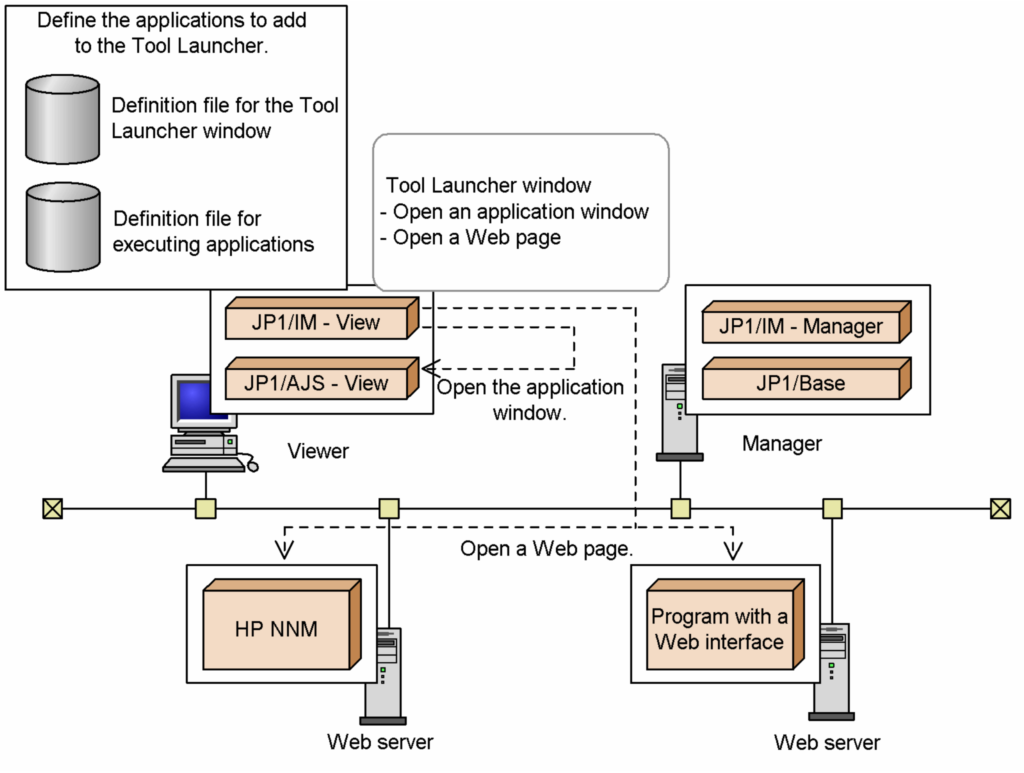
- Web page

  Specify the URL of the Web page you want to open.

Note that such application windows are controlled by the OS user who launched JP1/IM - View.

The following figure provides an overview of adding items to the Tool Launcher window.

Figure 3–106: Adding items to the Tool Launcher window


Define the applications to add to the Tool Launcher.
Definition file for the Tool Launcher window
Definition file for executing applications
Tool Launcher window
- Open an application window
- Open a Web page
JP1/IM - View
JP1/AJS - View
Open the application window.
Viewer
JP1/IM - Manager
JP1/Base
Manager
Open a Web page.
HP NNM
Program with a Web interface
Web server
Web server

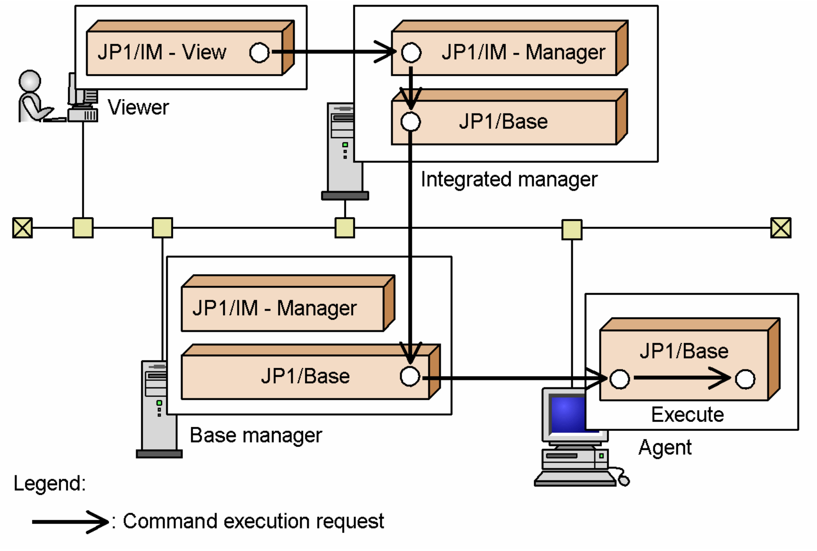
(2) Prerequisites

- To open an application program window, the executable file for that window must be placed on the machine on which JP1/IM - View is installed.
- To open a Web page, a Web server is required on the host specified in the URL (the host on which the product that provides the Web page is installed).

3.19.3 Executing commands on managed hosts from JP1/IM - View

In JP1/IM, requests can be issued from the Event Console window to execute a command on a managed host. You perform this request in JP1/IM - View's Execute Command window. The entered execution request is forwarded to the specified host from the manager that you are logged in to, according to the system configuration defined in the JP1/Base configuration management. The command is then executed on the target host.

Figure 3–107: Overview of how to execute commands on a managed host from JP1/IM - View



You can also execute commands on a client host (viewer). For details about how to execute commands on a client host, see *3.19.4 Executing commands on client hosts*.

The following describes the executable commands, the conditions required for issuing command requests to execute commands on managed hosts (agent hosts or manager hosts), and then the flow of processing for command execution.

(1) Executable commands

The following types of commands can be executed from JP1/IM - View:

When commands are targeted to managed Windows hosts:

- Executable file (`.com` or `.exe`)
- Batch file (`.bat`)
- Script file of JP1/Script (`.spt`) (provided the `.spt` file extension is associated with JP1/Script so that it can be executed)
- Data file (including `.vbs`) that has a file type (extension) associated with an application that can be run by an automated action

When commands are targeted to managed UNIX hosts:

- UNIX command
- Shell script

However, the following types of commands cannot be executed:

- Commands that require interactive operation
- Commands that display windows
- Commands that use an escape sequence or control code
- Internal commands, such as `echo` and `copy`
- Shortcuts# (in Windows)

#: You cannot even execute the shortcuts of the commands listed under *When commands are targeted to managed Windows hosts*.

Note that commands are executed by the OS user who is the JP1 user logged in to JP1/IM - View.

> **Note**
>
> When you execute commands from JP1/IM - View, you cannot directly shut down the OS, but you can control the OS by using JP1/Power Monitor.

(2) Conditions for command execution

The following conditions apply to command execution from JP1/IM - View:

- The JP1 user who requests command execution from JP1/IM - View must be registered in the authentication server and have the required permission for executing commands remotely.
- The system configuration must be defined using the JP1/Base configuration management.
- To execute a command on multiple hosts concurrently, the hosts must be grouped according to the host group definitions of the JP1/Base command execution function.
- The JP1 user issuing the request must be mapped to an OS user on the target host.
- To specify the command execution environment, you must first prepare an environment variable definition file on the target host.
- If the target host is a Windows host, the OS user subject to user mapping must have Windows-specific user permissions.
  For details about the user permissions required for the OS user subject to user mapping, see the chapter on granting user permissions to OS users in the *JP1/Base User's Guide*.

(3) Checking the command execution status and result

In the Execute Command window of JP1/IM - View, you can check the status and result of an executed command. To view the command execution log, execute the `jcocmdlog` command on the manager.

A JP1 event can be issued to report the execution status of a command. Because JP1 events are not issued by default, you must change the settings for issuing JP1 events by specifying the `-cmdevent` option of the `jcocmddef` command.

> **Important**
>
> - When multiple commands are executed, the results might be output in a different order from the execution order. The result output timing is affected by such things as the time required to execute each command, performance and workload differences among the hosts on which the commands are executed, and retry after a communication error.
> - The Execute Command window in JP1/IM - View shows the command execution results at the time they were received by the manager. Therefore, when you open this window, the displayed result might be for a previously executed command.
> - If you accidentally execute a command that cannot be executed from JP1/IM - View (see *3.19.3(1) Executable commands*), the command fails to terminate (message `KAVB2013-I` is not displayed in the **Log** area in the Execute Command window). In this situation, you can recover by using the status check and deletion commands provided by JP1/Base. For details, see *7.4.4(6) Commands for troubleshooting*.

(4) Flow of processing for command execution

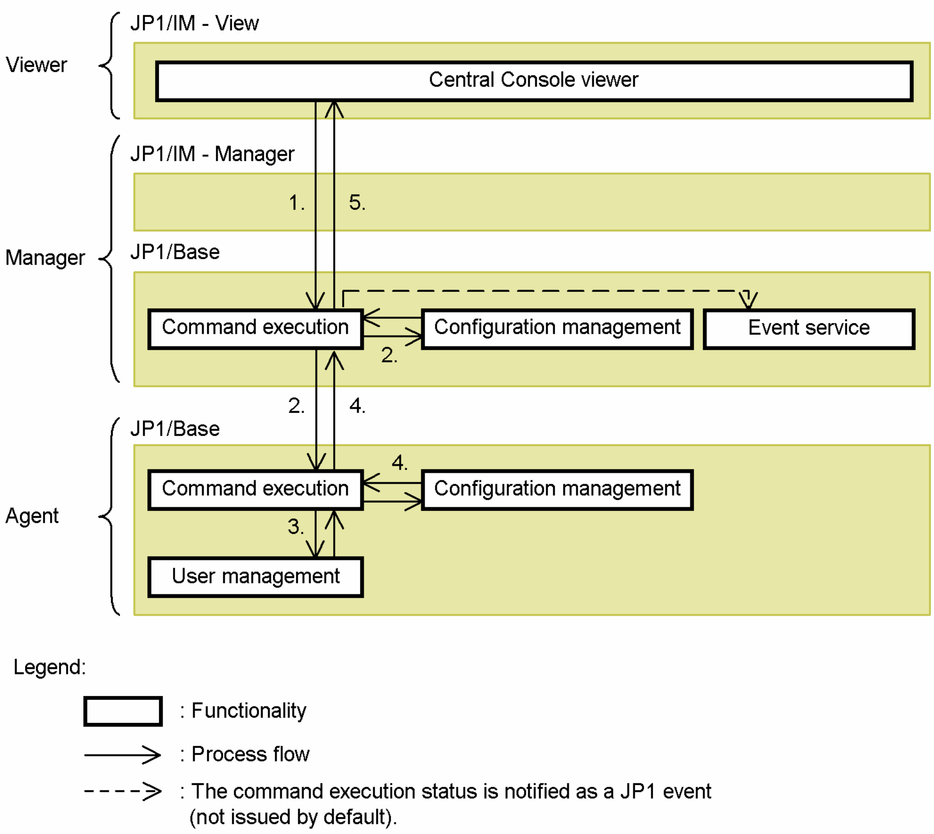
The following describes how the JP1/IM and JP1/Base functionality are inter-linked in command execution, taking as an example the flow of processing when a command is executed on an agent from a viewer.

The description below assumes that a JP1 user who has permission to execute commands is logged in to the manager. (For details about login requirements and the permissions required to execute commands, see *7.4.1 Managing JP1 users*.) There are two methods of command execution: executing a command by directly entering the command name, or executing a frequently-used command by clicking a command button after registering the command for a button.

For details about how to execute commands by directly entering the command names, see *7.1.1 Executing a command by using Command Execution* in the *JP1/Integrated Management - Manager Administration Guide*.

For details about how to execute commands by clicking command buttons, see *7.1.2 Executing a command by using the Command button* in the *JP1/Integrated Management - Manager Administration Guide*.

Figure 3–108: Flow of processing for command execution (command executed remotely on an agent)



The flow of processing is described below, following the numbers in the figure:

1. Open the Execute Command window in JP1/IM - View, and execute a command.

   In the Execute Command window, you can specify the command type, event information to inherit, target host, command, and the command execution environment. (The command execution environment must be defined in advance by setting up an environment variable definition file on the target host.)

   To issue a request to execute the command on an agent, select **Command of managed host** for **Command type**.

2. On receiving the command execution request, JP1/Base on the manager host references the configuration definitions and passes the request to the target host.

3. JP1/Base on the agent host where the request was received first references the user mapping definitions and then executes the command using the permissions of the mapped OS user.#

   #: User mapping (JP1/Base user management) is processed on the target host where the command is to be executed. Thus, user mapping must be set up in advance on the agent to execute a command from JP1/IM - View on an agent, or on the manager to execute a command from JP1/IM - View on a manager.

4. After the command has been executed, JP1/Base on the agent reports the result to the higher-level host defined in the configuration definitions.

5. On receiving the command execution result, JP1/Base on the manager records the result in a command execution log (ISAM) file, and then reports the result to JP1/IM - View.

Command execution from JP1/IM - View is realized by the JP1/Base command execution function. See also *7.4.4 Managing command execution*.

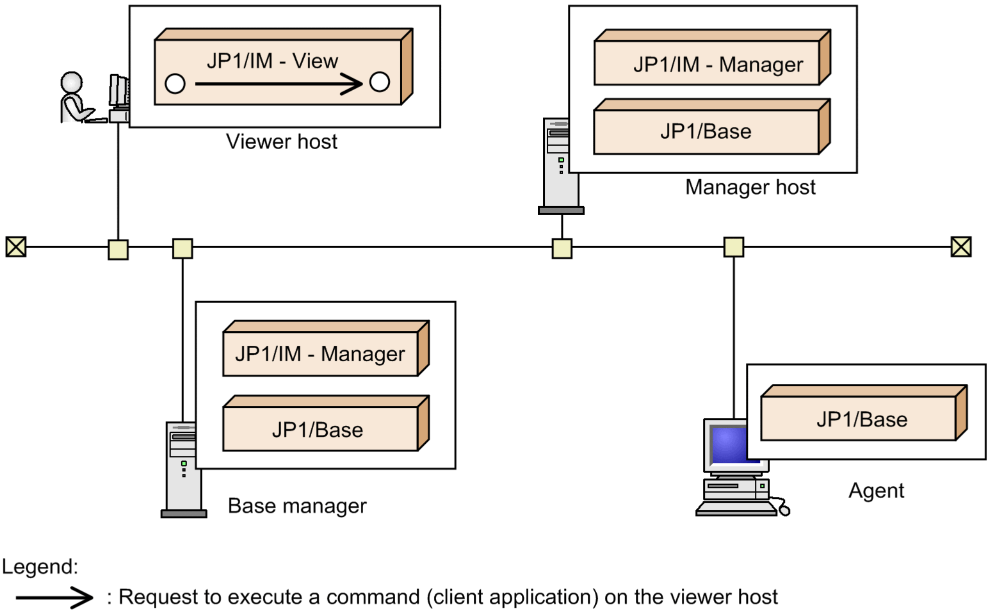
3.19.4 Executing commands on client hosts

In JP1/IM, you can issue command requests from the Execute Command window to execute commands on client hosts (viewer hosts) as well as on managed hosts (agent hosts or manager hosts). This function is called the *client application execution function*.

The client application execution function does not use the JP1/Base functionality. This function will also let you execute a command to display windows.

A command executed on a client host (viewer host) by using this function is called a *client application*. You can also let a client application inherit event information.

Figure 3–109: Overview of executing a client application from JP1/IM - View



For details about event inheritance, see *3.19.5 Inheriting event information when a command is executed*. For details about how to execute a client application, see *7.1.1 Executing a command by using Command Execution* and *7.1.2 Executing a command by using the Command button JP1/Integrated Management - Manager Administration Guide*. To execute command on managed hosts, see *3.19.3 Executing commands on managed hosts from JP1/IM - View*.

(1) Executable commands

The types of client applications are as follows:

- Executable files (`.exe`)
- Batch files (`.bat`)

However, the following commands cannot be executed:

- Commands that require standard input
- Commands that require redirection
- Commands that use an escape sequence or control code
- Internal commands, such as `echo` and `copy`

Note that client applications are executed by the OS user who launched JP1/IM - View.

Important

- Spaces and tabs (control code: `0x09`) specified for commands are identified as delimiters for command arguments. To specify a space or tab as a command argument, enclose the character string that contains the space or tab with double quotation marks (`"`).

  To specify a double quotation mark (`"`) as a command argument, specify as `\"` by adding a backslash (`\`) before the double quotation mark (`"`). Note that `\\"` is identified as `\` and `"`. If a backslash (`\`) is not placed before a double quotation mark (`"`), the character string subsequent to the double quotation mark (`"`) is identified as an argument.

  The following are examples of delimiting command arguments:

Example of delimiting command arguments 1

Assume that the following command is specified:

```
c:\AppCommand.exeΔtest1Δtest2<tab>"test3Δ
Δtest4"Δ"test5<tab><tab>test6"
```

Legend:

<tab>: Tab (`0x09`)

Δ: Space

Table 3–29: Results of delimiting command arguments 1

No.	Delimiting status	Delimiting results	Description
1	Command	`c:\AppCommand.exe`	N/A
2	Argument 1	`test1`	Delimited by the preceding and following spaces.
3	Argument 2	`test2`	Delimited by the preceding space and the following tab.
4	Argument 3	`test3Δ Δtest4`	Delimited by the tab before `"test3` and the space after `test4"`. Spaces enclosed with double quotation marks (`"`) are not delimited.

No.	Delimiting status	Delimiting results	Description
5	Argument 4	`test5<tab><tab>test6`	Delimited by the space before `"test5`. Tabs enclosed with double quotation marks (`"`) are not delimited.

Example of delimiting command arguments 2

Assume that the following command is specified:

```
c:\AppCommand.exeΔtest1Δtest2<tab>"test3\"<tab>\"test4"Δ"test5Δ\
\"Δtest6
```

Legend:

<tab>: Tab (`0x09`)

Δ: Space

Table 3–30: Results of delimiting command arguments 2

No.	Delimiting status	Delimiting results	Description
1	Command	`c:\AppCommand.exe`	N/A
2	Argument 1	`test1`	Delimited by the preceding and following spaces.
3	Argument 2	`test2`	Delimited by the preceding space and the following tab.
4	Argument 3	`test3"<tab>"test4`	Delimited by the tab before `"test3` and the space after `test4"`. `\"` is identified as `"`.
5	Argument 4	`test5Δ\`	Delimited by the spaces before `"test5` and after `\\"`. `\\"` is identified as `\` and `"`.
6	Argument 5	`test6`	Delimited by the preceding space.

- In 64-bit editions of Windows, if you execute a command in the `%WINDIR%\System32` folder, the WOW64 redirection function redirects the command to a command in the `%WINDIR%\SysWow64` folder. If the command does not exist at the redirection destination, the command execution might fail. Be careful when you specify a command in the `%WINDIR%\System32` folder as the execution command.
- The executed command process inherits the user environment variables and system environment variables. If you specify `%`*environment-variable-name*`%` on the command line, however, the environment variable is not inherited.

(2) Conditions required for command execution

The following commands can execute client applications:

- Commands placed on viewer hosts.
- Commands that can be executed with the permissions granted to the OS user who started JP1/IM - View.

(3) Checking the command execution status and results

After you execute a client application, you cannot check the execution results (return value of the command, standard output, and standard error output) and the execution status from the **Log** in the Execute Command window of JP1/IM - View. The **Log** displays a message indicating that either the command was executed or that command execution failed.

To check the execution results of client applications, create a batch file to output the execution results to a file.

Client applications cannot be stopped from JP1/IM - View. The user must stop the client applications.

(4) Handling of user account control

When the user account control (UAC) of Windows is used, if an OS user other than administrator user starts JP1/IM - View and executes a command that requires administrator permission, the command execution is interrupted. When the command execution is interrupted, the Log field of the Execute Command window displays a message to indicate that startup of a client application failed. The user can execute a command in JP1/IM - View that was launched by clicking **Run as an Administrator** or can execute a command from the command prompt launched by clicking **Run as an Administrator**.

Table 3–31: Whether commands can be executed for each execution permission (when Windows' UAC is used)

No.	Permission required for command execution	OS user who started JP1/IM - View		
		Administrator user	User in Administrators group	Other user
1	Administrator	Y	Δ	Δ
2	Administrators	Y	Y	Δ
3	None	Y	Y	Y

Legend:

Y: Executable.

Δ: A message is output, indicating that startup of the client application failed, and execution of the command is interrupted.

3.19.5 Inheriting event information when a command is executed

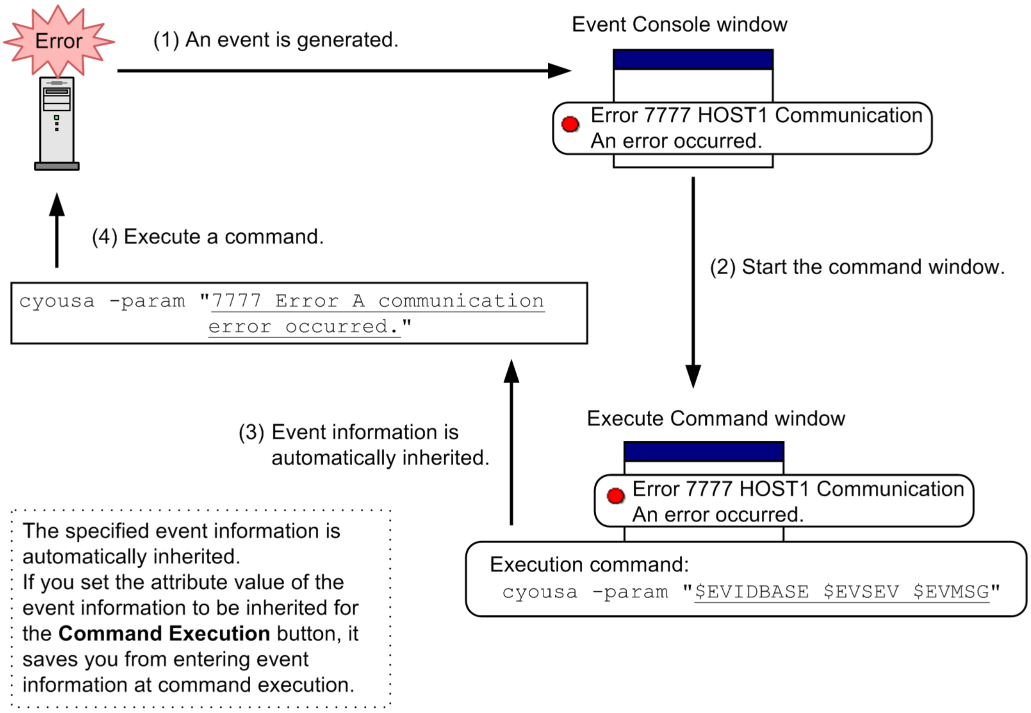
For the following items related to command execution, you can specify the variables for the JP1 event information displayed in the Event Console window:

- **Target host**
- **Command**
- **Environment variable file**

This function is called the *event information inheritance function*.

When this function is used, you do not have to directly enter, for the command argument, the event ID or message of the JP1 event for which investigation or handling is required. These pieces of event information can be specified for the command argument as variables.

Figure 3–110: Operation example when the event information inheritance function is used


Error
(1) An event is generated.
Event Console window
Error 7777 HOST1 Communication
An error occurred.
(2) Start the command window.
Execute Command window
Error 7777 HOST1 Communication
An error occurred.
(3) Event information is automatically inherited.
(4) Execute a command.

Execution command:

```
cyousa -param "$EVIDBASE $EVSEV $EVMSG"
```

```
cyousa -param "7777 Error A communication
               error occurred."
```

The specified event information is automatically inherited. If you set the attribute value of the event information to be inherited for the **Command Execution** button, it saves you from entering event information at command execution.

Legend:

Underline: Indicates the event information to be inherited.

(1) Specifiable event inheritance information

The event information inheritance function allows all JP1 events displayed in JP1/IM - View except dummy events (events that are not registered in the event database) to be inherited. Information in multiple events cannot be inherited at one time.

The JP1 events shown below can be inherited. These JP1 events are JP1 events issued by a JP1 series product such as JP1/IM - MO, JP1 events issued by a user program, or correlation events.

- JP1 events registered in the event database of the manager to which JP1/IM - View is logged in, or in the integrated monitoring database
- JP1 events registered in the event database on an agent host

The table below describes the specifiable variable names and inherited event information for each event attribute type. The legend of the tables below is as follows:

Legend:

--: Not applicable.

Δ: Space

Table 3–32: Variable names and inherited event information (Basic attributes of JP1 events)

No.	Event attribute	Variable	Inherited event information
1	--	`EVBASE`	A value obtained after the entire basic information of an event is converted to the following format: *event-IDΔevent-source-user-nameΔevent-source-user-IDΔevent-source-group-nameΔevent-source-group-IDΔevent-source-event-server-nameΔevent-source-process-IDΔevent-registration-date-month-and-yearΔevent-registration-timeΔevent-source-host-IP-address*

No.	Event attribute	Variable	Inherited event information
			If no value is set, the value is replaced with a null character.
2	B.ID B.IDEXT	EVID	A value obtained after the event ID is converted to the *basic-code*:*extended-code* format. Basic codes and extended codes are 8-digit hexadecimal numbers (uppercase letters are used for A to F). Preceding zeros are omitted from the ID. For example, if the extended code is 00000000, EVID is *basic-code*:0.
3	B.ID	EVIDBASE	A value obtained after the event ID is converted to the basic code format. EVIDBASE is an 8-digit hexadecimal number (upper letters are used for A to F), and preceding zeros are omitted from the ID.
4	B.TIME	EVDATE	A value obtained after the registration time is converted to the *yyyy*/*mm*/*dd* format. Conversion is for the time zone set for JP1/IM - View.
5	B.TIME	EVTIME	A value obtained after the registration time is converted to the *hh*:*mm*:*ss* format. Conversion is for the time zone set for JP1/IM - View.
6	B.PROCESSID	EVPID	A value for the event source process ID
7	B.USERID	EVUSRID	A value for the user ID of the event source process
8	B.GROUPID	EVGRPID	A value for the group ID of the event source process
9	B.USERNAME	EVUSR	A value for the event source user name
10	B.GROUPNAME	EVGRP	A value for the event source group name
11	B.SOURCESERVER	EVHOST	A value for the event source host name
12	B.SOURCEIPADDR	EVIPADDR	A character string for the event source IP address in IPv4 address format or IPv6 address format#
13	B.SEQNO	EVSEQNO	A value for the serial number in the event database
14	B.ARRIVEDTIME	EVARVDATE	A value obtained after the arrived time is converted to the *yyyy*/*mm*/*dd* format.
15	B.ARRIVEDTIME	EVARVTIME	A value obtained after the arrived time is converted to the *hh*:*mm*:*ss* format.
16	B.SOURCESEQNO	EVSRCNO	A value for the serial number in the source event database
17	B.MESSAGE	EVMSG	A value for the message. If the applicable attribute does not exist, the value is replaced with a null character.

#:

- IPv4 address format

  In this format, each 8 bits of a 32-bit address is delimited by periods (.), and is output as decimal numbers (from 0 to 255).

  Example: 0.64.128.255

- IPv6 address format

  In this format, each 16 bits of a128-bit address is delimited by colons (:), and is output as hexadecimal numbers (from 0000 to ffff).

  Example: 0011:2233:4455:6677:8899:aabb:ccdd:eeff

Table 3–33: Variable names and inherited event information (extended attributes of JP1 events (common information))

No.	Event attribute	Variable	Inherited event information
1	E.SEVERITY	EVSEV	A value for the event level#1

No.	Event attribute	Variable	Inherited event information
			`Emergency`, `Alert`, `Critical`, `Error`, `Warning`, `Notice`, `Information`, `Debug`, or a value set for the event level
2	`E.USER_NAME`	`EVUSNAM`	A value for the user name[#1]
3	`E.OBJECT_TYPE`	`EVOBTYP`	A value for the object type[#1]
4	`E.OBJECT_NAME`	`EVOBNAM`	A value for the object name[#1]
5	`E.ROOT_OBJECT_TYPE`	`EVROBTYP`	A value for the root object type[#1]
6	`E.ROOT_OBJECT_NAME`	`EVROBNAM`	A value for the root object name[#1]
7	`E.PRODUCT_NAME`	`EV"PRODUCT_NAME"`	A value for the product name[#2]
8	`E.OBJECT_ID`	`EV"OBJECT_ID"`	A value for the object ID[#2]
9	`E.OCCURRENCE`	`EV"OCCURRENCE"`	A value for the occurrence[#2]
10	`E.START_TIME`	`EV"START_TIME"`	A value for the start time[#2]
11	`E.END_TIME`	`EV"END_TIME"`	A value for the end time[#2]
12	`E.RESULT_CODE`	`EV"RESULT_CODE"`	A value for the result code[#2]
13	`E.JP1_SOURCEHOST`	`EV"JP1_SOURCEHOST"`	A value for the event source host name[#2]
14	--	`EV"`*extended-attribute-name*`"`[#1]	A value specified with the extended attribute name.[#2] For details about information contained in attributes, see the manual for each JP1 event source product.

#1

If the applicable attribute does not exist, the value is replaced with a null character.

#2

If the applicable attribute does not exist, the value is replaced with the character string for the variable.

Table 3–34: Variable names and inherited event information (others)

No.	Event attribute	Variable	Inherited event information
1	--	`EV"@JP1IM_ACTTYPE"`	A value indicating the action type • `0`: Not subject to the action. • `1`: Command • `2`: Rule • `3`: Command and rule
2	--	`EV"@JP1IM_ACTCONTROL"`	A value indicating whether the event is subject to the action • `0`: Not subject to the action. • `1`: Executed. • `2`: Suppressed. • `3`: Partially suppressed.

No.	Event attribute	Variable	Inherited event information
3	--	EV"@JP1IM_SEVERE"	A value indicating whether the event is a severe event - 0: Not a severe event - 1: A severe event
4	--	EV"@JP1IM_CORRELATE"	A value indicating whether the event is a correlation event - 0: Not a correlation event - 1: A correlation approval event - 2: A correlation failure event
5	--	EV"@JP1IM_RESPONSE"	A value indicating whether the event is a response-waiting event - 0: Not a response-waiting event - 1: A response-waiting event
6	--	EV"@JP1IM_ORIGINAL_SEVERITY"	A value for the event level (before changing the event level)# (Emergency, Alert, Critical, Error, Warning, Notice, Information, Debug, or a value set for the event level) This attribute is set only when the severity changing function is enabled.
7	--	EV"@JP1IM_CHANGE_SEVERITY"	A value indicating whether an event level has been changed - 0: Not changed. - 1: Changed.
8	--	EV"@JP1IM_DEALT"	A value indicating the handling status - 0: Not handled. - 1: Handled. - 2: Processing. - 3: Pending.
9	--	EV"@JP1IM_RELEASE"	A value indicating whether a severe event has been released - 0: Not released. - 1: Released.
10	--	EV"@JP1IM_DISMISSED"	A value indicating whether a severe event has been deleted - 0: Not deleted. - 1: Deleted.
11	--	EV"@JP1IM_MEMO"	A value for memo information#
12	--	EV"@JP1IM_DISPLAY_MESSAGE"	Value of message (after change) This attribute is set only when the display message change function is enabled.
13	--	EV"@JP1IM_CHANGE_MESSAGE"	Value indicating whether the display message has been changed - 0: The message has not been changed. - 1: The message has been changed. This attribute is set only when the display message change function is enabled.
14	--	ACTHOST	A value for the manager host name

#

If no applicable attribute exists, the value is replaced with the character string for the variable.

For details about the event inheritance information that can be specified for automated action, see *5.3.4 Inherited event information*.

(2) Specifying variables

The command execution function inherits event information through variables. JP1/IM - View converts the variables into JP1 event information, and then executes the command. Note that variables are case sensitive.

The following describes how to specify variables and the character strings resulting from the conversion.

Specify variables in the `$`*variable-name* format. If only `$` is specified, it is regarded as a variable, but is not converted. If you want to specify `$` as a character, place the escape character \ before `$`. For details about the character strings that can be specified, see *3.19.5(1) Specifiable event inheritance information*.

The following table gives examples of specifications and the conversion results when `server01` is set for the event source host name.

No.	Specification format	Conversion result
1	`ping $EVHOST`	`ping server01`
2	`/\$EVHOST`	`/$EVHOST`

If you place an alphanumeric character or underscore (_) immediately after the variable, the variable cannot be correctly converted. In such case, enclose the variable name with curly brackets (`{ }`).

The following table gives examples of specifications and the conversion results when `100` is set for the event ID (`$EVIDBASE`) and `ABC` is set for the extended attribute EX (`$EV"EX"`).

No.	Specification format	Conversion result
1	`$EVIDBASE abc`	`100 abc`
2	`$EVIDBASEabc`	`$EVIDBASEabc`#
3	`${EVIDBASE}abc`	`100abc`
4	`$EVIDBASE_abc`	`$EVIDBASE_abc`#
5	`${EVIDBASE}_abc`	`100_abc`
6	`$EV"EX" abc`	`ABC`
7	`$EV"EX"abc`	`ABCabc`

#:

When the command is specified on the command line and executed on a UNIX host, the variable is regarded as an environment variable of the OS during command execution, and then treated as a null character.

The following control characters contained in the character information to be converted are converted to spaces (0x20).

Control characters that are converted to spaces: 0x01 to 0x1F (excluding tabs (0x09)), and 0x7F

For example, if a message acquired by specifying `$EVMSG` contains a linefeed code (0x0A), the linefeed code (0x0A) is converted to a space (0x20).

Important

If \ is specified immediate before `$`, `$` is treated as a character. However, if you want to specify a variable subsequent to \, such as in a file path, \ is converted and is not treated as a character string. You can avoid this by performing the following:

When specifying it in the execution command:

Create a batch file in which a variable is specified for the argument. Specify the command line in which `\` is used in the batch file.

Example of specification of an execution command:

- Execution command: `AppTest.bat $ACTHOST`

- Batch file: `application.exe c:\work\%1\result.txt`

In this example, the conversion result of `$ACTHOST` is set for `%1`.

When using a variable in a file path:

Add a prefix to the variable.

The following shows examples when `IM-VIEW` is set for `EV"PRODUCT_NAME"`:

Example when the variable cannot be converted:

- Example specification: `C:\$EV"PRODUCT_NAME"`

- Conversion result: `C:$EV"PRODUCT_NAME"`

In this example, `EV"PRODUCT_NAME"` cannot be converted because `\$` is specified.

Example when the variable can be converted:

- Example specification: `C:\pre_$EV"PRODUCT_NAME"`

- Conversion result: `C:\pre_IM-VIEW`

In this example, `EV"PRODUCT_NAME"` can be converted because `pre_` is added before the variable.

Important

When an attribute value is inherited, a character the OS treats as a special meaning can be converted into another character string. This behavior is the same as when a command is executed by an automated action. For details about conversion of a special character, see the description in *Notes about specifying variables* in *Automated action definition file (actdef.conf)* in *Chapter 2. Definition Files* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*. Also, specific ASCII characters are converted to other characters according to the settings in the configuration file for converting information. For details about the configuration file for converting information, see *Configuration file for converting information (event_info_replace.conf)* in *Chapter 2. Definition Files* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

You can specify a URL-encoded or Base64 encoded value of a JP1 event in the contents of the command to be executed. You cannot specify such an encoded value for the execution target host name or in the environment variable file.

Specify the value in the following format:

`$`*variable-name*`$`*encoding-type*

The following table lists and describes the encoding types and specification formats that can be specified when event information is inherited.

Table 3–35: Encoding types and specification formats that can be specified when event information is inherited

No.	Encoding type	Specification format	Description
1	URL encoding	`$`*variable-name*`$URLENC`	The event information to be inherited is URL encoded as a UTF-8 character string.

No.	Encoding type	Specification format	Description

		`${`*variable-name*`$URLENC}`	The resulting character string is passed to the execution command.
			Specification example 1:
			`C:\WebBrowser.exe http://host/site?id=$EVMSG$URLENC`
			Specification example 2:
			`C:\WebBrowser.exe http://host/site?p1=${EVMSG$URLENC}_$EVPID`

2	Base64 encoding	`$`*variable-name*`$ENC`
		`${`*variable-name*`$ENC}`
			The event information to be inherited is Base64 encoded.
			The resulting character string is passed to the execution command.
			Specification example 1:
			`C:\UP\View.exe $EV"USER" $EV"PASS"$ENC`
			Specification example 2:
			`C:\UP\View.exe $EV"USER" ${EV"PASS"$ENC}_$EVPID`

3	Both the Base64 encoding and URL encoding	`$`*variable-name*`$ENC$URLENC`
		`${`*variable-name*`$ENC$URLENC}`
			The event information to be inherited is Base64 encoded, and then URL encoded.
			The resulting character string is passed to the execution command.
			Specification example 1:
			`C:\WebBrowser.exe http://host/site?pass=$EV"PASS"$ENC$URLENC`
			Specification example 2:
			`C:\WebBrowser.exe http://host/site?pass=${EV"PASS"$ENC$URLENC}_$EVPID`

4	No encoding	`$`*variable-name*
		`${`*variable-name*`}`
			Neither URL encoding nor the Base64 encoding is performed.
			The event information to be inherited is passed to the execution command as it is.
			For details, see the tables in *3.19.5(1) Specifiable event inheritance information*.
			Specification example 1:
			`C:\WebBrowser.exe http://host/site?id=$EVIDBASE`
			Specification example 2:
			`C:\WebBrowser.exe http://host/site?p1=${EVIDBASE}_$EVPID`

Important

If you place an alphanumeric character or underscore (_) immediately after the encoding type, enclose *variable-name*`$`*encoding-type* with curly brackets (`{ }`).

Also, in the following cases, `$`*variable-name*`$`*encoding-type* or `${`*variable-name*`$`*encoding-type*`}` is regarded as a character string, and is not converted:

- No event corresponding to *variable-name* exists.
- The specification format is incorrect.

The following table gives some specification formats and conversion results.

Table 3–36: Examples of the formats specifying encoding and conversion results

No.	Specification format	Conversion result	Description
1	`$EVMSG$URLENC`	`ABC%40DEF`	`$EVMSG` is `ABC@DEF`.
2	`$EVMSG$ENC`	`QUJDREVGRw==`	`$EVMSG` is `ABCDEFG`.
3	`$EVMSG$ENC$URLENC`	`QUJDREVGRw%3D%3D`	`$EVMSG` is `ABCDEFG`.
4	`$HOGE$URLENC`	`$HOGE$URLENC`	`$HOGE` is an invalid variable.
5	`${EV"A0"$URLENC}abc`	`${EV"A0"$URLENC}abc`	Attribute `EV"A0"` does not exist.
6	`$EVMSG$URL`	`ABCDEFG$URL`	`$EVMSG` is `ABCDEFG`. `$URL` is an invalid variable.
7	`${EVMSG$URL}abc`	`${EVMSG$URL}abc`	`$EVMSG` is `ABCDEFG`. `$URL` is an invalid variable.
8	`$EVMSG$ENC\$URLENC`	`QUJDREVGRw==$URLENC`	`$EVMSG` is `ABCDEFG`. Base64 encoded by `$ENC`. \ is escaped by the specification of `\$`.
9	`$EVMSG\$URLENC`	`ABC@DEF$URLENC`	`$EVMSG` is `ABC@DEF`. \ is escaped by the specification of `\$`.
10	`$EVMSG$URLENC`	Null character	`$EVMSG` is a null character.

(3) Specifying events to be inherited

The following table describes operations by which you can specify the JP1 events to be inherited by the command to be executed.

Table 3–37: Windows, menus, and buttons that can inherit event information

No.	Window type	Window name	Starting the Execute Command window#1	Event to be inherited
1	Event list	Event Console	Menu>**View**>**Execute Command (Event Inheritance)**	JP1 events selected on the following pages in the Event Console window: • **Monitor Events** • **Severe Events** • **Search Events** • **Response-waiting event**
2			Menu>**Options**>**Execute Command**#2	
3			Toolbar>**Execute Command** button#2	
4			Pop-up menu>**Execute Command (Event Inheritance)**	
5		Related Events (Summary)	Pop-up menu>**Execute Command (Event Inheritance)**	JP1 events selected in the following tables in the Related Events (Summary) window: • **Display Items** • **Related Events**
6		Related Events (Correlation)	Pop-up menu>**Execute Command (Event Inheritance)**	JP1 events selected in the following tables in the Related Events (Correlation) window: • **Display Items** • **Related Events**
7	Event details	Event Details	**Execute Command** button	JP1 events displayed in the window. However, event information for dummy events cannot be inherited.
8		Edit Event Details		

No.	Window type	Window name	Starting the Execute Command window[#1]	Event to be inherited
9		Event Details>Related Events (Summary)		
10		Edit Event Details>Related Events (Summary)		
11		Event Details>Related Events (Correlation)		
12		Edit Event Details>Related Events (Correlation)		

#1:

If the selected event meets any of the conditions below, the **Execute Command (Event Inheritance)** menu item becomes unavailable, and cannot be selected. Also, for a dummy event, the **Execute Command** button in the Event Details window becomes unavailable, and cannot be clicked.

- There is no JP1 event.
- Multiple JP1 events are selected.
- A dummy event is selected.

#2:

If the Execute Command window is already displayed, it becomes the foreground (active) window.

The specified event is displayed in the Execute Command window. The display items (attributes) for the displayed JP1 events are the same as the display items (attributes) for the event list in the Event Console window. For details about the display items (attributes), see *3.19.5(1) Specifiable event inheritance information*.

When the Execute Command window is displayed, if you specify a JP1 event again so that the event is inherited by the Execute Command window, the displayed JP1 events are changed. If the display items are changed in the Preferences window, the attribute values displayed in the Execute Command window are also changed.

If you open the Execute Command window after clicking a menu or button for which event information cannot be inherited, the events to be inherited cannot be displayed. In that case, the **Inherit event information** check box in the Execute Command window is not selected, and the event information is displayed as a blank.

(4) Preview of the command to be executed

When event information is inherited, the Preview Command Execution Content window is displayed before command execution. The Preview Command Execution Content window displays the contents of the command to be executed after its variables are replaced with event information.

The contents of the command displayed in the Preview Command Execution Content window can be modified, and you can execute the modified command. If the size of the command contents exceeds its upper limit after the variables are replaced with event information, the Preview Command Execution Content window displays the contents from which the excess information was truncated. After a part of the contents are truncated, you can also check the contents before being truncated.

For details about the Preview Command Execution Content window, see *2.41 Preview Command Execution Content window* in the manual *JP1/Integrated Management - Manager GUI Reference*.

Note that the value before the variables are replaced (the value displayed in the Execute Command window) is saved as a history item. The value displayed or edited in the Preview Command Execution Content window is not saved as a history item.

3.20 Email notification function (for Windows only)

JP1/IM - Manager provides the following method to send email by an automated action when a severe error is detected:

- Using JP1/TELstaff
- Using the `jimmail` command of JP1/IM - Manager

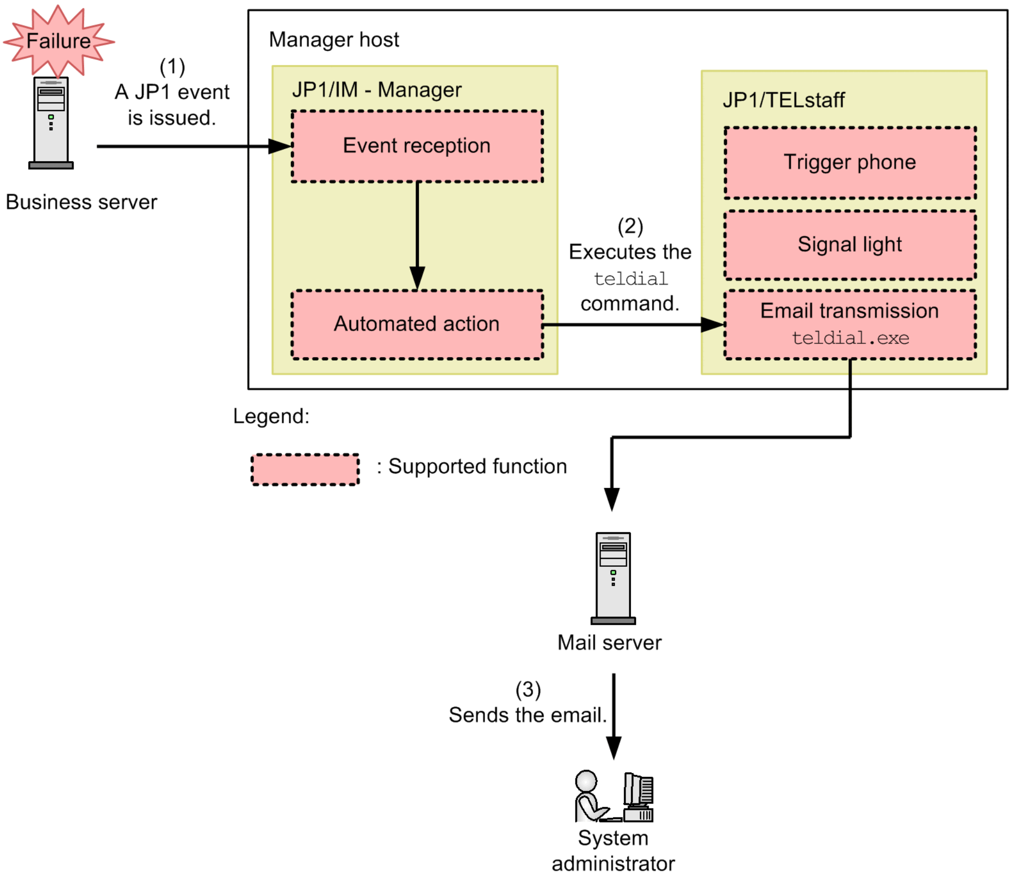
This section describes the email notification function.

3.20.1 Mechanism of mail notification function

This subsection describes the mechanism of the email notification function.

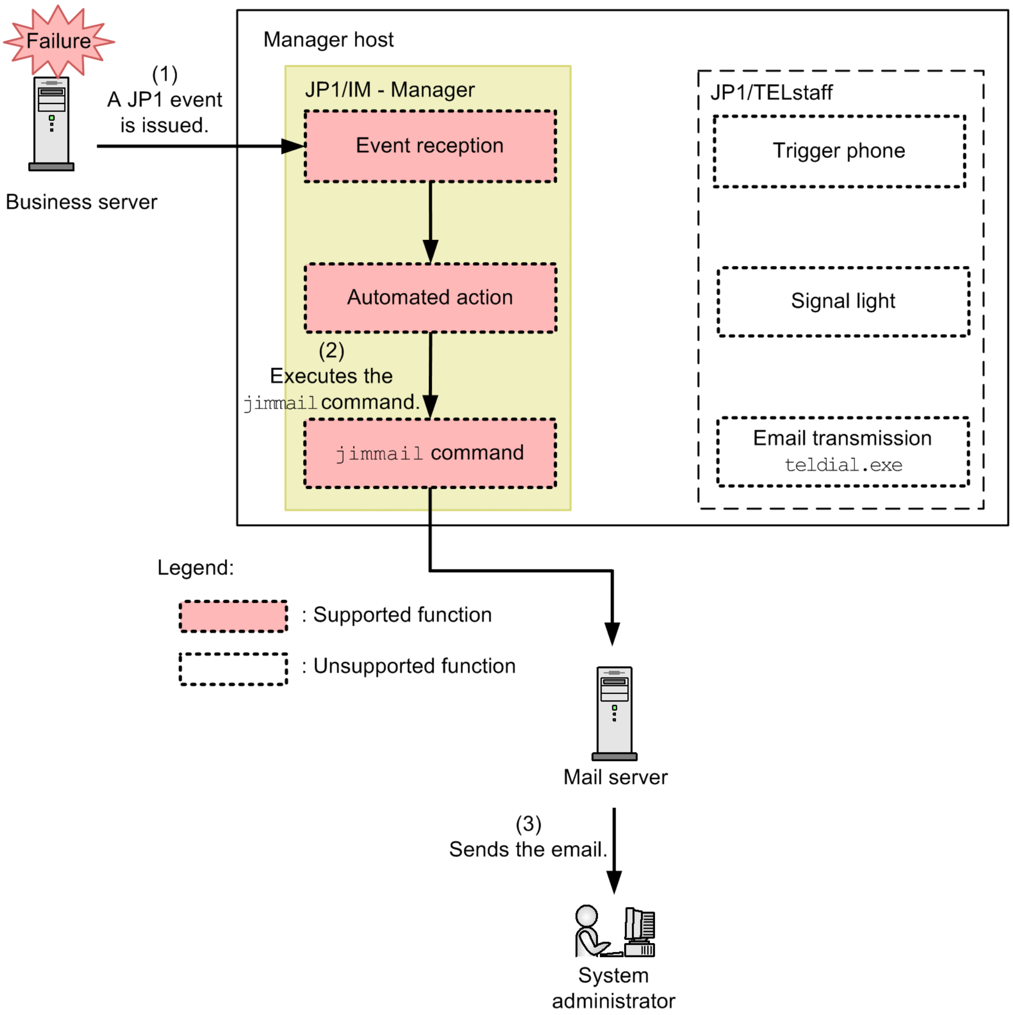
If JP1/TELstaff is linked for email notification purposes, when JP1/IM - Manager receives an event, JP1/TELstaff's `teldial` command is executed as an automated action and the email is sent to the mail server of the system administrator via JP1/TELstaff, as shown the figure below. Use JP1/TELstaff if you also use a trigger phone or a signal light.

Figure 3–111: Sending notification email by using JP1/TELstaff



When the `jimmail` command of JP1/IM - Manager is used to send a notification email, the email is sent from JP1/IM - Manager to the mail server of the system administrator without JP1/TELstaff having to be installed.

Figure 3–112: Sending notification email by using the jimmail command of JP1/IM - Manager



3.20.2 JP1/IM - Manager's email notification function

JP1/IM - Manager supports JP1/TELstaff and JP1/IM - Manager's `jimmail` command as methods for sending emails by automated action in the event of a severe failure.

The following table lists the functions of JP1/IM - Manager (`jimmail` command).

Note that the functions of JP1/TELstaff might change in the future as a result of addition of functions or changes in specifications. For details about the functions of JP1/TELstaff, see the *JP1/TELstaff System Configuration and User's Guide*.

Table 3–38: List of functions of JP1/IM - Manager (jimmail command)

Item		JP1/IM - Manager (jimmail command)
Monitoring using a trigger phone or a signal light		N
Setting multiple mail servers		N
SMTP authentication	No authentication	Y
	POP before SMTP authentication	Y

Item			JP1/IM - Manager (jimmail command)
	SMTP-AUTH authentication	PLAIN	Y
		LOGIN	Y
		CRAM-MD5	N
		DIGEST-MD5	N
Encryption of SMTP authentication passwords			Y[#1]
Encryption of communication	STARTTLS		N
	SMTPS (SMTP over SSL)		N
Address	Specifying a single address		Y
	Specifying multiple addresses		Y
	Specifying CC and BCC		N
	Specifying a sender's address		Y
	Specifying a recipient's address		N
	Specifying a group (communication network)		N
Email body	Specifying a subject		Y
	Specifying body text		Y
	Method for defining the subject and body of emails		CUI (command)
	Attachment of files		N
	Inheritance of information (using IM events and variables for action information)		Y
	Using variables[#2]		N
	Sending emails requesting a read receipt		N
	Adding severity information		N
Retry transmission in the event of a transmission error			N
Calendar function (weekday/holiday)			N
Schedule function (hourly)			N
Outgoing limits			N

Legend:

Y: Supported

N: Not supported

#1

Encrypted SMTP/POP3 authentication passwords are saved in the email environment definition file.

#2

This function defines variables and their corresponding character strings, and then replaces variable names with the corresponding character strings during email transmission.

For details about JP1/IM - Manager (`jimmail` command), see *jimmail (Windows only)* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

See the following table for limitations to JP1/IM - Manager (`jimmail` command).

Table 3–39: Limitations to JP1/IM - Manager (jimmail command)

Item	Limit value
Maximum length of an email address	256 bytes
Maximum length of an email subject	512 bytes
Maximum length of email body text	4,096 bytes
Maximum length of an email text line	512 bytes
Number of emails that can be sent at one time	20

The maximum length of a command line for an automated action is 4,096 bytes. If this maximum length is exceeded, the `jimmail` command cannot be executed.

3.20.3 Displaying linked applications from the URL in emails sent by automated action

If emails are to be sent by an automated action, the attribute values of a JP1 event that resulted in the automated action can be inherited as event inheritance information in the email text. In this case, event inheritance information values can be URL encoded.

Therefore, if you define the encoded event inheritance information in a URL in the email text, you can pass event information to the application that is linked from the URL.

For JP1 products, you can display the JP1/AJS - Web Console monitor window directly from sent email by specifying in the email text the URL of the JP1/AJS - Web Console monitor window that corresponds to the JP1/AJS job or jobnet. For details, see *8.7.2 Displaying a monitor window from an email sent by an automated action (automated action function)*.

For details about the encoding of event inheritance information in automated actions, see *5.3.4(2) Encoding of event inheritance information*.

3.21 Event-source-host performance report display function

You can directly display a JP1/PFM - Web Console report window that indicates the performance of a selected event-source-house at the time of an event (single sign-on). This function is called the event-source-host performance report display function.

By linking with JP1/PFM by using the event-source-host performance report display function, you can promptly check the host performance information at the time at which events occur.

For details about the event-source-host performance report display function, see *8.8 Linking with JP1/PFM*.

4 Objective-Oriented System Monitoring Using the Central Scope

The Central Scope provides functionality for monitoring a system according to objectives set by the system administrator.

This chapter describes the functions of the Central Scope.

4.1 Overview of Central Scope functions

The Central Scope supports objective-oriented system monitoring based on tree views, map views, and action guidance. You can easily build a Central Scope environment using the auto-generation and editing functions of the Monitoring Tree window.

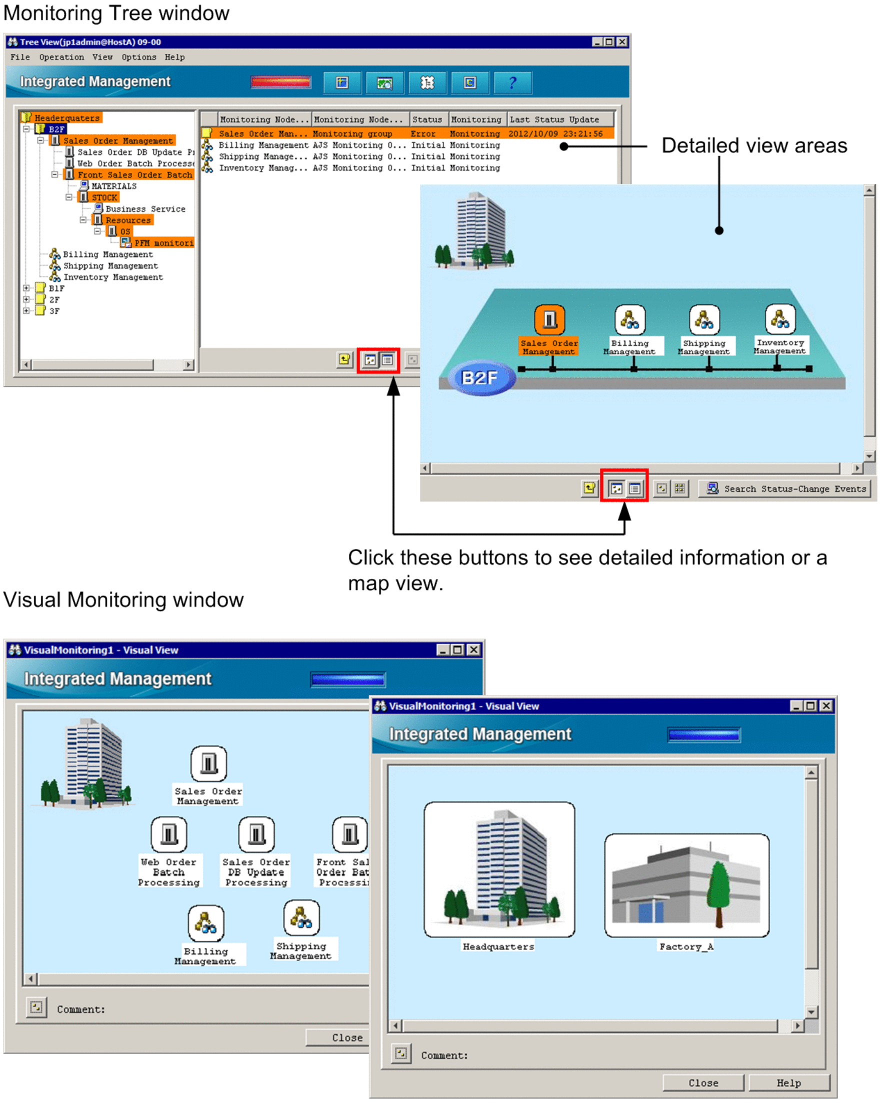
❗ **Important**

The Central Scope is disabled (does not run) by default. To use this functionality, you must create a monitoring object database with the `jcsdbsetup` command, and then enable the Central Scope in the `jcoimdef` command options.

For details, see the following subsection in the *JP1/Integrated Management - Manager Configuration Guide*:

- For Windows:
  1.18.1 Specifying settings for using the functions of Central Scope (for Windows)
- For UNIX:
  2.17.3 Specifying settings for using the functions of Central Scope (for UNIX)

Figure 4–1: Display examples of the Monitoring Tree window and Visual Monitoring window



	Monitoring Node...	Monitoring Node...	Status	Monitoring	Last Status Update
	Sales Order Man...	Monitoring group	Error	Monitoring	2012/10/09 23:21:56
	Billing Management	AJS Monitoring O...	Initial	Monitoring	
	Shipping Manage...	AJS Monitoring O...	Initial	Monitoring	
	Inventory Manag...	AJS Monitoring O...	Initial	Monitoring	

The functions of the Central Scope are summarized as follows.

- Monitoring Tree window

  Displays the resources managed by JP1/IM according to the monitoring objectives.

  The monitoring tree shows the *monitoring objects* monitored by the Central Scope, indicated by icons and arranged in *monitoring groups* in a tree structure.

  The icons are designed so that you can see, from the inter-relationship of jobs and servers in the tree, which jobs will be affected by a server failure, for example. In the detailed view area, you can view information in map format, like the Visual Monitoring window.

  By using JP1 resource groups, you can control the monitoring range permitted to individual JP1 users, and exercise precise control over access to the nodes in a monitoring tree.

- Auto-generation and editing of a monitoring tree

  A monitoring tree can be easily generated using the auto-generation and editing functions.

  To generate a monitoring tree, you simply select a purpose-built template from the Generation Tree list in the Auto-generation - Select Configuration window. The Central Scope automatically collects definition information from the JP1/IM agents, and creates a monitoring tree based on the template.

  A template consists of model definition information for producing a monitoring tree. Supported monitoring trees include work-oriented trees and server-oriented trees.

You can edit an automatically generated monitoring tree in the Monitoring Tree (Editing) window to suit your system operation and its requirements. Alternatively, you can output the monitoring tree definitions to a CSV file and then edit them.

- Visual monitoring

  The icons in a monitoring tree can be mapped on a corporate organizational chart or other image in a Visual Monitoring window.

  In addition to the icons provided as standard, you can register images of any size as Visual Icon. Key objects and groups that you particularly want to monitor can be placed on the map. This allows you to easily monitor even a large-scale system from the viewpoints you require.

- Guide information

  You can view guide information relevant to the monitoring nodes and generated JP1 events. Action flows and troubleshooting procedures can be registered as advice for handling problems that might arise during system monitoring, lessening the system administrator's workload at the initial response stage.

  Guide information can be preset by the user. As conditions for determining what information to display, you can specify information about a particular monitoring node or about a JP1 event that triggers a change in the status of a monitoring node.

You can also navigate from the Central Scope's Monitoring Tree window to the Event Console window in the Central Console.

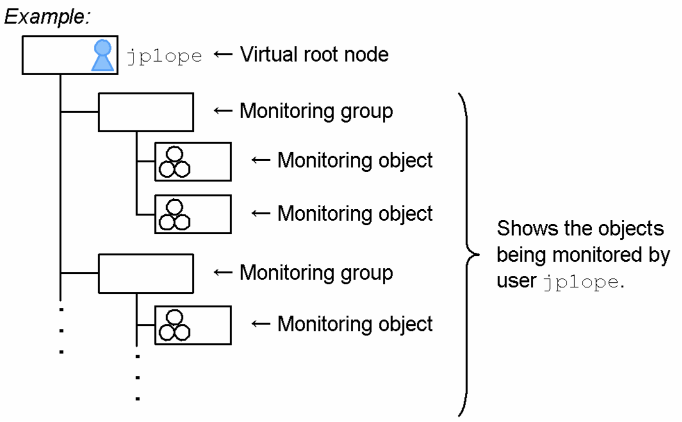
4.2 Monitoring tree

The following describes a monitoring tree.

4.2.1 Monitoring tree structure

A monitoring tree consists of monitoring objects, monitoring groups, and a virtual root node.

Table 4–1: Elements of a monitoring tree

Item	Description
Monitoring object	An object that you monitor using the Central Scope. A monitoring condition can be set for a monitoring object to change its icon to error status or other status under certain conditions. The icon status changes when a JP1 event related to the object is received by JP1/IM - Manager and is found to match the set monitoring condition.
Monitoring group	A group of monitoring objects. A monitoring group can contain monitoring objects and/or other monitoring groups. When the icon status of a lower-level object or group changes on receipt of a JP1 event, the icon status of the higher-level monitoring group containing that object or group also changes.
Virtual root node	Appears only when the monitoring range settings are enabled for the monitoring tree. For details, see *4.4.3 Setting the monitoring range of a monitoring tree*. For example, if the JP1 user `jp1ope` logs in to JP1/IM - Manager (Central Scope) while the monitoring range settings are enabled, the virtual root node will appear at the top of the monitoring tree as shown in the figure below. *Example:*  jp1ope ← Virtual root node ← Monitoring group ← Monitoring object ← Monitoring object ← Monitoring group ← Monitoring object Shows the objects being monitored by user jp1ope. As shown in the figure, the virtual root node is identified by an icon in the shape of a person. The name of the virtual root node is that of the JP1 user currently logged in to JP1/IM - Manager (Central Scope). Unlike a monitoring object or monitoring group, the information in a virtual root node cannot be edited (in the Properties window). Neither can you change the node status or perform any other direct operations on the virtual root node. (Its status changes accordingly when the status of a monitoring node below it changes, but you cannot change the virtual root node status directly. To change its status, you must change the status of a lower-level monitoring node.)

Monitoring objects and monitoring groups are referred to generically as *monitoring nodes*.

4.2.2 Statuses of monitoring nodes

The status of monitoring objects and groups is managed on the basis of the JP1 events generated in the particular object.

A monitoring node has two different types of statuses:

- Status

  The events occurring on a monitoring node are managed according to the status of the node.

  Node statuses, in order of priority, are `Emergency`, `Alert`, `Critical`, `Error`, `Warning`, `Normal`, `Debug`, and `Initial`.

  For example, if an error occurs on a node, resulting in a JP1 event of `Emergency` level, the Central Scope manages the event according to the current status of the node.

- Monitoring status

  Information that determines whether to monitor the node status.

  There are two monitoring statuses: **Monitor** and **Do not monitor**.

  When **Monitor** is set for a node, the status of the node changes when a JP1 event matching the monitoring conditions is received. Statuses are color-coded in the Monitoring Tree window and Visual Monitoring window.

  When **Do not monitor** is set for a node, the status of the node does not change even when a JP1 event is received from the node. The node is grayed out in the Monitoring Tree window and Visual Monitoring window.

A node has `Initial` status when monitoring begins. This means that the Central Scope does not yet have any information about the status of the node.

If **Monitor** is set for an object and a JP1 event of `Emergency` level occurs because of a failure, for example, the status of the object changes on receipt of the JP1 event by JP1/IM - Manager. Whether a status change occurs in an object is determined by a *status change condition*.

When the status of an object changes, its new status is passed in succession to each of the higher-level groups in the monitoring tree. If the new status has higher priority than the status of the receiving group, or if the status of the lower-level node satisfies the status change condition of the receiving group, the status of that group changes.

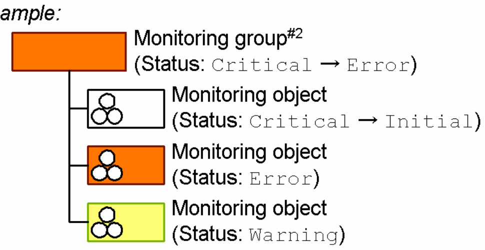
If **Do not monitor** is set for an object, the status of the monitoring node does not change, even when a JP1 event is received because of an error on the node. If the object's monitoring status is changed to **Monitor**, the status of the node will change according to JP1 events subsequently received from the object. **Do not monitor** is the default status for an automatically generated monitoring tree.

(1) Behavior when changing the status of a monitoring node manually

You can change the status of a monitoring node manually. The statuses that can be set, and the status change behavior, differ according to whether the monitoring node consists of monitoring objects or monitoring groups.

Table 4–2: Specifiable statuses and status change behavior based on monitoring node type

Monitoring node type	Specifiable statuses and status change behavior
Monitoring object	You can change the node status to `Emergency`, `Alert`, `Critical`, `Error`, `Warning`, `Normal`, `Debug`, or `Initial`#1. When the node status changes, the new information is relayed upward through the tree, and the status of each higher-level monitoring group changes to the status that has highest priority among the statuses of the lower-level monitoring nodes.

Monitoring node type	Specifiable statuses and status change behavior
	Example:  Monitoring group#2 (Status: Critical → Error) Monitoring object (Status: Critical → Initial) Monitoring object (Status: Error) Monitoring object (Status: Warning)
Monitoring group	You can change the node status to `Initial`[#1] only. When the node status changes, the new information is relayed upward through the tree, and the status of each higher-level monitoring group changes to the status that has highest priority among the statuses of the lower-level monitoring nodes (same behavior as for a monitoring object). The status of all lower-level monitoring nodes changes to `Initial`.

#1: Manually changing the status of a monitoring node deletes the status change events logged for that node (see *4.7.2 Searching for status change events*).

#2: The status of a monitoring group changes to the highest status among the lower-level nodes. However, when a status change condition is set for a group, that condition takes precedence.

You can change a node status manually using the GUI or the `jcschstat` command (for the command syntax, see *jcschstat* in *Chapter 1. Commands* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

When you change a node's monitoring status to **Do not monitor**, the monitoring status of all lower-level nodes is reset to **Do not monitor**. The node itself and all lower-level nodes revert to `Initial` status. Similarly, when you change a node's monitoring status to **Monitor**, all lower-level nodes also change to **Monitor**.

When a higher-level node has been reset to **Do not monitor**, you cannot change the lower-level nodes back to **Monitor** status. To change a lower-level node back to **Monitor** status, you must change the higher-level node from **Do not monitor** to **Monitor** again.

4.2.3 Status change conditions

A status change condition changes the status of a monitoring node. It can be set for both monitoring objects and monitoring groups, but there are differences in each case.

Status change condition for a monitoring object

> Determines what types of received JP1 events will trigger a status change in the monitoring object (for example, change the node status to `Warning` when a specific JP1 event of `Warning` level is received).

Status change condition for a monitoring group

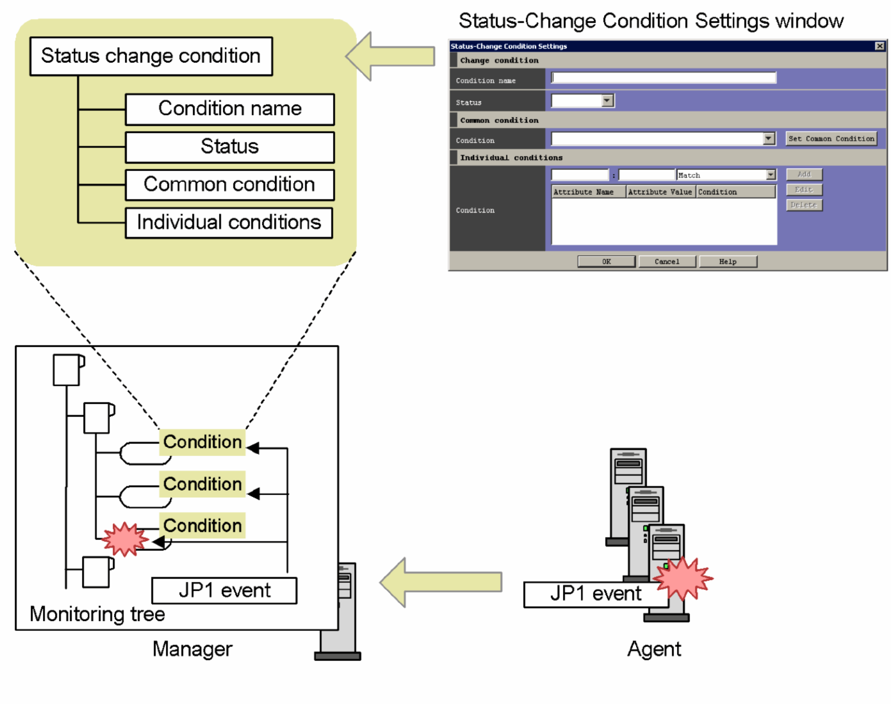
> Determines what lower-level node statuses will trigger a status change in the monitoring group (for example, change the node status to `Error` when two of three lower-level monitoring nodes have `Error` status).
>
> When no condition has been set, the monitoring group is set to the status that has highest priority among the lower-level monitoring nodes.

The status change conditions for monitoring objects and groups are further described below.

(1) Status change conditions for monitoring objects

The following figure shows status change conditions for monitoring objects.

Figure 4–2: Status change conditions for monitoring objects



Each monitoring object in a monitoring tree has its own status change condition. When JP1/IM - Manager receives a JP1 event, it checks the status change condition of each object. If the condition is satisfied, and the status of the received event has higher priority than the object's current status, JP1/IM - Manager changes the object's status accordingly. In this way, generated JP1 events are associated with the relevant objects in the monitoring tree, providing a visual representation of the system status.

A status change condition for a monitoring object consists of a condition name, status, common condition, and individual conditions, as described below. Multiple common conditions and individual conditions can be specified for a JP1 event.

- Condition name

  The name of the status change condition.

- Status

  The status of the monitoring object when the status change condition is satisfied.

  One of the following can be specified: `Emergency`, `Alert`, `Critical`, `Error`, `Warning`, `Normal`, `Debug`, or `Initial`.

- Common condition

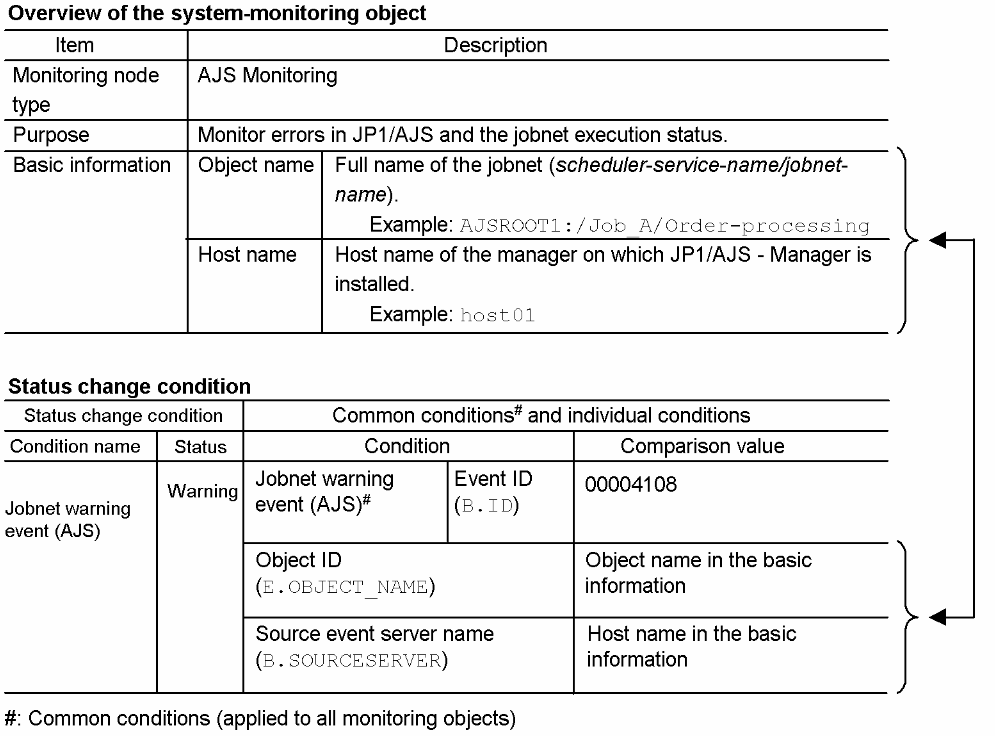
  A status change condition that applies to a number of monitoring objects. For example, for an object that monitors a jobnet, JP1 event ID 4108 (generated when a jobnet ends with a warning) is a common condition and applies to all such monitoring objects.

- Individual condition

  A condition whose value is specific to the object concerned. For example, a condition whose value changes for each monitoring object, such as the job name for a jobnet monitoring object, is an individual condition.

The following figure describes how a status change condition is set in practice, taking as an example a system-monitoring object.

Figure 4–3: Example of a system-monitoring object (extract from "AJS Monitoring")



Overview of the system-monitoring object

Item	Description	
Monitoring node type	AJS Monitoring	
Purpose	Monitor errors in JP1/AJS and the jobnet execution status.	
Basic information	Object name	Full name of the jobnet (*scheduler-service-name/jobnet-name*). Example: `AJSROOT1:/Job_A/Order-processing`
	Host name	Host name of the manager on which JP1/AJS - Manager is installed. Example: `host01`

Status change condition

Status change condition		Common conditions# and individual conditions		
Condition name	Status	Condition		Comparison value
Jobnet warning event (AJS)	Warning	Jobnet warning event (AJS)#	Event ID (`B.ID`)	00004108
		Object ID (`E.OBJECT_NAME`)		Object name in the basic information
		Source event server name (`B.SOURCESERVER`)		Host name in the basic information

#: Common conditions (applied to all monitoring objects)

This figure is an extract from the description of the system-monitoring object called *AJS Monitoring* in *Chapter 4. Lists of System-Monitoring Objects (for Central Scope)* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

The example in the figure defines a status change condition with the title *Jobnet warning event (AJS)*. As a common condition for all AJS Monitoring objects, the object status is set to `Warning` when event ID 4108 (indicating that the jobnet ended with a warning) is generated. As an individual condition set for each monitoring object, a condition related to the basic information held by the monitoring object (for identifying the object) identifies which of the objects in the monitoring tree changes its status.

In this way, a common condition related to the type of monitoring object (product name, for example) can be combined with an individual condition for identifying the specific monitoring object whose status will change.

Making status change conditions for monitoring objects resident in memory

When JP1/IM - Manager receives a JP1 event, it checks whether the status change condition of each monitoring object is satisfied. If a large number of JP1 events are received at once, the number of disk accesses increases accordingly and it could take longer to apply the new status to the monitoring objects. By making the status change conditions of the monitoring objects resident in memory, you can reduce the disk accesses during the Central Scope processing on receipt of an event.

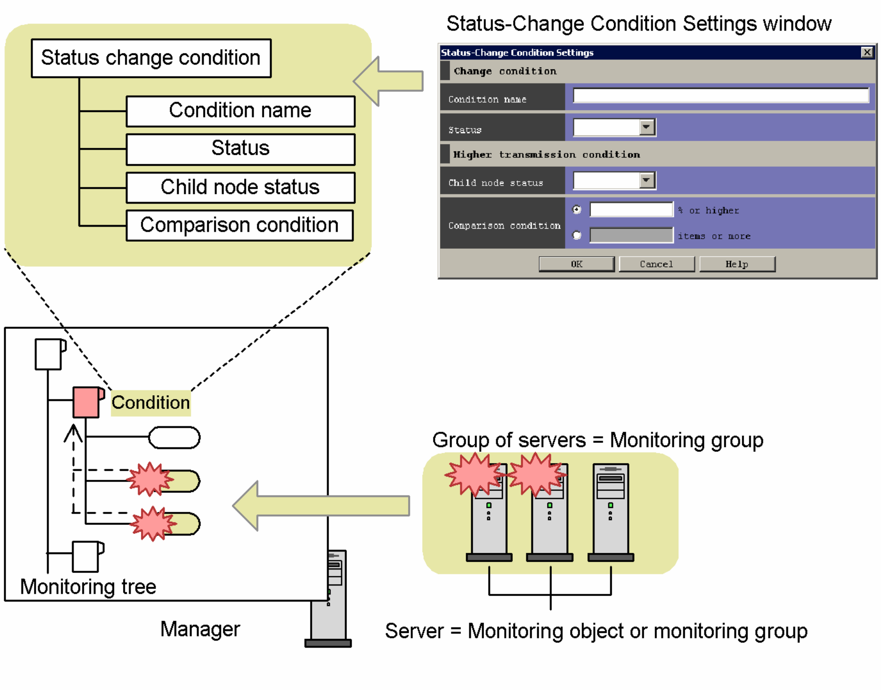
When you use this functionality, the status change conditions for all monitoring objects are kept in memory. Sufficient memory is needed for this purpose. We recommend that you estimate the memory requirements and set up this functionality if sufficient memory can be allocated.

For the equations used when estimating memory requirements, see the *Release Notes* for JP1/IM - Manager. For details about how to set up this functionality, see *5.7.5 Setting the memory-resident status change condition function* in the *JP1/Integrated Management - Manager Configuration Guide*.

(2) Status change conditions for monitoring groups

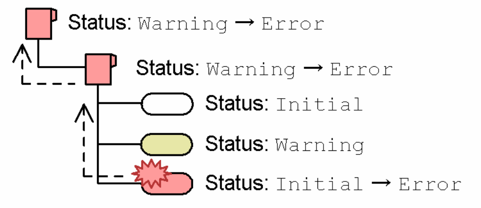
A *monitoring group* is a set of monitoring nodes. Therefore, the status of the monitoring group changes according to the status of its constituent nodes. The following figure shows status change conditions for monitoring groups.

Figure 4–4: Status change conditions for monitoring groups



When JP1/IM - Manager receives a specific JP1 event and changes the status of a monitoring object, the new status is passed to the higher-level monitoring groups. The default behavior is as follows.

Figure 4–5: Status change behavior of a monitoring group (default setting)



As shown in the figure, the monitoring group status changes to the status that has highest priority among the lower-level monitoring nodes. Thus, when the topmost monitoring node has `Error` status, it means that none of the nodes under it has a status of higher priority than `Error`.

While the default settings are appropriate in most cases, more detailed monitoring can be performed by defining a status change condition for the monitoring group in special circumstances (such as a load-balancing system).

A status change condition for a monitoring group consists of a condition name, status, child node status, and comparison condition, as described below.

- Condition name
  The name of the status change condition.
- Status
  The status of the monitoring group when the status change condition is satisfied.

In order of priority, the specifiable statuses are Emergency, Alert, Critical, Error, Warning, Normal, and Debug. Initial cannot be specified.

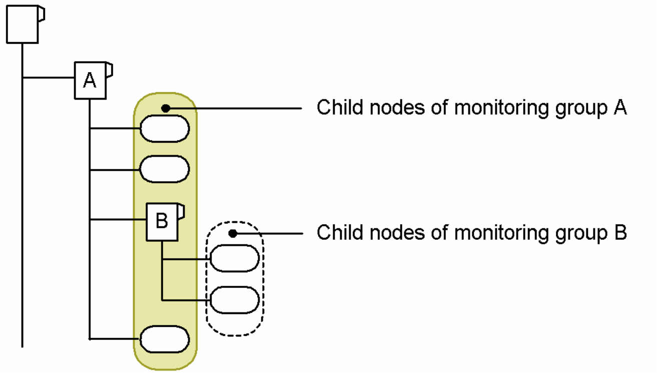
- Child node status

  The status of a lower-level monitoring node. Specify the status that will cause a change in the status of the monitoring group to which the node belongs. In order of priority, the specifiable statuses are Emergency, Alert, Critical, Error, Warning, Normal, and Debug. Initial cannot be specified.

  The status you specify here includes those of higher priority. For example, Error includes all statuses from Error upward.

  The following figure shows the child node concept.

Figure 4–6: Range of child nodes in a monitoring group

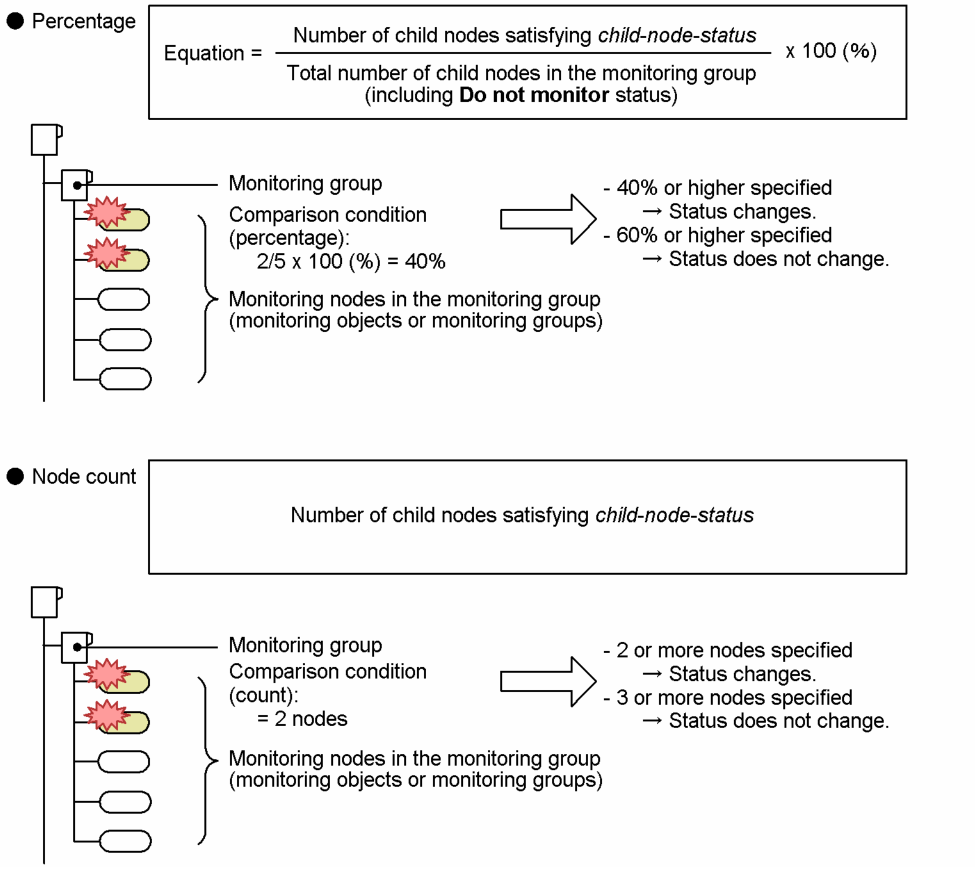

A
B
Child nodes of monitoring group A
Child nodes of monitoring group B

  As shown above, monitoring group B is included among the child nodes of monitoring group A, but its own child nodes are not included.

- Comparison condition

  A condition for comparing lower-level monitoring nodes within the group. You can specify a percentage (*x*% or higher) or a count (*x* nodes or higher), as follows.

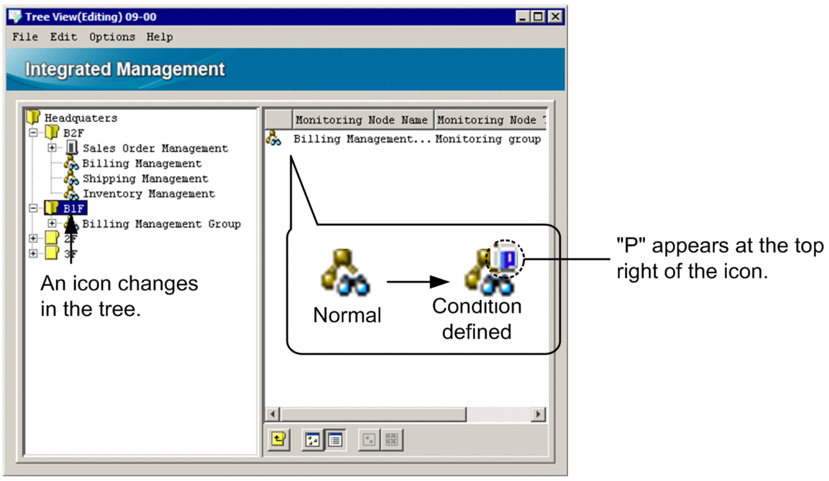
Figure 4–7: Comparison conditions (percentage-based and count-based)


● Percentage
Equation = Number of child nodes satisfying *child-node-status* / Total number of child nodes in the monitoring group (including **Do not monitor** status) x 100 (%)
Monitoring group
Comparison condition (percentage): 2/5 x 100 (%) = 40%
Monitoring nodes in the monitoring group (monitoring objects or monitoring groups)
- 40% or higher specified → Status changes.
- 60% or higher specified → Status does not change.
● Node count
Number of child nodes satisfying *child-node-status*
Monitoring group
Comparison condition (count): = 2 nodes
Monitoring nodes in the monitoring group (monitoring objects or monitoring groups)
- 2 or more nodes specified → Status changes.
- 3 or more nodes specified → Status does not change.

By setting a condition name, status, child node status, and comparison condition in this way, you can customize the conditions that cause the status of a monitoring group to change.

When you define a status change condition, the icon of the monitoring group changes as shown below. From the icon display you can tell whether a status change condition has been set for a particular group.

Figure 4–8: Change in icon display (example)



"P" is not added to Visual Icon registered by the user. Identify whether a status change condition has been defined from the icons in the tree.

4.2.4 Event generation condition

A monitoring node can issue a JP1 event when its status changes.

As an event generation condition, you can specify the type of status change that will cause the node to issue a JP1 event. This JP1 event cannot be issued when the node status changes to `Initial`.

The issued JP1 event has event ID 00003FB0.

Details about this JP1 event are as follows. This information is taken from *Chapter 3. JP1 Events* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

Table 4–3: Details about event ID 00003FB0 (from the above manual)

Attribute type		Item	Attribute name	Contents
Basic		Source event server name	`SOURCESERVER`	The name of the event server that issued the JP1 event
		Message	`MESSAGE`	`KAVB7900-I` message
Extended	Common information	Event level	`SEVERITY`	`Information`
		Product name	`PRODUCT_NAME`	`/HITACHI/JP1/IM/SCOPE`
		Object type	`OBJECT_TYPE`	`SERVICE`
		Object name	`OBJECT_NAME`	`IM_CS`
		Occurrence	`OCCURRENCE`	`STATUS_CHANGE`
	Program-specific information	Monitoring node ID	`MON_NODE_ID`	The ID of the monitoring node
		Monitoring node name	`MON_NODE_NAME`	The name of the monitoring node
		Monitoring node status#1	`MON_NODE_STATUS`	The StatusID of the monitoring node
		Information about the JP1 event that triggered the status change#2	*attribute-name*	The attribute value (basic attribute value prefixed with `JCS_B_` or extended attribute value prefixed with `JCS_E_`)

#1: The monitoring node status (`E.MON_NODE_STATUS`) is stored as one of the following numeric values, which is called the node's *StatusID*.

- Value of StatusID (monitoring node status):
  `Emergency`: 800, `Alert`: 700, `Critical`: 600, `Error`: 500,
  `Warning`: 400, `Normal`: 300, `Debug`: 200, `Initial`: 100

For example, the JP1 event issued when the status of the monitoring node changes to `Emergency` has a monitoring node status (`E.MON_NODE_STATUS`) of 800.

#2: You cannot check this information from JP1/IM - View. Every item of information is stored as an attribute name combined with the attribute value. Therefore, when JP1 event 00003FB0 exceeds the maximum length of a JP1 event (10,000 bytes), only the portion within that limit is stored as information about the JP1 event that triggered the status change. Similarly, when the number of extended attributes exceeds 100, only the JP1 event information up to the 100th attribute is stored. Attributes are stored only if the attribute name is within 26 characters; if the attribute name exceeds 26 characters, the attribute is not saved.

Setting an automated action for a monitoring node

To execute an automated action when the status of a monitoring node changes:

- In the **Event-Issue Conditions** page of the Properties dialog box for the selected monitoring node, select the node status that triggers the JP1 event.
- Add an automated action condition for JP1 event 00003FB0 to the automated action definitions.

Information about the JP1 event resulting in a node status change is included in JP1 event 00003FB0, as shown in *Information about the JP1 event that triggered the status change* in the above table. For example, the original event message (`B.MESSAGE`) can be used as the attribute name `E.JCS_B_MESSAGE` with the automated action.

4.3 Automatically generating a monitoring tree

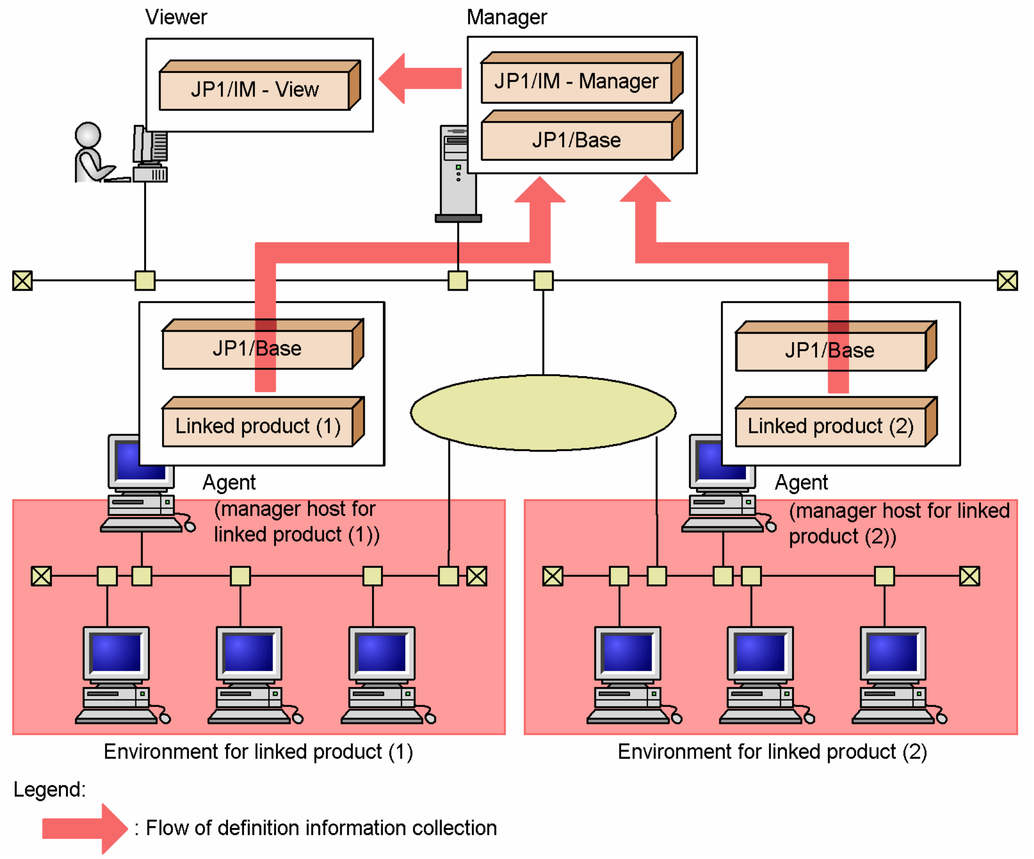
Using the auto-generation function, you can automatically collect definition information from the active hosts in the system and create a monitoring tree. If the system is reconfigured, you can collect difference information and update the monitoring tree.

The auto-generation function substantially simplifies the work involved in configuring a monitoring system. A monitoring tree can help you monitor even a large-scale system efficiently, but it still requires a vast amount of definition information. The tasks at the system configuration stage, and the updates required when the system is modified, mean a huge commitment of time and effort. The function for automatically generating a monitoring tree offers support for this undertaking.

4.3.1 Automatically generating a monitoring tree

When you use the auto-generation function, JP1/IM - Manager collects definition information from the agents and automatically generates a monitoring tree as shown below.

Figure 4–9: Overview of auto-generation of a monitoring tree


Viewer
JP1/IM - View
Manager
JP1/IM - Manager
JP1/Base
JP1/Base
Linked product (1)
Agent
(manager host for linked product (1))
JP1/Base
Linked product (2)
Agent
(manager host for linked product (2))
Environment for linked product (1)
Environment for linked product (2)
Legend:
: Flow of definition information collection

> **Important**
>
> To generate a monitoring tree automatically, the products to be monitored must support the auto-generation function.

4.3.2 Conditions for automatically generating a monitoring tree

You can automatically generate a monitoring tree for JP1 products (JP1/AJS, JP1/Cm2/SSO version 8 or earlier, JP1/PFM, JP1/IM, and JP1/ServerConductor), Cosminexus, and HiRDB. If you wish to monitor any other products in your system, you must set the definition information manually.

The following conditions apply when automatically generating a monitoring tree:

- JP1/Base (version 7 or later) is required on each agent.
  Definition information is collected using JP1/Base functionality.
- The products to be monitored must support the JP1/Base functionality for collecting definitions.
  You must execute the setup command for enabling this functionality in the relevant products on each agent.
- The service for each linked product must be active during auto-generation.
  Definition information cannot be collected from products whose service is inactive.

For the procedures to link these products with JP1/IM, see *5.8 Setting up for linked products* in the *JP1/Integrated Management - Manager Configuration Guide* and the documentation for the relevant linked product.

The following table describes the monitoring objects created by the auto-generation function.

Table 4–4: List of monitoring objects created at auto-generation

Product	Monitoring node type	Description
JP1/IM - Manager	IM Monitoring	Monitors the status of JP1/IM - Manager. Defined so that its status changes conditional on a JP1 event indicating an error in JP1/IM - Manager.
JP1/AJS - Manager	AJS Monitoring	Monitors the status of JP1/AJS - Manager and the jobnets executed under its control. Defined so that its status changes conditional on a JP1 event indicating an error in JP1/AJS - Manager or a change in the status of a jobnet.
	Jobnet Monitoring (AJS)	Monitors job execution status. Defined so that its status changes conditional on a JP1 event indicating a change in the status of the job.
JP1/Cm2/SSO#	SSO Monitoring	Monitoring object that monitors the status of JP1/Cm2/SSO. Defined so that its status changes conditional on a JP1 event indicating an error in JP1/Cm2/SSO.
	Category Monitoring (SSO)	Monitoring object that monitors the status of resource information collected by the SNMP agents managed by JP1/Cm2/SSO. The statuses are collected for all SNMP agents managed by JP1/Cm2/SSO. Defined so that its status changes conditional on a JP1 event indicating a status change in the resources.
JP1/PFM - Manager	Agent Monitoring (PFM)	Monitors the status of performance data monitored by an agent that is managed by JP1/PFM - Manager. The auto-generation function creates the same number of Agent Monitoring (PFM) objects as the JP1/PFM - Agents managed by JP1/PFM - Manager. Defined so that its status changes conditional on a JP1 event indicating a change in the status of the performance data.
Cosminexus	Logical Server Monitoring (Cosminexus)	Monitors the status of a Cosminexus logical server (J2EE server, Web server, naming service, CTM, and so on). Defined so that its status changes conditional on a JP1 event indicating that the Cosminexus logical server has started or stopped, or a JP1 event indicating an execution error.

Product	Monitoring node type	Description
	J2EE Application Monitoring (Cosminexus)	Monitors the status of a Cosminexus J2EE application. Defined so that its status changes conditional on a JP1 event indicating that the J2EE application has started or stopped, or a JP1 event indicating an execution error.
Cosminexus + JP1/Cm2/SSO[#]	J2EE Server Resource Monitoring (SSO)	General monitoring object that monitors the resource status of the Cosminexus J2EE server. Defined so that its status changes conditional on a JP1 event indicating a change in the resource status of the J2EE server.
	CTM Resource Monitoring (SSO)	General monitoring object that monitors the resource status of Cosminexus CTM. Defined so that its status changes conditional on a JP1 event indicating a change in the resource status of CTM.
	SFO Resource Monitoring (SSO)	General monitoring object that monitors the resource status of Cosminexus SFO. Defined so that its status changes conditional on a JP1 event indicating a change in the resource status of SFO.
	J2EE Application Resource Monitoring (Cosminexus)	General monitoring object that monitors the resource status of the Cosminexus J2EE application. Defined so that its status changes conditional on a JP1 event indicating a change in the resource status of the J2EE application.

#: JP1/Cm2/SSO version 8 or earlier is required.

Important

Before you begin operation, you should customize the automatically generated monitoring tree to suit the methods you will be using to monitor your system.

A monitoring tree created by the auto-generation function incorporates the collected information in its entirety. It represents the system configuration information as completely as possible, so that the system administrator can delete whatever is unnecessary for monitoring purposes.

For further details about the contents of the automatically generated nodes in a monitoring tree, see *Chapter 4. Lists of System-Monitoring Objects (for Central Scope)* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

4.3.3 Monitoring tree structures

The monitoring trees produced by the auto-generation function are based on a template which you select in the Auto-generation - Select Configuration window. A template is a set of model definitions for managing a system using the Central Scope.

JP1/IM provides the following two templates.

Table 4–5: Monitoring tree templates

Generation tree	Description
Work-oriented tree	Use this template to monitor the system from a work-oriented perspective. The generated monitoring tree is based on the jobnet organization in JP1/AJS or logical server configuration in Cosminexus. Typically, jobs are grouped together as jobnets to systematize job

Generation tree	Description
	execution, and logical servers are defined to systematize the applications used in a Web system. Hence, the generated tree reflects how work tasks are performed. If the linked JP1/AJS is version 8 or later, the function collects from JP1/AJS not only information about the jobnet organization, but also information about the JP1 resource groups set in each JP1/AJS unit.#
Server-oriented tree	Use this template to monitor the system from a server-oriented perspective. The generated monitoring tree is based on the system hierarchy in JP1/IM. In JP1/IM, the servers are typically arranged in a hierarchical structure. Hence, the generated tree reflects the manner in which servers are managed.

#: For details about using the acquired JP1 resource groups, see *4.4.3 Setting the monitoring range of a monitoring tree*.

The structure and monitoring objects of an automatically generated monitoring tree differ for each of the two templates. The following table describes the relationships between the type of template and the generated monitoring objects.

Table 4–6: Template type and generated monitoring objects

Monitoring object	Template		
	Work-oriented tree		Server-oriented tree
	JP1/AJS management group	Cosminexus management group	
AJS Monitoring	Y	--	Y
Jobnet Monitoring (AJS)	Y	--	Y
SSO Monitoring#1	--	--	Y
Category Monitoring (SSO)#1	Y	Y	Y
Application Monitoring (SSO)	Y	Y	Y
Agent Monitoring (PFM)	Y	Y	Y
Metric Monitoring (PAM)	--	--	--
Object Monitoring (PAM)	--	--	--
SD Monitoring	--	--	--
Distribution Job Monitoring (SD)	--	--	--
NNM Monitoring#2	--	--	--
Node Monitoring (NNM)#2	--	--	--
IM Monitoring	--	--	Y
Logical Server Monitoring (Cosminexus)	--	Y	Y
J2EE Application Monitoring (Cosminexus)	--	Y	Y
J2EE Server Resource Monitoring (SSO)#1	--	Y	--
CTM Resource Monitoring (SSO)#1	--	Y	--
SFO Resource Monitoring (SSO)#1	--	Y	--
J2EE Application Resource Monitoring (SSO)#1	--	Y	--
HiRDB Monitoring	--	--	--

Monitoring object	Template		
	Work-oriented tree		Server-oriented tree
	JP1/AJS management group	Cosminexus management group	
Physical Host Monitoring (System Manager)	--	--	--

Legend:

Y: Generated

--: Not generated

#1: JP1/Cm2/SSO must be version 8 or earlier.

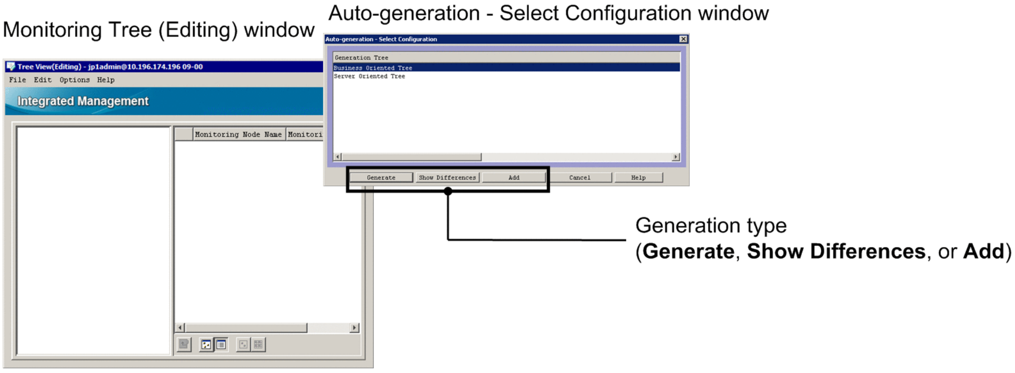
#2: HP NNM must be version 7.5 or earlier.

For details about the structure of automatically generated monitoring trees, see *Chapter 5. Monitoring Tree Models (for Central Scope)* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

4.3.4 Generation types

When generating a monitoring tree automatically, you can select one of three generation types: **Generate**, **Show Differences**, or **Add**.

Figure 4–10: Generation types


Monitoring Tree (Editing) window
Auto-generation - Select Configuration window
Tree View(Editing) - jp1admin@10.196.174.196 09-00
File Edit Options Help
Integrated Management
Monitoring Node Name
Monitori
Auto-generation - Select Configuration
Generation Tree
Business Oriented Tree
Server Oriented Tree
Generate
Show Differences
Add
Cancel
Help
Generation type
(**Generate**, **Show Differences**, or **Add**)

(1) Processing when you select "Generate" as the generation type

When you select **Generate** to create a monitoring tree, the information displayed in the Monitoring Tree (Editing) window is erased, and then the monitoring tree is redrawn according to the tree structure of the template you selected under **Generation Tree** in the Auto-generation - Select Configuration window. The existing monitoring tree is completely erased and the new, automatically generated monitoring tree is added. Use this processing to replace the existing system when a new system is installed.

(2) Processing when you select "Show Differences" as the generation type

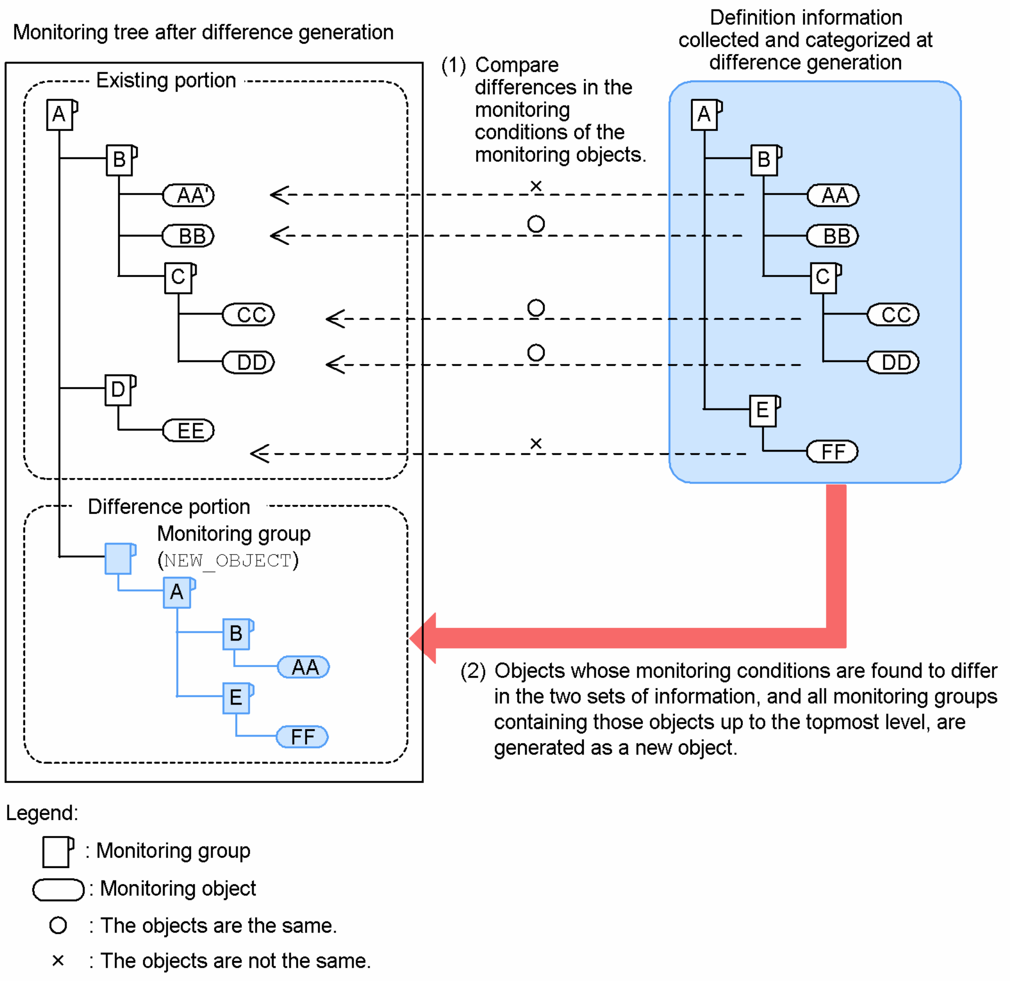
When you select **Show Differences** to create a monitoring tree, the monitoring conditions set for the monitoring objects stored in the JP1/IM - Manager monitoring objects database are compared with the monitoring conditions in the definition information (monitoring objects) that was collected and collated during the generation processing. Monitoring objects found to have different monitoring conditions than recorded in the database, and all monitoring groups containing those objects up to the topmost level, are created as difference information under a monitoring group called `NEW_OBJECT`.

This processing allows you to update a monitoring tree when a system is reconfigured, by collecting only the changed parts of the definition information.

This new monitoring node generated as difference information can be placed in an existing monitoring tree as required.

The following figure shows the generation of a monitoring tree that shows differences.

Figure 4–11: Generation of a 'differences' monitoring tree


Monitoring tree after difference generation
Existing portion
A
B
AA'
BB
C
CC
DD
D
EE
Difference portion
Monitoring group
(NEW_OBJECT)
A
B
AA
E
FF
(1) Compare differences in the monitoring conditions of the monitoring objects.
×
○
○
○
×
Definition information collected and categorized at difference generation
A
B
AA
BB
C
CC
DD
E
FF
(2) Objects whose monitoring conditions are found to differ in the two sets of information, and all monitoring groups containing those objects up to the topmost level, are generated as a new object.
Legend:
: Monitoring group
: Monitoring object
○ : The objects are the same.
× : The objects are not the same.

Monitoring objects in the *existing portion* of the figure:

AA' is created from the original monitoring object AA. BB, CC, and DD incorporate the auto-generated objects without change. EE is an object added by the user for monitoring purposes.

Definition information collected and collated at difference generation:

This area of the figure shows the definition information collected at difference generation from the products running in the current system, organized into tree form. This information is held internally by JP1/IM - Manager. The generated tree structure depends on the selected template.

Difference portion of the figure:

This node contains the monitoring objects AA and FF, which JP1/IM - Manager determined to be absent from the existing portion as a result of comparing the monitoring conditions of the objects in that portion with the monitoring conditions of the objects in the definition information collected and collated at difference generation. A, B, and E are also generated in this node because they are the higher-level monitoring groups containing AA or FF.

(3) Processing when you select "Add" as the generation type

When you select **Add** to create a monitoring tree, an additional monitoring tree is added to those in JP1/IM - Manager's monitoring objects database. The structure of the tree follows the template you selected under **Generation Tree** in the Auto-generation - Select Configuration window. The monitoring tree is added at the end of the existing monitoring trees. Use this processing to add monitoring trees when, for example, you add business systems.

4.4 Editing a monitoring tree

You can freely customize a monitoring tree to suit your purpose. Before you start monitoring operations, edit the monitoring tree that you easily created using the auto-generation function, according to the type of monitoring you want to perform.

For details about the actual editing procedure, see *Chapter 5. Setting Up Central Scope* in the *JP1/Integrated Management - Manager Configuration Guide*.

4.4.1 Editing a monitoring tree

Use the Monitoring Tree (Editing) window to edit a monitoring tree. You can add, delete, and move nodes in this window, according to how the tree is to be used.

To create or edit a monitoring node, you must set the following attributes in the node. All these attributes have been discussed earlier in this chapter.

Table 4–7: Monitoring node attributes defined in the Monitoring Tree (Editing) window

Attribute	Description
Monitoring node name	The name of the monitoring node.
Monitoring node type	The monitoring group or monitoring object. There are several types of monitoring objects, including system-monitoring objects such as the AJS Monitoring and SSO Monitoring, and general monitoring objects such as a user monitoring object.
Icon	An icon that represents a monitoring node.
Visual Icon	An icon that represents a monitoring node. Visual Icon are displayed only in map views and in the Visual Monitoring window.
Monitoring status	The monitoring status set for a node. The two statuses are **Monitor** and **Do not monitor**.
JP1 resource group	Information set for controlling the monitoring range permitted to individual JP1 users, and for exercising precise control over access to the nodes in a monitoring tree. For details about using resource groups, see *4.4.3 Setting the monitoring range of a monitoring tree*.
Basic information	Basic information for identifying a monitoring node. In the case of a monitoring group, this attribute is a name identifying the group. For example, you can assign a group name to a group of tasks or servers, such as *Daily accounting routines* or *Database server group*, according to the monitoring objectives. In the case of a monitoring object, this attribute is information for identifying the object. For example, you can define a combination of information for identifying the object within the system, such as the jobnet name and a host name. For a system-monitoring object, the same attribute as the basic information of the object to be monitored is defined as an individual condition in the status change conditions.
Status change condition	• Status change condition for a monitoring object A condition that determines which received JP1 events will change the status of the monitoring object. This attribute defines a JP1 event that triggers a status change, and the resulting status. • Status change condition for a monitoring group A condition that determines what lower-level node statuses will change the status of the monitoring group. The attribute defines the statuses of the lower-level nodes triggering a status change, the resulting status of the monitoring group, and a comparison condition.

Attribute	Description
Event generation condition	A condition that specifies the status of a monitoring node that will cause a JP1 event to be issued. The issued JP1 event has event ID 00003FB0.

You can create a monitoring group simply by specifying its name (unless you also need to define a status change condition for the group). However, when you create a monitoring object, you must also carefully consider and define what exactly you need to monitor and how this is to be done.

JP1/IM provides a number of *system-monitoring objects* to facilitate object definition.

The following types of monitoring objects are provided:

- System-monitoring object

  A monitoring object provided by the JP1/IM system. Each product in the JP1 series has its own monitoring object. The basic settings needed for monitoring are pre-defined, so that you can easily set up the monitoring environment.

  System-monitoring objects include a variety of types, such as an *AJS Monitoring*, *SSO Monitoring*, and so on. For details about the program products that are monitored by these objects, and how to set them up, see *Chapter 4. Lists of System-Monitoring Objects (for Central Scope)* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

  A system-monitoring object becomes a general monitoring object when edited as follows:

  - By changing the basic information on the **Basic Information** page of the Properties window
  - By adding, changing, or deleting a status change condition on the **Status-Change Condition** page of the Properties window
  - By changing a common condition in the Status-Change Condition Settings window
  - By adding, changing, or deleting an individual condition in the Status-Change Condition Settings window

  When you alter a system- monitoring object in any of these ways, a confirmation dialog box appears with the following message: `If this operation is continued, the monitoring node type will become User Monitoring Object. Do you want to continue?`

- General monitoring object

  An object for general monitoring purposes, created and customized by the user. This type of object is called a *User Monitoring Object*.

  A general monitoring object can be customized very flexibly, allowing precise settings to match the type of monitoring required. On the other hand, the system administrator needs to be well versed in the settings that can be performed. This type of object also takes time to create.

For most purposes, we recommend that you use system-monitoring objects to create your monitoring nodes, and customize the parts that need to be changed.

4.4.2 Map display settings

In the detailed view area of the Monitoring Tree window, you can view information in map format just as in the Visual Monitoring window. This allows the system administrator a more intuitive means of monitoring the system.

To display map views in the detailed view area, you must set the background image, arrange the monitoring nodes, and complete other settings. Otherwise, you will see icons without any background when you switch to the map view. Use the Monitoring Tree (Editing) window to enter the required settings.

Differences from the Visual Monitoring window

Unlike the Visual Monitoring window, you cannot use the map view in the detailed view area for the purpose of localized monitoring of a specific node only, such as monitoring a particular regional office or an important job.

For example, if there are three nodes displayed in the detailed view area of the Monitoring Tree window, all three will be displayed when you switch to a detailed view or map view. (You cannot hide one of them, for example.)

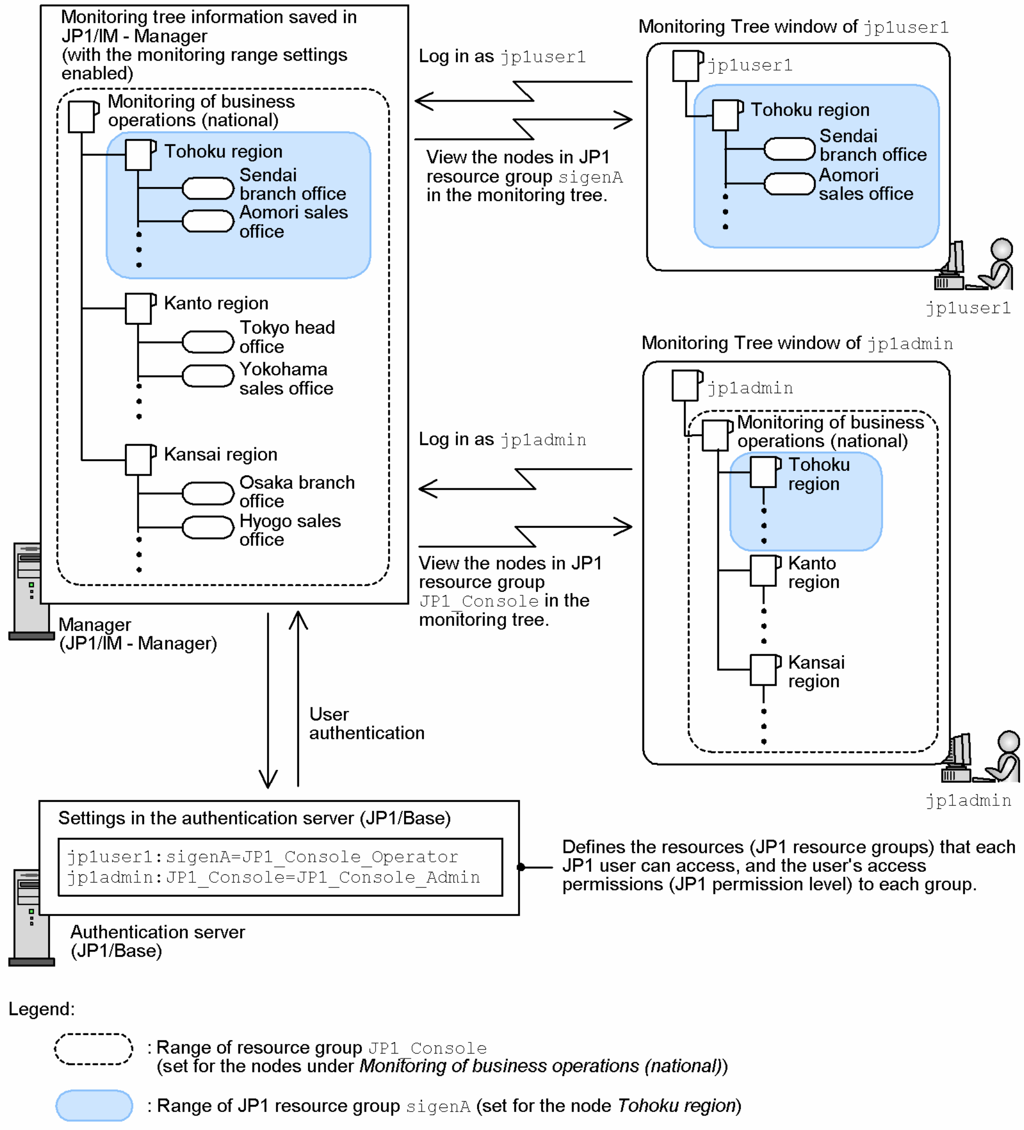
4.4.3 Setting the monitoring range of a monitoring tree

You can change the monitoring range of a monitoring tree for each JP1 user, by performing the following two settings:

- Enable the monitoring range settings, and then set JP1 resource groups for specific nodes (set in JP1/IM - View and save to JP1/IM - Manager).
- Allocate one or more JP1 resource groups to each JP1 user (set on the JP1/Base authentication server).

For example, by completing the above settings, you can permit a particular user (`jp1user1`) to monitor part of the tree, and another user (`jp1admin`) to monitor the entire tree, as shown in the figure below.

Figure 4–12: Changing the monitoring range using JP1 resource groups (access control to a monitoring tree)

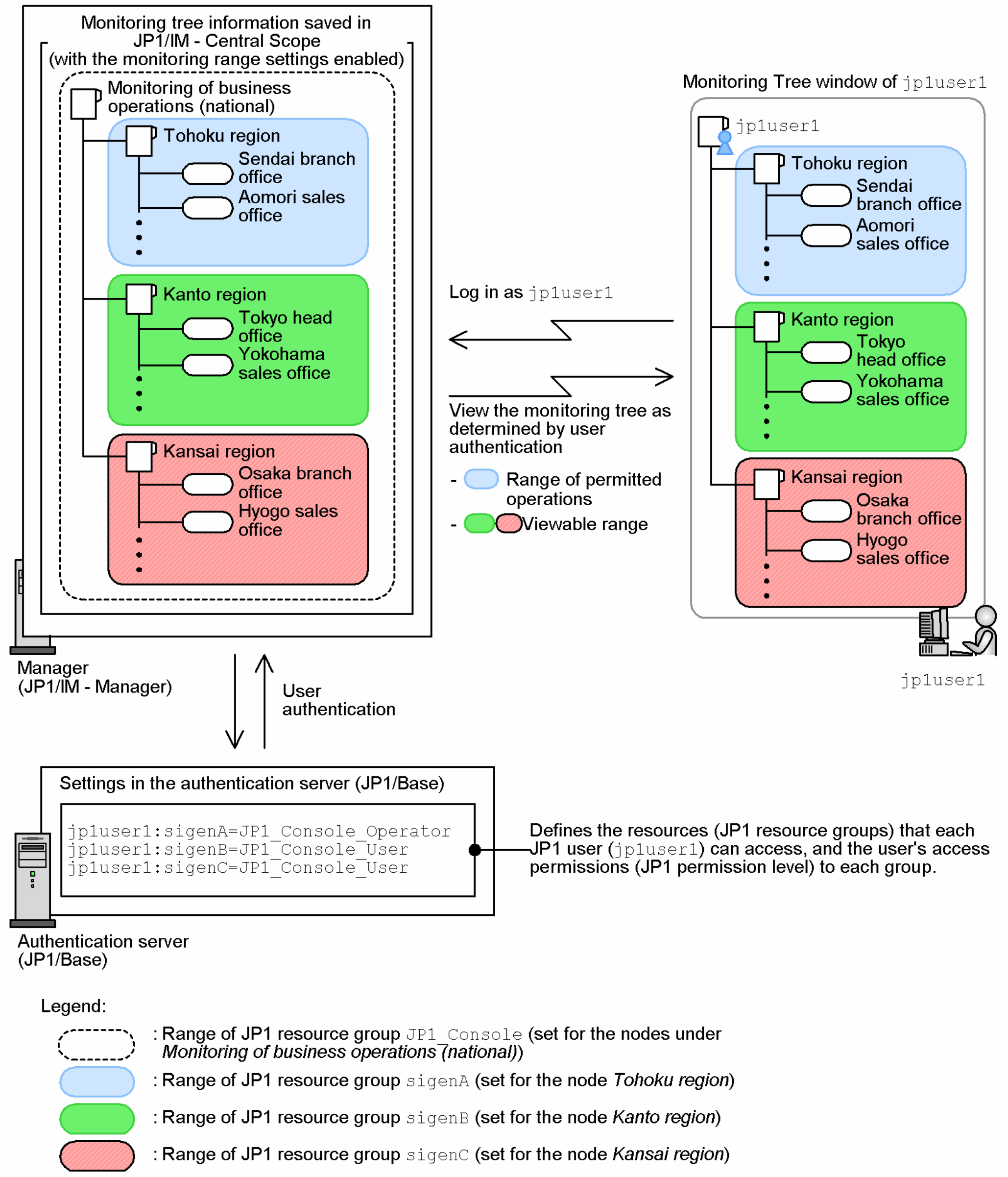

Monitoring tree information saved in JP1/IM - Manager
(with the monitoring range settings enabled)
Monitoring of business operations (national)
Tohoku region
Sendai branch office
Aomori sales office
Kanto region
Tokyo head office
Yokohama sales office
Kansai region
Osaka branch office
Hyogo sales office
Manager
(JP1/IM - Manager)
Log in as jp1user1
View the nodes in JP1 resource group sigenA in the monitoring tree.
Monitoring Tree window of jp1user1
jp1user1
Tohoku region
Sendai branch office
Aomori sales office
jp1user1
Log in as jp1admin
View the nodes in JP1 resource group JP1_Console in the monitoring tree.
Monitoring Tree window of jp1admin
jp1admin
Monitoring of business operations (national)
Tohoku region
Kanto region
Kansai region
jp1admin
User authentication
Settings in the authentication server (JP1/Base)
Authentication server
(JP1/Base)
Defines the resources (JP1 resource groups) that each JP1 user can access, and the user's access permissions (JP1 permission level) to each group.
Legend:
: Range of resource group JP1_Console
(set for the nodes under Monitoring of business operations (national))
: Range of JP1 resource group sigenA (set for the node Tohoku region)

```
jp1user1:sigenA=JP1_Console_Operator
jp1admin:JP1_Console=JP1_Console_Admin
```

When the monitoring range settings are enabled, the topmost node of the tree in the Monitoring Tree window is always the virtual root node. When the monitoring range settings are disabled, all tree information is displayed, regardless of the JP1 resource group settings (the virtual root node is not shown).

By allocating multiple JP1 resource groups to a particular JP1 user, and assigning a different JP1 permission level for each group, you can allow that JP1 user to operate on one part of a monitoring tree, but only view another part, as shown in the figure below.

Figure 4–13: Example of controlling monitoring tree operation using a combination of JP1 resource groups and JP1 permission levels


Monitoring tree information saved in JP1/IM - Central Scope
(with the monitoring range settings enabled)
Monitoring of business operations (national)
Tohoku region
Sendai branch office
Aomori sales office
Kanto region
Tokyo head office
Yokohama sales office
Kansai region
Osaka branch office
Hyogo sales office
Manager (JP1/IM - Manager)
User authentication
Log in as jp1user1
View the monitoring tree as determined by user authentication
- Range of permitted operations
- Viewable range
Monitoring Tree window of jp1user1
jp1user1
Tohoku region
Sendai branch office
Aomori sales office
Kanto region
Tokyo head office
Yokohama sales office
Kansai region
Osaka branch office
Hyogo sales office
jp1user1
Settings in the authentication server (JP1/Base)
Authentication server (JP1/Base)
Defines the resources (JP1 resource groups) that each JP1 user (jp1user1) can access, and the user's access permissions (JP1 permission level) to each group.

```
jp1user1:sigenA=JP1_Console_Operator
jp1user1:sigenB=JP1_Console_User
jp1user1:sigenC=JP1_Console_User
```

Legend:

- : Range of JP1 resource group `JP1_Console` (set for the nodes under *Monitoring of business operations (national)*)
- 🟦 : Range of JP1 resource group `sigenA` (set for the node *Tohoku region*)
- 🟩 : Range of JP1 resource group `sigenB` (set for the node *Kanto region*)
- 🟥 : Range of JP1 resource group `sigenC` (set for the node *Kansai region*)

(1) Enabling or disabling monitoring range settings, and setting a JP1 resource group for a monitoring node

To enable or disable the monitoring range settings, in the Monitoring Tree (Editing) window, choose **Options** and then **Monitoring Range Settings**. When **Monitoring Range Settings** is checked, the settings are enabled; when there is no check mark, the settings are disabled.

The monitoring range settings in JP1/IM - View might be automatically enabled or disabled when a monitoring tree is auto-generated, depending on the generation type and the server (JP1/IM - Manager) settings. This occurs in the following two cases:

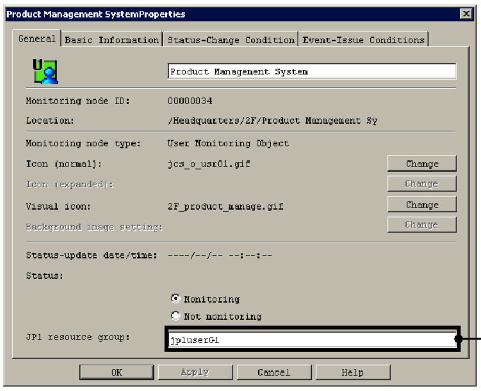
1. The monitoring range settings are disabled in JP1/IM - View but enabled in JP1/IM - Manager, and **Show Differences** or **Add** is set as the generation type.
2. The monitoring range settings are enabled in JP1/IM - View but disabled in JP1/IM - Manager, and **Show Differences** or **Add** is set as the generation type.

In the first case, the JP1/IM - View monitoring range settings are automatically enabled after auto-generation.

In the second case, the JP1/IM - View monitoring range settings are automatically disabled after auto-generation.

When the monitoring range settings are enabled, you can set a JP1 resource group for any monitoring node from the **General** page of the Properties window for that node. The **JP1 resource group** box appears only when the monitoring range settings are enabled.

Figure 4–14: Properties window when the monitoring range settings are enabled



Product Management SystemProperties

General | Basic Information | Status-Change Condition | Event-Issue Conditions

Product Management System

Monitoring node ID: 00000034

Location: /Headquarters/2F/Product Management Sy

Monitoring node type: User Monitoring Object

Icon (normal): jcs_o_usr01.gif [Change]

Icon (expanded): [Change]

Visual icon: 2F_product_manage.gif [Change]

Background image setting: [Change]

Status-update date/time: ----/--/-- --:--:--

Status:

● Monitoring

○ Not monitoring

JP1 resource group: jp1userG1

[OK] [Apply] [Cancel] [Help]

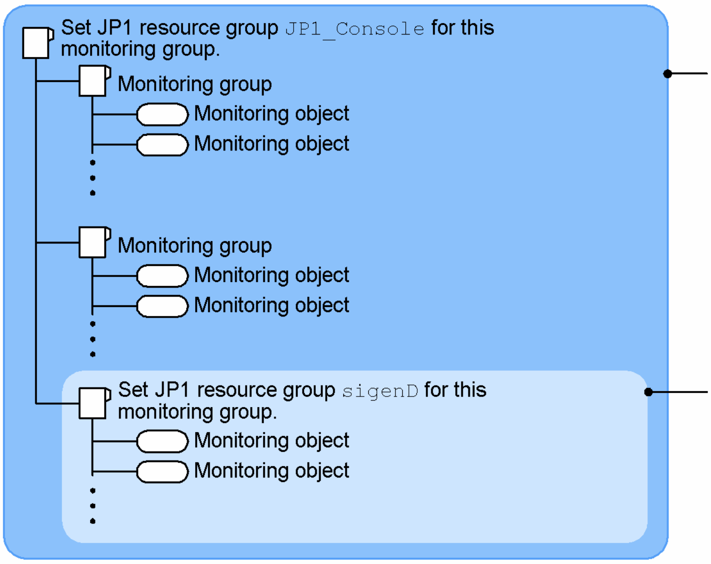
Displayed when the **Monitoring Range Settings** command is checked in the **Options** menu of the Monitoring Tree (Editing) window.

Once set, the JP1 resource group setting is saved as internal information even if you subsequently disable the monitoring range settings. (When you re-enable them, the resource group you set previously is again displayed.)

You can set a JP1 resource group only for the highest node within the range of control (that is, you do not need to repeat the setting for each child node). The JP1 resource group set for a node applies to all its child nodes.

For example, if you set `JP1_Console` as the JP1 resource group for the topmost monitoring group in the tree, all nodes under that group will belong to JP1 resource group `JP1_Console`. If you then set JP1 resource group `sigenD` for a monitoring group under the topmost monitoring group, the group itself and all its lower-level nodes will belong to both `JP1_Console` and `sigenD`.

Figure 4–15: Applicable range of JP1 resource groups



Applicable range of `JP1_Console`

Applicable range of `sigenD`

The JP1 users granted access to `JP1_Console` can view the range `JP1_Console` (all nodes in the monitoring tree); the JP1 users granted access to `sigenD` can view the range `sigenD`.

Initial JP1 resource group setting for a monitoring node

Regardless of whether the monitoring range settings are enabled, the JP1 resource group `JP1_Console` is automatically set for the topmost node. You can change this setting, but you cannot make it blank (a value must be entered).

When you auto-generate a monitoring tree under the following conditions, the JP1 resource group already set in the linked product is imported as the initial value for that monitoring node. This applies when:

- You generate a monitoring tree automatically by selecting the work-oriented tree template for JP1/AJS version 8.

The monitoring range settings in JP1/IM - View and JP1/IM - Manager are completed when you finish setting JP1 resource groups for the nodes and save the changes to JP1/IM - Manager.

(2) Allocating JP1 resource groups to JP1 users

When you set the monitoring range of a monitoring tree, you must also review the JP1/Base (authentication server) settings and add or edit the JP1 user settings as required.

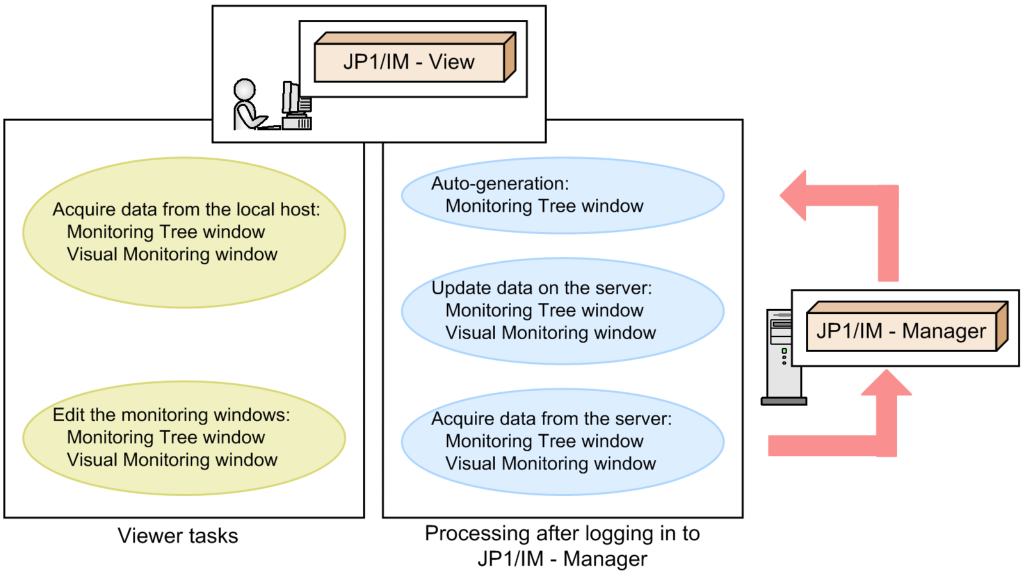
For information about how to manage JP1 users in JP1/Base, see *7.4.1 Managing JP1 users*.

For setting particulars, see the chapter about user management setup in the *JP1/Base User's Guide*.

4.4.4 Setting the Central Scope monitoring windows

Two main tasks are involved in setting the monitoring windows of the Central Scope (Monitoring Tree window and Visual Monitoring window): editing the windows on the viewer, and connecting to the manager to update or acquire the existing settings.

Figure 4–16: Setting the Central Scope monitoring windows



- Editing the monitoring windows (tasks on the viewer host)

  Edit information in the Monitoring Tree (Editing) window and Visual Monitoring (Editing) window on the viewer host. You do not need to connect to the manager (JP1/IM - Manager (Central Scope)) to perform these tasks.

  Required permissions:

Any user who can log in to the operating system is able to perform editing. No particular JP1 user permissions are required.

- Acquiring and updating monitoring window settings (processing after connecting to the manager host)
  Processing of the following operations is performed after you log in to the server (manager):
  - Auto-generate a monitoring tree
  - Acquire the existing settings of a monitoring tree
  - Save edited monitoring tree settings
  - Acquire the existing settings of the Visual Monitoring window
  - Save the settings edited in the Visual Monitoring window
  - Acquire update data for the common condition of a status change condition

  To perform the above operations, you must log in to JP1/IM - Manager (Central Scope). When the Login window appears, log in as a JP1 user.#

  Required permissions:

  The JP1 user who logs in to JP1/IM - Manager (Central Scope) requires the following permissions:
  - JP1 resource group: `JP1_Console`
  - JP1 permission level: `JP1_Console_Admin`

  A JP1 user who wants to auto-generate a monitoring tree must log in as the `jp1admin` user.

  This is because a permission other than `JP1_Console_Admin` might be required to access definition information for a linked product during auto-generation. (If the `jp1admin` user has been deleted for operational reasons, the JP1 user will require a permission level that allows access to the definition information of the linked product. For example, to acquire JP1/AJS jobnet information, the JP1 user will require a permission level that grants jobnet access.)

  #: If you have checked the **Save Login Information** command in the **File** menu of the Monitoring Tree (Editing) window, your login user name, password, and host name are preserved until you log out, and the Login window does not appear during subsequent operations to connect to the server.

Before you perform settings in a monitoring window of the Central Scope, make sure that you know the `jp1admin` user password, or the password and user name of the JP1 user who has `JP1_Console_Admin` permission.

Important

When you update the server to apply the changed settings in the Monitoring Tree (Editing) window, the status of all monitoring nodes and status change events is initialized.

4.5 Visual monitoring

Creating and editing Visual Monitoring windows

You can create and edit a Visual Monitoring window to suit your purpose. This is useful for localized monitoring of specific nodes only (such as a node related to operations at the Kyushu branch office, for example).

The Visual Monitoring window supports the display of background images and Visual Icon. We recommend that you use these tools to create highly flexible Visual Monitoring windows.

You can perform the following operations:

- Set or edit a Visual Monitoring window name.
- Set or edit comments about a Visual Monitoring window.
- Arrange nodes, set attributes, change the monitoring status, or perform a search in a Visual Monitoring window.
- Change the background image.

Use the Visual Monitoring (Editing) window for creating or editing a Visual Monitoring window.

Monitoring operations in the Visual Monitoring window

You can perform the following operations in the Visual Monitoring window:

- Launch a Monitoring Tree window.
- Perform operations from a pop-up menu.

  You can also perform the following operations in the same way as in the Monitoring Tree window:

  - Change the node status
  - Change the monitoring status
  - Conduct a search
  - Display guidance
  - Search for status change events
  - Display properties

When the monitoring range settings are enabled for a monitoring tree, they also affect the Visual Monitoring window display. For example, if a Visual Monitoring window contains a node that the user is not permitted to access, it will not appear when the window is displayed.

4.6 Customizing monitoring node settings

You can customize monitoring node settings by editing the system profile of Central Scope.

You can customize the following settings:

- Whether to suppress display of monitoring node name and the margins of monitoring node icon
- Settings of the status colors for monitoring node name and monitoring node
- Whether to suppress moving of monitoring node icon

For details about customizing procedures, see the following descriptions:

For details about customizing monitoring node settings

- For suppressing the display of monitoring node name and the margins of monitoring node icon:
  See *5.7.7 Settings for suppressing the display of a monitoring node name and the icon margin* in the *JP1/Integrated Management - Manager Configuration Guide*.
- For setting status colors for monitoring node name and monitoring node
  See *5.7.8 Settings of the status color of a monitoring node name and monitoring node* in the *JP1/Integrated Management - Manager Configuration Guide*.
- For suppressing moving of monitoring node icon
  See *5.7.9 Settings for suppressing the movement of the icon of a monitoring node* in the *JP1/Integrated Management - Manager Configuration Guide*.

4.6.1 Suppressing display of monitoring node name and the margins of monitoring node icon

The map view in the Monitoring Tree window and the Visual Monitoring window displays a monitoring node name under each monitoring node icon. The map view and the Visual Monitoring window displays margins around the monitoring node icon as an area to show the color that indicates the current status of the monitoring node. The monitoring node name and the margins around the monitoring node icon are not displayed when suppression of their display is enabled.

The following table lists the windows of the Central Scope to which the suppression of the display of monitoring node name and the margins for monitoring node icon is applied when the suppression is enabled.

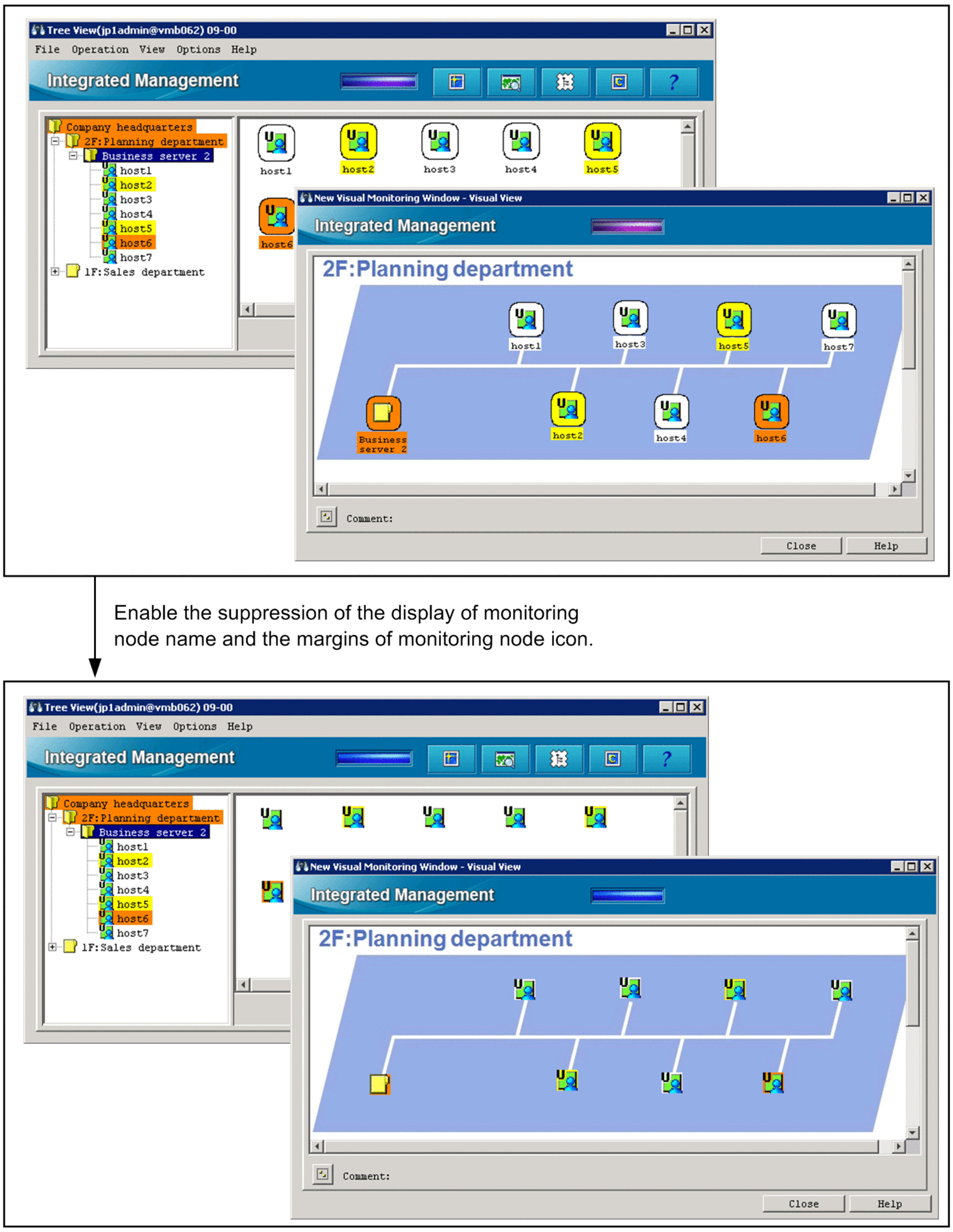
Table 4–8: Applicable range of the suppression of the display of monitoring node name and the margins for monitoring node icon

Window name	Applicability
Monitoring Tree window	Y
Monitoring Tree (Editing) window	Y
Visual Monitoring window	Y
Visual Monitoring (Editing) window	Y

Legend:
Y: Applicable

The following figure shows examples of windows for which the suppression of the display of monitoring node name and the margins for monitoring node icon are enabled.

Figure 4–17: Examples of windows for which the suppression of the display of monitoring node name and the margins for monitoring node icon are enabled



Enable the suppression of the display of monitoring node name and the margins of monitoring node icon.

4.6.2 Setting status colors for monitoring node name and monitoring node

You can specify status colors for monitoring node names with RGB values. You can also specify the colors of individual statuses (including `Initial` and `Error`) of monitoring node with RGB and alpha (A) values. According to the settings of status colors for monitoring nodes, the color of the area (around the monitoring node icon) that indicates the status of each monitoring node changes. Note, however, that A values are applied to windows only when the suppression of the display of monitoring node name and the margins of monitoring node icon are enabled.

Note also that, in the Monitoring Tree (Editing) and Visual Monitoring (Editing) windows, only the status color for the `Initial` status is used to indicate the status of the monitoring node.

The following table lists the windows of the Central Scope to which the settings of status colors for monitoring node names and monitoring nodes are applied when the settings are enabled.

Table 4–9: Applicable range of the settings of status colors for monitoring node name and monitoring node

Window name	Applicability
Monitoring Tree window	Y
Monitoring Tree (Editing) window#	Y
Visual Monitoring window	Y
Visual Monitoring (Editing) window#	Y

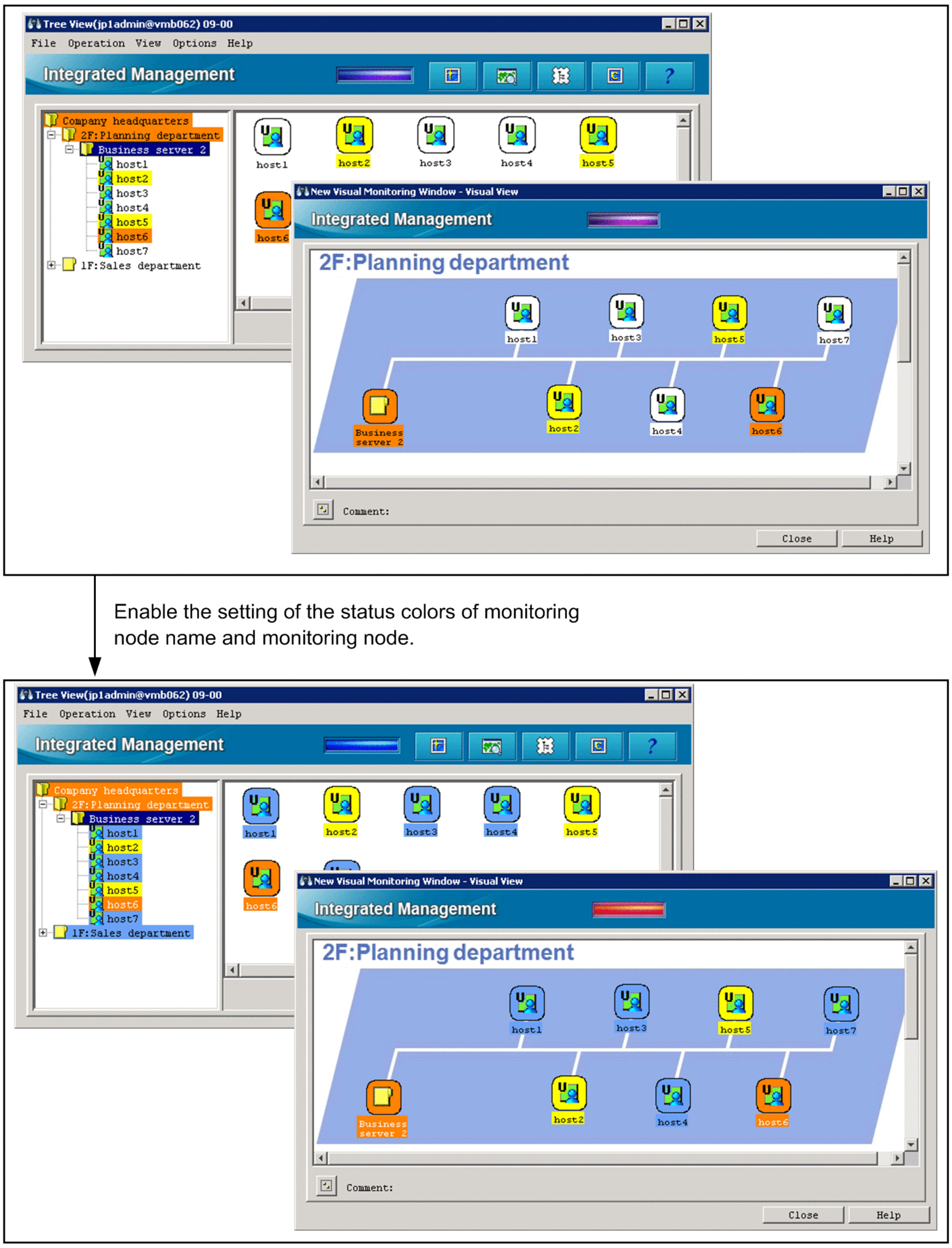
Legend:

Y: Applicable

#: Only the status color for the Initial status is used to indicate the status of the monitoring node.

The following figure shows examples of windows for which the settings of the status colors for monitoring node names and monitoring nodes are enabled.

Figure 4–18: Examples of windows for which the settings of the status colors for monitoring node names and monitoring nodes are enabled



Enable the setting of the status colors of monitoring node name and monitoring node.

4.6.3 Suppressing moving of monitoring node icon

You can suppress moving of monitoring node icons in the Monitoring Tree and Visual Monitoring windows so as to prevent the layout of monitoring nodes from being disordered.

The following table lists the windows of the Central Scope to which the suppression of moving of monitoring node icons is applied when the suppression is enabled.

Table 4–10: Applicable range of the suppression of moving of monitoring node icons

Window name	Applicability
Monitoring Tree window	Y
Monitoring Tree (Editing) window	N
Visual Monitoring window	Y
Visual Monitoring (Editing) window	N

Legend:

Y: Applicable

N: Not applicable

4.7 Searching for monitoring nodes or status change events

4.7.1 Searching for monitoring nodes

You can search for monitoring nodes in the Monitoring Tree window and Visual Monitoring window.

For example, you can execute a search to see whether any monitoring objects have changed their status (indicating that an event has occurred) or to find a specific monitoring object.

When performing a monitoring node search, you can specify various conditions in the displayed Search window. The following items can be specified as search conditions:

- Monitoring node name
- Monitoring node ID
- Monitoring node type
- Status
- Monitoring status
- JP1 resource group#
- Basic information
- Status change condition
- Event generation condition

  #: Appears only when the monitoring range settings are enabled for the monitoring tree. For details, see *4.4.3 Setting the monitoring range of a monitoring tree*.

These conditions are related by an AND condition. Use regular expressions when entering a monitoring node name, basic information, or status change condition.

The search results are displayed in the Search window. You can change the status and monitoring status of a selected node in this window. By double-clicking a displayed node, you can display the node in its selected status in the Monitoring Tree window.

4.7.2 Searching for status change events

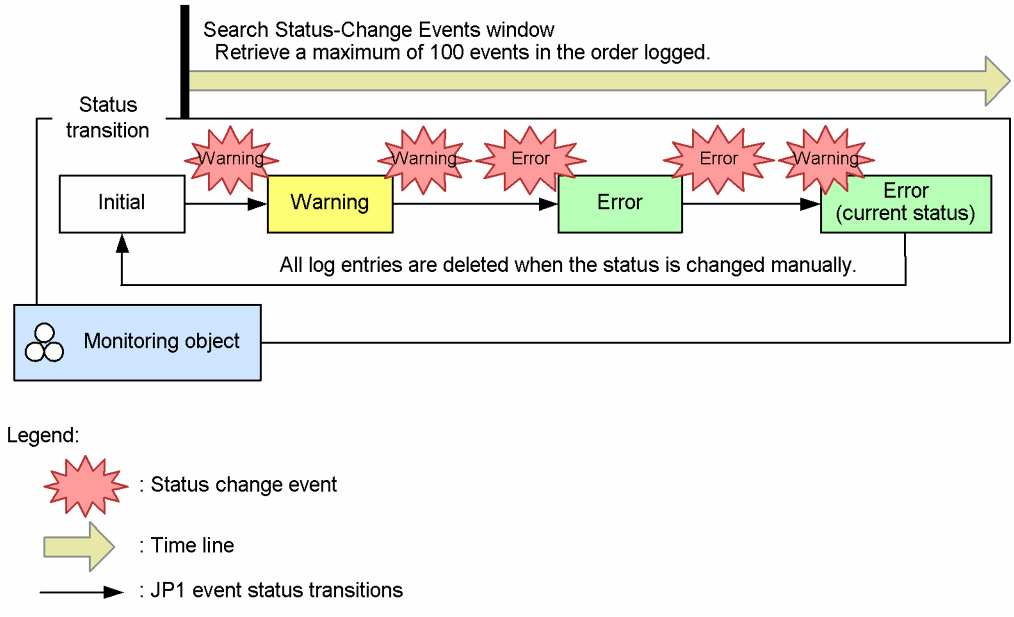
In the Monitoring Tree window and Visual Monitoring window, you can search for status change events in a particular monitoring object. A maximum of 100 events can be retrieved in the order they were logged, starting from the oldest (you cannot search for events exceeding this maximum number). A *status change event* is a JP1 event that acts as a monitoring target (status change condition) in the Central Scope.

(1) Searching for logged status change events

Perform a search when you need to check the logged status change events that have resulted in the present status of a monitoring object or group, or to view detailed information about any of the logged status change events. The JP1 event details appear on the **Search Events** page of the Event Console window.

If you manually change the status of a monitoring node, all status change events are deleted from the log.

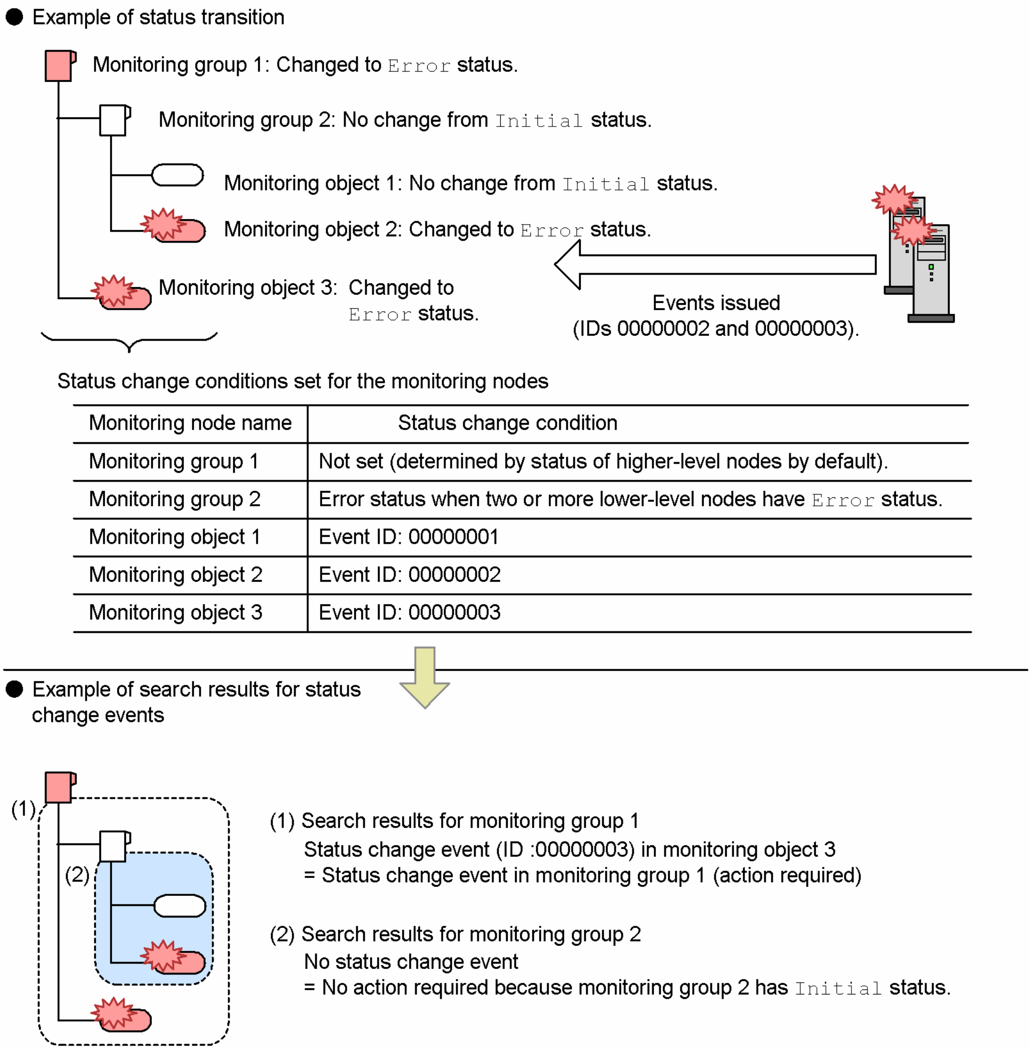
Figure 4–19: Status transition of a monitoring object and searching for status change events


Search Status-Change Events window
Retrieve a maximum of 100 events in the order logged.
Status transition
Warning
Warning
Error
Error
Warning
Initial
Warning
Error
Error (current status)
All log entries are deleted when the status is changed manually.
Monitoring object
Legend:
: Status change event
: Time line
: JP1 event status transitions

When you search for status change events affecting a monitoring group, the results show the status change events that occurred in the lower-level monitoring nodes, to a maximum of 100 starting from the oldest.

However, if a status change condition is defined for the monitoring group, the status change events that occurred in lower-level nodes are shown in the results only if they require a response, to a maximum of 100 starting from the oldest. The following figure shows an example.

Figure 4–20: Example of searching for status change events in a monitoring group


● Example of status transition
Monitoring group 1: Changed to Error status.
Monitoring group 2: No change from Initial status.
Monitoring object 1: No change from Initial status.
Monitoring object 2: Changed to Error status.
Monitoring object 3: Changed to Error status.
Events issued (IDs 00000002 and 00000003).
Status change conditions set for the monitoring nodes

Monitoring node name	Status change condition
Monitoring group 1	Not set (determined by status of higher-level nodes by default).
Monitoring group 2	Error status when two or more lower-level nodes have `Error` status.
Monitoring object 1	Event ID: 00000001
Monitoring object 2	Event ID: 00000002
Monitoring object 3	Event ID: 00000003

● Example of search results for status change events
(1)
(2)
(1) Search results for monitoring group 1
Status change event (ID :00000003) in monitoring object 3
= Status change event in monitoring group 1 (action required)
(2) Search results for monitoring group 2
No status change event
= No action required because monitoring group 2 has Initial status.

As shown in the figure, only the status change events that require a response are shown in the search results.

To view the search results for status change events in monitoring object 2, you can drill down the monitoring tree to that object, or you can search for status change events in monitoring object 2 itself. To search for status change events in all nodes from the higher-level monitoring group 2 down to monitoring object 2, you can define one or more child nodes in `Error` status as the condition for changing monitoring object 2 to `Warning` status.

Event issued when the number of status change events exceeds 100

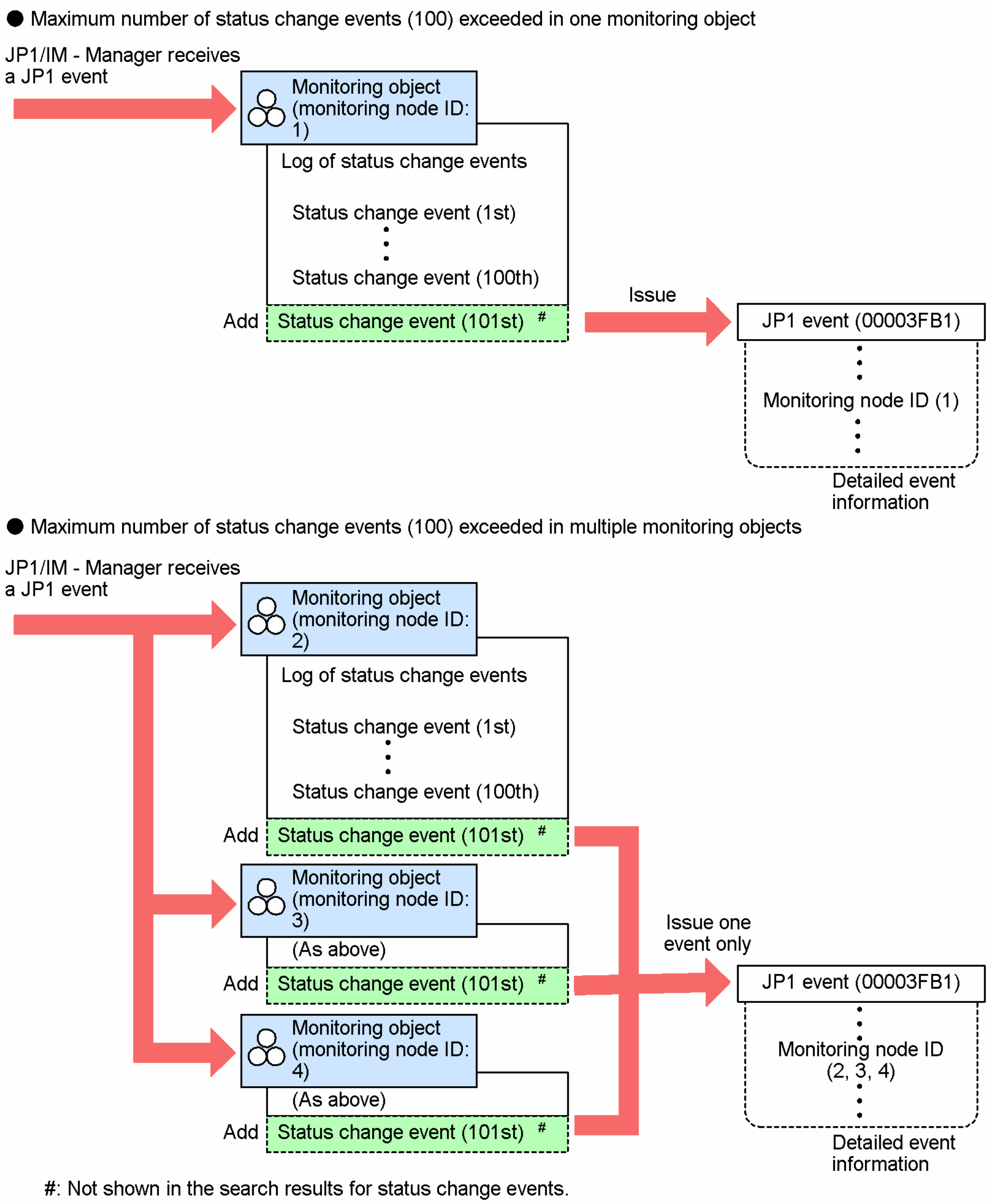
When the number of status change events in a monitoring object exceeds 100, a warning JP1 event is issued.

Issued JP1 event

- Event ID: 00003FB1
- Message: KAVB7901-W

Only one warning JP1 event (ID 00003FB1) is issued even if a single JP1 event causes the number of status change events to exceed 100 in multiple monitoring objects. The IDs of the affected objects are listed in comma-separated form in *monitoring-node-ID* in the message text, to a maximum of 10. If there are more than 10 affected objects, the IDs are followed by an ellipsis (...).

Figure 4–21: Issuing of event ID 00003FB1


● Maximum number of status change events (100) exceeded in one monitoring object
JP1/IM - Manager receives a JP1 event
Monitoring object (monitoring node ID: 1)
Log of status change events
Status change event (1st)
Status change event (100th)
Add
Status change event (101st) #
Issue
JP1 event (00003FB1)
Monitoring node ID (1)
Detailed event information
● Maximum number of status change events (100) exceeded in multiple monitoring objects
JP1/IM - Manager receives a JP1 event
Monitoring object (monitoring node ID: 2)
Log of status change events
Status change event (1st)
Status change event (100th)
Add
Status change event (101st) #
Monitoring object (monitoring node ID: 3)
(As above)
Add
Status change event (101st) #
Monitoring object (monitoring node ID: 4)
(As above)
Add
Status change event (101st) #
Issue one event only
JP1 event (00003FB1)
Monitoring node ID (2, 3, 4)
Detailed event information

#: Not shown in the search results for status change events.

Note

The log of status change events for a monitoring object can only be managed to a maximum of 100 events. We recommend that you periodically check the number of logged status change events (by executing a search) and purge the log if it is getting too large. You can do so by manually changing the status of the monitoring object, or you can choose to delete the log automatically.

Before you manually purge a log, make sure that the JP1 events listed in the search results have all been dealt with.

The log can be deleted automatically in either of two ways:

- Set the monitoring object to `Initial` status on receipt of a specific JP1 event.
- Delete the log when the response status of JP1 events changes to **Processed**.

For details about how to set a monitoring object to `Initial` status on receipt of a specific JP1 event, see *4.7.2(2) Setting a monitoring object to initial status on receipt of a JP1 event*. For details about how to delete a log of status change events when the response status of JP1 events is changed to **Processed**, see *4.9.3 Automatically deleting processed status change events*.

(2) Setting a monitoring object to initial status on receipt of a JP1 event

A monitoring object can be placed in `Initial` status on receipt of a particular JP1 event. This automatically deletes the log of status change events for that monitoring object. This functionality is referred to as *automatically initializing a monitoring object*. The functionality is disabled by default.

For example, by using a JP1 event that is issued when an error has been resolved, you can automatically initialize a monitoring object based on a recovery notification. To set this up, you would need to define a status change condition which changes the monitoring object to `Initial` status on receipt of a recovery-notification JP1 event.

You can define an `Initial` status change condition only for a monitoring object, not for a monitoring group.

As a note of caution when using this functionality, consider the possibility of two or more different errors being reported as JP1 events for the same monitoring object. If a recovery-notification JP1 event is received for one of these errors, the monitoring object will be forcibly initialized and its log of status change events will be deleted, even if the other error is unresolved. For this reason, we recommend that you use the automatic initialization functionality only under the following conditions:

- The issuing of one notification JP1 event guarantees that all errors occurring in a monitoring object have been resolved.
- Error recovery does not require the user to check the error log for the monitoring object in question.

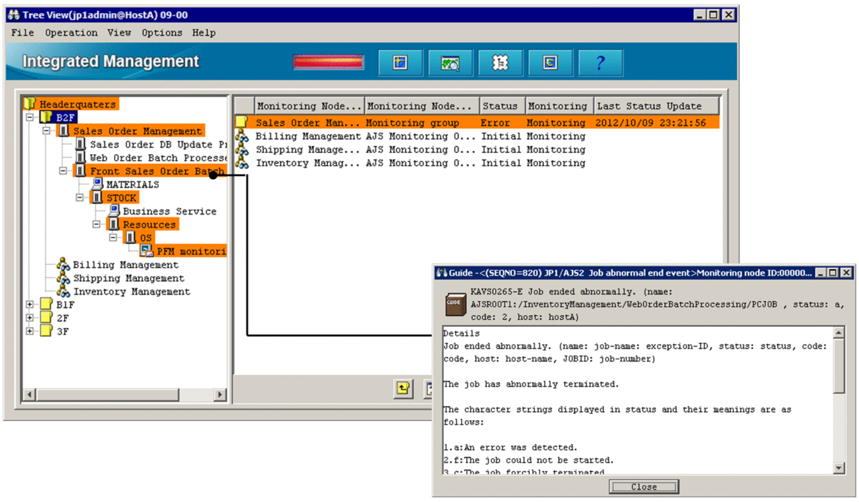
For details about how to set the automatic initialization function, see *5.7.4 Settings for initializing monitoring objects when JP1 events are received* in the *JP1/Integrated Management - Manager Configuration Guide*.

4.8 Guide function

The guide function displays information relating to the type and status of a monitoring node in the Monitoring Tree window or Visual Monitoring window.

Using this function, you can view troubleshooting advice, such as action procedures and response methods for various errors, in accordance with the type and status of the monitoring object or group. For example, you can register troubleshooting procedures as guide information for each of the jobs in a monitoring group associated with a jobnet. This makes it easy to find pertinent information in a crisis. You can also use the guide function to describe the particular job that a monitoring node is associated with, and the specific aspects it is monitoring, and to accumulate operating know-how as guide information. Utilizing guide information in this way, as reference material when a problem occurs, lessens the system administrator's workload at the initial response stage.

Figure 4–22: Troubleshooting advice displayed as guide information



Monitoring Node...	Monitoring Node...	Status	Monitoring	Last Status Update
Sales Order Man...	Monitoring group	Error	Monitoring	2012/10/09 23:21:56
Billing Management	AJS Monitoring O...	Initial	Monitoring	
Shipping Manage...	AJS Monitoring O...	Initial	Monitoring	
Inventory Manag...	AJS Monitoring O...	Initial	Monitoring	

Guide -<(SEQNO=820) JP1/AJS2 Job abnormal end event>Monitoring node ID:00000...

```
KAVS0265-E Job ended abnormally. (name:
AJSROOT1:/InventoryManagement/WebOrderBatchProcessing/PCJOB , status: a,
code: 2, host: hostA)
```

```
Details
Job ended abnormally. (name: job-name: exception-ID, status: status, code:
code, host: host-name, JOBID: job-number)

The job has abnormally terminated.

The character strings displayed in status and their meanings are as
follows:

1.a:An error was detected.
2.f:The job could not be started.
3.c:The job forcibly terminated
```

View guide information to find out methods and procedures for handling the problem.

Example:

Guide information before a status change: Description of the associated job and the purpose of monitoring.

Guide information after a status change: Explanation of how to handle the error that has occurred.

The information displayed by the guide function is called *guide information*. Its contents and format (text or HTML) can be set by the user.

For details about how to set guide information, see *5.6.1 How to edit guide information* in the *JP1/Integrated Management - Manager Configuration Guide*.

4.8.1 Settings for guide information

The contents displayed as guide information are set in a *guide information file* managed by JP1/IM - Manager.

- Guide information file

  Windows: *scope-path*`\conf\jcs_guide_`*xxx*`.txt`

  UNIX: `/etc/opt/jp1scope/conf/jcs_guide.txt`

For the format of a guide information file, see below.

About the guide information file

- Format of a guide information file

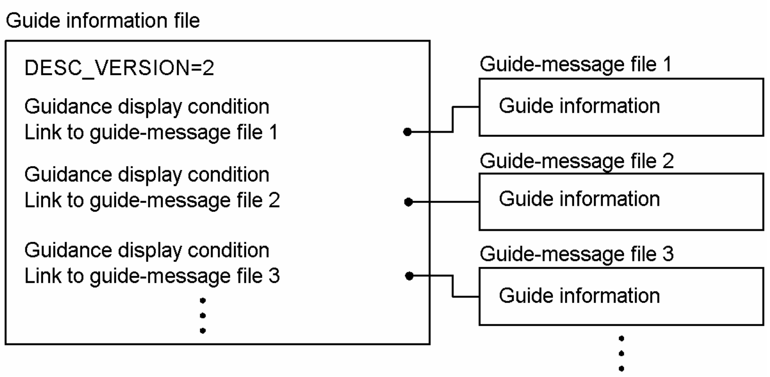
  See *Guide information file (jcs_guide.txt)* in *Chapter 2. Definition Files* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

In a guide information file, you can specify the contents to be displayed as guide information and the conditions about when to display the information.

The information to be displayed can be stored and managed in individual files. In JP1/IM, these separate files are known as *guide-message files*.

To use guide-message files, the guide information file must be version 2 (`DESC_VERSION=2`). In the guide information file, instead of writing out the information itself, you simply write links to the guide-message files.

Figure 4–23: Using guide-message files


Guide information file
DESC_VERSION=2
Guidance display condition
Link to guide-message file 1
Guidance display condition
Link to guide-message file 2
Guidance display condition
Link to guide-message file 3
Guide-message file 1
Guide information
Guide-message file 2
Guide information
Guide-message file 3
Guide information

(1) Conditions for displaying guide information

Using a condition `EV_COMP_`*n* (where *n* represents a number), you can specify when to display a particular item of guide information. You can specify multiple conditions in the form `EV_COMP_1`, `EV_COMP_2`, and so on. The specified conditions are related by an AND condition.

As the condition, you can specify the type of JP1 event received by the monitoring node, or information about the node itself, as follows:

- Basic attribute or extended attribute of a JP1 event

  For example, you can specify the event ID (`B.ID`), event level (`E.SEVERITY`), or other attribute.

  You can also specify program-specific information (provided as an extended attribute of JP1 events) for a particular JP1 product. For example, you can specify the host that executes JP1/AJS jobs (`E.C0`).

  For the basic attributes and extended attributes of JP1 events, see the appropriate manual for information about JP1 events issued by the product concerned.

- Monitoring node attribute

  You can specify a monitoring node ID (`T.MONNODEID`) identifying a specific node. Check the ID in the Properties window or Search window for the monitoring node you want to specify.

When guide information is displayed in JP1/IM - View, the contents of the guide information file are referenced from the top. When an item matching the conditions is found, referencing stops and the applicable information appears in the Guide window.

Important

Because the Guide window displays only the first of possibly multiple items in the guide information file that match the conditions, bear the following in mind when setting display conditions:

- Set multiple display conditions for an item of guide information so that the condition does not duplicate a display condition set for a different guide item.

  For example, by setting multiple JP1 event attributes in a display condition, such as the event ID, event level, or message, you can differentiate the display condition from that set for another guide item.

  A regular expression can be written as the contents of an attribute, but it must require a complete match.
- Write the contents of the guide information file starting from the highest event level.

  For example, if status change conditions have been defined to change the status of a monitoring node to `Warning` and `Error`, respectively, write the information displayed when the node status changes to `Error` before the information displayed when the node status changes to `Warning`.

  To display a description of the monitoring node as guide information, simply specify the node ID as the display condition. Write low-priority information of this nature at the very end of the guide information file.

(2) Contents displayed as guide information

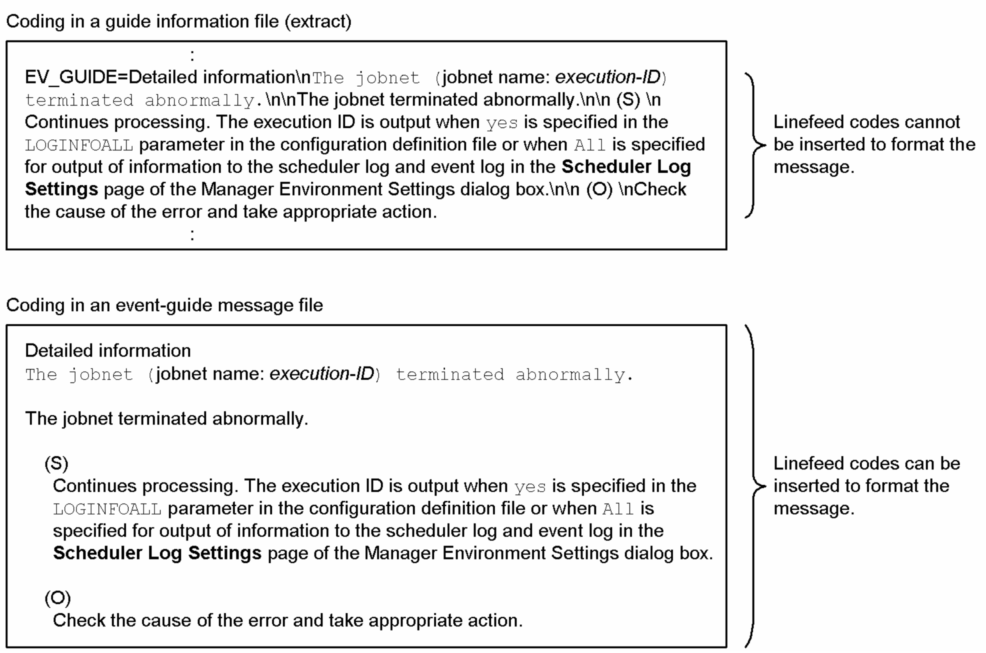
To write messages to be displayed as guide information, specify `EV_GUIDE` in the guide information file. To use guide-message files, specify `EV_FILE` instead of `EV_GUIDE`.

Messages can be written in text format or HTML format. The attribute values of JP1 events can also be used as variables in messages (by prefixing the attribute value with `$`). For example, if you write `$B.MESSAGE`, JP1 event messages (`B.MESSAGE`) will be handled as variables, and the attribute value of the JP1 event will be displayed in the guide message.

Reference note:

- You cannot format the message layout in a guide information file by inserting linefeed codes. However, you can do so in a guide-message file.

Figure 4–24: Examples of writing guide information



Coding in a guide information file (extract)

```
:
EV_GUIDE=Detailed information\nThe jobnet (jobnet name: execution-ID) terminated abnormally.\n\nThe jobnet terminated abnormally.\n\n (S) \nContinues processing. The execution ID is output when yes is specified in the LOGINFOALL parameter in the configuration definition file or when All is specified for output of information to the scheduler log and event log in the Scheduler Log Settings page of the Manager Environment Settings dialog box.\n\n (O) \nCheck the cause of the error and take appropriate action.
:
```

Linefeed codes cannot be inserted to format the message.

Coding in an event-guide message file

```
Detailed information
The jobnet (jobnet name: execution-ID) terminated abnormally.

The jobnet terminated abnormally.

  (S)
   Continues processing. The execution ID is output when yes is specified in the
   LOGINFOALL parameter in the configuration definition file or when All is
   specified for output of information to the scheduler log and event log in the
   Scheduler Log Settings page of the Manager Environment Settings dialog box.

  (O)
   Check the cause of the error and take appropriate action.
```

Linefeed codes can be inserted to format the message.

Because you can apply formatting, guide-message files are useful when you are preparing messages in HTML format, and there is a large amount of information or you need to periodically review the message contents.

- Only one item of information can be written in a guide-message file. If you are writing a large amount of information, you might end up with a considerable number of files. Bear the following in mind when using guide-message files:
  - Use file names that will be easy to manage.
    Name the files based on set conventions, using keywords (event IDs and message IDs, product names (AJS), monitoring node IDs, and so on) that are contained in the display conditions or display contents.
  - Include the guide-message file name in the guide title (`EV_TITLE`) written in the guide information file.
    For example, suppose you are creating a guide-message file with the name `guide001`. Write the title as follows.

```
:
EV_TITLE=guide001: Abnormal job termination
EV_FILE=guide001
:
```

This makes it easier to edit the information later because you can tell from the display in the Guide window which guide-message file is being referenced.

4.8.2 Utilizing guide information tailored to the system operation

In the Guide window, you can choose to display any type of information as guide information, according to how the system is to be monitored.

For example, guide information could be utilized in the following ways.

Guide information tailored to system operation (examples)

- Guide information about troubleshooting procedures
  First, suggest ways of handling particular problems, and advise what action to take in a crisis. Register these ideas as guide information.

Investigate the problem in detail at the follow-up stage, using all the various JP1/IM functions.

- Guide information about particular problems (JP1 events)

  Prepare guide information about the causes of particular problems.

  As a display condition, you can use information about the JP1 event that caused a status change in the monitoring node. Register this information as guide information

You can also set different types of guide information for different types of monitoring nodes. For example, you could display troubleshooting procedures for monitoring groups, and details about error causes for monitoring objects.

(1) Guide information about action procedures

To display guide information about action procedures, you must register information with the relevant monitoring nodes (that is, the monitoring viewpoints associated with a jobnet or other processing).

Each monitoring node has its own ID. Set guide information using the node ID as a condition.

Monitoring node IDs are unique to a node and are assigned automatically when a node is created. The node ID does not change when a node is moved in a monitoring tree.

1. Verify the monitoring node ID.

   In the Monitoring Tree window, verify the ID of the node that you want to set guide information for in either of the following ways:

   - Select the node, and then right-click and choose **Properties** from the pop-up menu. View the **General** page in the displayed Properties window. The node ID appears in the **Monitoring node ID** field.
   - Execute a node search: Choose **View** and then **Search** to open the Search window, and then search for the monitoring node you require. The node ID appears in the **Monitoring node ID** field in the search results.

2. Write guide information using the monitoring node ID as the condition.

   In the guide information file (`jcs_guide.txt`), write guide information specifying the monitoring node ID (`T.MONNODEID`) as the condition (`EV_COMP` specified).

   For example, write the guide information as follows.

   Coding example:

   ```
   [EV_GUIDE_1]
   NUM=1
   EV_COMP_1=T.MONNODEID:(monitoring-node-ID)
   EV_TITLE=Action for error in Accounts_DailyTotals
   EV_GUIDE=Action procedure when an error occurs in Accounts_DailyTotals\nSee:
   User's Guide 3.11 Troubleshooting\nSummary: (For details, see the User's Guide.)
   \nCheck the error cause. If the error has major impact, suspend related jobs and
   contact the administrator (contact route C).
   [END]
   ```

   Explanation of coding example:

   In `T.MONNODEID:(`*monitoring-node-ID*`)`, specify the node ID you verified above.

(2) Guide information about an error (JP1 event)

To display guide information about an error, you must register information about the JP1 event that caused a status change in the monitoring node.

1. Investigate the JP1 event.

   Investigate the JP1 event related to the problem.

   As a display condition, you can use the event ID (`B.ID`) or other attribute of the JP1 event.

   If you want to include a message (`B.MESSAGE`) or other JP1 event information in the guide information, also check message contents and attribute names.

2. Write guide information using the JP1 event as the condition.

   In the guide information file (`jcs_guide.txt`), write guide information specifying the JP1 event ID (`B.ID`) or other JP1 event information as the condition (`EV_COMP` specified).

   For example, write the guide information as follows.

   Coding example:

   ```
   [EV_GUIDE_1]
   NUM=1
   EV_COMP_1=B.ID:00004107
   EV_TITLE=Abnormal job termination
   EV_GUIDE=The job ended abnormally.\nJob name: $E.OBJECT_NAME\nJob execution host:
   $E.C0\nMessage--\n$B.MESSAGE\n--\n<Case>\nIf job A and job B are executed
   concurrently, job B will end abnormally because there is insufficient work area:
   Check the log (jobexe.log).
   [END]
   ```

4.9 Completed-action linkage function

The completed-action linkage function automatically changes the status of monitoring objects according to the response status of the associated JP1 event. Thus, the status of each monitoring object in the Central Scope is linked to the response status of the corresponding JP1 event in the Central Console, and changes accordingly.

For example, suppose that an object has `Error` status because an error event has been received. When you change the response status of this error event to **Processed**, the status of the object changes from `Error` to `Normal`.

This function saves you from having to manually change the status of monitoring objects and monitoring groups and facilitates Central Scope operations.

The function does not work in reverse: Changing the status of a monitoring object in the Central Scope does not change the response status of the JP1 event matching a status change condition in the Central Console. For example, if you change the status of an object in the Central Scope from `Error` to `Normal`, the JP1 event in the Central Console does not change to **Processed**.

> **Important**
>
> If you change the status of an object in the Central Scope, and then change the JP1 event response status in the Central Console, the status of the object will change again as a result.
>
> However, because the log of status change events managed by the Central Scope is deleted when an object's status is changed manually, the completed-action linkage function is disabled at that point.

If there are any JP1 events not yet set to **Processed** status, the monitoring object will be in a corresponding status. In order of priority, its status will be one of the following: `Emergency`, `Alert`, `Critical`, `Error`, `Warning`, `Normal`, or `Debug`. When the user has changed all the JP1 events in the search results to **Processed** status, the monitoring object changes to `Normal`.

If a JP1 event has been changed from **Processed** to **Processing**, **Held**, or **Unprocessed** status, the object will revert to its previous status accordingly.

4.9.1 Behavior of the completed-action linkage function

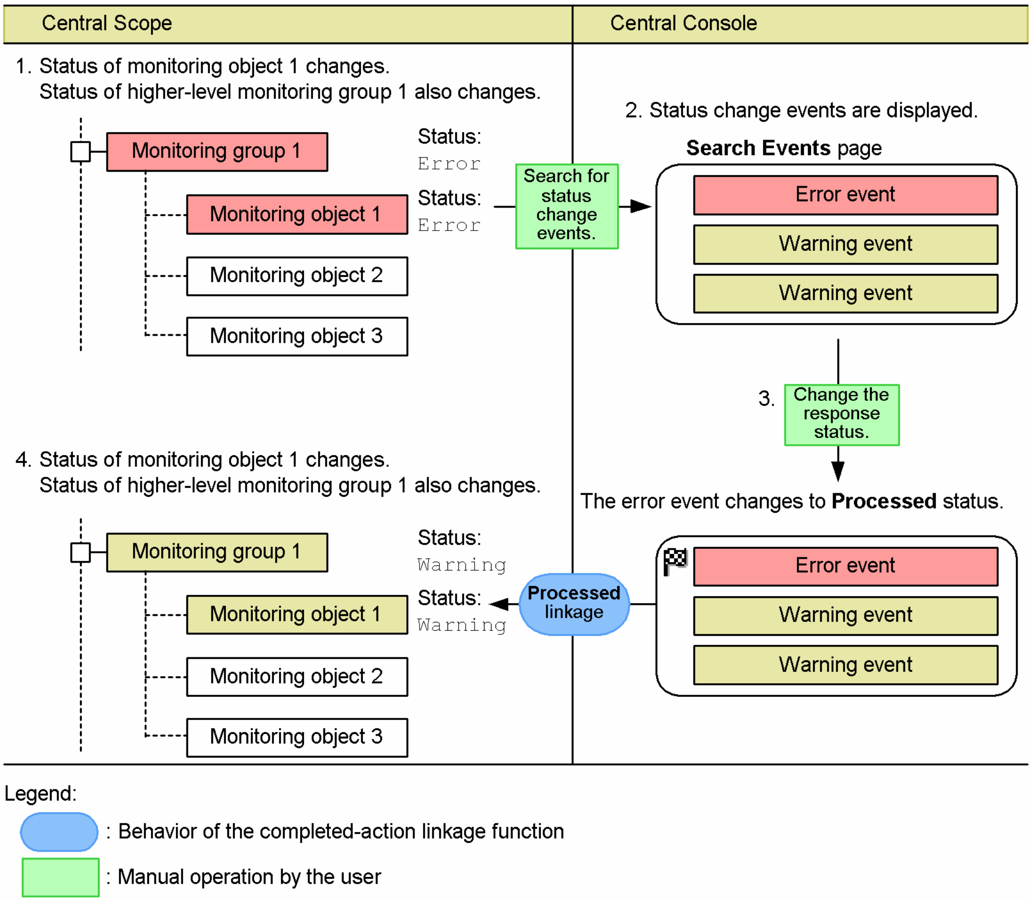
The following describes, by way of examples, how the completed-action linkage function works when the user manually changes the response status of a JP1 event in the Central Console after a monitoring object change status while the system is being monitored from the Central Scope.

The example below is based on the following assumptions:

- Both error events and warning events are set as status change conditions for monitoring object 1.
- Monitoring object 1 is defined so that its status changes to `Error` when an error event occurs, and to `Warning` when a warning event occurs.
- No status change condition is set for monitoring group 1 (the default applies).

The following example shows the behavior of the completed-action linkage function when the user changes the response status of a JP1 event to **Processed**.

Figure 4–25: Example of the completed-action linkage function (1)



Central Scope
Central Console
1. Status of monitoring object 1 changes.
Status of higher-level monitoring group 1 also changes.
Monitoring group 1
Status: Error
Monitoring object 1
Status: Error
Monitoring object 2
Monitoring object 3
Search for status change events.
2. Status change events are displayed.
Search Events page
Error event
Warning event
Warning event
3. Change the response status.
The error event changes to Processed status.
4. Status of monitoring object 1 changes.
Status of higher-level monitoring group 1 also changes.
Monitoring group 1
Status: Warning
Monitoring object 1
Status: Warning
Processed linkage
Monitoring object 2
Monitoring object 3
Error event
Warning event
Warning event
Legend:
: Behavior of the completed-action linkage function
: Manual operation by the user

The flow of processing is described below, following the numbers in the figure:

1. JP1/IM receives a JP1 event matching a status change condition of monitoring object 1, and the object's status changes to `Error`. The status of the higher-level monitoring group 1 also changes to `Error`.

   The user investigates the cause of the error by searching for status change events, for example.

2. The status change events that occurred in monitoring object 1 appear on the **Search Events** page of the Central Console.

   In this example, both error events and warning events will change the status of monitoring object 1. The object's status has changed to `Error` here as a result of both types of events.

   The user acts on the problem that needs to be resolved first, according to the event level of the JP1 events.

3. The user changes the response status of the error event that caused the status change in monitoring object 1 to **Processed**.

   The user sets **Processed** only for the event that has been resolved.

4. In tandem with the JP1 event changing to **Processed**, the `Error` status of monitoring object 1 is cleared, and its status changes to `Warning`. The status of the higher-level monitoring group 1 also changes to `Warning`.

   Because the error event has changed to **Processed**, monitoring object 1 changes to the status corresponding to a warning event.

   The user investigates and resolves the remaining warning events. When all the JP1 events matching the status change conditions have been changed to **Processed**, the status of the monitoring object changes to `Normal`.

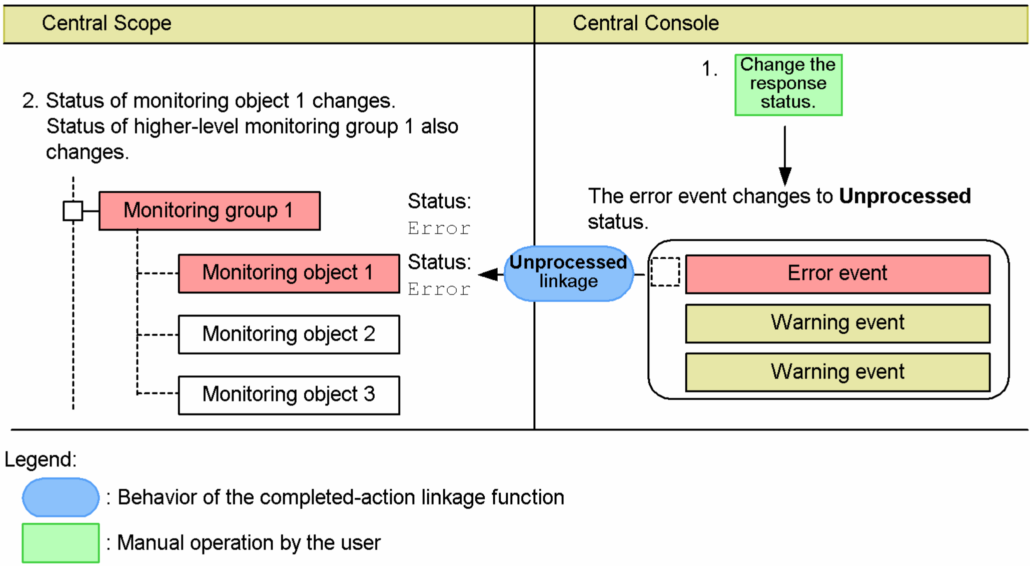
The next example shows the behavior of the completed-action linkage function when the user changes the response status of a JP1 event from **Processed** to a different value.#

#

Other possible values are **Processing**, **Held**, or **Unprocessed**.

Delete is not included. **Delete** simply hides the JP1 event on the **Severe Events** page. JP1 events deleted on this page might still be listed on the **Monitor Events** page and **Search Events** page. Thus, setting the response status of a JP1 event to **Delete** does not change the status of the monitoring object.

Figure 4–26: Example of the completed-action linkage function (2)


Central Scope
Central Console
1.
Change the response status.
2. Status of monitoring object 1 changes. Status of higher-level monitoring group 1 also changes.
Monitoring group 1
Status: Error
Monitoring object 1
Status: Error
Monitoring object 2
Monitoring object 3
The error event changes to **Unprocessed** status.
Unprocessed linkage
Error event
Warning event
Warning event
Legend:
: Behavior of the completed-action linkage function
: Manual operation by the user

The flow of processing is described below, following the numbers in the figure:

1. The user changes the response status of the JP1 event to **Unprocessed**.

   A processed JP1 event might need to be changed to another response status if the problem had not been resolved after all, or if the **Processed** status was set by mistake, for example.

2. In tandem with the JP1 event changing to **Unprocessed**, the status of monitoring object 1 changes back to `Error`. The status of the higher-level monitoring group 1 also changes back to `Error`.

   Because the error event is now **Unprocessed**, the object's status also changes back to `Error`, which has higher priority than `Warning`.

   The user now proceeds to fix the problem.

4.9.2 Disabling the completed-action linkage function

When the number of status change events exceeds the maximum (100), the completed-action linkage function is disabled. This is because integrity cannot be maintained between the log of status change events managed by the Central Scope and the JP1 events displayed in the Central Console.

For this reason, search for status change events on a regular basis and, if number of JP1 events in the search results is approaching the maximum, change the status of the monitoring objects manually to clear the log entries.

Manually changing the status of monitoring objects makes the completed-action linkage function usable once more. It also means that the corresponding JP1 events will not appear on the **Search Events** page, although they might still appear on the **Monitor Events** page and **Severe Events** page. Changing the response status of the JP1 events displayed on these pages has no effect on the status of the monitoring objects.

4.9.3 Automatically deleting processed status change events

The log of status change events can be deleted automatically when the response status of a JP1 event is changed to **Processed**. When this functionality is enabled, if all status change events for the monitoring object are changed to **Processed** status, the log is deleted and the monitoring object reverts to `Initial` status.

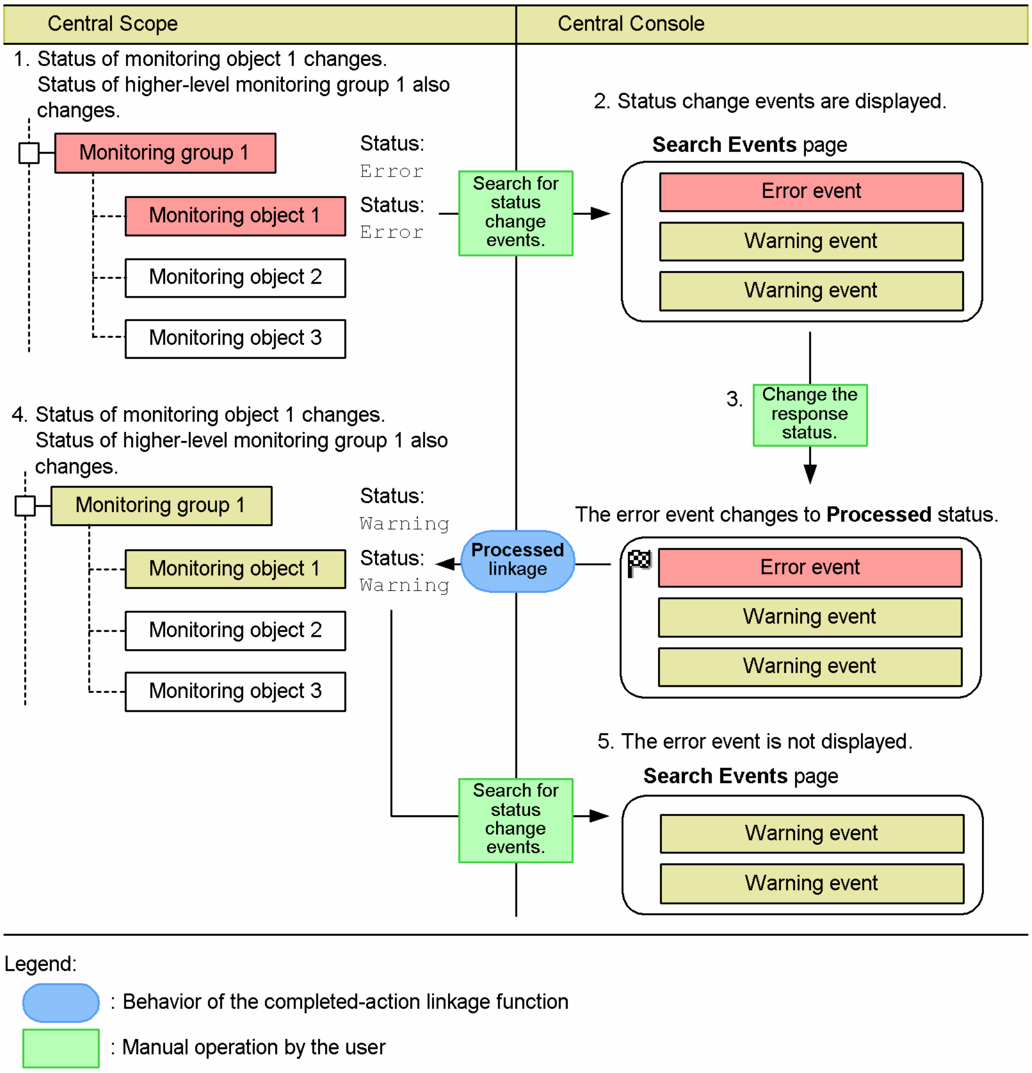
This functionality is disabled by default.

The following describes by way of an example how the log of status change events is automatically deleted. The example is based on the following assumptions:

- Both error events and warning events are set as status change conditions for monitoring object 1.
- Monitoring object 1 is defined so that its status changes to `Error` when an error event occurs, and to `Warning` when a warning event occurs.
- No status change condition is set for monitoring group 1 (the default applies).

The example below shows the behavior of the automatic deletion function when the user changes the response status of a JP1 event to **Processed**.

Figure 4–27: Example of automatically deleting processed status change events


Central Scope
Central Console
1. Status of monitoring object 1 changes.
Status of higher-level monitoring group 1 also changes.
Monitoring group 1
Status: Error
Monitoring object 1
Status: Error
Monitoring object 2
Monitoring object 3
Search for status change events.
2. Status change events are displayed.
Search Events page
Error event
Warning event
Warning event
3. Change the response status.
The error event changes to Processed status.
Error event
Warning event
Warning event
Processed linkage
4. Status of monitoring object 1 changes.
Status of higher-level monitoring group 1 also changes.
Monitoring group 1
Status: Warning
Monitoring object 1
Status: Warning
Monitoring object 2
Monitoring object 3
Search for status change events.
5. The error event is not displayed.
Search Events page
Warning event
Warning event
Legend:
: Behavior of the completed-action linkage function
: Manual operation by the user

Numbers 1 to 4 in the figure indicate the same actions as those in *Figure 4-25 Example of the completed-action linkage function (1)*. Of the status change events for monitoring object 1, the error event is set to **Processed**.

At step 5 in the figure, the user opens the **Search Events** page of the Central Console to search for status change events for monitoring object 1. However, because entries about JP1 events whose status was changed to **Processed** at step 3 have already been deleted from the log of status change events, these processed JP1 events do not appear on the **Search Events** page. Only unprocessed status change events are listed.

Automatic deletion applies only to status change events issued after the function was enabled. Status change events that occurred before the function was enabled and are already set to **Processed** status are not deleted from the log. To delete these events, delete them manually by changing the monitoring node to `Initial` status in the Monitoring Tree window or by using the `jcschstat` command.

For the setup required to delete processed status change events, see *5.7.3 Settings for automatically deleting status change events when JP1 event handling is completed* in the *JP1/Integrated Management - Manager Configuration Guide*.

Important

If you mistakenly change a JP1 event to **Processed**, and then change it to **Error** or another status, the status of the monitoring object and the log of status change events do not revert to their previous state. Consequently, you cannot search for that JP1 event from the Central Scope. You will need to search for **Processed** JP1 events from the Event Console window.

Do not use automatic deletion in normal circumstances because of the considerable caution is required in performing status operations with this functionality enabled. We recommend that you delete the log of status change events by manually setting the monitoring object to `Initial` status in the Central Scope. Enable automatic deletion only in special circumstances, such as restricting user operations to the Central Console only.

Note

Even if you enable automatic deletion of processed status change events, when the number of events exceeds the maximum (100), the completed-action linkage function is disabled. For this reason, periodically change the status change events to **Processed** to clear them from the log.

4.10 Performing system operations from JP1/IM

When a problem is detected during system monitoring, you can investigate using the Tool Launcher.

4.10.1 Tool Launcher

From the Tool Launcher window in JP1/IM - View, you can launch the GUI for products in the JP1 series and for many other applications. The Tool Launcher window lists the application functions that are linked with JP1/IM, allowing the windows of the appropriate application to be launched directly from the listing.

For details about the functions available in the Tool Launcher window, see *3.19.2 Tool Launcher*.

4.11 Central Scope

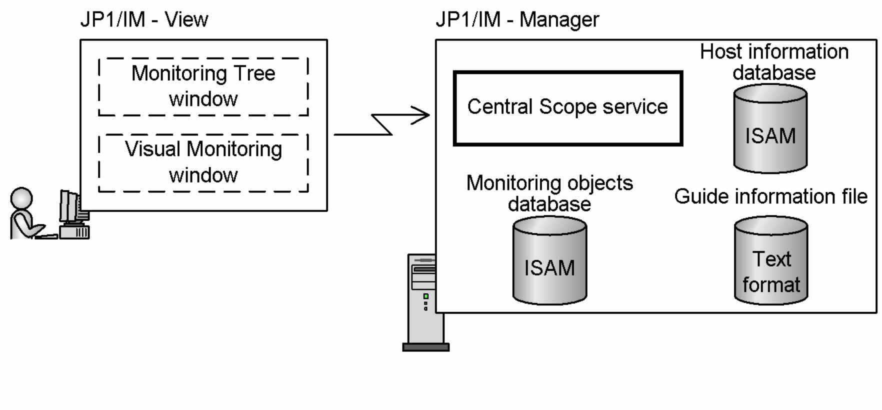
The following describes how the Central Scope works.

The Central Scope is designed so that it can be used without knowing how it works, but an understanding of Central Scope processes is useful if you want to customize settings or design a sophisticated system.

4.11.1 Overview of the Central Scope

The Central Scope incorporates the following functionality.

Figure 4–28: Overview of the Central Scope



4.11.2 Host information

JP1/IM - Manager (Central Scope) has its own host information database to manage host information (IP addresses and the corresponding actual host names).

The processing carried out by JP1/IM - Manager (Central Scope) includes managing the JP1 events occurring on the agents and automatically generating monitoring trees from definition information. JP1/IM - Manager must therefore recognize the host names and IP addresses of the agents correctly, and associate the right information.

To prevent discrepancies between the host names recognized by other products and those recognized by JP1/IM - Manager (Central Scope), association information can be stored in the JP1/IM host information database.

The host names that need to be registered in the host information are as follows:

- The host name for which **Host name comparison** is selected in individual conditions for monitoring objects
- The following host names when using auto-generation of monitoring trees:
  - The host names managed by JP1/AJS or other linked product
  - The host names defined in the JP1/IM configuration definition

To find host information that is not registered in the host information database, JP1/IM - Manager (JP1/IM - Central Scope) references the settings in the JP1/Base `jp1hosts` information or `p1hosts2` information, the OS `hosts` file, and the DNS.

We recommend that you select **Host name comparison** when specifying a host name in an individual condition for a monitoring object.

About host information:

- Format of the host information file

  See *Host information file (jcs_hosts)* in *Chapter 2. Definition Files* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.
- Commands for setting and referencing host information

  See *jcshostsimport* in *Chapter 1. Commands* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

  See *jcshostsexport* in *Chapter 1. Commands* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.
- How to specify a host name in an individual condition for a monitoring object

  See *3.12 Status-Change Condition Settings window* in the manual *JP1/Integrated Management - Manager GUI Reference*.

Note

When you select **Match**, JP1/IM - Manager (Central Scope) determines that the individual condition is satisfied only when there is a complete match between the attribute value (string) of a received JP1 event and the string specified as the individual condition.

In contrast, when you select **Host name comparison**, JP1/IM - Manager (Central Scope) compares the event attribute value with the host information in the database.

For example, suppose that the following is defined in the host information database of JP1/IM - Manager (Central Scope) or in the DNS or `hosts` file of the host on which JP1/IM - Manager (Central Scope) runs:

```
111.111.111.111 server1 webserver
```

The differences between specifying **Match** and specifying **Host name comparison** in this environment are as follows:

Specified individual condition: `E.OBJECT_ID` **:** `server1` **: Match**

If `E.OBJECT_ID` of a JP1 event is `server1`: Condition is satisfied.

If `E.OBJECT_ID` of a JP1 event is `webserver`: Condition is not satisfied.

If `E.OBJECT_ID` of a JP1 event is `111.111.111.111`: Condition is not satisfied.

Specified individual condition: `E.OBJECT_ID` **:** `server1` **: Host name comparison**

If `E.OBJECT_ID` of a JP1 event is `server1`: Condition is satisfied.

If `E.OBJECT_ID` of a JP1 event is `webserver`: Condition is satisfied.

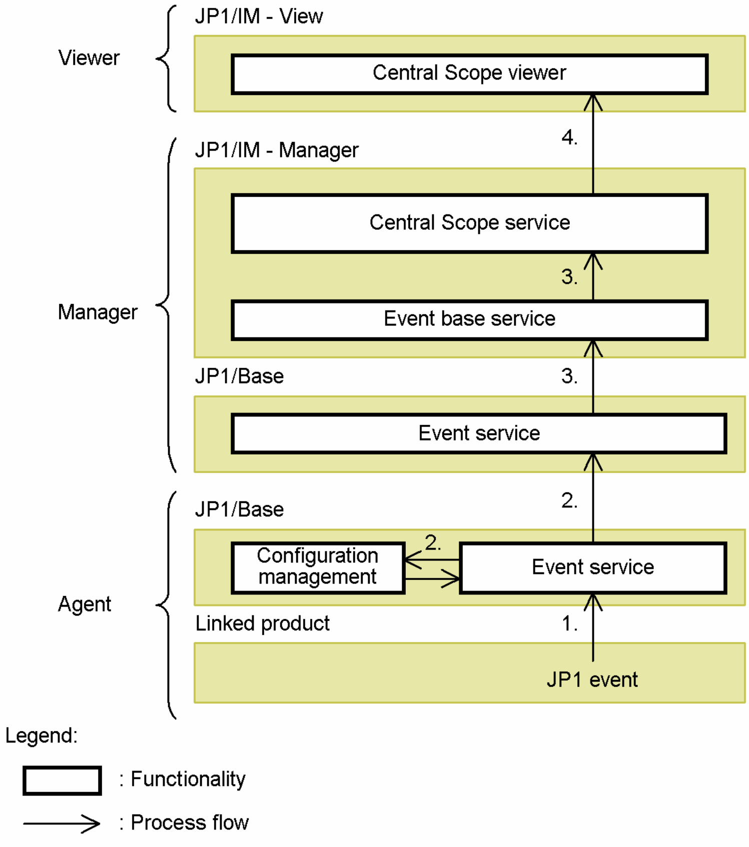
If `E.OBJECT_ID` of a JP1 event is `111.111.111.111`: Condition is satisfied.

4.11.3 System monitoring using the Central Scope

The Central Scope visually represents events occurring in the system by analyzing JP1 events, determining where they occurred in the monitoring tree, and changing the status of the icon at that location.

The following figure shows the flow of processing.

Figure 4–29: Flow of processing to change the status of a monitoring object



The flow of processing is described below, following the numbers in the figure:

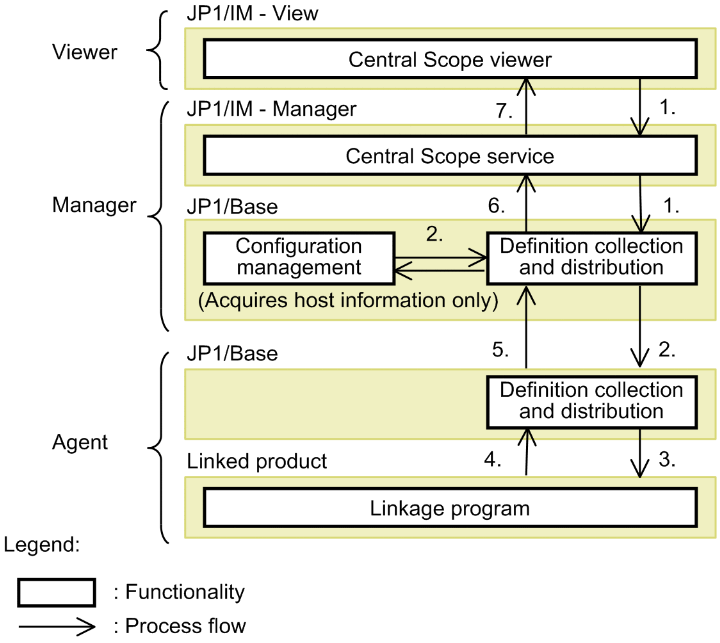
1. A JP1 event is generated on the agent and is registered with the event service.
2. The registered JP1 event is forwarded to a higher-level manager. The higher-level manager is determined from the configuration definitions of the configuration management function.
   The event base service on the manager acquires the JP1 event from the event service. The event base service is solely responsible for processing JP1 events in JP1/IM. (For details about JP1 event acquisition and JP1 event control within JP1/IM - Manager, see *3.1.3 Internal control of JP1 events by JP1/IM - Manager*.)
3. The JP1 event is passed to JP1/IM - Manager (Central Scope service), which analyzes the JP1 event, determines its severity, and associates it with a position in the monitoring tree.
   The monitoring objects database is used for these processes.
4. The system event is displayed visually in the Central Scope viewer (Monitoring Tree window and Visual Monitoring window) of JP1/IM - View.

In this way, the JP1 events generated on the agents in the system are accumulated on the JP1/IM managers, and the system is represented visually in the monitoring windows.

4.11.4 Automatic generation of a monitoring tree

The flow of processing in automatic generation of a monitoring tree when the work-oriented tree or server-oriented tree is selected as the template is described below. The following figure is an example.

Figure 4–30: Flow of processing to automatically generate a monitoring tree (when the work-oriented tree or server-oriented tree is selected)



The flow of processing is described below, following the numbers in the figure:

1. An auto-generation request is sent from a window on the viewer to JP1/IM - Manager on the manager. On receiving the request, JP1/IM - Manager instructs JP1/Base on the manager to collect the monitoring objects (definition information) that will constitute the monitoring tree.
2. On receiving the collection instruction, JP1/Base (definition collection and distribution function) on the manager references the configuration definition (configuration management) information and sends collection requests to JP1/Base on the agents.
3. On receiving the collection request, JP1/Base on each agent requests the linked product (which supports the JP1/Base definition collection and distribution function) on that host to forward the required definition information.
4. On receiving the request, the linked product passes the definition information to JP1/Base on that agent. (This information will be the source data for defining the monitoring objects.)
5. JP1/Base on each agent forwards the transferred definition information to JP1/Base on the manager.
6. JP1/Base on the manager passes the received definition information to JP1/IM - Manager, which re-organizes the data into monitoring objects.

   At this point, the definition information is not yet saved to the object database managed by JP1/IM - Manager.
7. JP1/IM - Manager passes the re-organized monitoring object information to JP1/IM - View. The information appears in tree format in the JP1/IM - View windows.

   If the generated monitoring tree and objects are adequate for your requirements, you can save them to the manager and immediately begin monitoring from JP1/IM - View. If any adjustments are needed, you can modify the tree configuration and monitoring object definitions, and then save the changes to the manager. (For details about how to modify a monitoring tree, see *4.4 Editing a monitoring tree*.)

4.11.5 Central Scope databases

The Central Scope has two databases: a *monitoring objects database* and a *host information database*.

- Managing the monitoring objects database

  The monitoring objects database is managed by JP1/IM - Manager and contains the object information displayed in JP1/IM - View.

  This database is updated on request from JP1/IM - View and on receipt of a JP1 event that changes the status of a monitoring object.

  Note that the following processing to update the monitoring objects database might take some time to complete:

  - Updating a server tree from the Monitoring Tree (Editing) window
  - Importing database information to the monitoring objects database by the `jcsdbimport` command

  If the OS shuts down, or if a failover occurs in a cluster system, while this update processing is in progress, the database could become corrupted.

  To prevent corruption of the database, JP1/IM provides an automatic backup and recovery function. When this function is enabled, the database is automatically backed up before either of the above types of update processing is performed, and is automatically restored to its former state if a problem occurs. If the update processing is successful, the backup data is automatically deleted.

  This function is enabled for a new installation of JP1/IM, but is disabled when an upgrade installation is performed. To enhance the system's fault tolerance, we recommend that you enable the function if upgrading JP1/IM.

  To enable the function, prepare an automatic backup and recovery settings file (`auto_dbbackup_`*xxx*`.conf`) for the monitoring objects database, and then apply the setting using the `jbssetcnf` command.

- Managing the host information database

  The host information database contains information specific to JP1/IM - Manager (Central Scope) and is managed within JP1/IM - Manager (Central Scope).

You can import and export information to the Central Scope databases using the commands shown in the table below.

Table 4–11: Commands for importing and exporting database information

Command name	Purpose
`jcsdbexport` command	Acquire information from the monitoring objects database.
`jcsdbimport` command	Save information to the monitoring objects database.
`jcshostsexport` command	Acquire information from the host information database.
`jcshostsimport` command	Save information to the host information database.

You can check database information using the `jcs`*xx*`export` commands, and you can migrate the environment to another server using the `jcs`*xx*`export` commands in conjunction with the `jcs`*xx*`import` commands.

The following describes how to migrate the tree configuration information and the status change conditions for monitoring objects from the local Central Scope to another server.

(1) Using commands (jcsdbexport and jcsdbimport) for migration

1. On the migration-source server, execute the `jcsdbexport` command.

   The information stored in the monitoring object database is locally output as a tree configuration file.

   The information output in this tree configuration file contains monitoring tree configuration information, common event monitoring conditions, and the information about Visual Monitoring window configuration.

2. Transfer the output file to the migration-destination server.

3. On the migration-destination server, execute the `jcsdbimport` command.

The data in the monitoring object database on the migration-source server is applied on the monitoring-destination server.

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

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

(2) Using the GUI for migration

1. On the migration-source server, in the Monitoring Tree (Editing) window, select **File**, and then choose **Save Tree** to save the output CSV file.

   The information output to the CSV file contains the monitoring tree configuration information about the currently displayed tree and common event monitoring conditions. The information about Visual Monitoring window configuration is not output. Note that the output information also includes the changes in information for which the menu command **Update Server Tree** has not been executed.

2. Transfer the output CSV file to the migration-destination server.

3. On the migration-destination server, in the Monitoring Tree (Editing) window, select **File**, and then choose **Open Tree** to read the CSV file.

4. On the migration-destination server, in the Monitoring Tree (Editing) window, select **File** and then **Update Server Tree**.

   The data in the monitoring object database on the migration-source server is applied on the monitoring-destination server.

(3) Notes on migrating the tree configuration information and the status change conditions for monitoring objects from the local Central Scope to another server

- To migrate the information about Visual Monitoring window configuration, use the `jcsdbexport` and `jcsdbimport` commands, which can output and input all information with a single execution. If you use the GUI, you need to read the CSV file (output by selecting **Save Visual Monitoring Data**) by selecting **Open Visual Monitoring Data** on the migration-destination server.
- The format of the output file differs between the migration using commands and the migration using the GUI. Therefore, the file output by using a command cannot be input by using the GUI, or the file output by using the GUI cannot be input by using a command.

5 Command Execution by Automated Action

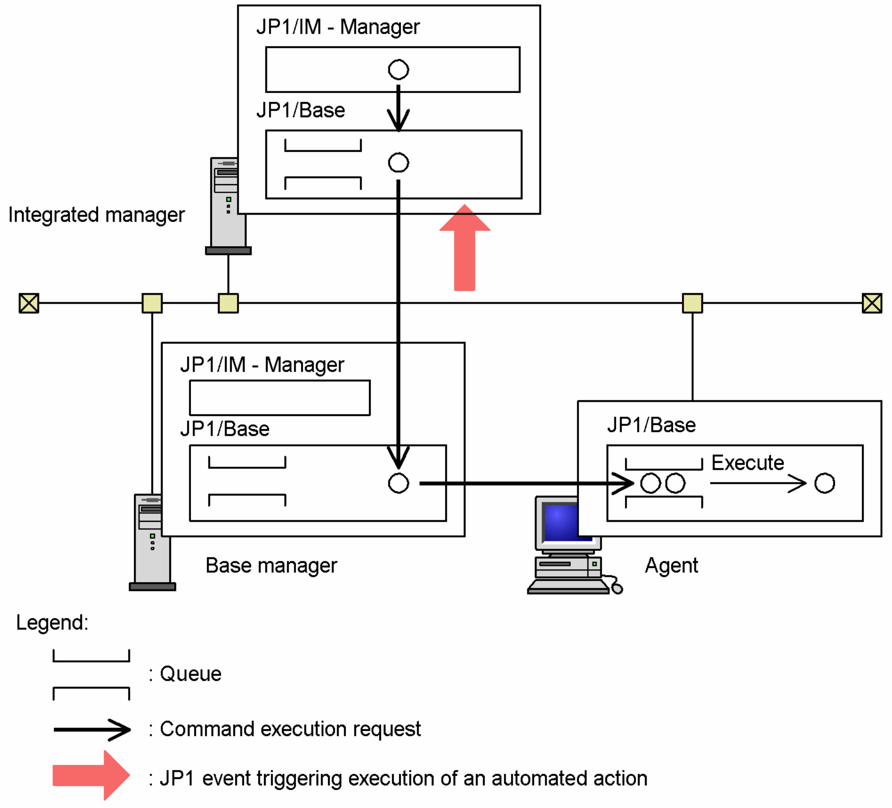
This chapter describes the automated action function provided by JP1/IM - Manager.

5.1 Overview of automated actions

In JP1/IM, you can execute a command automatically when a specific JP1 event is received by a manager. This function is called *automated actions*.

By using automated actions, you can advise the system administrator, by executing a command that sends an email or makes a phone call, whenever a JP1 event reporting an error is received, for example.

Figure 5–1: Overview of automated actions



By defining the following items, you can execute a specified command as an automated action under set conditions.

- Define the automated action to be executed:
  - Specify a condition for executing the automated action.
  - Specify the command to be executed as an automated action, the target host, the user account, and whether identical actions are to be suppressed#
- Set the environment for executing the automated action:
  - Customize the automated action execution environment.
  - Set up user mapping on the target host.

# You can suppress identical actions in the following ways:

- Suppress automated actions to suppress identical actions.
  For details, see *5.4.4 Suppressing identical actions*.
- Suppress the monitoring of repeated events to suppress actions.
  For details, see *3.5.8 Suppressing the execution of automated actions triggered by a large number of events*.

In addition to identical-action suppression, you can also use the following ways to prevent automated actions from being executed:

- Use common exclusion-conditions to exclude events from action execution.

  For details, see *3.2.7 Common exclusion-conditions*.
- Disable the action definition through the Action Parameter Definitions window in JP1/IM - View.

  For details, see *2.32 Action Parameter Definitions window* in the manual *JP1/Integrated Management - Manager GUI Reference*.
- Disable the action definition with the `jcachange` command.

  For details, see *jcachange* in *Chapter 1. Commands* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

JP1/IM provides the following functionality to enable early detection of any problems during processing of an automated action.

- Automated action execution monitoring
  - Monitoring for delayed automated actions
  - Monitoring of automated action status

The next section describes how JP1/IM manages the status of automated actions. The following sections describe how to define an automated action, and the processes of monitoring and executing automated actions.

Important

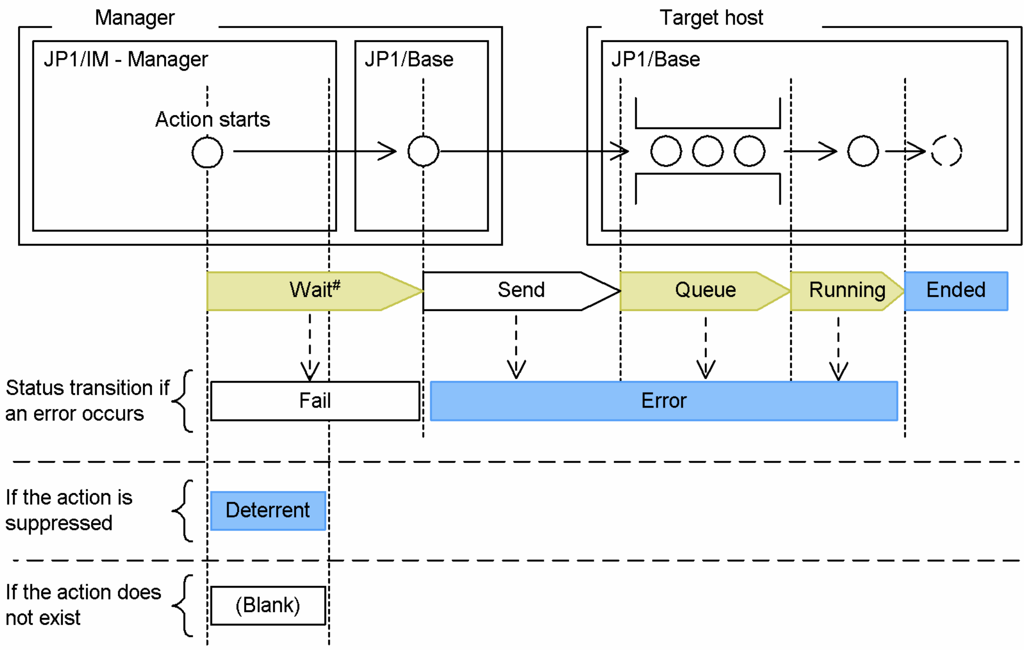
When the automated action function requests a large number of agents at once to execute a command, a heavy load might be applied on the manager host. To reduce the load, we recommend that you divide the agents into host groups and then execute the command for each group.

5.2 Managing the status of automated actions

When an automated action is executed, the processing is carried out through JP1/IM - Manager and JP1/Base. JP1/IM manages the processing in its domain as the action *status*.

The following figure shows in diagrammatic form the status transition of an automated action.

Figure 5–2: Status transition of an automated action



Legend:

🟨 : The action can be canceled.

🟦 : The action can be re-executed.

#: Occurs only if a retry is performed during the transfer of processing from JP1/IM - Manager to JP1/Base.

The flow of processing is always from JP1/IM - Manager to JP1/Base on the manager, and then from JP1/Base on the manager to JP1/Base on the target host. When the processing is successful, the status transition is `Send`, `Queue`, `Running`, and `Ended`, in that order. When the send buffer to JP1/Base is full, the status transition is `Wait`, `Send`, `Queue`, `Running`, and `Ended`, in that order. If an error occurs, the action status is set to `Fail` or `Error`, and processing terminates.

In the following cases, the status of the automated action is `Deterrent` or blank, and the processing terminates within JP1/IM - Manager:

- *Suppress* is set and the automated action meets the specified suppression conditions.

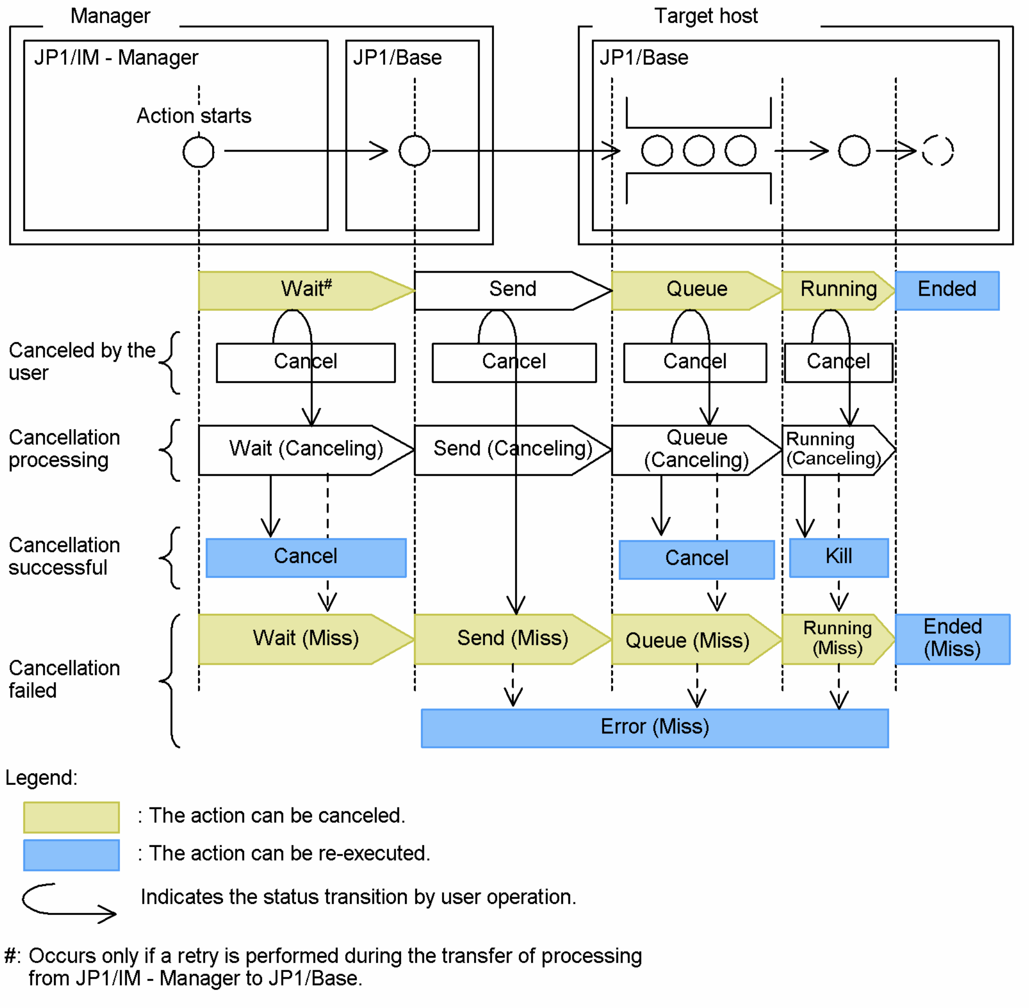
  In this case, the status of the automated action is set to `Deterrent`, and processing terminates without the command being executed (for details, see *5.4.4 Suppressing identical actions*).

- An execution condition has been set for the automated action, but the action definition (command to be executed) has not been set.

  In this case, the automated action is executed, but because there is no command to execute, its status is blank and processing ends.

An automated action can be canceled while its status transition is still in progress (`Wait`, `Queue`, or `Running` status), but not while in `Send` status. The following figure shows the status transition when an automated action is canceled.

Figure 5–3: Status transition when an automated action is canceled



Legend:

🟨 : The action can be canceled.

🟦 : The action can be re-executed.

Indicates the status transition by user operation.

#: Occurs only if a retry is performed during the transfer of processing from JP1/IM - Manager to JP1/Base.

When an action in `Wait`, `Queue`, or `Running` status is canceled unsuccessfully, it remains in the same status instead of shifting to `Cancel` or `Kill`.

When an action in `Send` status is canceled unsuccessfully, its status becomes `Send (Miss)`.

When a cancellation request is issued for an action in `Send` status, the deletion processing is not performed until the action execution request is queued in JP1/Base on the target host. Depending on the action status when the cancellation request reaches JP1/Base, the cancellation processing might fail. If the action has reached `Ended` or `Error` status, cancellation fails.

The following table describes details about action statuses.

Table 5–1: List of automated action statuses

Status	Description
`Wait`	Because the send buffer[#1] is full, JP1/Base declined the execution request from JP1/IM - Manager, which is now waiting to retry. (This status is cleared as soon as the buffer becomes available.)
`Send`	The execution request from JP1/IM - Manager is being sent from JP1/Base on the manager to JP1/Base on the target host.
`Queue`	The execution request from JP1/IM - Manager is queued in JP1/Base on the target host. If this status persists for some time, the following problem might have occurred in JP1/Base:

Status	Description
	• More automated actions are being generated than anticipated at the system design stage, leading to a massive backlog of redundant actions in the queue. In this situation, you can cancel the redundant automated actions using the JP1/IM cancellation function (for details, see *5.7 Canceling automated actions*).
`Running`	The execution request from JP1/IM - Manager is being executed by JP1/Base on the target host. If this status persists for some time, the following problem might have occurred in JP1/Base: • A command executed by a previous automated action has hung or is taking longer than expected to complete. Subsequent automated actions cannot be executed for that reason. In this situation, you can cancel the automated action that caused the problem using the JP1/IM cancellation function (for details, see *5.7 Canceling automated actions*).
`Ended`	The command has completed execution in JP1/Base, and the action result has been reported to JP1/IM - Manager. The action result has already been logged to the action re-execution file at startup of the automatic action service. This status is not affected by value of the result code (`E.RESULT_CODE`).
`Fail`	An error occurred before the execution request was passed to JP1/Base. The reason is: • An internal error occurred in the automatic action service; • JP1/Base (command execution management) that performs the processing is inactive; or • No host has been registered in the business or monitoring group specified as the execution target host.
`Error`	An error occurred in processing at the JP1/Base side, and command execution failed. In this situation, the text of the message (KAVB*xxxx*-E) output by JP1/Base is passed to JP1/IM - Manager as the action result. For the texts of the messages output by JP1/Base, see *2.3 Messages related to command execution (KAVB2001 to KAVB2999)* in the manual *JP1/Integrated Management - Manager Messages*.
`Deterrent`	A JP1 event met the condition for executing the automated action, but it occurred within the specified suppression time. Therefore, the action was suppressed (for details, see *5.4.4 Suppressing identical actions*).
(blank)	An automated action with a set execution condition, but without a set action definition (command to be executed), has been executed.
`Wait (Canceling)`	Cancellation processing is being executed for an automated action in `Wait` status (the cancellation processing is incomplete).
`Send (Canceling)`	Cancellation processing is being executed for an automated action in `Send` status (the cancellation processing is incomplete).
`Queue (Canceling)`	Cancellation processing is being executed for an automated action in `Queue` status (the cancellation processing is incomplete).
`Running (Canceling)`	Cancellation processing is being executed for an automated action in `Running` status (the cancellation processing is incomplete).
`Cancel`	An automated action was canceled before it reached `Running` status.
`Kill`	An automated action was canceled (killed) while in `Running` status.
`Wait (Miss)`	An automated action was canceled while in `Wait` status, but the processing failed.
`Send (Miss)`	An automated action was canceled while in `Send` status, but the processing failed. Or, an automated action was canceled unsuccessfully while in the previous status (`Wait`), and then shifted to `Send` status.
`Queue (Miss)`	An automated action was canceled while in `Queue` status, but the processing failed. Or, an automated action was canceled unsuccessfully while in a previous status (`Wait` or `Send`), and then shifted to `Queue` status.
`Running (Miss)`	An automated action was canceled while in `Running` status, but the processing failed. Or, an automated action was canceled unsuccessfully while in a previous status (`Wait`, `Send`, or `Queue`), and then shifted to `Running` status.

Status	Description
`Ended (Miss)`	An unsuccessfully canceled action is in `Ended` status.
`Error (Miss)`	An unsuccessfully canceled action is in `Error` status.
`Unknown`#2	The execution result of an automated action cannot be verified because a problem of some sort has caused inconsistencies in the files containing execution results (action information file, action hosts file, and command execution log file). In this case, you must delete the files. Once these files are deleted, the execution results of past automated actions cannot be referenced. For the deletion procedure, see *10.5.1(10) Actions to take when Unknown is displayed as the automated action execution status* in the *JP1/Integrated Management - Manager Administration Guide*.

#1: The buffer used when sending a request to execute an automated action from JP1/IM - Manager to JP1/Base on the manager.

#2: This is not an action status, but indicates that JP1/IM - Manager was unable to acquire the status of the automated action.

When the automated action definition is disabled, the action is not executed. That is, the status does not change and thus the action status is not stored in the action information file.

You can check the execution status of an automated action in JP1/IM - View or by executing a command. For details, see *5.6 Checking the execution status and results of automated actions*.

5.3 Defining an automated action

You can define an automated action in either of two ways: Using the Action Parameter Definitions window in JP1/IM - View, or by creating an automated action definition file and applying its contents using the `jcachange` command.

JP1/IM provides an automated action definition file and an automatic action definition file (for compatibility). The Action Parameter Definitions window differs depending on which of these two files you are using.

For details about the contents you can define in an automated action definition file and automatic action definition file (for compatibility), see the references given in the following table.

Table 5–2: References for defining an automated action

Version information (value of DESC_VERSION)	Version of the automated action definition file	Action Parameter Definitions window	Further details about the automated action definition file	Further details about the Action Parameter Definitions window
`1`	Indicates that the automated action definition file is version 08-01.	Action Parameter Definitions (for compatibility) window	See *Automated action definition file (actdef.conf) (for conversion)* in *Chapter 2. Definition Files* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.	See *2.33.2 Action Parameter Detailed Definitions (for compatibility) window* in the manual *JP1/Integrated Management - Manager GUI Reference*.
`2`	Indicates that the automated action definition file is version 08-01.			
`3`	Indicates that the automated action definition file is version 09-00 to 11-10.	Action Parameter Definitions window	See *Automated action definition file (actdef.conf)* in *Chapter 2. Definition Files* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.	See *2.32 Action Parameter Definitions window* in the manual *JP1/Integrated Management - Manager GUI Reference*.
`4`	Indicates that the automated action definition file is version 11-50 or later.	Action Parameter Definitions window (A check box appears allowing you to enable or disable the automated action definition.)		

When a value other than 1 to 4 is specified in `DESC_VERSION`, version information "3" is assumed.

When `DESC_VERSION` is unspecified, the automatic action definition file (for compatibility) (version information "2") is assumed.

We recommend that you check the contents of the definition file by executing the `jcamakea` command.

Important

The action definition file for migration (`replaceactdef.conf`) is supplied for compatibility when using version 5 of the automated action function. You cannot simply edit this file for use with version 09-00 or later. Instead, create an `actdef.conf` file that matches the contents of `replaceactdef.conf`. For details about the automated action definition files, see *Automated action definition file (actdef.conf)* and `ACTIONDEFFILE` in *Automated action environment definition file (action.conf.update)* in *Chapter 2*.

Definition Files in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

You cannot use both `replaceactdef.conf` and `actdef.conf`.

5.3.1 Items that can be specified as execution conditions

You can specify any of the following items as a condition for executing an automated action:

- JP1 event ID
  Specify the event ID of the JP1 event that triggers the automated action. You can select All IDs or specify a particular event ID.
- Event condition
  Specify the event condition of the JP1 event that triggers the automated action. The items you can specify depend on whether you are using an automated action definition file or automatic action definition file (for compatibility).

Table 5–3: Specifiable event conditions

Attribute		Item	Event condition#1	
			Automated action definition file	Automatic action definition file (for compatibility)
Basic attribute		Registered reason	• Match • Does not match	--
		Event ID	• Match • Does not match • Regular expression	• Match • Regular expression
		Source process ID		• Regular expression
		Source user ID		
		Source group ID		
		Source user name	• Match • Does not match • Is contained • Is not contained • First characters • Regular expression	
		Source group name		
		Source event server name		
		Source IP address		
		Event details		
		Message		
		Registered time	• Regular expression • *YYYYMMDDhhmmss* format (*YYYY*: year, *MM*: month, *DD*: day, *hh*: hour, *mm*: minute, *ss*: second)	• Regular expression • *YYYY*/*MM*/*DD* *hh*:*mm*:*ss* format (*YYYY*: year, *MM*: month, *DD*: day, *hh*: hour, *mm*: minute, *ss*: second)
		Arrived time		--
Extended attribute	Common information	Start time	• Regular expression (specifying cumulative seconds)	• Regular expression (specifying cumulative seconds)
		End time		

Attribute		Item	Event condition#1	
			Automated action definition file	Automatic action definition file (for compatibility)
		Product name	• Match • Does not match • Is contained • Is not contained • First characters • Regular expression	• Regular expression
		Object type		
		Object name		
		Root object type		
		Root object name		
		Object ID		
		Occurrence		
		User name		
		Result code		
		Source host name#2	• Match • Does not match • Is contained • Is not contained • First characters • Regular expression	--
		Event level	• Match#2 • Regular expression	• Match#3 • Regular expression
	Program-specific information	`E.`	• Match • Does not match • Is contained • Is not contained • First characters • Regular expression	• Regular expression
For compatibility		Basic event information	• Regular expression	

Legend:

--: None

#1: By default, only extended regular expressions can be specified in comparison conditions. For details about regular expressions, see *Appendix G. Regular Expressions*. However, if you have upgraded from a previous version of JP1/IM - Manager, the information set in the previous version is carried over.

If you are using version 8 or earlier of JP1/IM - View, you can edit event conditions only if you are using the automatic action definition file (for compatibility).

#2: To specify the source host name in the automatic action definition file (for compatibility), specify `E.JP1_SOURCEHOST (`Event source host name`)` as an item of the program-specific information of the extended attributes.

#3: You can specify the following attribute values: `Emergency`, `Alert`, `Critical`, `Error`, `Warning`, `Notice`, `Information`, and `Debug`.

When `DESC_VERSION` is `4`, the automated action definition file (`actdef.conf`) allows you to specify the following:

- Use the `aid` parameter to specify an ID of the action definition to be enabled or disabled.
- Use the `valid` parameter to enable or disable the action definition.

5.3.2 Precedence of execution conditions

If a JP1/IM manager receives a JP1 event, the JP1/IM manager compares the JP1 event with the execution conditions defined in the automated action definitions in order of priority for each parameter group. An execution condition that matches the JP1 event and that has the highest priority is executed for each parameter group.

The priority is set with the ACTIONPRIORITY parameter in the automated action environment definition file, and applied to the JP1 common definition information. As an option, you can specify DEFAULT or V8COMPATIBLE.

After JP1/IM - Manager is installed, DEFAULT is set for the ACTIONPRIORITY parameter.

After JP1/IM - Manager is upgraded, the ACTIONPRIORITY parameter is not set. When the ACTIONPRIORITY parameter is not set, V8COMPATIBLE (the priority for executing automated actions when JP1/IM - Manager version 8 or earlier is used) is used.

If DEFAULT is specified for the ACTIONPRIORITY parameter, automated actions are executed in the order set in the automated action definitions (the order described in actdef.conf).

If you specify V8COMPATIBLE for the ACTIONPRIORITY parameter, the automated actions are executed in the following priority: First, the definition information for the automated actions for which the relevant event ID is explicitly specified is judged in the order set in the automated action definitions (the order described in actdef.conf). Then, the execution conditions for the automated action definition for which * is specified for the relevant event ID are judged.

The following table shows how the order of precedence differs between DEFAULT and V8COMPATIBLE when the specified event ID is 00000001, 00000002, or All IDs.

Table 5–4: Difference in action precedence when the event IDs 00000001, 00000002, and "All IDs" are specified in that order in the definition file

Event ID	Order in the definition file	Parameter group	Precedence with the DEFAULT option	Precedence with the V8COMPATIBLE option
00000001	1	1	1	1
00000002	2	1	2	2
All IDs	3	1	3	3

Table 5–5: Difference in action precedence when the event IDs "All IDs", 00000001, and 00000002 are specified in that order in the definition file

Event ID	Order in the definition file	Parameter group	Precedence with the DEFAULT option	Precedence with the V8COMPATIBLE option
All IDs	1	1	1	3
00000001	2	1	2	1
00000002	3	1	3	2

Table 5–6: Difference in action precedence when the event IDs 00000001, "All IDs", and 00000002 are specified in that order in the definition file

Event ID	Order in the definition file	Parameter group	Precedence with the DEFAULT option	Precedence with the V8COMPATIBLE option
00000001	1	1	1	1
All IDs	2	1	2	3

Event ID	Order in the definition file	Parameter group	Precedence with the `DEFAULT` option	Precedence with the `V8COMPATIBLE` option
00000002	3	1	3	2

5.3.3 Parameter groups and AND condition

By using parameter groups and AND conditions, you can set complex conditions for executing automated actions.

- Parameter groups

  A parameter group is a set of judgment conditions for executing an automated action. There are 10 parameter groups. Each automated action definition belongs to one parameter group only.

  You can use parameter groups to execute multiple actions in response to one event, or to associate multiple execution conditions using an AND condition (as explained later). A parameter group is specified with one-digit number (0 to 9).

  If a JP1/IM manager receives a JP1 event, the JP1/IM manager compares the JP1 event with the execution conditions of the action definition parameters for each parameter group, from the parameter group with the smallest number to the parameter group with the largest number. Only one automated action is executed for a JP1 event for each parameter group.

  If multiple execution conditions match an event in a parameter group, only the action definition parameter with the highest priority is executed (as explained in *5.3.2 Precedence of execution conditions*).

  If multiple action conditions match a JP1 event, command execution requests are issued to the JP1/Base in the order the comparison of the action conditions is performed. However, command execution requests might not be performed in order if execution requests are issued to multiple hosts or if two or more commands are executed concurrently.

- AND condition

  An AND condition is a setting that requires all the execution conditions to be satisfied before an action is executed.

  When an ampersand (`&`) is specified instead of a number in a parameter group specification, the relationship with the preceding execution condition in the automated action definition (displayed one line above in the GUI, or written one action block above in the definition file) is handled as an AND condition. You can define a maximum of 10 automated action definitions joined by an AND condition.

  When a received event matches one of the execution conditions joined by an AND condition, it waits for another event matching another execution condition to be received. When all the execution conditions joined by the AND condition are satisfied, the automated action is executed.

  However, disabled automated action definitions are not evaluated to determine whether to execute the automated action.

  You can specify an AND-event keep limit as a timeout for the AND condition to be satisfied. If the required JP1 event arrives after expiry of the AND-event keep limit, it does not satisfy the AND condition.

  Note that when the event base service (`evflow` process) stops, all events waiting for an AND condition to be satisfied are discarded. Take care if the system is restarted, by process management after an error, for example, or in a cluster system when a failover occurs.

When `DESC_VERSION` of the automated action definition file (`actdef.conf`) is `4`, with one of the operations listed below, you can ensure that the status of a satisfied AND-joined condition remains the same unless the automated action definition of the conditions is changed.

- In the Action Parameter Definitions window, select the **Retain the conditions for which the definition was not changed** check box and click the **Apply** button.
- Execute the `jcachange` command with the `-on`, `-off`, `-e`, or `-st` option specified.

When DESC_VERSION is 3 or earlier or when you use any way other than those listed above to update the action definition, the status (satisfied or unsatisfied) of every AND-joined condition is initialized.

5.3.4 Inherited event information

When defining an automated action, by using a variable you can specify information about the JP1 event that triggers the action as inherited event information. Inherited event information can be specified for the following items:

- Target host
- Execution user name
- Environment variable file
- Action

JP1 event attribute values are inherited to automated actions when those values are handed from the event base service to the automatic action service.

The following table lists the inherited event information you can specify.

Table 5–7: Variables that can be specified in an action definition

Attribute	Variable name	Inherited event information
Basic attribute	EVBASE	• Basic event information
	EVID	• Event ID (*basic-code*:*extended-code*) Event ID as a character string in the format *basic-code*:*extended-code*.
	EVIDBASE	• Event ID (*basic-code*) Event ID as a character string in the format *basic-code*.
	EVDATE	• Date when the event was registered (*YYYY*/*MM*/*DD*) Registered time as a character string in the format *YYYY*/*MM*/*DD*.
	EVTIME	• Time when the event was registered (*hh*:*mm*:*ss*) Registered time as a character string in the format *hh*:*mm*:*ss*.
	EVPID	• ID of the process that issued the event Value of the source process ID.
	EVUSRID	• User ID of the process that issued the event Value of the source user ID.
	EVGRPID	• Group ID of the process that issued the event Value of the source group ID.
	EVUSR	• User name of the process that issued the event Value of the source user name.
	EVGRP	• Group name of the process that issued the event Value of the source group name.
	EVHOST	• Host name of the server that issued the event Value that depends on the HOSTINEVENT parameter value in the automated action environment definition file: - remote: Name of the server that issued the event - local: Host name obtained from the IP address of the server that issued the event

Attribute	Variable name	Inherited event information
	EVIPADDR	• IP address of the server that issued the event Character string indicating the source IP address in IPv4 address format or IPv6 address format. <IPv4 address format> In this format, each 8 bits of a 32-bit address is delimited by periods (`.`), and is output as decimal numbers (from 0 to 255). Example: 0.64.128.255 <IPv6 address format> In this format, each 16 bits of a128-bit address is delimited by colons (`:`), and is output as hexadecimal numbers (from 0000 to ffff). Example: 0011:2233:4455:6677:8899:aabb:ccdd:eeff
	EVSEQNO	• Serial number in the event database Value of the serial number.
	EVARVDATE	• Date when the event arrived (*YYYY*/*MM*/*DD*) Arrived time as a character string in the format *YYYY*/*MM*/*DD*.
	EVARVTIME	• Time when the event arrived (*hh*:*mm*:*ss*) Arrived time as a character string in the format *hh*:*mm*:*ss*.
	EVSRCNO	• Serial number in the source event database Value of the source serial number.
	EVMSG	• Message Text of the message.
	EVDETAIL	• Detailed information about the event Event details as character strings in the format *Info-1*Δ*Info-2*Δ...*Info-n*Δ (where Δ represents a space).
Extended attribute	EVSEV	• Event level in the extended event information (`Emergency`, `Alert`, `Critical`, `Error`, `Warning`, `Notice`, `Information`, or `Debug`) Value of the event level.
	EVUSNAM	• User name Value of the user name.
	EVOBTYP	• Object type Value of the object type.
	EVOBNAM	• Object name Value of the object name.
	EVROBTYP	• Root object type Value of the root object type.
	EVROBNAM	• Root object name Value of the root object name.
	EV"PRODUCT_NAME"	• Product name Value of the product name.
	EV"OBJECT_ID"	• Object ID Value of the object ID.
	EV"OCCURRENCE"	• Occurrence Value of the occurrence.
	EV"START_TIME"	• Start time

Attribute	Variable name	Inherited event information
		Value of the start time.
	EV"END_TIME"	- End time Value of the end time.
	EV"RESULT_CODE"	- Result code Value of the result code.
	EV"JP1_SOURCEHOST"	- Source host name Value of the source host name.
	EV *extended-attribute-name*	- User-specified extended attribute Value of the attribute specified in the extended attribute name.
Other	EV"@JP1IM_CORRELATE"	- Correlation event Value indicating whether the event is a correlation event. - 0: Not a correlation event - 1: A correlation approval event - 2: A correlation failure event
	EV"@JP1IM_ORIGINAL_SEVERITY"	- Severity of extended event attributes (before changing the event level) (Emergency, Alert, Critical, Error, Warning, Notice, Information, Debug, or a value set for the event level) This attribute is set only when the severity changing function is enabled.
	EV"@JP1IM_CHANGE_SEVERITY"	- Severity changing A value indicating whether an event level has been changed. - 0: Not changed. - 1: Changed.
	EV"@JP1IM_DISPLAY_MESSAGE"	- Value of the message (after change) This attribute is set only when the display message change function is enabled.
	EV"@JP1IM_CHANGE_MESSAGE"	- Display message change Value indicating whether the display message has been changed; this attribute is set only when the display message change function is enabled: - 0: The message has not been changed. - 1: The message has been changed.
	ACTHOST	- Host name of the manager that requested execution of the action Manager host name.
	EVENV1 to EVENV9	- Data extracted by specifying "( )" in a regular expression in an action execution condition Can be specified only when extended regular expressions are used on the manager.

(1) Specification method

Inherited event information is specified using a variable. Specify the variable in the form $*variable-name*. To specify a dollar sign as a character, type a backslash (\) before the dollar sign (\$).

The following control characters contained in the character information to be converted are converted to single-byte spaces (0x20).

Control characters that are converted to single-byte spaces: `0x01` to `0x1F` (excluding tabs (`0x09`)), and `0x7F`

(2) Encoding of event inheritance information

For **Action** in the action-related items, you can URL encode or Base64 encode the event inheritance information values.

The specification format is `$`*variable-name*`$`*encoding-type*. To specify a single-byte alphanumeric character or an underscore (_) immediately after *encoding-type*, use the format `${`*variable-name*`$`*encoding-type*`}`. If you want to treat a dollar sign (`$`) as a character, specify the escape character (`\`) immediately before the `$`.

In the following cases, `$`*variable-name*`$`*encoding-type* and `${`*variable-name*`$`*encoding-type*`}` will be interpreted as character strings and will not be converted:

- There is no event that corresponds to *variable-name*.
- The specification format is invalid.

The following table describes the encoding types for event inheritance information and the specification formats.

Table 5–8: Encoding types for event inheritance information and specification formats

No.	Encoding type	Specification format	Description
1	URL encoding	`$`*variable-name*`$URLENC`	The event inheritance information value is URL encoded as a UTF-8 character string.
		`${`*variable-name*`$URLENC}`	
2	Base64 encoding	`$`*variable-name*`$ENC`	The event inheritance information value is Base64 encoded.
		`${`*variable-name*`$ENC}`	
3	Both Base64 encoding and URL encoding	`$`*variable-name*`$ENC$URLENC`	The event inheritance information value is Base64 encoded and then is URL encoded.
		`${`*variable-name*`$ENC$URLENC}`	
4	No encoding is performed	`$`*variable-name*	Neither URL encoding nor Base64 encoding is performed.
		`${`*variable-name*`}`	

Note that encoding of inheritance information cannot be used in the automated action definition file (for compatibility).

(3) Converting inherited event information

You can convert special ASCII characters included in inherited event information into a different character string.

This functionality allows you to convert characters in event information that have a special meaning in the OS into different characters. For example, if the JP1 event information specified by a variable contains characters that have a special meaning in commands, such as a double quotation mark (`"`) or a single quotation mark (`'`), the command might not be interpreted correctly. We recommend that you use the configuration file for converting information to convert such characters.

Specify the special characters and the characters they are to be converted into using a configuration file for converting information. For details about this file, see *Configuration file for converting information (event_info_replace.conf)* in *Chapter 2. Definition Files* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

5.4 Specifying a command to be executed as an automated action

The following describes how to specify the command to be executed as an action when the execution conditions are fulfilled.

5.4.1 Executable commands

The following types of commands can be executed as automated actions:

On a Windows host:

- Executable file (`.com` or `.exe`)
- Batch file (`.bat`)
- Script file of JP1/Script (`.spt`) (provided the `.spt` file extension is associated with JP1/Script so that it can be executed)
- Data file (including `.vbs`) that has a file type (extension) associated with an application that can be run as an automated action

On a UNIX host:

- UNIX command
- Shell script

However, the following types of commands cannot be executed:

- Commands that require interactive operation
- Commands that display windows
- Commands that use an escape sequence or control code
- Non-terminating commands such as daemons
- Commands (Windows only) that require interaction with the desktop, such as the Windows message structure or DDE
- Commands that shut down the OS, such as `shutdown` and `halt`

Important

In 64-bit editions of Windows, if you execute a command in the `%WINDIR%\System32` folder, the WOW64 redirection function redirects the command to a command in the `%WINDIR%\SysWow64` folder. If the command is not found in the destination folder, command execution might fail. Therefore, be careful when you specify a command in the `%WINDIR%\System32` folder as the execution command.

Important

If a command is executed by an automated action or from a command execution window and the executed command produces child processes, information such as the standard output of the child processes and detection of terminations is also acquired. However, if the executed command terminates before all of its child processes, the standard output of those child processes cannot be acquired. In addition, termination of those child processes cannot be detected correctly. This is because the command execution function manages only those commands that are executed directly. If an executed command produces child processes and grandchild processes, the child and grandchild processes must be managed by the command that is executed.

Important

When a command or automated action executes a Windows PowerShell script, the script might seem to continue running because `powershell.exe` cannot exit properly. To execute a Windows PowerShell scrip, use the following command line to redirect the script from standard input to `nul`:

```
powershell.exe xxx.ps1 < nul
```

5.4.2 Target host

As the target host on which to execute a command as an automated action, you can specify a JP1/IM agent or manager.

The agent must be defined in the configuration management information as a host managed by JP1/IM.

By defining multiple agents in a host group, you can execute the same command on multiple hosts.

5.4.3 User account

Specify the JP1 user under whose account the command is to be executed.

The command is executed under the name of the OS user mapped to that JP1 user on the agent.

If the target host is a Windows host, the OS user subject to user mapping must have Windows-specific user permissions. For details about the user permissions required for the OS user subject to user mapping, see the chapter on granting user permissions to OS users in the *JP1/Base User's Guide*.

5.4.4 Suppressing identical actions

You can suppress the execution of an automated action that is identical to a previous action and occurs within a set time after that action.

This applies to automated actions that only need to be executed once during a set time period, such as actions that flash a signal light or send a notification email to the user. If these sorts of automated actions were allowed to accumulate in the JP1/Base command execution queue, they could delay the execution of urgent actions, such as those that perform error recovery.

You can avoid such situations by suppressing automated actions that do not need to be executed more than once during a set duration.

You can enable or disable suppression, and set the suppression time, for individual actions. This allows you to build an environment that suppresses actions that do not need to be repeated and executes only those that are required.

Suppression is cleared for an automated action being suppressed when a process is restarted by the process management functionality or if a failover occurs in a cluster system.

You can suppress actions by using either the suppression settings or the function for suppressing repeated-event monitoring.

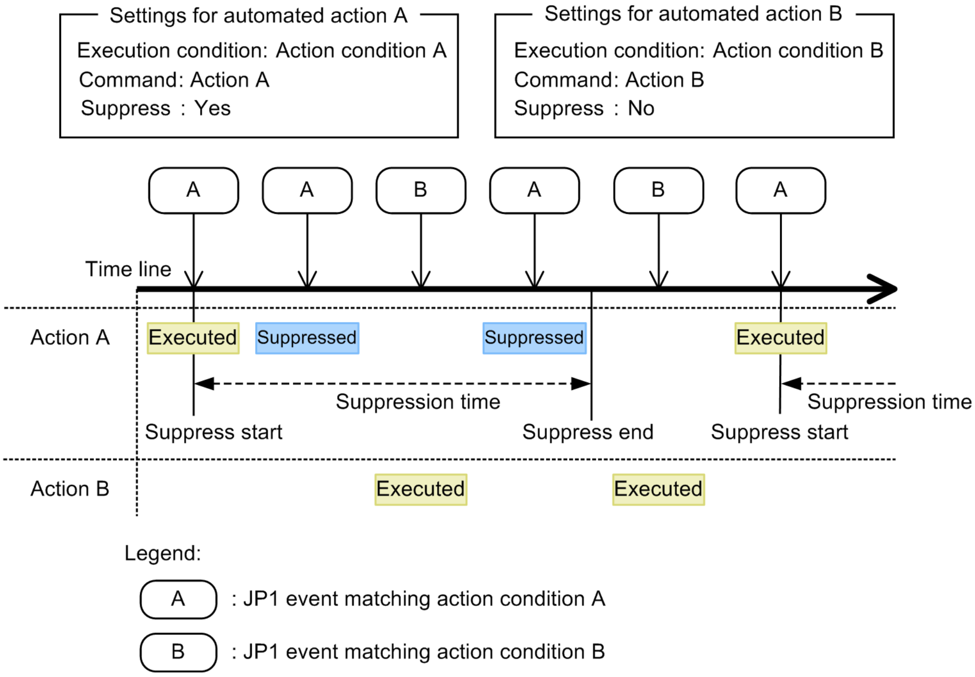
This subsection describes how the suppression settings for automated actions suppress actions. If you want to prevent automated actions from being executed in other ways, see the following sections:

- Use common exclusion-conditions to exclude events from action execution.
  3.2.7 Common exclusion-conditions
- Suppress the monitoring of repeated events to suppress actions.
  3.5.8 Suppressing the execution of automated actions triggered by a large number of events
- Disable the action definition through the Action Parameter Definitions window in JP1/IM - View.
  2.32 Action Parameter Definitions window in the manual *JP1/Integrated Management - Manager GUI Reference*
- Disable the action definition with the `jcachange` command.
  jcachange in *Chapter 1. Commands* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*

(1) Behavior of an automated action when suppression is enabled

The following figure shows how an automated action works when suppression is enabled.

Figure 5–4: Behavior of an automated action when suppression is enabled



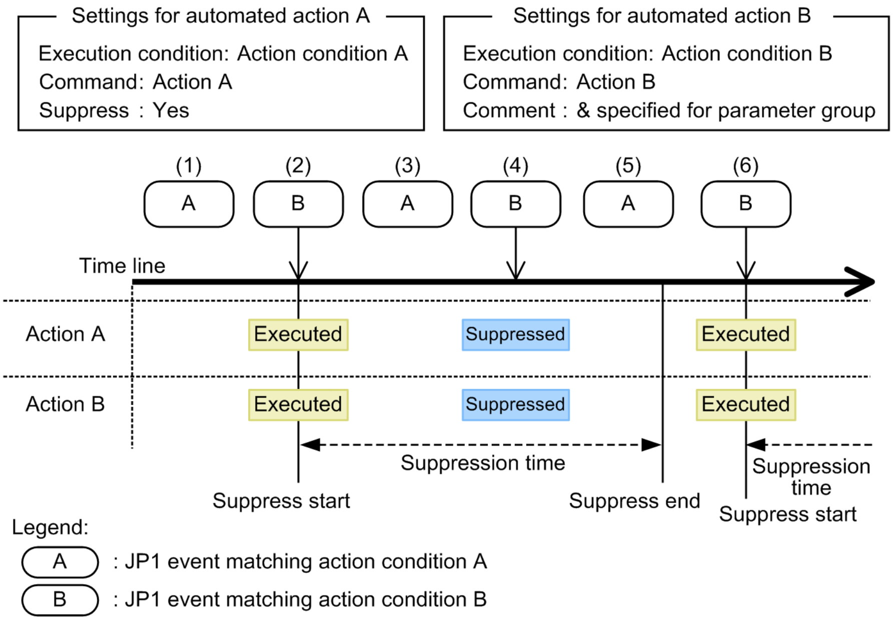
As shown by automated action A in the figure, when *Suppress* is set, the action is executed only in response to the first of multiple JP1 events that match the action's execution condition and occur within the set suppression time. The action is not executed for the second and subsequent identical JP1 events. The status of the unexecuted action is `Deterrent`.

As shown by automated action B in the figure, when *Suppress* is not set, the action is executed in response to every JP1 event that matches the action's execution condition (the behavior is unaffected by other JP1 events that are being suppressed).

(2) Behavior of automated actions joined by an AND condition when suppression is enabled

The following figure shows the behavior of automated actions joined by an AND condition when suppression is enabled.

Figure 5–5: Behavior of automated actions joined by an AND condition when suppression is enabled


Settings for automated action A
Execution condition: Action condition A
Command: Action A
Suppress : Yes
Settings for automated action B
Execution condition: Action condition B
Command: Action B
Comment : & specified for parameter group
(1)
A
(2)
B
(3)
A
(4)
B
(5)
A
(6)
B
Time line
Action A
Executed
Suppressed
Executed
Action B
Executed
Suppressed
Executed
Suppression time
Suppress start
Suppress end
Suppression time
Suppress start
Legend:
A
: JP1 event matching action condition A
B
: JP1 event matching action condition B

The automated action behavior is described below, following the numbers in the figure:

1. A JP1 event matching execution condition A is received by JP1/IM - Manager. The action is not executed yet because actions A and B are joined by an AND condition.
2. A JP1 event matching execution condition B is received by JP1/IM - Manager. Because a JP1 event matching condition A has been received, the AND condition is satisfied and actions A and B are executed.
3. A JP1 event matching execution condition A is received by JP1/IM - Manager (same situation as 1).
4. A JP1 event matching execution condition B is received by JP1/IM - Manager (same situation as 2). A JP1 event matching condition A has been received and the AND condition is therefore satisfied, but the suppression time set for action A is still in effect. Therefore, actions A and B are not executed; both are set to `Deterrent` status.
5. A JP1 event matching execution condition A is received by JP1/IM - Manager (same situation as 1).
6. A JP1 event matching execution condition B is received by JP1/IM - Manager (same situation as 2). Although a JP1 event matching condition A has been received within the suppression time for action A, this new event satisfying the AND condition was received after the suppression time elapsed. Therefore, actions A and B are not suppressed; both are executed.

5.5 Monitoring the execution of an automated action

JP1/IM - Manager provides functionality for monitoring the execution of automated actions so that any problems can be quickly detected. This is realized by the following two functions, which can each be set independently:

- Automated action delay monitoring
  Execution is monitored so that if the action fails to complete within a set time, the problem is detected and the user notified.
- Automated action status monitoring
  Action status is monitored so that if execution of an action fails, the problem is detected and the user notified.

5.5.1 Automated action delay monitoring

The following problems might occur during execution processing of automated actions:

- An action did not complete within the expected time.
- An action has not completed after a considerable time.

These types of problems affect the execution processing not only of the action in question but of subsequent actions too.

By monitoring the execution time of an automated action (delay monitoring), you can reduce the time it takes for the operator to respond to a problem. Any delay will be reported to the operator by a JP1 event or notification command.

For details on setting up delay monitoring, see *5.5.3 Setting up execution monitoring*.

(1) Delay monitoring start time and end time

Delay monitoring starts at the time when the JP1 event that triggers execution of the automated action arrives at JP1/Base on the manager.

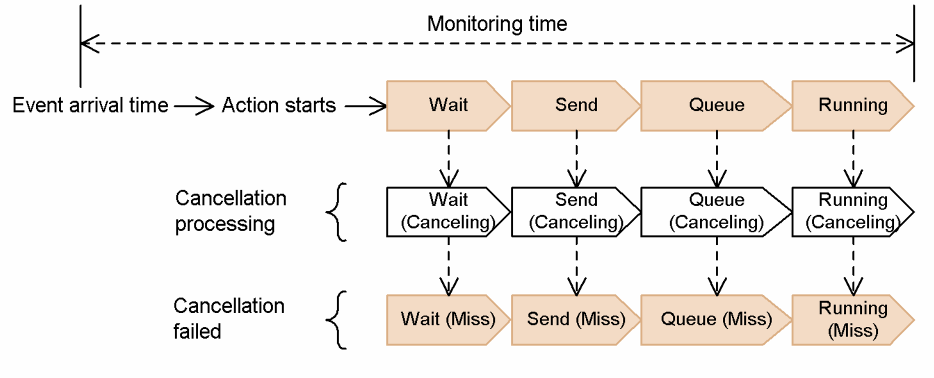
Delay monitoring ends when the action reaches one of the following statuses:

- `Ended`, `Cancel`, `Kill`, `Fail`, or `Error`
- `Ended (Miss)` or `Error (Miss)`

If the action fails to reach one of the above statuses within the time set for delay monitoring, its status becomes `Delay`.

The following figure shows the time frame and statuses monitored during delay monitoring.

Figure 5–6: Delay monitoring time and monitored statuses



When an automated action is re-executed at failover in a cluster system, the delay monitoring time and monitored statuses are no different from normal operation (the figure above). If you are using a cluster system, you must consider the time required for failing over the system when you set a delay monitoring time.

Important

Delay monitoring does not apply to an automated action that is re-executed manually. This is because you are re-executing the action yourself, and can see when it starts and how long it takes.

Also, automated actions whose status is displayed as blank or as `Deterrent` are not monitored for execution delays.

5.5.2 Automated action status monitoring

The following problem might occur during execution processing of automated actions:

- JP1/IM - Manager or JP1/Base detects an error, the action status consequently changes to `Fail`, `Error`, or `Error (Miss)`, and processing terminates.

Because the automated action fails to complete execution as the user intended, this type of problem has a major impact on monitoring jobs.

By detecting errors in automated action processing, you can reduce the time it takes for the operator to respond to a problem. Errors are reported to the operator by JP1 events and notification commands.

For details on setting up status monitoring, see *5.5.3 Setting up execution monitoring*.

5.5.3 Setting up execution monitoring

The functions for delay monitoring and status monitoring of automated actions are not enabled at installation and must be set up as required.

The table below describes the settings required to perform automated action delay monitoring and status monitoring. For details about the window, see the manual *JP1/Integrated Management - Manager GUI Reference*. For details about the definition file, see the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

Table 5–9: Settings required for delay monitoring and status monitoring

Function	Setting	Where
Delay monitoring	• Enable or disable delay monitoring • Delay monitoring time	Action Parameter Detailed Definitions window or the automated action definition file
	• Issue JP1 event	Automatic action notification definition file
	• Execute notification command	
Status monitoring	• Enable or disable status monitoring	Action Parameter Definitions window or automated action definition file
	• Issue JP1 event	Automatic action notification definition file
	• Execute notification command	

Delay monitoring can be set for an individual action, whereas status monitoring is set for the whole system (JP1/IM - Manager). JP1 events are issued by default: When monitoring is enabled, a JP1 event is issued on detection of an error. Notification commands are not executed by default: To execute a notification command on detection of an error, you must edit the automatic action notification definition file.

If you disable both JP1 events and notification commands, detected errors will not be reported to the user even if you set *Apply* for **Delay monitoring** or **Status monitoring**. You must specify either means of notification to perform delay monitoring or status monitoring.

5.5.4 Automated action error monitoring using the execution monitoring function

When delay monitoring or status monitoring is enabled, detected errors are reported to the user by means of a JP1 event or notification command.

However, notification via these monitoring functions is performed once only. Further notification is suppressed and any subsequent errors are not reported.

For this reason, when you have finished dealing with a problem reported by an automated action, you must re-enable notification: In the Event Console window of JP1/IM - View, choose **Options** and then **Function-Status Notification Return**.

5.6 Checking the execution status and results of automated actions

You can check the execution status and result of an automated action using the following:

- List of Action Results window, Action Log window, and Action Log Details window (for further specifics) in JP1/IM - View
- `jcashowa` command

  When you execute the `jcashowa` command, the results of executed automated actions that have been stored in the action information file are displayed.

To check the contents of the command execution log, use the `jcocmdlog` command.

A JP1 event can be issued to report the execution status of an automated action. Because JP1 events are not issued by default, you must change the settings for issuing JP1 events by specifying the `-actevent` option of the `jcocmddef` command.

5.7 Canceling automated actions

You can cancel automated actions whose status is any of the following:

- `Wait`, `Queue`, or `Running`
- `Send (Miss)`#, `Wait (Miss)`#, `Queue (Miss)`#, or `Running (Miss)`#

  #: Before you cancel an automated action in a status tagged `(Miss)`, you should identify and fix whatever caused the cancellation failure (`Miss`), by examining the execution result in detail (error log) or by conducting an event search to check what happened on the target host, for example.

When you cancel an automated action, its status is tagged as `(Canceling)`, and then becomes `Cancel` or `Kill`. If the cancellation processing fails, the action status is tagged as `(Miss)`, and then proceeds through the usual status transitions (for details, see *5.2 Managing the status of automated actions*).

You can cancel an automated action and check whether cancellation was successful using the following:

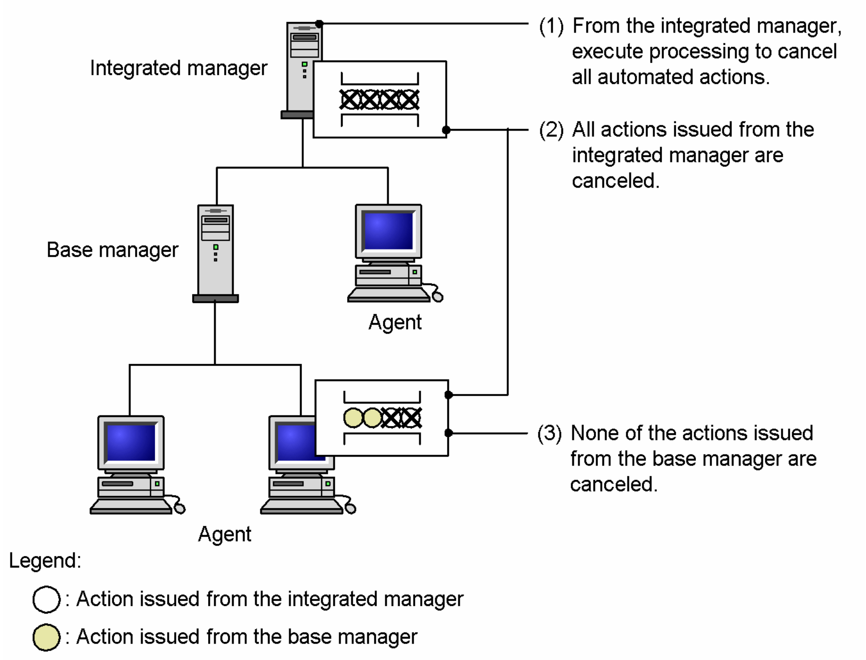
- List of Action Results window, Action Log window, and Action Log Details window (cancel only) in JP1/IM - View
- `jcacancel` command (cancel), `jcashowa` command (cancellation status check)

Range of actions that can be canceled

Only actions issued from the manager on which you are executing the cancellation processing can be canceled. That is, actions issued from a base manager cannot be canceled from the integrated manager.

The following figure shows the range of actions that can be canceled.

Figure 5–7: Range of actions that can be canceled


Integrated manager
(1) From the integrated manager, execute processing to cancel all automated actions.
(2) All actions issued from the integrated manager are canceled.
Base manager
Agent
(3) None of the actions issued from the base manager are canceled.
Agent
Legend:
○: Action issued from the integrated manager
●: Action issued from the base manager

As shown in the figure, when action cancellation processing is executed from the integrated manager, only those action issued from the integrated manager are affected. Because actions executed from the base manager are not affected, they are processed as usual on the agent. To cancel actions issued from the base manager, you must execute the cancellation processing from that host.

5.8 Re-executing an automated action

You can re-execute an automated action whose status is any of the following:

- `Deterrent`, `Ended`, `Error`[#], `Cancel`, or `Kill`
- `Ended (Miss)` or `Error (Miss)`[#]
  #: Before you re-execute an automated action in `Error` or `Error (Miss)` status, you should identify and fix whatever caused the error, by examining the execution result in detail (error log) or by conducting an event search to check what happened on the target host, for example.

When you re-execute an automated action, it proceeds through the same status transitions as when processed by the system (for details, see *5.2 Managing the status of automated actions*).

You can re-execute an automated action and check whether execution was successful using the following:

- List of Action Results window, Action Log window, and Action Log Details window (re-execute only) in JP1/IM - View
- `jcashowa` command (re-execution status check)

5.9 Operation settings for automated actions

As internal processing, JP1/IM acquires events from JP1/Base, judges whether each event is a JP1 event that triggers an automated action, and executes the appropriate action if so. There is usually no need to change this internal processing, but you can halt it temporarily when a large number of redundant automated actions have been generated due to maintenance or some other activity.

To change JP1/IM settings, use the `jcachange` command. To check the settings, use the `jcastatus` command.

If you suspend internal processing, no automated actions will be executed after the system is operational again for any events that might have been received while processing was suspended. Do not suspend internal processing if there is an automated action that needs to be executed.

Note

About the `jcachange` command and `jcastatus` command:

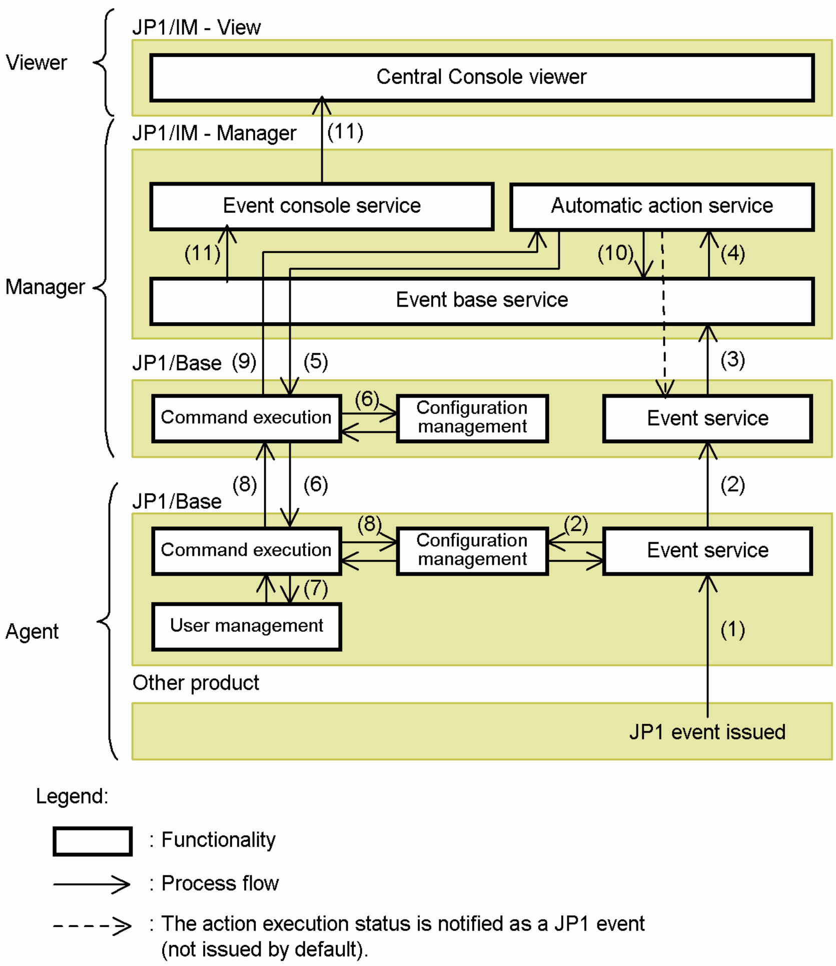
See *jcachange* and *jcastatus* in *Chapter 1. Commands* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

5.10 Flow of automated action execution

The following describes how the JP1/IM and JP1/Base functionality are inter-linked in automated action execution, taking as an example the flow of processing from the time a manager receives a JP1 event that triggers an automated action until the action is executed on an agent.

The description below assumes that the definition of the automated action has been completed. (For details on defining an automated action, see *5.3 Defining an automated action*).

Figure 5–8: Flow of processing for automated action execution (command executed on an agent by an automated action)



The flow of processing is described below, following the numbers in the figure:

1. A JP1 event that triggers an automated action occurs on the agent and is registered with the event service.
2. The registered JP1 event is forwarded to a higher-level host in accordance with the configuration management definitions, and is registered with that manager's event service.
3. JP1/IM - Manager (event base service) acquires the registered JP1 event from the event service.
4. The acquired JP1 event is compared with the automated action definitions, and is passed to the automatic action service if a match is found.
5. On receiving the JP1 event, the automatic action service passes a command execution request to JP1/Base on the manager.

6. On receiving the command execution request, JP1/Base on the manager references the configuration information and sends a command execution request to the target host.
7. JP1/Base on the agent that received the request references the user mapping definitions and then executes the command using the permissions of the mapped OS user.#

   #: User mapping (JP1/Base user management) is processed on the target host where the command is to be executed. Thus, user mapping must be set up in advance on the agent where the automated action is to be executed, or on the manager if the automated action is to be executed on the manager.
8. After the command has been executed, JP1/Base on the agent reports the result to the higher-level host defined in the configuration definitions.
9. On receiving the command execution result, JP1/Base on the manager records the result in a command execution log (ISAM) file, and then reports the result to the automatic action service.
10. The automatic action service outputs the execution result received from JP1/Base to a log, and then passes the execution result to the event base service.
11. The JP1 event information held by the event base service is displayed in JP1/IM - View through the event console service.

Automated actions are executed by the JP1/Base command execution function. See also *7.4.4 Managing command execution*.

Important

If any of the following events occurs during the execution processing of an automated action, the action ceases to proceed through the usual status transition (this applies only to actions whose status is `Wait`, `Send`, `Queue`, `Running`, `Wait (Canceling)`, `Send (Canceling)`, `Queue (Canceling)`, or `Running (Canceling)`):

- The manager, action relay host, or action target host is shut down or otherwise stopped.
- Network error
- JP1/Base failure

In such cases, check the status of the automated actions as follows.

Using the JP1/Base `jcocmdshow` command (supported in version 07-51):

You can check the action status using this command if the automated action was being processed by JP1/Base (command execution management) on the target host.#

#: If the processing request has not yet been received or if processing has ended, you cannot use this command to check the action status.

If an automated action ceases to progress and the `jcocmdshow` command cannot be used to check its status, evaluate whether it needs to be re-executed, and do so if necessary from the Execute Command window.

6 System Hierarchy Management Using IM Configuration Management

This chapter describes central management of the system hierarchy (IM configuration) from the manager by using IM Configuration Management. To manage the system hierarchy, you must first set up the IM Configuration Management database.

For the settings to use the IM Configuration Management functionality, see *1.4.4 Settings for using the functions of IM Configuration Management (for Windows)* in the *JP1/Integrated Management - Manager Configuration Guide*.

For information about defining the system hierarchy and collecting and distributing definition information using the functionality provided by JP1/Base, see *7.4.3 Managing the system hierarchy* and *7.4.5 Collecting and distributing definition information*, and see also *3.2.1 Collecting the system hierarchy* in the *JP1/Integrated Management - Manager Configuration Guide*.

6.1 Host management

Using IM Configuration Management, you can operate the IM configuration management viewer to manage hosts on the network. The following types of host management are available:

- Registering, listing, and deleting hosts

  You can register the hosts below in IM Configuration Management as management targets. You can also list or delete the registered hosts.

  - Hosts in agent configuration, on which JP1/Base is running (hereinafter called *agent hosts*)
  - Hosts in a remote monitoring configuration, for which settings for remote communication have been configured (hereinafter called *remotely monitored hosts*)
  - Hosts in virtualization configuration
- Collecting information from hosts

  You can acquire information including the host name and the IP address of the host (hereinafter called *host information*) and product information from JP1/Base on each agent host. You can also acquire the host name, IP address, and information about the OS from each remotely monitored host.

  Managing agents requires JP1/Base to be running on the management-target agent hosts. Also, managing remotely monitored hosts requires that the remote communication settings be complete.
- Changing the attributes of host information

  You can change the attributes (the host name, host type, comment, active host, standby host, and settings for remote communication) of each host.
- System common settings

  For remotely monitored hosts, you can save and manage the setting values for host information as common values.

This section describes the host information you can manage by using IM Configuration Management, and the functionality provided for this purpose.

6.1.1 Host information managed by IM Configuration Management

The following table lists the host information managed by IM Configuration Management.

Table 6–1: Host information managed by IM Configuration Management

Type	Item	Description	Method of specification
Basic information	Configuration application status	The configuration status when a host is added to the system hierarchy, registered as one of the following: • Not applied The change has not been applied to the system hierarchy (the host has not been added). • Applied The change has been applied to the system hierarchy. • Application failed The host has been added, but the change has not been applied to the system hierarchy.	Registered automatically when host information is read from the system definitions at addition or deletion of a host in the system hierarchy. Cannot be specified directly.
	Configuration application date/time	The date and time when the system hierarchy was updated on the manager. Even for hosts to which configuration definition information is not distributed,	

Type	Item	Description	Method of specification
		the displayed date and time is updated when the system hierarchy is updated. This item is displayed in *yyyy*/*mm*/*dd* *hh*:*mm*:*ss* format.	
	Configuration verification status	The status of a host in agent configuration, displayed when the system hierarchy is verified. This status is registered as one of the following: • Not yet verified The system hierarchy has not yet been verified. • Match The configuration definition information in the IM Configuration Management database matches the information in the host. • Does not match The configuration definition information in the IM Configuration Management database does not match the information in the host. • Verification failed The host's configuration definition information could not be verified because JP1/Base could not be reached. • Not supported The host does not support IM Configuration Management because it is running a version of JP1/Base earlier than version 9.	
	Configuration verification date and time	The date and time at which the system hierarchy was verified. This item is displayed in *yyyy*/*mm*/*dd* *hh*:*mm*:*ss* format.	
	Profile application status	The status when a profile is applied to agent hosts and remotely monitored hosts, registered as one of the following: • Not applied The edited profile has been saved in the server, but application has not yet executed. • Applied Application of the profile has been completed. • Application failed Application of the profile has failed.	Registered automatically when the profile is applied. Cannot be specified directly.
	Profile application date/time	The date and time at which application of the profile was completed. This item is displayed in *yyyy*/*mm*/*dd* *hh*:*mm*:*ss* format.	
	Profile collection status	The status when profiles are collected from agent hosts and remotely monitored hosts, registered as one of the following: • Not collected Collection of profiles has not yet been executed. • Partially collected One or more profiles have been collected without failing. • Collected Collection of profiles has been completed. • Collection failed Collection of profiles has failed.	Registered automatically when profiles are collected. Cannot be specified directly.

Type	Item	Description	Method of specification
	Profile collection date / time	The date and time at which collection of profiles was completed or application of the profiles was completed. This item is displayed in *yyyy*/*mm*/*dd* *hh*:*mm*:*ss* format.	
	Host information collection status	The status of a host when the host information is collected, registered as one of the following: • Not collected Collection of host information has not yet been executed. • Collected Collection of host information has been completed. • Collection failed Collection of host information has failed.	Registered automatically when host information is collected. Cannot be specified directly.
	Host information collection date/time	The date and time at which collection of host information was last completed. This item is displayed in *yyyy*/*mm*/*dd* *hh*:*mm*:*ss* format.	
	Virtualization configuration collection status	The status of a host when information about virtualization system configuration is collected, registered as one of the following: • Not collected Information about virtualization system configuration has not yet been collected. For example, at such times as immediately after the host is registered or management information is imported to IM Configuration Management. • Collected Collection of information about virtualization system configuration has been normally completed. • Collection failed Collection of information about virtualization system configuration has failed. (Due to some reason such as: virtualization software or virtualization environment management software cannot be connected, user authentication is unavailable, or the environment is insufficient). • Does not match The host type differs between the collected virtualization system configuration information and the virtualization system configuration information stored in IM Configuration Management.	Registered automatically when virtualization configuration information is collected. Cannot be specified directly.
	Virtualization configuration collection date/time	The date and time at which collection of information about virtualization system configuration was completed. This item is displayed in *yyyy*/*mm*/*dd* *hh*:*mm*:*ss* format.	
Host information	IP address	The IP address of a host recognized by the manager. IP addresses cannot be specified directly. The value that is registered as the IP address is the result of name resolution that uses the OS `jp1hosts` definition file, `jp1hosts2` definition file, or `hosts` file or DNS when the manager registers the applicable host or collects host information. The value is not the IP address actually set on the host. Also, the value might have changed when host information was	Acquired automatically when you register a host, change host information, or collect host information. Cannot be specified directly.

Type	Item	Description	Method of specification
		collected. This is particularly true if NAT is used or multiple LANs are configured in the system.	
	OS	The name of the OS on the physical host.	Acquired automatically when host information is collected. Cannot be specified directly.
	VMM host	The name of a host on which a Virtual Machine Monitor, such as VMware ESX and Hyper-V, is running, registered when the host type is `Virtual host`.	Specified directly when you register a host or change host information.
	Comment	Comment about the host.	
	Host	The host name registered in IM Configuration Management. You cannot register identical host names.	
	Host name list	A list of the authoritative names and aliases of the hosts recognized by the manager. No more than five aliases can be registered by default. When the OS on the collection target host is Windows, however, only one alias can be registered.	Acquired automatically when you register a host, change host information, or collect host information. Cannot be specified directly.
	Host type	The type of host, registered as one of the following: • Physical host • Virtual host • Logical host • Unknown	Specified directly when you register a host or change host information. Can be acquired when host information is collected.
	Collection date/time	The date and time at which collection of host information was last completed. This item is displayed in *yyyy*/*mm*/*dd* *hh*:*mm*:*ss* format.	
	Collection status	The status of a host when information about the agent host or remotely monitored host is collected, registered as one of the following: • Not collected • Collected • Collection failed	
	Collection status of a host in agent configuration	The status of a host when host information of the agent host is collected, registered as one of the following: • Not collected • Collected • Collection failed	
	Collection status of a host in a remote monitoring configuration	The status of a host when host information of the remotely monitored host is collected, registered as one of the following: • Not collected • Collected • Collection failed	
	Actual host name	The host name actually set for the host.	
	Active host	The host name of the physical host used as the active node of a logical host. Registered when you select **Logical host** as the host type at registration. You cannot register the same host name as a standby host.	Specified directly when you register a host or change host information.
	Standby host	The host name of the physical host used as the standby node of a logical host. No more than four names can be	

Type	Item	Description	Method of specification
		registered by default. Registered when you select **Logical host** as the host type at registration. You cannot register the same host name as an active host.	
	Configuration type	The type of host in a system managed by JP1/IM, registered as one of the following: • Integrated manager • Base manager • Relay manager • Agent • Remote • Not set	Registered automatically when host information is read from the system definitions at addition or deletion of a host in the system hierarchy. Cannot be specified directly.
	Remote communication type	The remote communication type set for a remotely monitored host, registered as one of the following: • WMI/NetBIOS • SSH • Blank (initial value)	Specified directly when you set or change the settings for remote communication.
	Authentication information category	The category of authentication information, registered as one of the following: • Default • Host • Blank (initial value)	
Product information	Installation path	The installation path for the JP1 product installed on a physical host.	Acquired automatically when host information is collected. Cannot be specified directly.
	Version	The version of the JP1 product installed on a physical host.	
	Product name	The name of the JP1 product installed on a physical host.	
	Product module name	The module name of the JP1 product installed on a physical host.	
Virtualization configuration information	Version[#1]	The version of the virtualization software or virtualization environment management software. If this information is registered, the virtualization configuration collection date and time is registered as the update date and time.	
	User name	The user name for the VMM host.	Specified directly when you register a host or change host information.
	Password	The password for the user name.	
	Virtual manager type	The type of virtualization software or virtualization environment management software, registered as one of the following: For a virtualization system management host: • `vCenter` • `JP1/SC/CM` • `SCVMM` • `HCSM` For a VMM host: • `ESX`[#2] • `Hyper-V` • `KVM`	Specified directly when you register a host or change host information. Also, this information can be acquired automatically when virtualization configuration information is collected.

Type	Item	Description	Method of specification
		- `Hitachi Compute Blade logical partitioning feature`	
	Port number	The port number used for communication with the VMM host. The port number is registered when the virtual manager type is HCSM or KVM.	Specified directly when you register a host or change host information.
	Secret key file name	The absolute path of the secret key file used for SSH connection to the VMM host. The secret key file name is registered when the virtual manager type is KVM.	
	Communication type	The type of communication with the VMM host. The communication type is registered when the virtual manager type is vCenter, HCSM, or KVM.	
	Domain name	The domain name of the VMM host. The domain name is registered when the virtual manager type is SCVMM and the domain name is specified as account information for connection to SCVMM.	

Note: For details about virtualization software and virtualization environment management software, see *6.3 Virtualization configuration management*.

#1: When the virtual manager type is HCSM, the version information indicates the version of the HCSM external connection interface. Therefore, the indicated version might differ from the actual HCSM version. When virtualization configuration information is collected from HCSM, a version number is not displayed on a host whose virtual manager type is Hitachi Compute Blade logical partitioning feature.

#2: ESX represents VMware ESX.

6.1.2 Registering hosts

Using IM Configuration Management, you can register hosts in the network as hosts to be managed in the IM Configuration Management database. You can also list the registered hosts.

After registering hosts, you can add them to the system hierarchy or check the operating status of their services in IM Configuration Management.

You can register the following three types of hosts as management targets in IM Configuration Management:

- Agent host
- Remotely monitored host
- Host in virtualization configuration

An agent means a host managed by JP1/IM on which JP1/Base installed. A remotely monitored host means a host managed by JP1/IM on which JP1/Base is not installed.

For remotely monitored hosts, communication settings for remote connection are required. WMI/NetBIOS (NetBIOS over TCP/IP) is used for Windows, and SSH is used for UNIX.

For details when registering a host in FQDN format, see *12.3.11 System configuration for managing monitored hosts with host names in FQDN format*.

The following describes the methods of registering the hosts to be managed in IM Configuration Management:

- Registering from the IM configuration management viewer

  In the Register Host window of the IM configuration management viewer, you can set and register information including the host name and host type.

- Automatically acquiring host information from definition information of the system hierarchy

  The host information contained in definition information of the system hierarchy (configuration definition information) can be registered into the IM Configuration Management database. Information about the host names, IP addresses, list of host names, host types, configuration types, and configuration application dates and times can be acquired. Host information can be acquired from the system hierarchy (IM configuration) by the following three methods:

  - Using the IM configuration management viewer to acquire the system hierarchy

    For details about how to acquire the system hierarchy, see *6.2.2 Acquiring the system hierarchy*.

  - Using the IM configuration management viewer to load the system hierarchy from the configuration definition file

    For details about how to load the system hierarchy, see *6.2.5(6) Loading the system hierarchy*.

  - Importing the system hierarchy on the server on which IM Configuration Management is running

    For details about how to import the system hierarchy, see *6.8.3 Importing IM Configuration Management information*.

- Importing host information of remotely monitored hosts

  You can import host information of remotely monitored hosts, and then register the information in the IM Configuration Management database. Information about the host names, IP addresses, list of host names, and host types can be acquired.

  Host information of the remotely monitored hosts is acquired in the following ways:

  - In the Edit Remote Monitoring Configuration window of the IM configuration management viewer, the **Open Remote Monitoring Configuration** menu command is executed.

  - Remote monitoring configuration information is imported from a manager on which IM Configuration Management is running.

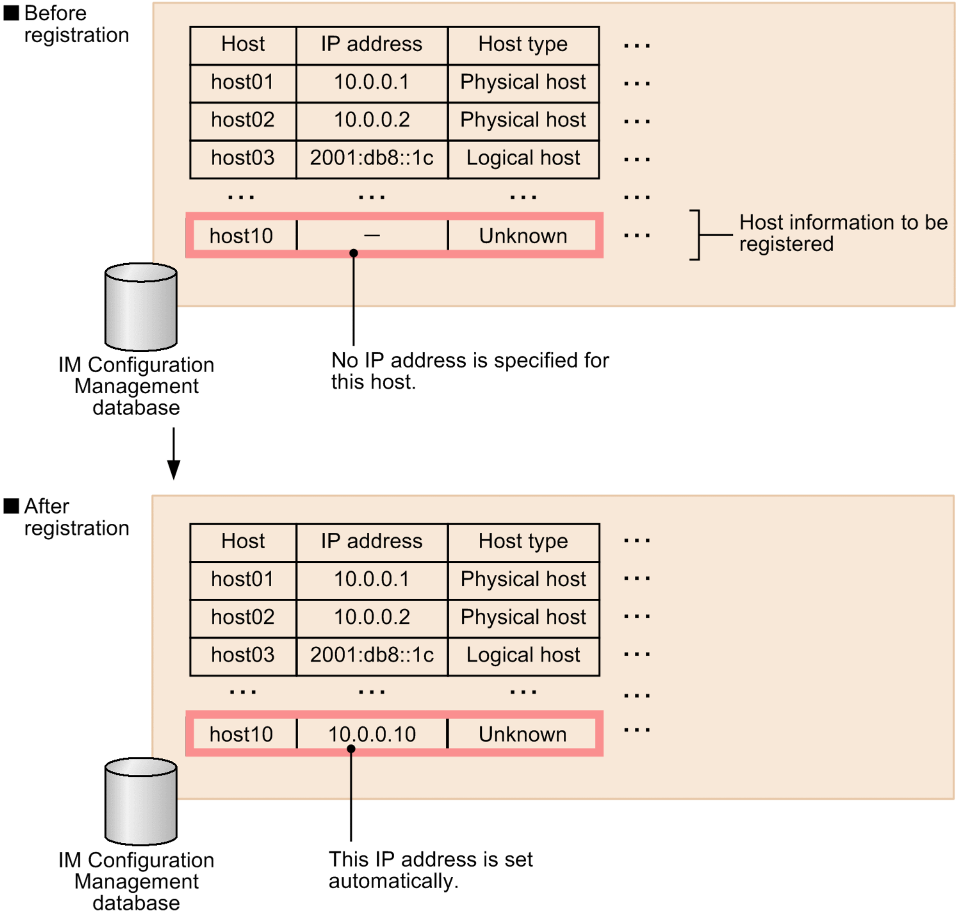
- Acquiring virtualization configuration information

  You can acquire virtualization environment information, and then register the information for host management. For details, see *6.3 Virtualization configuration management*.

After registering hosts, host information is registered in the IM Configuration Management database, and the IP addresses set for the relevant hosts are automatically registered.

The figure below shows an example of the host information registered in the database at host registration.

Figure 6–1: Example of host information registered in the IM Configuration Management database at host registration


■ Before registration
Host information to be registered
No IP address is specified for this host.
IM Configuration Management database
■ After registration
This IP address is set automatically.
IM Configuration Management database

Before registration:

Host	IP address	Host type	...
host01	10.0.0.1	Physical host	...
host02	10.0.0.2	Physical host	...
host03	2001:db8::1c	Logical host	...
...	...	...	...
host10	—	Unknown	...

After registration:

Host	IP address	Host type	...
host01	10.0.0.1	Physical host	...
host02	10.0.0.2	Physical host	...
host03	2001:db8::1c	Logical host	...
...	...	...	...
host10	10.0.0.10	Unknown	...

Legend: —: Not specified.

Any unregistered hosts in the system hierarchy are automatically registered in the IM Configuration Management database when configuration definition information is collected from the hosts.

After IM Configuration Management is started, if no hosts are registered in the IM Configuration Management database, host information of the host (physical or logical host) on which IM Configuration Management is running is automatically registered in the IM Configuration Management database.

If the number of hosts loaded from the system hierarchy exceeds the maximum number of hosts that can be registered in the IM Configuration Management database, only the maximum number of hosts are registered in the IM Configuration Management database.

The following checks are performed on the acquired system hierarchy when the acquisition is performed by IM Configuration Management - View is used:

- Whether the local host name in the acquired system hierarchy matches the local host name registered in the IM Configuration Management database. If different, the following message is output and processing is canceled:
  `Collection of the IM configuration failed because the local host name "host1" is different from the registered host name "host2".`
- Whether two or more hosts with the same host name exist in the acquired system hierarchy. If so, a message reports that the host name is duplicated and processing is canceled.

After these checks, if there is no higher-level host in the acquired system hierarchy, the configuration type of the local host changes to **Integrated manager**. If there is a higher-level host in the acquired system hierarchy, the configuration type of the local host changes to **Relay manager**.

When you import the system hierarchy on the server running IM Configuration Management, the hosts' IP addresses are not registered in the IM Configuration Management database even if set in the export file (`host_input_data.csv`).

When you register the remotely monitored hosts, you can save and manage the communication settings of the OS as the system common settings in the System Common Settings window of the IM configuration management viewer.

The following table describes the system common settings information that can be managed.

Table 6–2: System common settings information

Item	Description
WMI/NetBIOS#	Authentication information details required for a WMI/NetBIOS (NetBIOS over TCP/IP) connection are managed as common values. If you specify **Common** for **Setting method** in the communication settings for the OS, you can use the saved authentication information.
SSH	Manages authentication information using the public key authentication method.
IM host account#	Manages the account information required by a Windows manager host for remote monitoring, as the IM host account.

#:

For the account used for a WMI/NetBIOS (NetBIOS over TCP/IP) connection or the IM host account, specify a user with Administrator's permissions.

For remote monitoring, the account specified as the IM host account when JP1/IM - Manager is started is used to start the process that will be used for remote monitoring. If you change the account information of the OS, also change the IM host account. The new IM host account will be used when JP1/IM - Manager is started next time. Current remote monitoring continues operating using the old account, so you do not have to immediately restart JP1/IM - Manager and apply the setting change.

6.1.3 Collecting host information

IM Configuration Management can collect host information stored in JP1/Base on agents and host information on the remotely monitored hosts, and then apply the information to the IM Configuration Management database. However, when you collect host information on remotely monitored hosts, host information cannot be collected if OS communication is set to off in the OS communication settings.

Collect host information on the **Host List** page or **IM Configuration** page of the IM Configuration Management window.

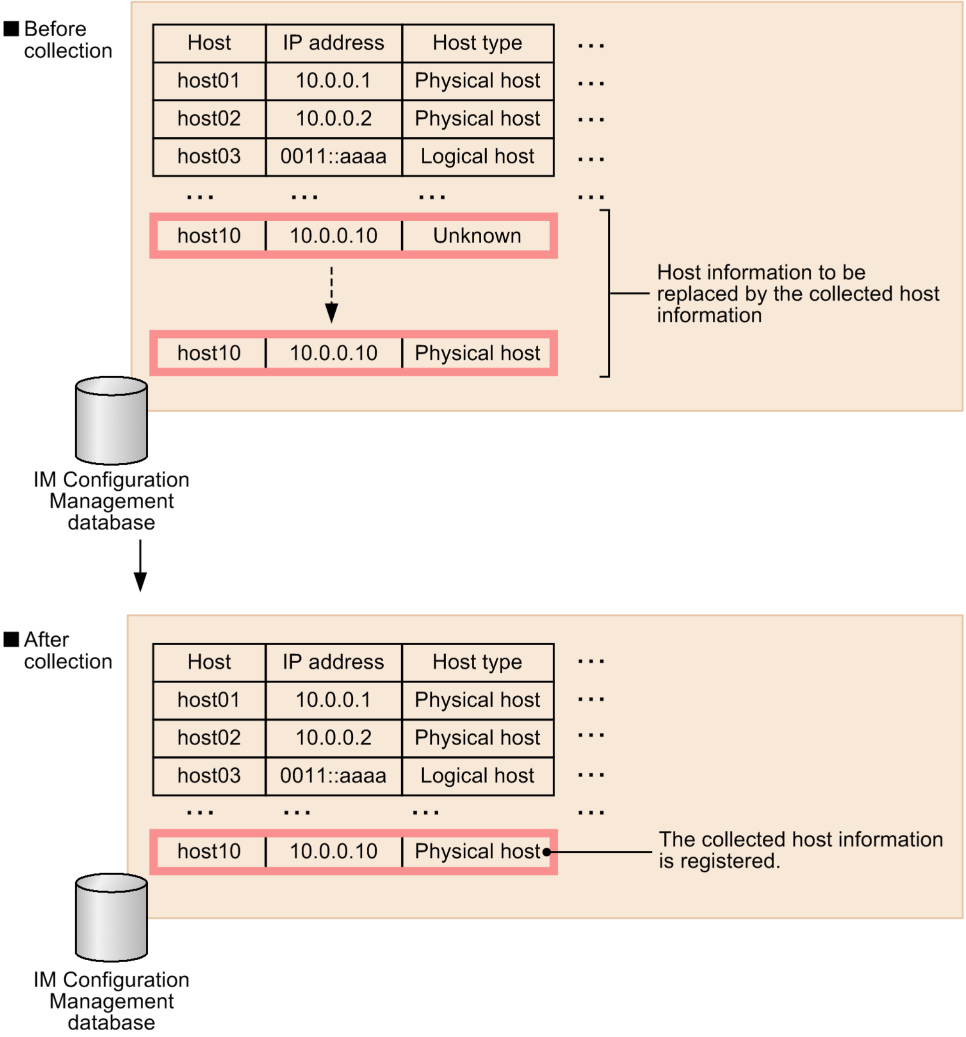
The collected host information is saved to the IM Configuration Management database, replacing the existing data.

If host information is to be collected while a remote-monitoring log file trap or remote-monitoring event log trap is running on a selected host, the host information is collected according to the reply to the confirmation message. Remote monitoring is stopped when host information is to be collected but no information can be obtained from the monitored host, or when the OS name differs from the OS name used for a previous collection.

To collect host information from remotely monitored hosts, a WMI/NetBIOS (NetBIOS over TCP/IP) connection is used for Windows, and an SSH connection is used for UNIX.

The figure below shows an example of the host information registered in the IM Configuration Management database when collection is performed.

Figure 6–2: Example of host information registered in the IM Configuration Management database when collection is performed



■ Before collection

Host	IP address	Host type	...
host01	10.0.0.1	Physical host	...
host02	10.0.0.2	Physical host	...
host03	0011::aaaa	Logical host	...
...	...	...	...
host10	10.0.0.10	Unknown	
host10	10.0.0.10	Physical host	

Host information to be replaced by the collected host information

IM Configuration Management database

■ After collection

Host	IP address	Host type	...
host01	10.0.0.1	Physical host	...
host02	10.0.0.2	Physical host	...
host03	0011::aaaa	Logical host	...
...	...	...	...
host10	10.0.0.10	Physical host	

The collected host information is registered.

IM Configuration Management database

The following table describes host information that can be collected on each type of host.

Table 6–3: Host information that can be collected

Host information		Host in agent configuration (When JP1/Base version 9 or later is used)	Remotely monitored host
IP address#		Y	Y
Host name list		Y	Y
Host type		Y	N
Actual host name		Y	N
OS		Y	Y
Product information	Product name	Y	N
	Product module	Y	N
	Version	Y	N
	Installation path	Y	N

Legend:

Y: Can be collected.

N: Cannot be collected.

#

IP address whose name was resolved by the manager

The following table lists the JP1 products from which product information can be collected.

Table 6–4: JP1 products from which product information can be collected

Product name	Product version	Whether collectable
JP1/Base	Version 9 or later	Y
JP1/IM - Manager	Version 9 or later	Y

Legend:

Y: Can be collected.

After host information is collected successfully from a host running JP1/Base version 9 or later, JP1/IM performs one of the following checks on the collected information, as applicable:

- Host type determination

  If the host information was collected from a host registered as **Unknown** type in the IM Configuration Management database, the host type is determined automatically. The registered host type is changed to the host type contained in the collected host information.

  Host type determination does not distinguish between a physical host and a virtual host. If the host is actually a virtual host, after the determination you must change the host type to Virtual host and set a VMM host in IM Configuration Management - View.

  For details about how to set the host type, see *6.1.5 Changing host information*.

- Host type check

  If the host information was collected from a host registered as other than **Unknown** type in the IM Configuration Management database, its host type is verified. The registered host type is compared with the host type contained in the collected host information. If a mismatch is found, the host type registered in the database is judged to be incorrect and an error message is displayed.

  The host type check does not distinguish between a physical host and a virtual host. The host is assumed to be a physical host in all cases. The following table describes the results of a host type check.

Table 6–5: Results of a host type check

Host type of the collection target host	Host type registered in the IM Configuration Management database	Check result
Physical host	Physical host or virtual host	Y
Physical host	Logical host	N
Logical host	Physical host or virtual host	N
Logical host	Logical host	Y

Legend:

Y: Correct

N: Incorrect

Note:

If the host type is incorrectly specified as a physical host or virtual host in the IM Configuration Management database, the setting is not regarded as incorrect by the host type check.

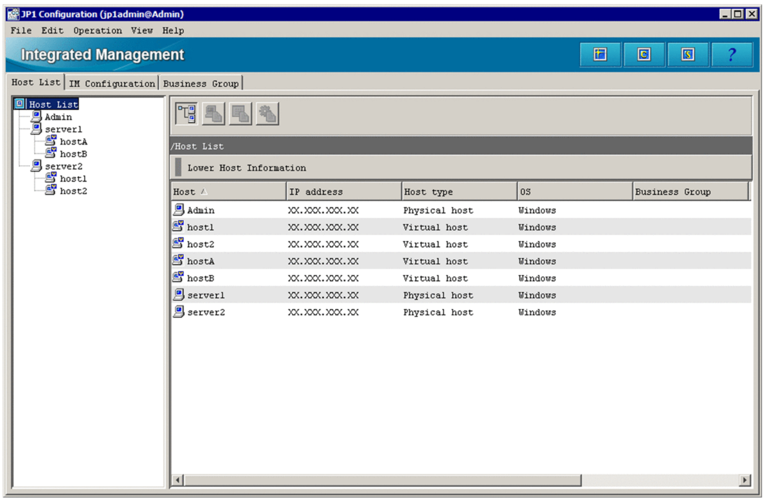
On the **Host List** page of the IM Configuration Management window, you can check the status of the hosts after host information is collected. If collection fails for any host, the host's icon appears grayed in the tree display area. To see more details, click the **Basic Information** button in the node display area on the **Host List** page.

6.1.4 Displaying host information

On the **Host List** page of the IM Configuration Management window, you can display a list of hosts registered in the IM Configuration Management database. On the **IM Configuration** page, you can view information about a particular host.

The following figure shows an example of a display of host information.

Figure 6–3: Example of a display of host information (Host List page in the IM Configuration Management window)



Host	IP address	Host type	OS	Business Group
Admin	XX.XXX.XXX.XX	Physical host	Windows	
host1	XX.XXX.XXX.XX	Virtual host	Windows	
host2	XX.XXX.XXX.XX	Virtual host	Windows	
hostA	XX.XXX.XXX.XX	Virtual host	Windows	
hostB	XX.XXX.XXX.XX	Virtual host	Windows	
server1	XX.XXX.XXX.XX	Physical host	Windows	
server2	XX.XXX.XXX.XX	Physical host	Windows	

For details about this window, see *4.1.1 Host List page* and *4.1.2 IM Configuration page* in the manual *JP1/Integrated Management - Manager GUI Reference*.

6.1.5 Changing host information

Using IM Configuration Management, you can change the host information registered in the IM Configuration Management database.

To change host information, use the Edit Host Properties window.

After you change host information, the hosts and host information that were changed in the Edit Host Properties window are registered in the IM Configuration Management database.

The following table describes the item names of host information and whether their contents can be changed.

Table 6–6: Items of host information and whether they can be changed

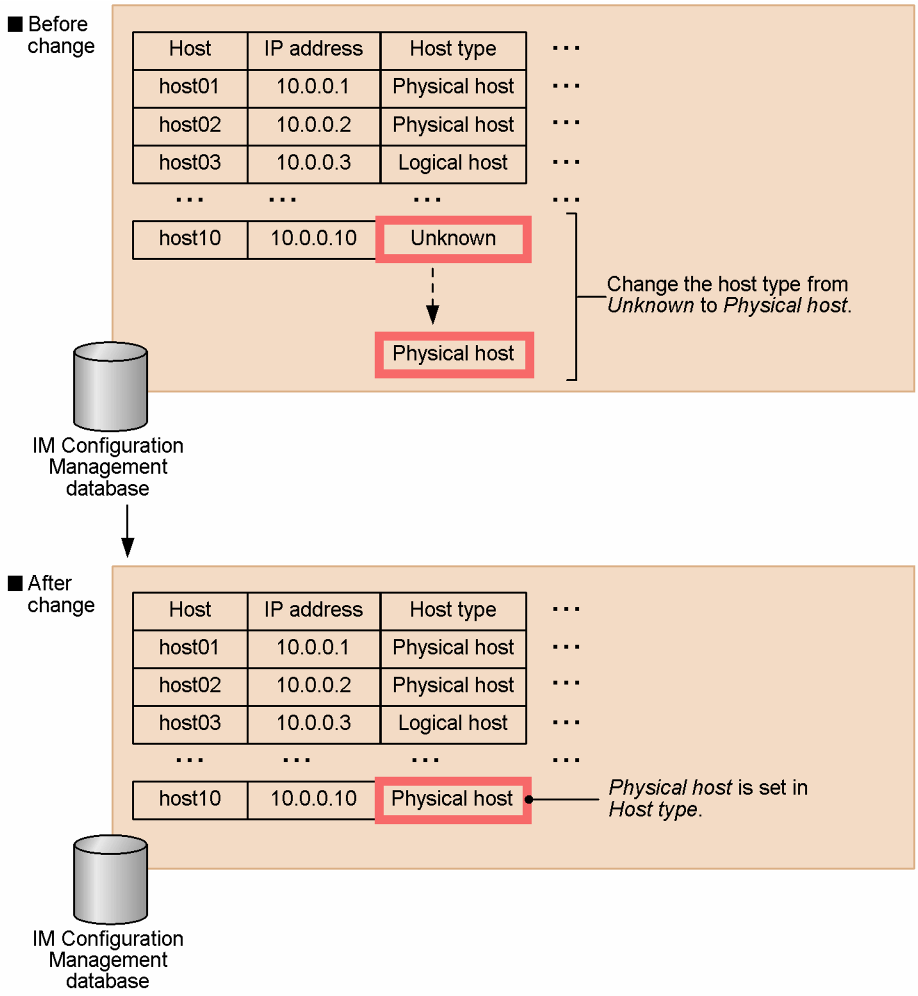
Item	Changeable	Conditions
Host name	Y	This item cannot be changed if the new host name has already been registered in the IM Configuration Management database or in the business group. Change a host name only after the host name is changed on the actual host.

Item	Changeable	Conditions
		After changing a host name, collect host information again.
IP address	N	--
Comment	Y	--
Host type	Y	This item cannot be changed in the following cases: • Physical host You cannot change the host type of a physical host that is specified as the VMM host on a virtual host. • Physical host and virtual host You cannot change the host type to `Logical host` or `Unknown` for a physical host or virtual host that is specified as the active host or standby host on a logical host.
Active host	Y	This item can be changed only when the host type is `Logical host`.
Standby host	Y	This item can be changed only when the host type is `Logical host`.
VMM host	Y	This item can be changed only when the host type is `Virtual host`.
Remote monitoring settings	Y	To enable the new setting for a remotely monitored host, either of the following must be reloaded: • Remote-monitoring log file trap • Remote-monitoring event log trap If you change the communication type when a remote-monitoring log file trap or remote-monitoring event log trap is running on the selected host, a message is displayed, and the communication type is returned to the one before changing. Stop remote monitoring, and then change the setting.

Legend: Y: Can be changed. N: Cannot be changed. --: Not applicable.

The figure below shows an example of the host information registered in the IM Configuration Management database after a property is changed.

Figure 6–4: Example of host information registered in the IM Configuration Management database after a property is changed



■ Before change

Host	IP address	Host type	···
host01	10.0.0.1	Physical host	···
host02	10.0.0.2	Physical host	···
host03	10.0.0.3	Logical host	···
···	···	···	···
host10	10.0.0.10	Unknown	

Physical host
Change the host type from *Unknown* to *Physical host*.
IM Configuration Management database

■ After change

Host	IP address	Host type	···
host01	10.0.0.1	Physical host	···
host02	10.0.0.2	Physical host	···
host03	10.0.0.3	Logical host	···
···	···	···	···
host10	10.0.0.10	Physical host	

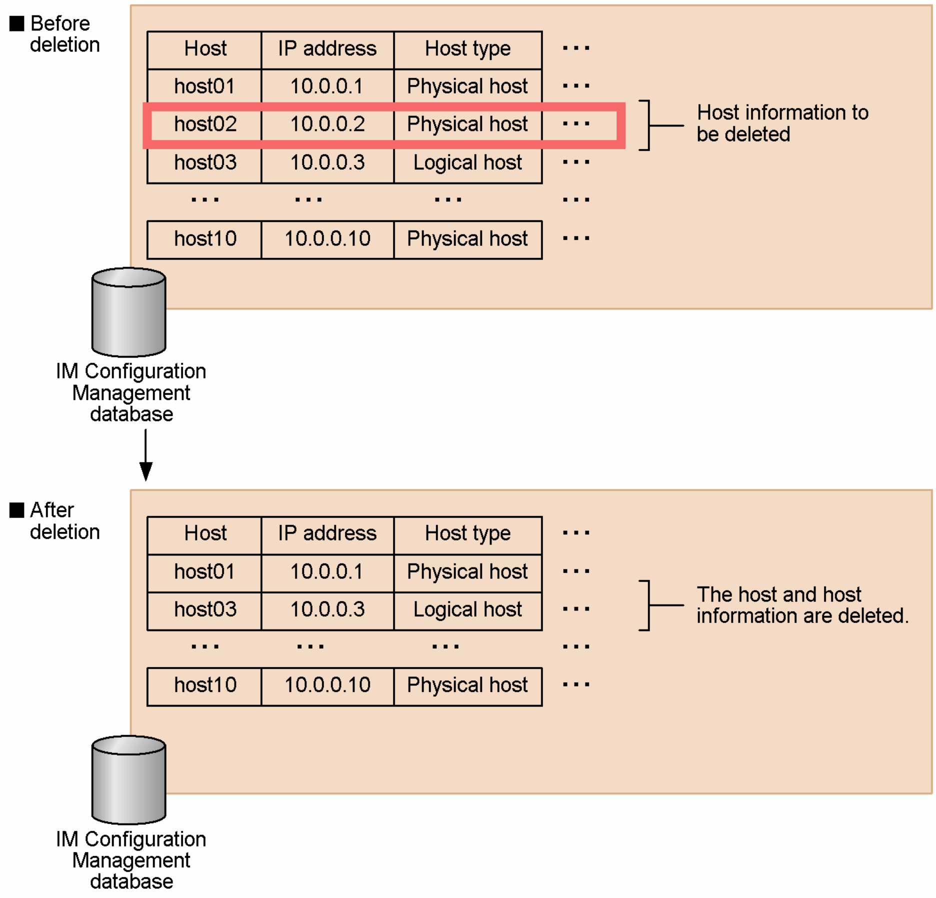
Physical host is set in *Host type*.
IM Configuration Management database

6.1.6 Deleting hosts

Using IM Configuration Management, you can delete a host registered in the IM Configuration Management database.

Delete the host on the **Host List** page of the IM Configuration Management window. The figure below shows an example of host information erased from the IM Configuration Management database after a host is deleted.

Figure 6–5: Example of host information erased from the IM Configuration Management database when a host is deleted


■ Before deletion
Host information to be deleted
IM Configuration Management database
■ After deletion
The host and host information are deleted.
IM Configuration Management database

Host	IP address	Host type	...
host01	10.0.0.1	Physical host	...
host02	10.0.0.2	Physical host	...
host03	10.0.0.3	Logical host	...
...	...	...	...
host10	10.0.0.10	Physical host	...

Host	IP address	Host type	...
host01	10.0.0.1	Physical host	...
host03	10.0.0.3	Logical host	...
...	...	...	...
host10	10.0.0.10	Physical host	...

The host and host information that you specify in the IM Configuration Management window are erased from the IM Configuration Management database. In addition to the host information, the profile information in JP1/Base (profile list and profile configuration files) are also erased. For details about profile information, see *6.5 Profile management*. Note that the local host cannot be deleted from the IM Configuration Management database.

You cannot delete a host from the IM Configuration Management database in the following cases:

- Host registered in a business group
- Host registered in the configuration definition information

  Before you delete the host from the IM Configuration Management database, you must delete the host from the system hierarchy in the Edit Agent Configuration window or in the Edit Remote Monitoring Configuration window.
- Host of **Physical host** type being used as a VMM host in a virtual host

  Before you delete the physical host, you must first perform either of the following:

  - Change the VMM host used by the virtual host to a different physical host.
  - Delete the virtual host.
- Host of **Physical host** type being used as an active or standby host in a logical host

  Before you delete the physical host, you must first perform either of the following:

  - Delete the physical host from the active host or standby host used by the logical host.
  - Delete the logical host.
- Host of **Virtual host** type being used as an active or standby host in a logical host

Before you delete the virtual host, you must first perform either of the following:

- Delete the virtual host from the active host or standby host used by the logical host.
- Delete the logical host.

6.2 System hierarchy management

In IM Configuration Management, you can operate the IM configuration management viewer to manage agents and remotely monitored hosts on an integrated basis through the system hierarchy (IM configuration).

By defining the system hierarchy, you will be able to manage the JP1/Base profiles (for agent configuration) and profiles of remote monitored hosts.

To manage the system hierarchy, you must first register the hosts configured in the system in the IM Configuration Management database. For agents, JP1/Base must be running on the agent hosts.

When you use IM Configuration Management to manage the system hierarchy, either of the following operations causes an inconsistency between the configuration definition information held by IM Configuration Management and that held by JP1/Base:

- Editing the JP1/Base configuration definition file
- Executing the `jbsrt_distrib` command

We therefore recommend that if you use IM Configuration Management to manage the system hierarchy, you use IM Configuration Management to centralize configuration management.

If you have used JP1/Base functionality to distribute the system hierarchy definition, you must obtain the system hierarchy to make the configuration definition information held by IM Configuration Management consistent with that held by JP1/Base.

This section describes the hierarchical configurations you can manage using IM Configuration Management, and the functionality provided for this purpose.

6.2.1 Hierarchical configurations managed by IM Configuration Management

Using IM Configuration Management, you can define the host relationships and manage the JP1/IM system configuration as a hierarchy.

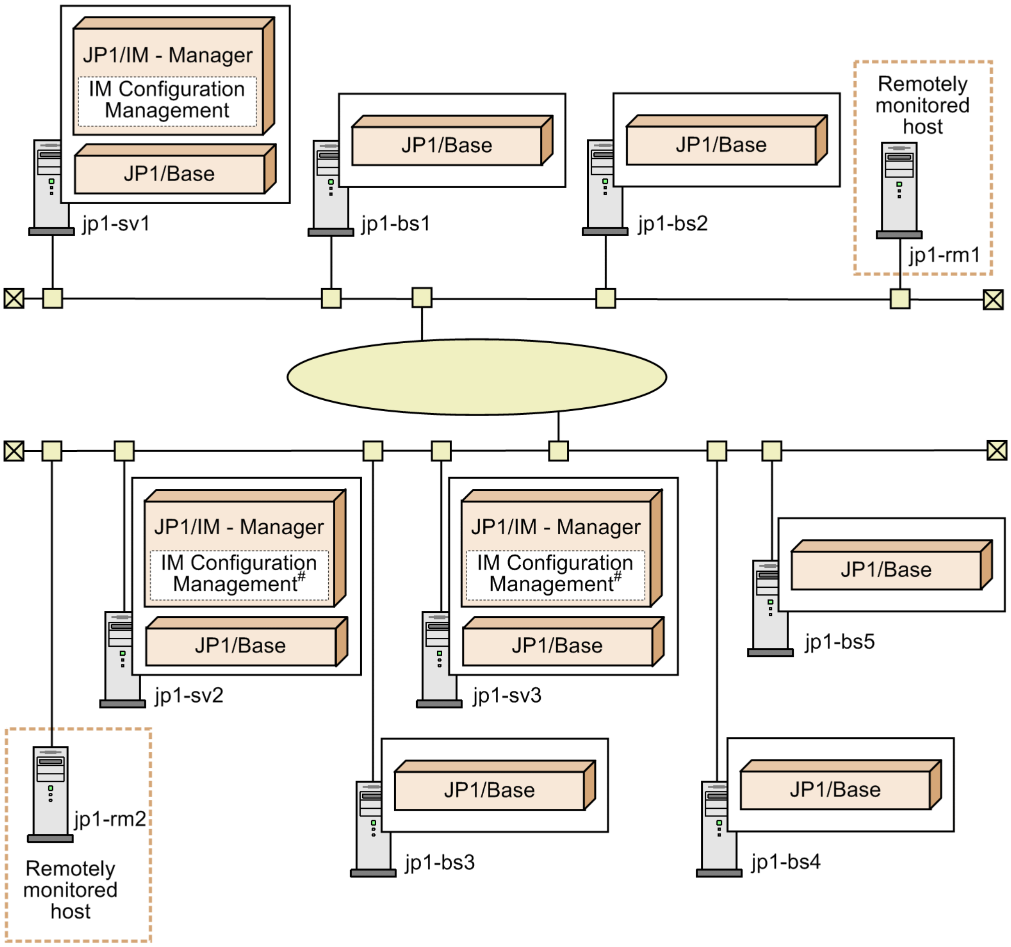
Defining the system hierarchy in IM Configuration Management allows you to perform the following operations in JP1/IM:

- Forward JP1 events to a higher-level host
- Execute commands from JP1/IM - View
- Execute automated actions from JP1/IM
- Collect and distribute definition information

For the hosts added to the system hierarchy, you are also allowed to manage the JP1/Base profiles and the profiles of the remotely monitored hosts from IM Configuration Management.

The figure below shows an example of defining a system hierarchy using IM Configuration Management.

Figure 6–6: System hierarchy example (physical configuration)



#: Required to use the node as a base manager. Not required for a relay manager.

Two types of 3-tier system configurations can be defined in IM Configuration Management:

- A configuration where the agents are centrally managed by an integrated manager
- A configuration where the agents are managed by base managers in separate domains

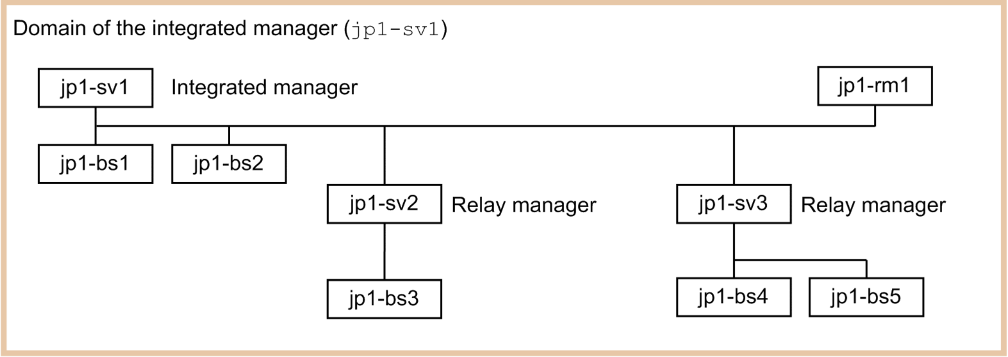
For remotely monitored hosts, a hierarchical configuration cannot be defined. When you centrally manage agents, use the integrated manager to operate on the agents and add agents under the integrated manager. When you manage agents by base managers, operate on each base manager and add the agents for the domain to under each base manager.

(1) Centralized management by an integrated manager

In a configuration where the agents in the JP1/IM system are centrally managed by an integrated manager, agent information is collected by relay managers placed in the middle tier.

The relay managers do not provide the IM Configuration Management functionality.

Figure 6–7: System hierarchy example (centralized management by an integrated manager)



The following table describes the operations that can be performed from the integrated manager on the hosts in the above configuration example.

Table 6–7: Operations that can be performed from the integrated manager (with relay managers in the middle tier)

Target host		Operation			
		View the system configuration	Change the system configuration	View host information	View and change profile information
Integrated manager (jp1-sv1)		Y	Y	Y	Y
Relay manager (jp1-sv2 and jp1-sv3)		Y	Y	Y	Y
Agent	Under the integrated manager (jp1-bs1 and jp1-bs2)	Y	Y	Y	Y
	Under relay managers (jp1-bs3, jp1-bs4, and jp1-bs5)	Y	Y	Y	Y

Legend:

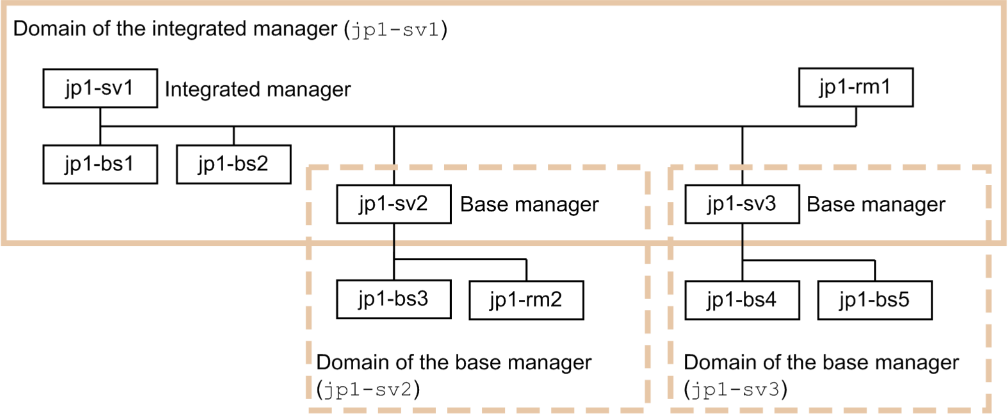
Y: Can be performed.

(2) Agent management in separate domains

In a configuration where the agents are managed by base managers in separate domains, base managers are placed in the middle tier.

The base managers provide the IM Configuration Management functionality.

Figure 6–8: System hierarchy example (agent management in separate domains)


Domain of the integrated manager (jp1-sv1)
jp1-sv1
Integrated manager
jp1-rm1
jp1-bs1
jp1-bs2
jp1-sv2
Base manager
jp1-sv3
Base manager
jp1-bs3
jp1-rm2
jp1-bs4
jp1-bs5
Domain of the base manager (jp1-sv2)
Domain of the base manager (jp1-sv3)

The following table describes the operations that can be performed from the integrated manager on the hosts in the above configuration example.

Table 6–8: Operations that can be performed from the integrated manager (with base managers in the middle tier)

Target host		Operation			
		View the system configuration	Change the system configuration	View host information	View and change profile information
Integrated manager (jp1-sv1)		Y	Y	Y	Y
Base manager (jp1-sv2 and jp1-sv3)		Y	Y	Y	Y
Agent	Under the integrated manager (jp1-bs1 and jp1-bs2)	Y	Y	Y	Y
	Under base managers (jp1-bs3, jp1-bs4, and jp1-bs5)	Y	N	N	N

Legend:

Y: Can be performed.

N: Cannot be performed.

The following table describes the operations that can be performed from a base manager on the hosts in the configuration example shown in *Figure 6-8 System hierarchy example (agent management in separate domains)*.

Table 6–9: Operations that can be performed from a base manager (base managers in the middle tier)

Target host		Operation			
		View the system configuration	Change the system configuration	View host information	View and change profile information
Integrated manager (JP1-sv1)		Y#	N	N	N
Base manager (local host)		Y	Y	Y	Y
Base manager (remote host)		N	N	N	N
Agent	Under the integrated manager (jp1-bs1 and jp1-bs2)	N	N	N	N
	Under base managers (local host)	Y	Y	Y	Y
	Under base managers (remote host)	N	N	N	N

Legend:

Y: Can be performed.

N: Cannot be performed.

#

Viewable only when the integrated manager is a level above the base managers.

(3) Management of remotely monitored hosts by an integrated manager

In a configuration where the remotely monitored hosts are centrally managed by an integrated manager, the remotely monitored hosts are placed directly under the integrated manager.

The following table describes the operations that can be performed from the integrated manager on the hosts in the configuration example shown in *Figure 6-7 System hierarchy example (centralized management by an integrated manager)*.

Table 6–10: Operations that can be performed from the integrated manager (for remotely monitored hosts)

Target host		Operation			
		View the system configuration	Change the system configuration	View host information	View and change profile information
Remotely monitored hosts	Under the integrated manager (jp1-rm1)	Y	Y	Y	Y
	Under base managers	N	N	N	N
	Under relay managers (jp1-rm2)	N	N	N	N

Legend:

Y: Can be performed.

N: Cannot be performed.

(4) Management of remotely monitored hosts in separate domains

In a configuration where the remotely monitored hosts are managed by base managers, the remotely monitored hosts in each domain are placed directly under each base manager.

The following table describes the operations that can be performed from a base manager on the hosts in the configuration example shown in *Figure 6-8 System hierarchy example (agent management in separate domains)*.

Table 6–11: Operations that can be performed from a base manager (for remotely monitored hosts)

Target host		Operation			
		View the system configuration	Change the system configuration	View host information	View and change profile information
Remotely monitored hosts	Under the integrated manager (jp1-rm1)	N	N	N	N
	Under the base manager (local host) (jp1-rm2)	Y	Y	Y	Y
	Under the base manager (remote host)	N	N	N	N
	Under relay managers	N	N	N	N

Legend:

Y: Can be performed.

N: Cannot be performed.

6.2.2 Acquiring the system hierarchy

Using IM Configuration Management, you can acquire from the manager on which IM Configuration Management is running, the definition information of the system hierarchy (configuration definition information) held in JP1/Base on manager hosts. You can then save that information as the configuration definition information in the IM Configuration Management database on the manager on which IM Configuration Management is running. Note that you cannot collect the system hierarchy information from remotely monitored hosts.

Acquire the system hierarchy on the configuration definition information on the **IM Configuration** page of the IM Configuration Management window.

When the system hierarchy is applied, the content of system hierarchy displayed by the IM configuration management viewer is applied. If the system hierarchy has not been acquired, a system hierarchy different from the currently configured hierarchy might be applied. To avoid this problem, you must be sure to acquire the system hierarchy.

Acquire the system hierarchy as follows:

- When the system hierarchy has been changed without using IM Configuration Management as in the following cases, acquire the system hierarchy on the integrated manager:
  - When IM Configuration Management is deployed in an existing JP1/IM system
  - When the system hierarchy is altered by executing the `jbsrt_distrib` command on the manager running IM Configuration Management
- After the system hierarchies are synchronized between the integrated manager and the base managers, acquire the system hierarchy on each base manager.

The configuration definition information held in the IM Configuration Management database is updated when the system hierarchy is acquired. If you want to save the existing information before it is updated, you must export it in advance on the manager running IM Configuration Management.

After the acquisition, the system hierarchy is displayed as follows in IM Configuration Management:

- Any unregistered hosts included in the acquired information are automatically registered in the IM Configuration Management database. No host information is acquired for these hosts, however. Instead, you must collect the information manually on the **Host List** page or **IM Configuration** page of the IM Configuration Management window.

  If duplicated host names exist in the acquired information, an error message appears and the acquired information is not applied in the configuration definition information held in the IM Configuration Management database.

  Make sure no hosts with the same host name exist in the configuration definition information.
- Acquired information containing duplicated host names is discarded and the IM configuration tree appears grayed on the **IM Configuration** page.
- If the acquired information differs from the information in the IM Configuration Management database, the affected host is represented by an error-status icon in the tree display area of the **IM Configuration** page.
- If the configuration definition information held by JP1/Base on the manager running IM Configuration Management has been deleted, the following message appears: `IM configuration does not exist. Do you want to reflect to the IM configuration maintained in server?`

  Click the **Yes** button to erase the deleted information from the IM Configuration Management database. Click the **No** button to keep the deleted information. This will make the system hierarchy appear grayed on the **IM Configuration** page.
- In an agent configuration, if the system hierarchy appears grayed in the tree display area of the **IM Configuration** page, check and, if necessary, revise the configuration definition information (agent configuration), and then apply the agent configuration. For details about how to apply the agent configuration, see *3.2.4(3) Applying a system*

hierarchy to a system managed by IM Configuration Management in the *JP1/Integrated Management - Manager Configuration Guide*.

When IM Configuration Management starts, configuration definition information is acquired automatically so that the information held by JP1/Base on the manager running IM Configuration Management can be checked for consistency with the definitions in the IM Configuration Management database.

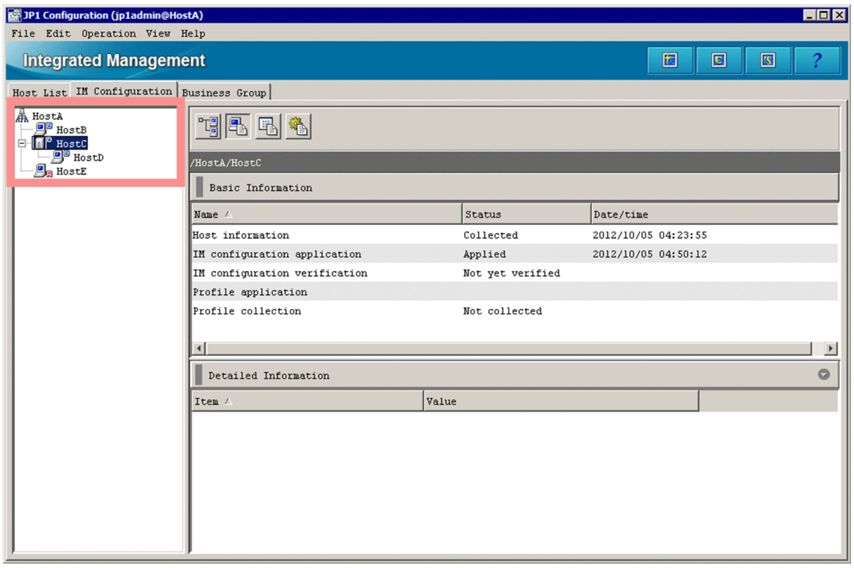
6.2.3 Displaying the system hierarchy

Using IM Configuration Management, you can display the configuration definition information held in the IM Configuration Management database. The information appears on the **IM Configuration** page of the IM Configuration Management window.

The hosts defined in agent configuration and the hosts defined in a remote monitoring configuration by the integrated manager or base managers are displayed in the tree display area on the **IM Configuration** page. This is where you can check the system hierarchy. If the acquired configuration definition information (agent configuration) does not match with the configuration definition information held in the IM Configuration Management database, the system hierarchy appears grayed in the tree display area. In this case, perform the following to make the information of the different configuration definitions the same:

- In the IM Configuration Management window, from the **Operation** menu, select **Collect IM Configuration** to acquire the configuration definition information.
- In the Edit Agent Configuration window, from the **Operation** menu, select **Apply Agent Configuration** to apply the agent configuration.

Figure 6–9: Display example of the contents of the configuration definition information (IM Configuration page of the IM Configuration Management window)



Name	Status	Date/time
Host information	Collected	2012/10/05 04:23:55
IM configuration application	Applied	2012/10/05 04:50:12
IM configuration verification	Not yet verified	
Profile application		
Profile collection	Not collected	

Item	Value

For details about the displayed information, see *4.1.2 IM Configuration page* in the manual *JP1/Integrated Management - Manager GUI Reference*.

The following table describes the information displayed for individual components of the system hierarchy.

Table 6–12: Components of the system hierarchy and displayed information

Component	Information about lower-level hosts	Basic information	Product information	Service operating information
Integrated manager	Y	Δ	Δ	Δ
Base manager	Y	Δ	Δ	Δ
Relay manager	Y	Δ	Δ	Δ
Agent under a base manager	N	N	N	N
Agent under the integrated manager or a relay manager	N	Y	Δ	Δ
Remotely monitored host under a base manager	N	N	N	N
Remotely monitored host under the integrated manager	N	Y	Δ#	Δ#

Legend:

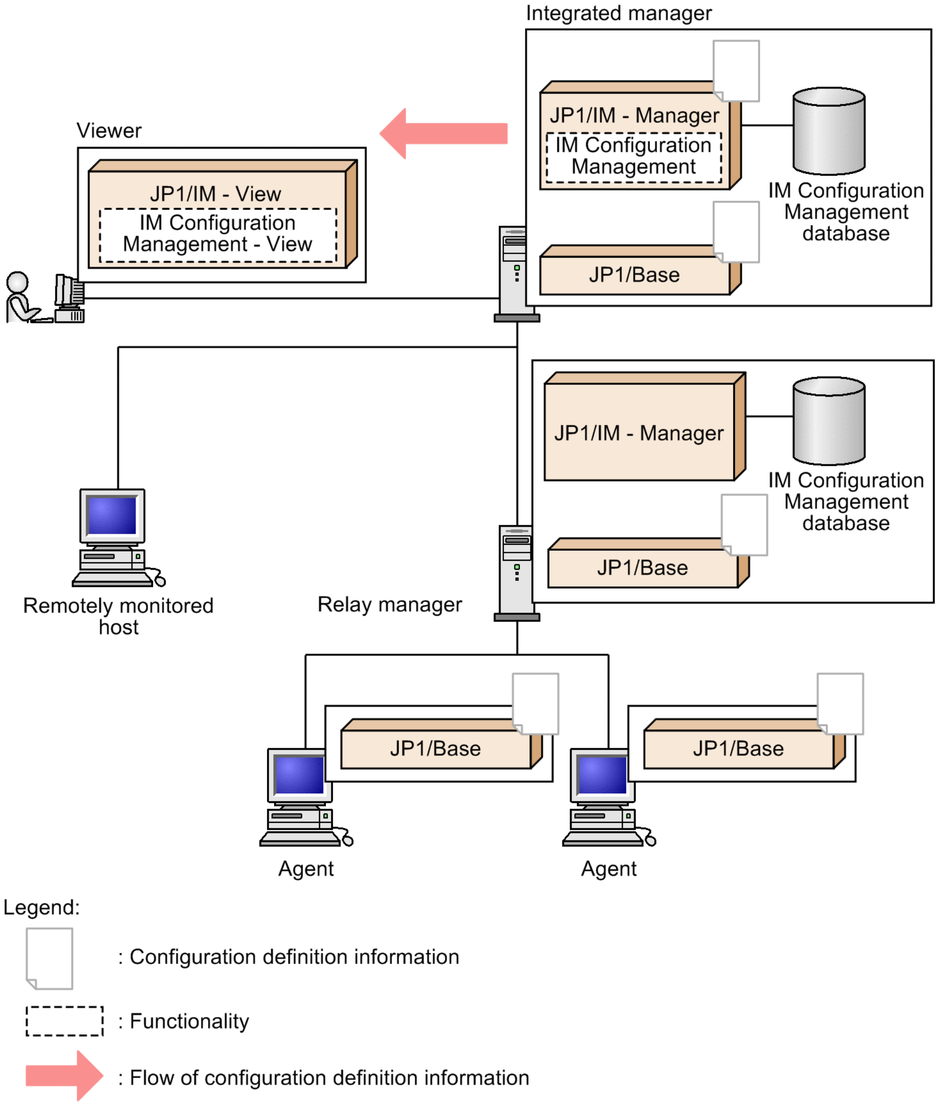
Y: Can be displayed by default. Δ: Can be displayed. N: Cannot be displayed.

#

This information can be displayed only when the host information is collected by JP1/Base.

The figure below shows the flow of processing when displaying the system hierarchy with IM Configuration Management.

Figure 6–10: Displaying the system hierarchy with IM Configuration Management


Integrated manager
JP1/IM - Manager
IM Configuration Management
IM Configuration Management database
JP1/Base
Viewer
JP1/IM - View
IM Configuration Management - View
JP1/IM - Manager
IM Configuration Management database
JP1/Base
Remotely monitored host
Relay manager
JP1/Base
JP1/Base
Agent
Agent
Legend:
: Configuration definition information
: Functionality
: Flow of configuration definition information

6.2.4 Verifying the system hierarchy

You can use IM Configuration Management to verify whether the configuration definition information held in JP1/Base on an agent in the JP1/IM system matches the configuration definition information held in the IM Configuration Management database. For a remotely monitored host, you can verify the remote connection by using the authentication information for remote setting.

Verify the system hierarchy on the **IM Configuration** page of the IM Configuration Management window.

The following table describes the range of hosts whose system configuration information you can verify from the integrated manager.

Table 6–13: Range of hosts whose system configuration information can be verified from the integrated manager

Host type	Verify
Local host	Y

Host type		Verify
Relay manager		Y
Base manager		Y
Agent	Directly under the local host	Y
	Under a relay manager	Y
	Under a base manager	N[#]
Remotely monitored host	Under the local host	Y
	Under a base manager	N[#]

Legend:

Y: The information can be verified.

N: The information cannot be verified.

#

Verify the system hierarchy on the base manager because a firewall might prevent the integrated manager from connecting to the agent or remotely monitored host under a base manager.

The following table describes the range of hosts whose system configuration information you can verify from a base manager.

Table 6–14: Range of hosts whose system configuration information can be verified from a base manager

Host type		Verify
Local host		Y
Parent host		N
Relay manager		Y[#1]
Base manager		Y[#1]
Agent	Directly under the local host	Y[#1]
	Under a relay manager	Y[#1]
	Under a lower-level base manager	N[#2]
Remotely monitored host	Under the local host	Y
	Under a lower-level base manager	N[#2]

Legend:

Y: The information can be verified.

N: The information cannot be verified.

#1

Not recommended because the system configuration, including the integrated manager, would be more than three tiers.

#2

Verify the system hierarchy on the lower-level base manager because a firewall might prevent the integrated manager from connecting to the agent or remotely monitored host under the lower-level base manager.

Verify the system hierarchy while connection can be established with the monitored host. If connection cannot be established, the verification process might require a considerable amount of time.

You can check the verification results in the following windows:

- **Host List** page or **IM Configuration** page of the IM Configuration Management window
- Execution Results window

If the information held by JP1/Base on the manager running IM Configuration Management differs from the information in the IM Configuration Management database, the affected hosts are represented by error-status icons in the tree display area of the **IM Configuration** page.

If verification fails, an error-status icon is displayed for the affected host in the tree display area of the **IM Configuration** page.

Configuration definition information cannot be verified on hosts running a version of JP1/Base earlier than version 9. In this case, the affected hosts are represented by error-status icons in the tree display area of the **IM Configuration** page.

If the configuration definition information on the manager does not exist or if the information held by JP1/Base and the information in the IM Configuration Management database do not match, verification on the manager fails, the processing is terminated, and the system hierarchy appears grayed in the tree display area on the **IM Configuration** page.

If the system hierarchy appears grayed in the tree display area on the **IM Configuration** page, check and, if necessary, revise the configuration definition information (agent configuration), and reapply the agent configuration.

For a base manager, first execute **Synchronize IM Configuration** on the integrated manager, and then check, on the base manager, whether **Collect IM Configuration** was executed.

For details, see *3.2.4(3) Applying a system hierarchy to a system managed by IM Configuration Management* in the *JP1/Integrated Management - Manager Configuration Guide*.

6.2.5 Editing the system hierarchy

Using IM Configuration Management, you can create and edit configuration definition information by adding, moving, or deleting hosts.

You can edit the system hierarchy in the IM configuration management viewer. Use the Edit Agent Configuration window for agents, or the Edit Remote Monitoring Configuration window for remotely monitored hosts.

If the configuration definition information is changed by any method other than IM Configuration Management, verify the system hierarchy to check whether the configuration definition information held in JP1/Base matches the configuration definition information held in the IM Configuration Management database.

For details, see *6.2.4 Verifying the system hierarchy*.

The functions for editing the system hierarchy using IM Configuration Management are described next.

(1) Obtaining update rights

When you apply the system configuration definition information, you must acquire update rights for configuration definition information so that the information cannot be applied from another IM configuration management viewer.

To acquire update rights for configuration definition information, perform either of the following:

- In an agent configuration
  In the Edit Agent Configuration window, select the **Acquire update right** check box.

- In a remote monitoring configuration
  In the Edit Remote Monitoring Configuration window, select the **Acquire update right** check box.

If you attempt to obtain update rights while IM Configuration Management - View on another host has exclusive rights to the configuration definition information and profiles, an error message appears and the attempt fails. In this case, you must find out which user has exclusive rights in the Login User List window and revoke those rights.

(2) Adding hosts

You can add agents and remotely monitored hosts to the system hierarchy.

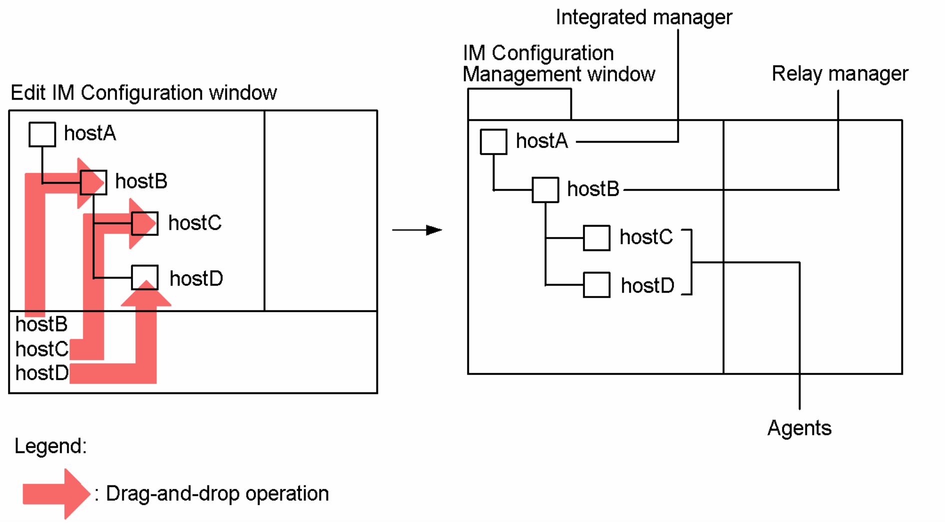
(a) Adding a host to the system hierarchy by using the Edit Agent Configuration window

To add a host to the system hierarchy, perform either of the following in the Edit Agent Configuration window:

- Select a host in the **Host List**, and then move it to the tree display area by drag-and-drop operation.
- Select a host in the tree display area, and then choose **Edit** and **Add Host**.

If a 3-tier system configuration is defined in the tree display area in the Edit Agent Configuration window, after the system hierarchy is applied, a manager defined in the middle tier is displayed as a relay manager in the tree display area on the **IM Configuration** page of the IM Configuration Management window.

Figure 6–11: Adding hosts to the system hierarchy with IM Configuration Management



(b) Adding a remotely monitored host to the system hierarchy by using the Edit Remote Monitoring Configuration window

To add a host to a system hierarchy, in the Edit Remote Monitoring Configuration window, select a host in the Host List, and drag it to the tree display area. Note that you cannot define a hierarchical configuration for remotely monitored hosts. If you manage remotely monitored hosts from the integrated manager, use the integrated manager to add the remotely monitored hosts directly under the integrated manager. If you manage remotely monitored hosts from base managers, use each base manager to add the corresponding remotely monitored hosts under that base manager.

(3) Moving hosts

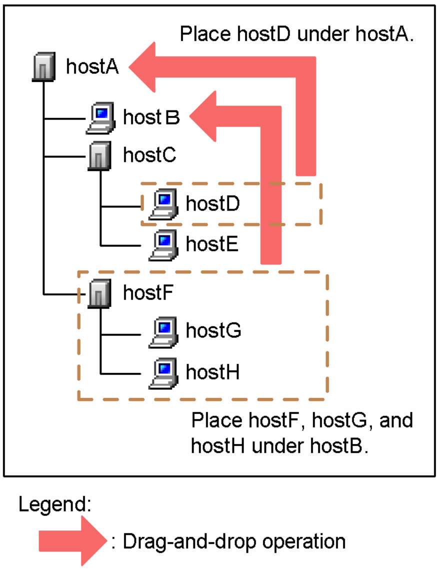
In a system hierarchy, you can move base managers, relay managers, and agents. You cannot move remotely monitored hosts in a system hierarchy. To move a remotely monitored host, delete it from the system hierarchy, and then add it at the preferred position in the system hierarchy.

If you want to move an agent host to another tier in a system hierarchy, in the Edit Agent Configuration window, perform either of the following:

- Select a host in the tree display area, and then move it to another level by drag-and-drop operation.
- Select a host in the tree display area and choose **Edit** and **Cut**. Then select a higher-level host to place the selected host under, and choose **Edit** and **Paste**.

When you move a relay manager, the agents in its domain are also moved.

Figure 6–12: Moving a host in the system hierarchy with IM Configuration Management



The following table describes the types of higher-level hosts you can specify for each type of target host.

Table 6–15: Types of higher-level hosts that can be specified when moving a target host

Target host	Specifiable higher-level host	Moved hosts
Integrated manager	--	--
Base manager	• Integrated manager • Relay manager	The selected base manager
Relay manager	• Integrated manager • Relay manager	The selected relay manager and the agents in its domain
Agent	• Integrated manager • Relay manager	The selected agent
Remotely monitored host	--	--

Legend:

--: Cannot be moved.

(4) Deleting hosts

You can delete base manager hosts, relay manager hosts, agent hosts, and remotely monitored hosts from the system hierarchy.

To delete the entire system hierarchy, from the **File** menu, select **New**.

(a) Deleting an agent from the system hierarchy by using the Edit Agent Configuration window

To delete a host from the system hierarchy, perform either of the following in the Edit Agent Configuration window:

- Select a host in the tree display area, and then move it the **Host List** by drag-and-drop operation.
- Select a host in the tree display area, and then choose **Edit** and **Delete Host**.

When you delete a base manager or relay manager, the agents in its domain are also deleted from the system hierarchy. An integrated manager cannot be deleted.

(b) Deleting a remotely monitored host from the system hierarchy by using the Edit Remote Monitoring Configuration window

To delete a host from the system hierarchy, perform either of the following in the Edit Remote Monitoring Configuration window:

- Select a host in the tree display area, and then move it the **Host List** by drag-and-drop operation.
- Select a host in the tree display area, and then choose **Edit** and **Delete Host**.

(5) Saving edited information

You can save edited configuration definition information as a configuration definition file (`jbs_route.conf`) on a host on which the IM configuration management viewer is running.

Use the **Save** command to temporarily save a system hierarchy you are creating, or to manage records of a system configuration.

(a) Saving edited configuration information on an agent by using the Edit Agent Configuration window

To save edited configuration definition information as a configuration definition file (`jbs_route.conf`) on a host on which the IM configuration management viewer is running, in the Edit Agent Configuration window, select **Save Agent Configuration** from the **File** menu.

(b) Saving edited configuration information on a remotely monitored host by using the Edit Remote Monitoring Configuration window

To save edited configuration definition information as a configuration definition file (`jbs_route.conf`) on a host on which the IM configuration management viewer is running, in the Edit Remote Monitoring Configuration window, select **Save Remote Monitoring Configuration** from the **File** menu.

(6) Loading the system hierarchy

You can load the configuration definition information held in the IM Configuration Management database and the configuration definition information saved on a host on which the IM configuration management viewer is running.

(a) Reading the agent configuration information by using the Edit Agent Configuration window

In the Edit Agent Configuration window, you can load configuration definition information in either of the following two ways:

- Information in the IM Configuration Management database
  To load the configuration definition information held in the IM Configuration Management database, in the Edit Agent Configuration window, select **Acquire Agent Configuration from Server** from the **File** menu.
- Information on the IM Configuration Management - View host
  To load the configuration definition information saved in a configuration definition file (`jbs_route.conf`) on a host on which the IM configuration management viewer is running, in the Edit Agent Configuration window, select **Open Agent Configuration** from the **File** menu.

(b) Reading the remote monitoring configuration information by using the Edit Remote Monitoring Configuration window

In the Edit Remote Monitoring Configuration window, you can load configuration definition information in either of the following two ways:

- Information in the IM Configuration Management database
  To load the configuration definition information held in the IM Configuration Management database, in the Edit Remote Monitoring Configuration window, select **Acquire Remote Monitoring Configuration from Server** from the **File** menu.
- Information on the IM Configuration Management - View host
  To load the configuration definition information saved in a configuration definition file (`jbs_route.conf`) on a host on which the IM configuration management viewer is running, in the Edit Remote Monitoring Configuration window, select **Open Remote Monitoring Configuration** from the **File** menu.

(7) Exchanging hosts

You can exchange an agent or a remotely monitored host in the system hierarchy and an agent or a remotely monitored host in the **Host List**.

(a) Exchanging agents by using the Edit Agent Configuration window

To exchange hosts, perform the following in the Edit Agent Configuration window:

1. Select a host in the tree display area, and select **Exchange Hosts** from the **Edit** menu.
2. In the **Exchange Hosts** dialog box, enter a value for **Host after the exchange**.

(b) Exchanging remotely monitored hosts by using the Edit Remote Monitoring Configuration window

To exchange hosts, perform the following in the Edit Remote Monitoring Configuration window:

1. Select a host in the tree display area, and select **Exchange Hosts** from the **Edit** menu.
2. In the **Exchange Hosts** dialog box, enter a value for **Host after the exchange**.

(8) Configuring a base manager

To configure a host as a base manager, you must configure the settings both on the integrated manager host and on the host you want to configure as a base manager.

For details, see *3.2.4(1)(e) Setting a site manager* in the *JP1/Integrated Management - Manager Configuration Guide*.

(9) Releasing the settings for a base manager

To release the settings for a base manager on a host, you must release the settings both on the integrated manager and on the base manager.

For details, see *3.2.4(1)(f) Removing a site manager* in the *JP1/Integrated Management - Manager Configuration Guide*.

6.2.6 Applying the system hierarchy

You can use IM Configuration Management to apply the agent configuration in the edited configuration definition information to all agents in the system hierarchy.

For the agent configuration, the following methods for applying the system hierarchy are available:

- Differential distribution method

  The configuration definition information is deleted from or distributed to only those hosts that have been changed in the current agent configuration. For hosts that have been deleted, the configuration definition information is deleted. For hosts that have been added to the agent configuration, the configuration definition information is distributed to the hosts and higher manager hosts. This enables the system hierarchy to be applied without affecting the monitoring of the hosts that are unchanged in the agent configuration. Note that the manager host's JP1/Base version must be 11-10 or later.
- Batch distribution method (with deletion of the configuration)

  The configuration definition information is deleted from all hosts in the current agent configuration, and then the configuration definition information is distributed to all hosts in the newly defined agent configuration.
- Batch distribution method (without deletion of the configuration)

  The configuration definition information is distributed to all hosts in the newly defined agent configuration without deleting the configuration definition information.

The following shows how to specify the methods for applying the system hierarchy.

- Differential distribution method

  To use the differential distribution method, specify it in the settings for the distribution of the configuration definition information in JP1/Base.
- Batch distribution method

  To use the batch distribution method, specify it in the settings for the distribution of the configuration definition information in JP1/Base. In the following setting conditions, specify either with deletion of the configuration or without deletion of the configuration.
  - Batch distribution method (with deletion of the configuration)

    To use the batch distribution method (with deletion of the configuration), disable the restrictions on viewing and operating business groups, and specify APPLY_CONFIG_TYPE as 00000000 in the common definition information.
  - Batch distribution method (without deletion of the configuration)

To use the batch distribution method (without deletion of the configuration), enable the restrictions on viewing and operating business groups, or specify APPLY_CONFIG_TYPE as 00000001 in the common definition information.

For details about the methods for distributing configuration definition information in JP1/Base, see the *JP1/Base User's Guide*. For details about the restrictions on viewing and operating business groups, see *4.20 Setting reference and operation restrictions on business groups* in the *JP1/Integrated Management - Manager Configuration Guide*. For details about the `APPLY_CONFIG_TYPE` settings in the common definition information, see *Apply-IM-configuration-method definition file (jp1cf_applyconfig.conf)* in *Chapter 2. Definition Files* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

If an agent configuration is applied after the system hierarchy has been defined and synchronized between the integrated manager and a base manager, the information under the base manager is cleared. In this case, you must synchronize the system hierarchy again.

(1) System hierarchy application methods

To apply the configuration definition information in the system hierarchy, perform the following:

- For an agent configuration

  In the Edit Agent Configuration window, from the **Operation** menu, select **Apply Agent Configuration**.

  For details, see *3.2.4(3) Applying a system hierarchy to a system managed by IM Configuration Management* in the *JP1/Integrated Management - Manager Configuration Guide*.

- For a remote monitoring configuration

  In the Edit Remote Monitoring Configuration window, from the **Operation** menu, select **Apply Remote Monitoring Configuration**.

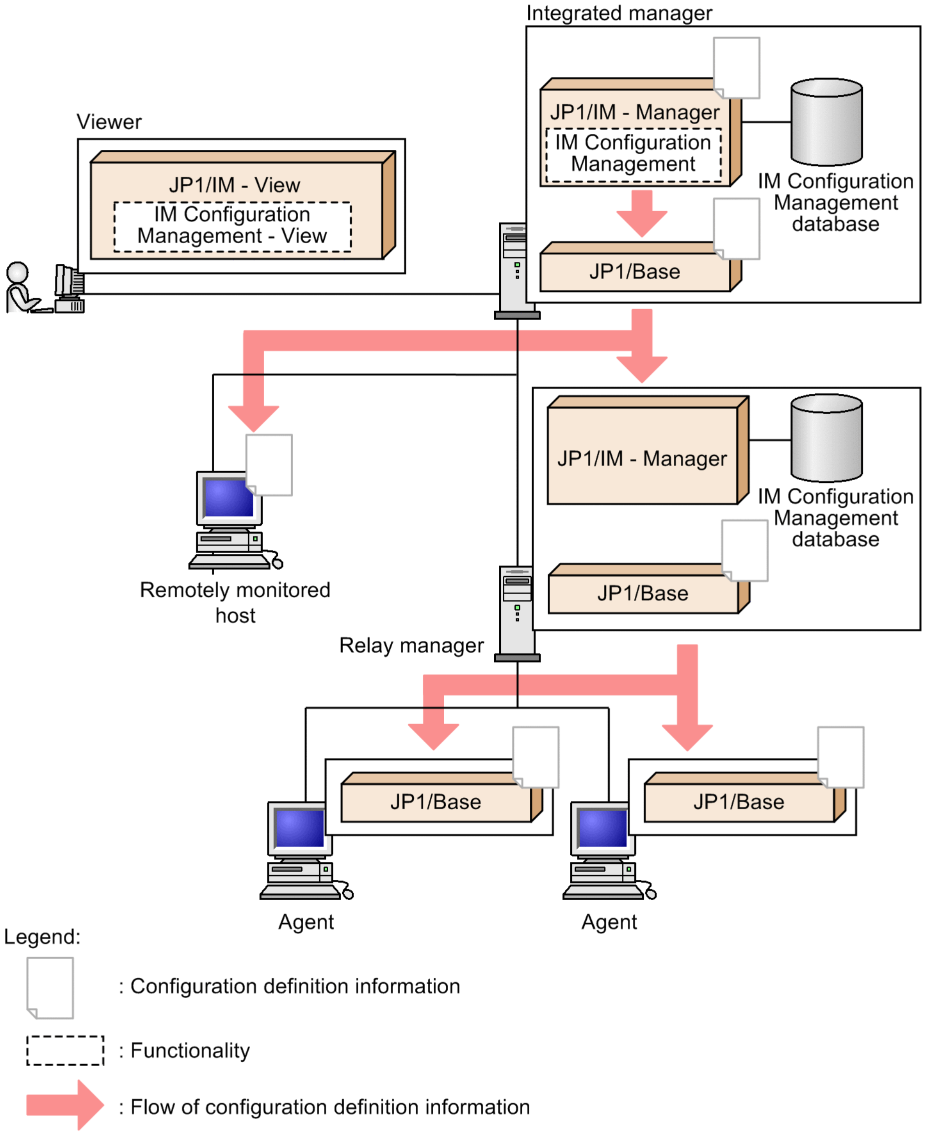
  To use a remote monitoring configuration, you must apply an agent configuration beforehand. When you apply an agent configuration, even if no agents exist on the hosts other than the manager hosts in that configuration, apply that configuration.

To apply the system hierarchy, you must obtain update rights. For details, see *6.2.5(1) Obtaining update rights*.

(2) General procedure for applying the system hierarchy with IM Configuration Management

The figure below shows the flow of processing when applying configuration definition information with IM Configuration Management.

Figure 6–13: Applying configuration definition information with IM Configuration Management


Integrated manager
Viewer
JP1/IM - View
IM Configuration Management - View
JP1/IM - Manager
IM Configuration Management
IM Configuration Management database
JP1/Base
Remotely monitored host
JP1/IM - Manager
IM Configuration Management database
JP1/Base
Relay manager
JP1/Base
JP1/Base
Agent
Agent
Legend:
: Configuration definition information
: Functionality
: Flow of configuration definition information

If an agent configuration is applied, the configuration definition file (`jbs_route.conf`) is overwrite-saved on a host on which IM Configuration Management is running. If you want to save the file contents before they are replaced, you must take a backup by saving the file under another name or by other means.

If an agent configuration is applied, the `jbsrt_distrib` command is executed on the manager on which IM Configuration Management is running. In this case, the configuration definition information is deleted from all agents in the system hierarchy, and the edited configuration definition information is distributed. For this reason, the same agent cannot be monitored from multiple manager hosts.

When a remote monitoring configuration is applied, **Remote** is added to the IM configuration types for the remotely monitored hosts.

If there is an agent host or remotely monitored host for which the system hierarchy cannot be applied, the host name is displayed in the dialog box.

The result of applying a system hierarchy are shown in a dialog box. Also, you can check the new system hierarchy on the **IM Configuration** page of the IM Configuration Management window. If processing failed, the affected host is represented by an error-status icon in the tree display area of the **IM Configuration** page. To view further details, click the **Basic Information** button in the node display area of the **IM Configuration** page.

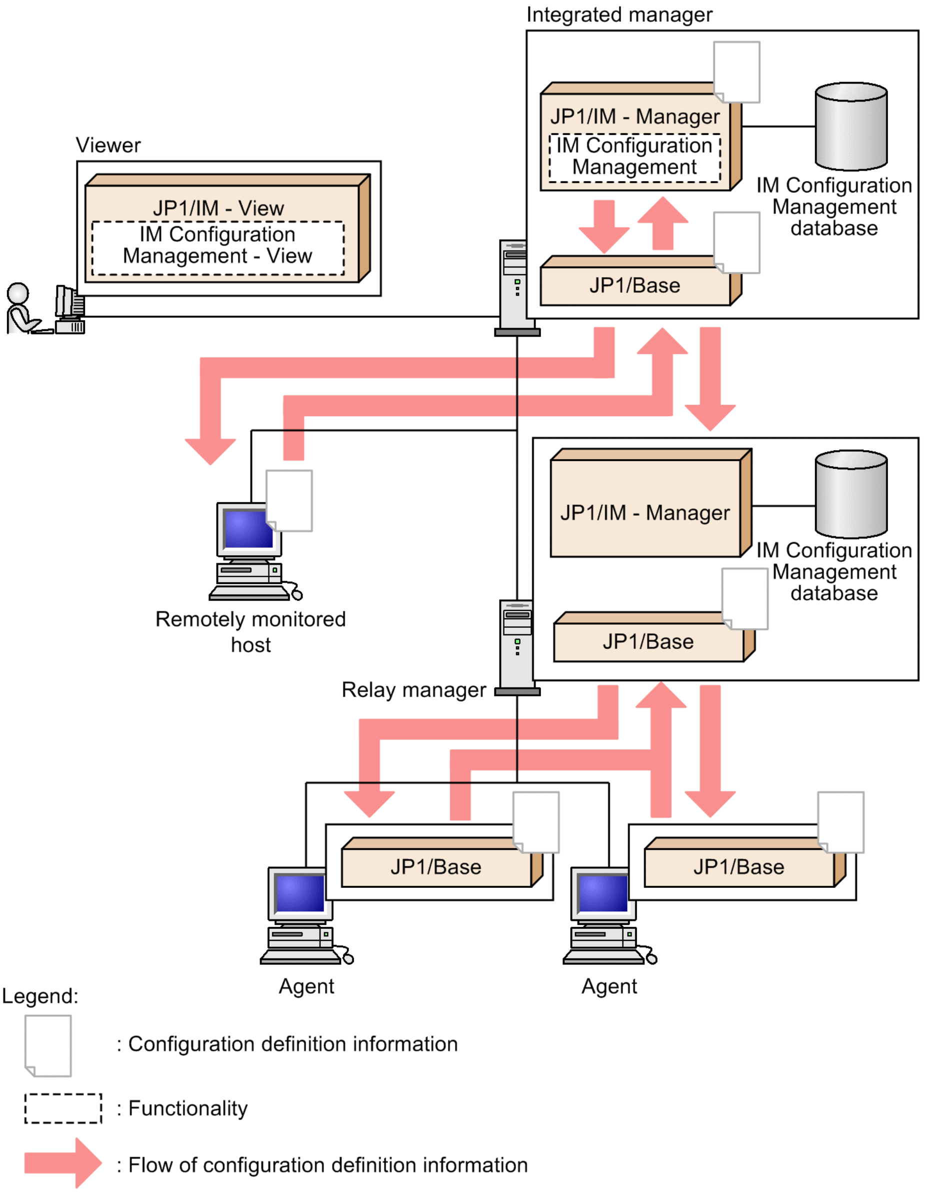
6.2.7 Synchronizing the system hierarchy

When using IM Configuration Management, if the system hierarchy is defined on base managers, you must synchronize the system hierarchy between the integrated manager and the base managers.

For details, see *3.2.4(3) Applying a system hierarchy to a system managed by IM Configuration Management* in the *JP1/Integrated Management - Manager Configuration Guide*.

To synchronize information among the systems, use the **Host List** page or **IM Configuration** page of the IM Configuration Management window.

Figure 6–14: Synchronizing configuration definition information with IM Configuration Management



Integrated manager
JP1/IM - Manager
IM Configuration Management
IM Configuration Management database
JP1/Base
Viewer
JP1/IM - View
IM Configuration Management - View
JP1/IM - Manager
IM Configuration Management database
JP1/Base
Remotely monitored host
Relay manager
JP1/Base
JP1/Base
Agent
Agent
Legend:
: Configuration definition information
: Functionality
: Flow of configuration definition information

When you synchronize configuration definition information, the `jbsrt_sync` command is executed on the integrated manager. This command collects and synchronizes the information on the integrated manager, and then updates the configuration definition information on all the hosts in the system hierarchy. Also, information about the remote monitoring configuration managed by base managers is collected. To synchronize the remote monitoring configuration, the version of JP1/IM - Manager must be 09-50 or later and the IM Configuration Management service must be running on base managers. If the IM Configuration Management service is not running, an error message appears, and acquisition of the remote monitoring configuration fails. You can ignore the error message indicating the failure of acquiring the remote monitoring configuration if only synchronization of agent configuration is required. If synchronization of a remote monitoring configuration is also required, start the IM Configuration Management service. The hosts in the IM configuration (agent configuration and remote monitoring configuration) managed by each base manager appear grayed out under the base manager in the tree display area of the IM Configuration Management window.

If no base managers are defined under the integrated manager, an error message is displayed and the system hierarchy is not synchronized among the hosts.

6.2.8 Selection of agent configuration or remote monitoring configuration

Using IM Configuration Management, you can use JP1/Base to monitor hosts in agent configuration, or remotely monitor hosts in a remote monitoring configuration.

In remote monitoring, a communication failure related to functional errors might cause log monitoring to stop or events to be lost. If the system cannot tolerate temporary stoppage of log monitoring, install JP1/Base and use it for log monitoring.

Use the following table to help decide whether to use monitoring using JP1/Base or remote monitoring.

Table 6–16: Guidelines for selecting a monitoring method

Item	Monitoring using JP1/Base	Remote monitoring
You perform monitoring that exceeds the restrictions for remote monitoring.	Y	N
The stoppage of log monitoring and loss of events is undesirable in the system.#1	Y	N
Log monitoring is required even while JP1/IM - Manager is stopped.	Y	Y#2
Monitored hosts are frequently stopped.	Y	N
WMI/NetBIOS (NetBIOS over TCP/IP) or SSH cannot be used on the system.#3	Y	N
Other than above.	Y	Y

Legend:

Y: Monitoring is performed.

N: Monitoring is not performed.

#1: When monitoring using JP1/Base, if a network failure occurs, JP1/Base acquires logs during the network failure. With remote monitoring, the monitoring stops if the failure cannot be recovered by retrying the operation.

#2: Not trapped if the event that occurred during the stop period exceeds the maximum size that can be collected by remote monitoring.

#3: With remote monitoring, settings for remote communication must be configured on the host on which JP1/IM - Manager has been installed and on the monitored hosts. The communication method depends on the OS of the monitored host. WMI/NetBIOS (NetBIOS over TCP/IP) must be configured if the monitored host is a Windows host, or SSH must be configured if the monitored host is a UNIX host.

For details about remote monitoring, see *6.6 Managing remotely monitored hosts*.

Some limitations apply to remote monitoring. For the limit values, see the following table.

Table 6–17: Limit values for remote monitoring

Item	Limit
Maximum number of remote monitoring units#1	1,024
Maximum size of the log files that can be remotely monitored	64 MB

Item	Limit
Maximum amount of log data that can be collected per monitoring interval (Windows)#2	10 KB#4
Maximum amount of log data that can be collected per monitoring interval (UNIX)#2	10 KB#4
Maximum amount of event log data that can be collected per monitoring interval#3	10 KB#4
Maximum amount of log data that can be collected by one JP1/IM - Manager	10 MB

#1: Total value of the number of log files monitored by remote log file trapping and the number of servers monitored by remote event-log trapping

#2: Total size of log data collected.

#3: Total size of Windows event log data collected.

#4: Default value. This limit value can be changed in the remote log trap environment definition file (`jp1cf_remote_logtrap.conf`). For details about the remote log trap environment definition file (`jp1cf_remote_logtrap.conf`), see *Remote log trap environment definition file (jp1cf_remote_logtrap.conf)* (*Chapter 2. Definition Files*) in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

(1) Functional differences between the agent configuration and the remote monitoring configuration

Table 6–18: Functional differences between the agent configuration and the remote monitoring configuration

Item	Agent configuration	Remote monitoring configuration
Use	• Monitoring of mission-critical applications (monitoring accuracy has priority) • Monitoring of JP1 products	When reducing load in the construction of an environment and for other operations has priority over monitoring accuracy#1
Monitored logs and file formats	• Syslog • User log • Event log (Windows version only) Log file formats - Sequential file (SEQ) - Sequential file (SEQ2) - Sequential file (SEQ3) - Wrap-around file (WRAP1) - Wrap-around file (WRAP2) - JP1 integrated trace log (HTRACE) - UPD-type log file (UPD)	• Syslog • User log • Event log (Windows version only) Log file formats - Sequential file (SEQ) - Sequential file (SEQ2) - Wrap-around file (WRAP2)
Scale	Log file monitoring#2 In Windows, the maximum number of log files that can be monitored is determined by the following formula: $(a + m) + (b + n) \leq 508$ Legend: *a*: Total number of log files that are monitored (identical files are counted as separate files) *b*: Total number of log files that are monitored by JP1/AJS log file monitoring jobs (identical files are counted as separate files) *m*: Number of `jevlogstart` commands that are executed *n*: Number of JP1/AJS log file monitoring jobs that are executed	Maximum total of log files and event logs monitored for each JP1/IM - Manager 1,024

Item	Agent configuration	Remote monitoring configuration
	In UNIX, the maximum number of files that can be monitored by one log file trap is 100. Therefore, the maximum number of files that can be monitored in a UNIX system depends on a kernel parameter setting (number of files that can be opened).	
Event issued	Log file monitoring User-specified event ID Event log monitoring Event ID specified in the filter in the event log trap action-definition file. If the event ID is not specified, `00003A71` is assumed.	Log file monitoring User-specified event ID Event log monitoring Event ID specified in the filter in the event log trap action-definition file. If the event ID is not specified, `00003A71` is assumed.
Size of log files that can be monitored	2 gigabytes or less	64 megabytes or less
Size of log data that can be collected during a monitoring interval	Unlimited	In Windows: 200 kilobytes or less In UNIX: 50 kilobytes or less
Maximum size of event log that can be collected per monitoring interval	Unlimited	200 kilobytes or less
Log file trap start option	• Monitoring interval 1 to 86,400 seconds	• Monitoring interval 60 to 86,400 seconds An interval of 5 minutes is recommended when the maximum configuration is used.
	• Number of log files that can be monitored per monitoring (number of log file names that can be specified) In Windows: 1 to 32 In UNIX: 1 to 100	• Number of log files that can be monitored per monitoring (number of log file names that can be specified): 1 to 32
	• Read from the start of log files Can be specified.	• Read from the start of log files Cannot be specified.
	• Display command name Can be specified.	• Display command name Cannot be specified.
	• Destination server name Can be specified.	• Destination server name Cannot be specified.
	• Monitored host name Cannot be specified.	• Monitored host name Can be specified.
	• Logical host name Cannot be specified.	• Logical host name Can be specified.
	In Windows, Unicode can be specified.	Various character encodings that can be specified for the OS.
	• Log data output source host name Can be specified.	• Log data output source host name Cannot be specified.
	• Regular expression type Cannot be specified (common definition information is specified).	• Regular expression type Extended regular expressions can be specified.

Item	Agent configuration	Remote monitoring configuration
Log file trap action definition	• Retry interval 1 to 600 seconds	• Retry interval 3 to 600 seconds
	• Number of held JP1 events 0 to 1,000	• Number of held JP1 events 0 to 100
	• Record format of log files Variable-length record format: `\n`, a line termination character, or a line termination symbol can be specified. Fixed-length record format: Record length can be specified as the line delimiter.	• Record format of log files `\n` in the variable-length record format.
	• Threshold value of retry count Can be specified.	• Threshold value of retry count Cannot be specified.
	• File type One of `SEQ`, `SEQ2`, `SEQ3`,[#3] `WRAP1`, `WRAP2`, `HTRACE`, or `UPD`[#3] can be specified.	• File type One of `SEQ`, `SEQ2`, or `WRAP1` can be specified.
	• Header size Can be specified.	• Header size Cannot be specified.
	• JP1 event for the UPD type Can be specified.[#4]	• JP1 event for the UPD type Cannot be specified.
Event log trap action definition	• Destination event server Can be specified.	• Destination event server For a physical host, the physical host is connected. For a logical host, the logical host is connected.
	• Monitoring interval 1 to 180 seconds	• Monitoring interval 60 to 86,400 seconds An interval of 5 minutes is recommended when the maximum configuration is used.
	• Number of retries Cannot be specified.	• Number of retries 1 to 3,600
	• Retry interval Cannot be specified.	• Retry interval 3 to 600 seconds
	• Extended attribute name Can be specified.	• Extended attribute name Cannot be specified.
Operation when manager stops	If the manager host stops or a network failure occurs between the manager host and a monitored host, an agent host can convert the event into a JP1 event, and retry transfer of the generated JP1 event to the manager host.	The log files and Windows event logs generated while JP1/IM - Manager is stopped are trapped the next time remote monitoring is started.
Operation when network fails		If network operation is restored after a failure before the maximum number of retries is reached and monitoring stops, the manager host will be notified of the log data collected during the failure period. Notification will be done only when none of the following restrictive conditions exist: • The difference in the size of the log data exceeds 10 kilobytes.[#1] • The size of the monitored log exceeds 64 megabytes. • When the file format is WRAP2, the log was wrapped around and log data was deleted during the failure period.

Item	Agent configuration	Remote monitoring configuration
Host name	A host name registered in the `hosts` file or DNS or a host name defined in `jp1hosts` or `jp1hosts2` is specified for a host name.	A host name registered in the `hosts` file or DNS is specified for a host name. The settings of `jp1hosts` and `jp1hosts2` are not referenced.

#1: If the amount of log data output during the monitoring interval exceeds this limit value in UTF-8, JP1 events cannot be displayed in JP1/IM - View. If this is a possibility, consider using log monitoring in an agent configuration. For details about the limit values, see *Table 6-17 Limit values for remote monitoring*.

#2: When IM Configuration Management is used, the maximum number of log file traps that can be managed is 100 for each agent host.

#3: Can be specified only if the agent's JP1/Base version is 10-00 or later.

#4: The default value is 10 kilobytes. This limit value can be changed in the remote log trap environment definition file (`jp1cf_remote_logtrap.conf`). For details about the remote log trap environment definition file (`jp1cf_remote_logtrap.conf`), see *Remote log trap environment definition file (jp1cf_remote_logtrap.conf)* (*Chapter 2. Definition Files*) in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

For details about each function in an agent configuration, see the documentation for the JP1/Base version that is installed on the monitoring target.

6.3 Virtualization configuration management

IM Configuration Management makes it possible to specify any host type (physical host or virtual host) for a registered host. When host types are specified, the system hierarchy of virtual hosts running on multiple virtualization system management hosts and on VMM hosts (called *virtualization system configuration hereafter*) is displayed in tree form for easy understanding. You can use the following functions to manage a virtualization system configuration:

- Collecting and setting the virtualization system configuration information

  In IM Configuration Management, you can set the host type, VMM host name, type of virtualization environment management software for the management software, and other information related to the virtualization system configuration.
- Displaying the virtualization system configuration

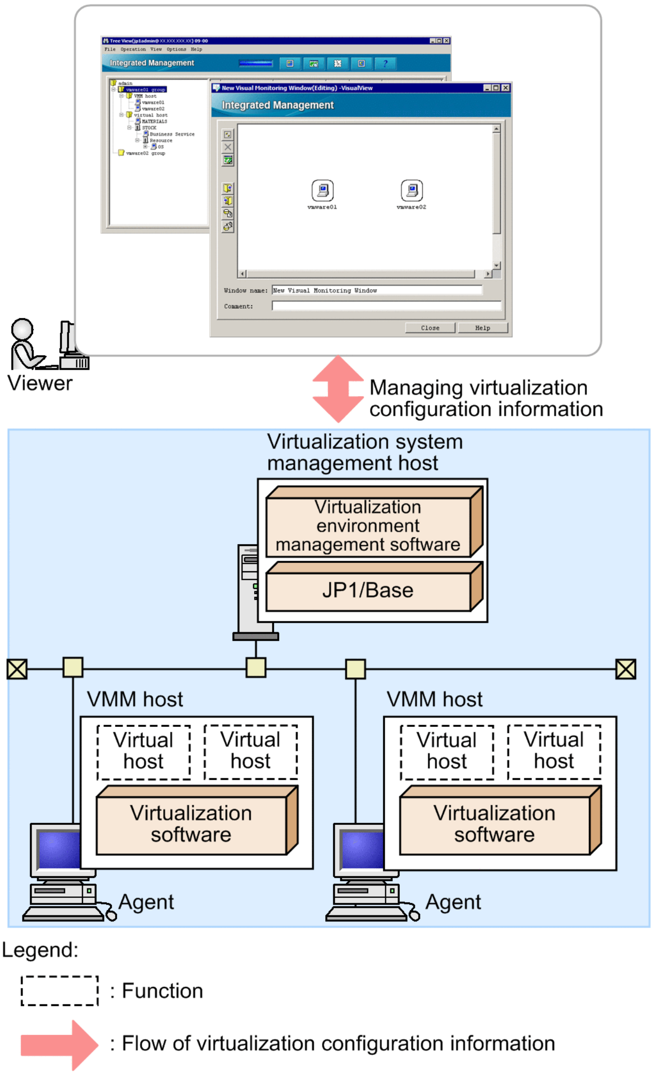
  You can display the virtual system configuration in a tree view on the **Host List** page of the IM Configuration Management window.
- Importing the virtualization system configuration into the Central Scope

  You can import the virtualization system configuration into the Central Scope and monitor it there.

Even if you are managing a system hierarchy that includes virtual hosts, you can specify *physical host* as the host type without problems when you do not use these functions.

The following figure overviews management of virtualization system configurations.

Figure 6–15: Management of virtualization system configurations



To collect virtualization system configuration information (hereinafter called *virtualization configuration information*), the following virtualization software and virtualization environment management software are required:

- Virtualization environment management software that can be used for a virtualization system management host:
  vCenter, JP1/SC/CM, SCVMM, and HCSM
- Virtualization software that can be used for a VMM host:
  Hyper-V, Hitachi Compute Blade logical partitioning feature, VMware ESX, and KVM

The following describes functionality for managing virtualization system configuration by using IM Configuration Management.

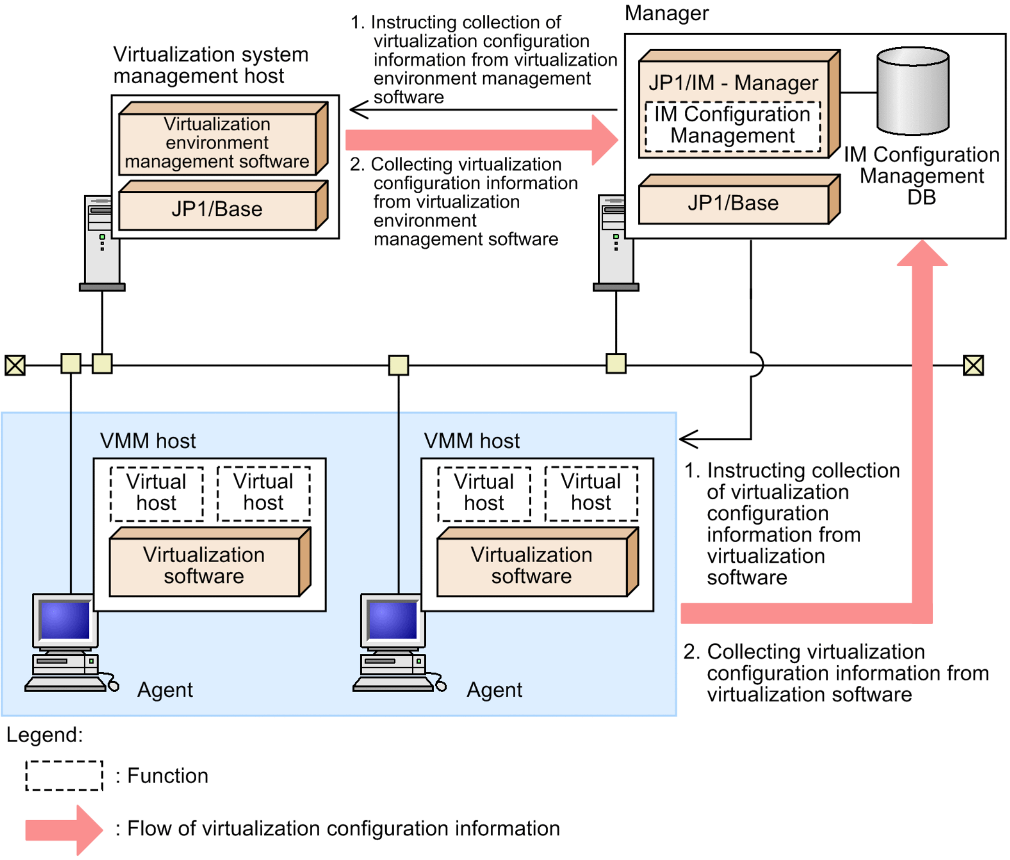
6.3.1 Collecting virtualization configuration information

You can use a command or the IM Configuration Management window to collect virtualization configuration information.

The communication described for this function requires host names to be able to be resolved by the OS.

The following figure shows how virtualization configuration information is collected.

Figure 6–16: Collection of virtualization configuration information


Manager
Virtualization system management host
1. Instructing collection of virtualization configuration information from virtualization environment management software
Virtualization environment management software
JP1/Base
2. Collecting virtualization configuration information from virtualization environment management software
JP1/IM - Manager
IM Configuration Management
JP1/Base
IM Configuration Management DB
VMM host
Virtual host
Virtual host
Virtualization software
Agent
VMM host
Virtual host
Virtual host
Virtualization software
Agent
1. Instructing collection of virtualization configuration information from virtualization software
2. Collecting virtualization configuration information from virtualization software
Legend:
: Function
: Flow of virtualization configuration information

The flow is described below. Follow the numbers in the figure.

1. Perform the following to order collection of virtualization configuration information:
   - On the manager, execute the command for collecting virtualization configuration.
   - In the IM Configuration Management window, execute **Collect Virtualization Configuration** or **Batch Collect Virtualization Configurations**.
2. Collect virtualization configuration information from the following hosts:
   - Virtualization system management host
   - Virtual host running KVM
   - Virtual host running VMware ESX

(1) When executing a command for collecting virtualization configuration information from the manager

The following table describes the supported types of virtualization software and virtualization environment management software and the corresponding command names.

Table 6–19: Types of virtualization software and virtualization environment management software (when a command is used)

Type of virtualization software or virtualization environment management software	Command name	Scope of collection
vCenter	`jcfcolvmvc`	- Virtualization system management hosts running with vCenter - Virtual hosts running with VMware ESX
JP1/SC/CM	`jcfcolvmvirtage`	Virtual hosts running with Hitachi Compute Blade logical partitioning feature
SCVMM#1	`jcfcolvmscvmm`	- Virtualization system management hosts running with SCVMM - Virtual hosts running with Hyper-V - Virtual hosts running with vCenter and VMware ESX when vCenter is managed by SCVMM
HCSM	`jcfcolvmhcsm`	Virtual hosts running Hitachi Compute Blade logical partitioning feature and host names that can be obtained from HCSM#2
KVM	`jcfcolvmkvm`	Virtual hosts running KVM#3
VMware ESX	`jcfcolvmesx`	Virtual hosts running with VMware ESX

#1: Supported on Windows only.

#2: You can collect only host names and host types as the virtualization configuration information on hosts that are not virtual hosts running Hitachi Compute Blade logical partitioning feature. Also, the host type that is collected from these hosts is `Unknown`.

#3: When virtualization configuration information is collected from KVM, the host identification names defined in KVM are collected. (A host identification name, called a *domain name* in KVM, is the name that is shown as `Id Name` when the `virsh list` command is executed.) As the host name of a virtual host, specify the same name as the corresponding host identification name defined in KVM. If you change the host name of a virtual host, redefine the corresponding host identification name defined in KVM so that they are identical.

(2) When performing collection or batch-collection of virtualization configuration in the IM Configuration Management window

You can collect virtualization configuration information on the virtualization system management host and the virtual hosts running on VMM hosts.

The virtualization configuration information on virtual hosts running KVM can be collected from any host on which KVM is running. The virtualization configuration information on the virtual hosts running virtualization software other than KVM can be collected from the virtualization system management host.

The virtualization software from which information can be collected varies according to the software installed on the host that collects virtualization information. The following table describes the software installed on the host that collects virtualization information and the corresponding virtualization software from which information can be collected.

Table 6–20: Software installed on hosts that collect information and corresponding software from which information is collected (when the IM Configuration Management window is used)

Software installed on the host collecting virtualization configuration information	Collection target	Scope of collection
vCenter	VMware ESX	- Virtualization system management host running with vCenter - Virtual hosts running with VMware ESX

Software installed on the host collecting virtualization configuration information	Collection target	Scope of collection
JP1/SC/CM	Hitachi Compute Blade logical partitioning feature	Virtual hosts running with Hitachi Compute Blade logical partitioning feature
SCVMM[#1]	• Hyper-V • vCenter[#2] • VMware ESX[#2]	• Virtualization system management host running with SCVMM • Virtual hosts running with Hyper-V • Virtual hosts running with vCenter and VMware ESX when vCenter is managed by SCVMM
HCSM	Hitachi Compute Blade logical partitioning feature	Virtual hosts running Hitachi Compute Blade logical partitioning feature and host names that can be obtained from HCSM[#3]
KVM	• KVM	Virtual hosts running KVM [#4]

#1: Supported on Windows only.

#2: vCenter and VMware ESX are collected when vCenter is managed by SCVMM.

#3: You can collect only host names and host types as the virtualization configuration information on hosts that are not virtual hosts running Hitachi Compute Blade logical partitioning feature. Also, the host type that is collected from those hosts is `Unknown`.

#4: When virtualization configuration information is collected from KVM, the host identification names defined in KVM are collected. (A host identification name, called a *domain name* in KVM, is the name that is shown as `Id Name` when the `virsh list` command is executed.) As the host name of a virtual host, specify the same name as the corresponding host identification name defined in KVM. If you change the host name of a virtual host, redefine the corresponding host identification name defined in KVM so that they are identical.

6.3.2 Setting virtualization configuration information

To manage a virtualization system configuration, you must set virtualization configuration information in IM Configuration Management. Even if you manage a system hierarchy that includes virtual hosts, you do not have to set virtualization configuration information when you do not use the function that displays virtual system configuration on the **Host List** page. For details, see *6.3 Virtualization configuration management*.

The following three methods can be used to set virtualization configuration information.

(1) Entering host information of virtual hosts in IM Configuration Management

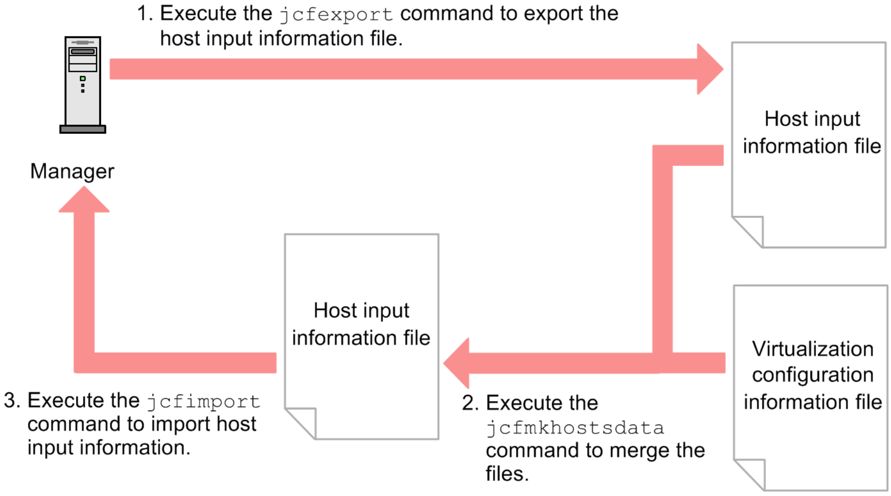
Directly register virtual hosts as the hosts to be managed. Select **Virtual host** for the host type, and then specify **VMM host**.

(2) Importing information of hosts in virtualization configuration

Acquire information of hosts in virtualization configuration, and merge it with the host input information file that is output from IM Configuration Management. Then import the merged host input information file into IM Configuration Management.

The following figure shows the flow of updating information of hosts in virtualization configuration.

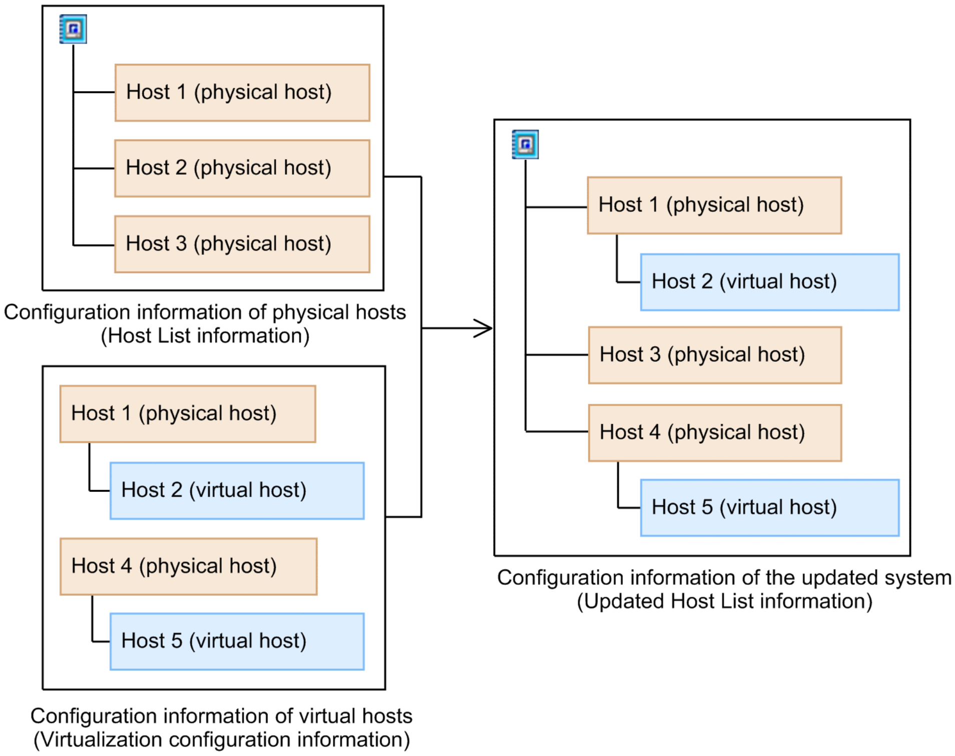
Figure 6–17: Flow of updating information of hosts in virtualization configuration


1. Execute the jcfexport command to export the host input information file.
Manager
Host input information file
Virtualization configuration information file
Host input information file
2. Execute the jcfmkhostsdata command to merge the files.
3. Execute the jcfimport command to import host input information.

If there are multiple virtualization configuration information files, repeat the `jcfmkhostsdata` command as many times as the number of files to complete updating host information.

The following figure shows an example of updating virtualization configuration information.

Figure 6–18: Example of updating virtualization configuration information



(3) Performing collection or batch-collection of virtualization configuration from the IM Configuration Management window

Addition of VMM hosts and changes of virtualization configuration are applied to virtualization configuration information, and the information is displayed in the IM Configuration Management window.

(a) When host information is updated

If collected virtualization configuration information includes host information that indicates that a host is already registered in the IM configuration management database, IM Configuration Management treats the collected host information and the registered host information as being the same and updates the host type in the host information. If the host type in the collected host information differs from the host in the host information registered in the IM configuration management database, IM Configuration Management does not update the host information because the hosts might be different despite having the same host name. If, however, the host type of the hosts is `Unknown`, IM Configuration Management updates the host information. Note also that the status of the collection of virtualization configuration information is not the same for a registered host whose host type is different and for a virtualization system management host managing a registered host whose host type is different. Table 6-21 describes the host type conditions for updating host information, and Table 6-22 describes changes in the status of the collection for virtualization configuration information.

Table 6–21: Host type conditions for updating host information

Type of host from which information collected	Registered host type			
	Physical host	Logical host	Virtual host	Unknown
Physical host	Y	N	N	Y
Logical host	--	--	--	--
Virtual host	Y/N#1	N	Y	Y
Unknown (hosts managed by HCSM not running Hitachi Compute Blade logical partitioning feature)	N	N	N	Y
Unknown#2	Y	--	Y	--

Legend:

Y: Can be updated.

Y/N: Can be updated conditionally.

N: Cannot be updated.

--: Not applicable.

#1: Host information can be updated if the host meets both of the following conditions. The host type of the host meeting the conditions is `Virtual host`.

- KVM is the registered virtual manager type of the host.
- Hitachi Compute Blade logical partitioning feature is the virtual manager type of the VMM host.

#2: The relevant host does not exist in the collected data, or the data has been deleted.

Table 6–22: Changes in the status of virtualization configuration information collection

Status of virtualization configuration information collection	Trigger for changing the status of virtualization configuration information collection
No information collected	Host information has not been collected yet.
Collection failed	The collection of host information failed because an attempt to connect to the host failed, the user could not be authenticated in the OS, or a condition for managing the virtualization system configuration was not met.
Information collected	The collection of host information was successful.

Status of virtualization configuration information collection	Trigger for changing the status of virtualization configuration information collection
Mismatch	The host type in the collected host information differs from the host type registered in the IM configuration management database.

When virtualization configuration information is collected from the virtualization system management host, the virtualization configuration information on the hosts managed by the virtualization system management host is updated. Also, when this information is collected, the information (VMM host information) about the relationship between the virtualization system management host and VMM hosts is collected and stored in the IM configuration management database. However, if the virtualization system management host is deleted or the virtualization configuration information of the virtualization system management host is changed, the stored VMM host information will be deleted. For details, see *6.3.2(3)(c) When VMM host information is deleted*.

If virtualization configuration is changed when virtualization configuration is collected, the virtualization configuration is changed as shown in the following table.

Table 6–23: Virtualization configuration after collection

Change	Virtualization configuration after collection
A virtual host is added.	The host is added, and VMM host information is provided.
A virtual host is deleted.	• VMM host information of the host is deleted. • The host is displayed directly under the Host List because the relationship between the virtual host and the VMM host is broken.
A virtual host is moved.	VMM host information of the host is updated.
A stopped virtual host starts.	No configuration change.
A running virtual host stops.	No configuration change.
A running virtual host is suspended.	No configuration change.
A VMM host is added.	The VMM host and virtual hosts running on the VMM host are registered.
A VMM host is deleted.	• VMM host information of the host is deleted. • Information about the virtualization system management host that manages the VMM host is deleted. • The VMM host is displayed directly under the Host List because the relationship between the virtual host and the VMM host is broken.

(b) When virtualization configuration information is deleted

If the host type in the collected virtualization configuration information is **Logical host** or **Unknown**, virtualization configuration information cannot be maintained. Therefore, even if virtualization configuration information is set when the host type is **Physical host** or **Virtual host**, if the host type is changed to **Logical host** or **Unknown**, the virtualization configuration information is deleted.

The following table describes the cases when virtualization configuration information is deleted when the host type is changed.

Table 6–24: Cases when virtualization configuration information is deleted when the host type is changed

Host type before change	Host type after change			
	Physical host	Logical host	Virtual host	Unknown
Physical host	N	Y	N	Y
Logical host	--	--	--	--
Virtual host	N	Y	N	Y
Unknown#	--	--	--	--

Legend:

Y: Deleted.

N: Not deleted.

--: Not applicable.

#: The relevant host does not exist in the collected data, or the data has been deleted.

(c) When VMM host information is deleted

VMM host information is deleted from the IM configuration management database in the following cases:

- The virtualization system management host on which vCenter, JP1/SC/CM, SCVMM, or HCSM is installed is deleted.
- The virtual manager type of the virtualization system management host on which vCenter, JP1/SC/CM, SCVMM, or HCSM is installed is changed.
- The host type of the virtualization system management host on which vCenter, JP1/SC/CM, SCVMM, or HCSM is installed is changed.

6.3.3 Exclusive rights for virtualization configuration information

When you edit virtualization configuration information with an IM configuration management viewer, the IM configuration management viewer automatically acquires update rights to prevent other IM configuration management viewers from editing information while you are editing it. You cannot acquire update rights when another IM configuration management viewer has already acquired exclusive rights for virtualization configuration information. If you try to acquire them, an error message is displayed. In that case, in the Login User List window, find the user who has acquired exclusive rights, and request them to release the exclusive rights.

The following table describes the exclusive relationship of virtualization configuration information.

Table 6–25: Exclusive relationship of virtualization configuration information

Operation from another IM configuration management viewer		Collection of virtualization configuration		Batch-collection of virtualization configuration
		Same host	Different host	
Host	View	Y	Y	Y
	Edit	N	Y	N
	Collect information	N	Y	N
	Collect virtualization configuration	N	Y	N

Operation from another IM configuration management viewer		Collection of virtualization configuration		Batch-collection of virtualization configuration
		Same host	Different host	
	Batch-collect virtualization configurations	N	N	N
IM configuration	Collect	N	N	N
	Exclusive-update	N	N	N
	Synchronize	N	N	N
	Verify	N	N	N
Profile	View	Y	Y	Y
	Exclusive-edit	N	Y	N
Export		N	N	N
Import		N	N	N

Legend:

Y: Can perform the operation.

N: Cannot perform the operation.

6.3.4 Displaying virtualization system configuration

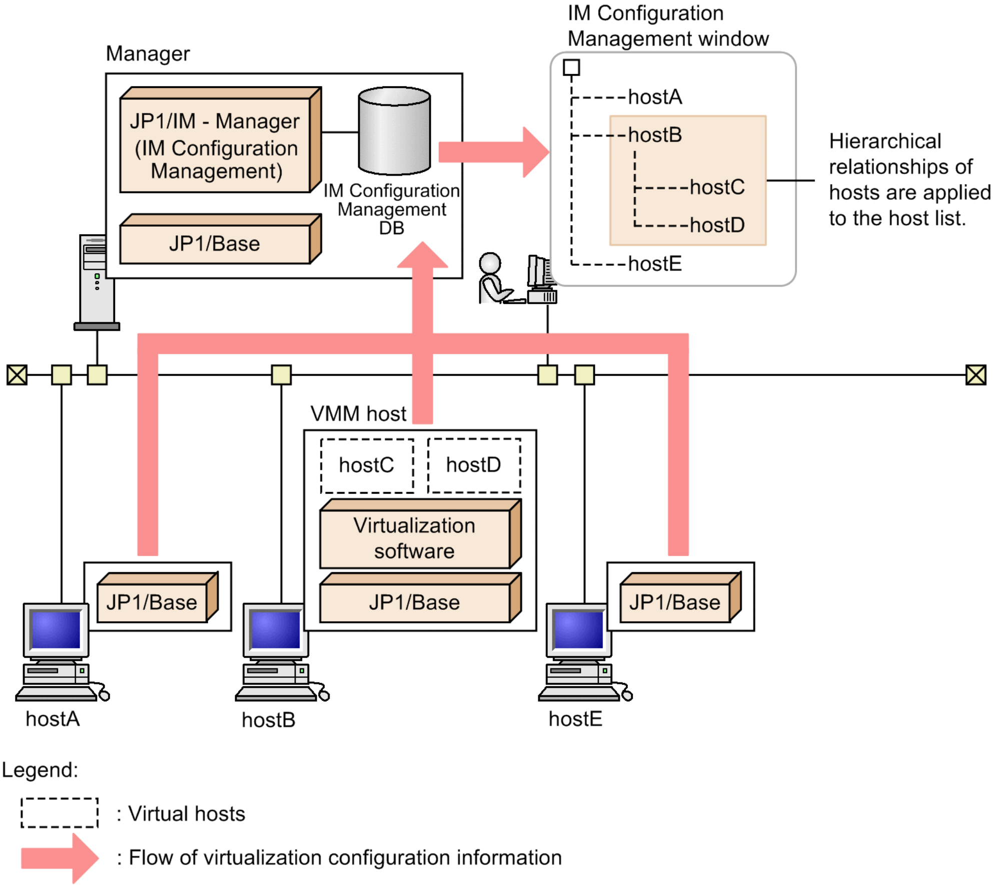
You can display a virtualization system configuration in the tree display area on the **Host List** page of the IM Configuration Management window. If all of the following conditions are met, the window displays a host hierarchy in which physical hosts on which virtual hosts are running are displayed as parent hosts and virtual hosts are displayed as subordinate hosts:

Conditions for displaying the host hierarchy on the **Host List** page:

- **Virtual host** is set for the host type in the host information.
- A VMM server is installed on the relevant host.
- The VMM server installed on the relevant host appears on the **Host List** page.

The following figure illustrates how to display a virtualization system configuration.

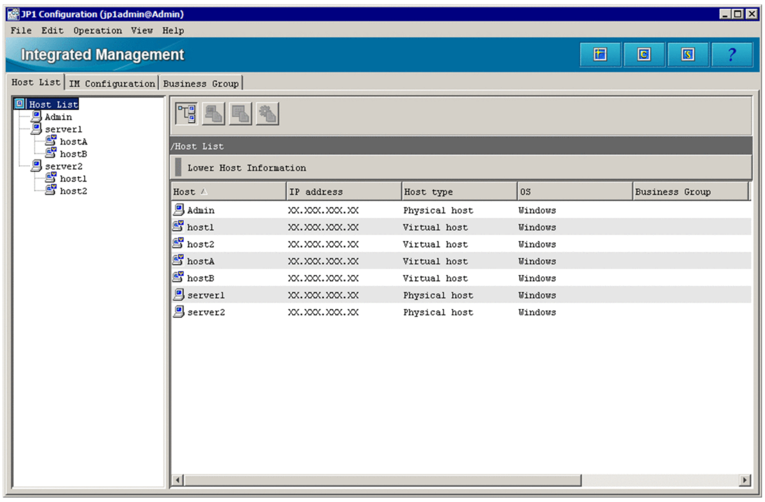
Figure 6–19: Display of a virtualization system configuration


Manager
JP1/IM - Manager (IM Configuration Management)
IM Configuration Management DB
JP1/Base
IM Configuration Management window
hostA
hostB
hostC
hostD
hostE
Hierarchical relationships of hosts are applied to the host list.
VMM host
hostC
hostD
Virtualization software
JP1/Base
JP1/Base
JP1/Base
hostA
hostB
hostE
Legend:
: Virtual hosts
: Flow of virtualization configuration information

In the above figure, `hostA`, `hostB`, and `hostE` are physical hosts, and `hostC` and `hostD` are virtual hosts configured on the physical host `hostB`. You can check a virtualization system configuration by collecting host information and virtualization configuration information from individual hosts and displaying the information in the IM configuration management viewer.

The following figure shows an example window displaying a virtualization system configuration in the IM configuration management viewer.

Figure 6–20: Example window displaying a virtualization system configuration in the IM configuration management viewer



Host	IP address	Host type	OS	Business Group
Admin	XX.XXX.XXX.XX	Physical host	Windows	
host1	XX.XXX.XXX.XX	Virtual host	Windows	
host2	XX.XXX.XXX.XX	Virtual host	Windows	
hostA	XX.XXX.XXX.XX	Virtual host	Windows	
hostB	XX.XXX.XXX.XX	Virtual host	Windows	
server1	XX.XXX.XXX.XX	Physical host	Windows	
server2	XX.XXX.XXX.XX	Physical host	Windows	

Virtual hosts registered by executing **Collect Virtualization Configuration** are displayed in the order they are registered.

Importing information of hosts in virtualization system configuration deletes host information, system hierarchy (IM configuration), and profiles that are held by IM Configuration Management. To manage profiles, you must collect host information, IM configuration, and profiles after importing the host information.

(1) Displaying both higher and lower hierarchical levels for the same host

If a virtual host in a virtualization system configuration displayed on the **Host List** page meets the following two conditions, the **Host List** page displays two hierarchies. One shows the VMM server of the virtual host as a higher-level host, and one shows other hosts that are configured as VMM servers as lower-level hosts.

- The VMM server of the virtual host is a physical host.
- The host list includes hosts configured as VMM servers.

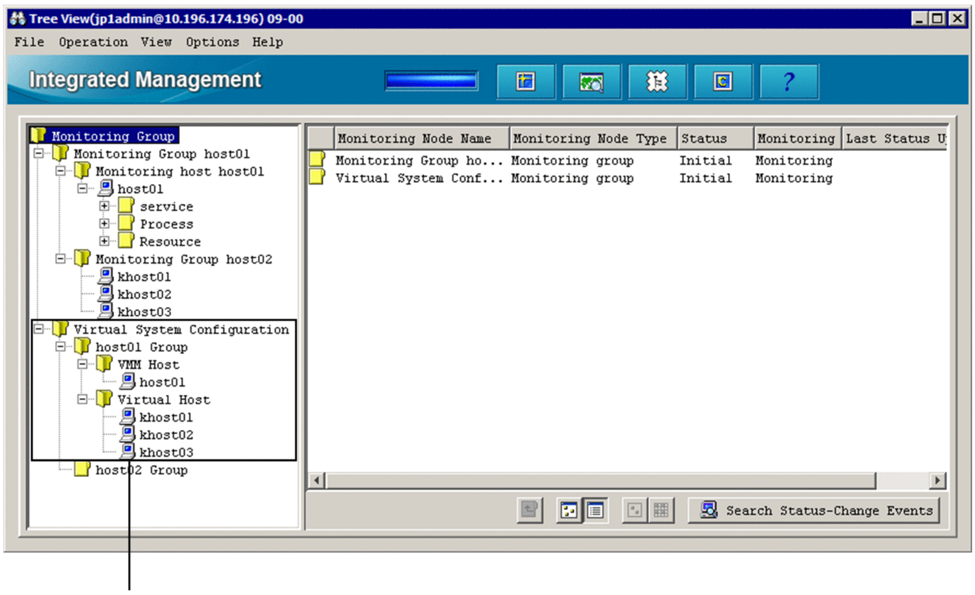
A hierarchy displaying hosts that are configured as VMM servers as lower-level hosts is displayed at the same level as the VMM server of the virtual host.

6.3.5 Importing into the Central Scope

You can monitor a virtualization system configuration managed by IM Configuration Management, by using the Central Scope.

The following figure shows an example of displaying a virtualization system configuration in the Central Scope viewer.

Figure 6–21: Example of displaying a virtualization system configuration in the Central Scope viewer



Monitoring Node Name	Monitoring Node Type	Status	Monitoring	Last Status U
Monitoring Group ho...	Monitoring group	Initial	Monitoring	
Virtual System Conf...	Monitoring group	Initial	Monitoring	

Represents the virtualization configuration monitoring tree

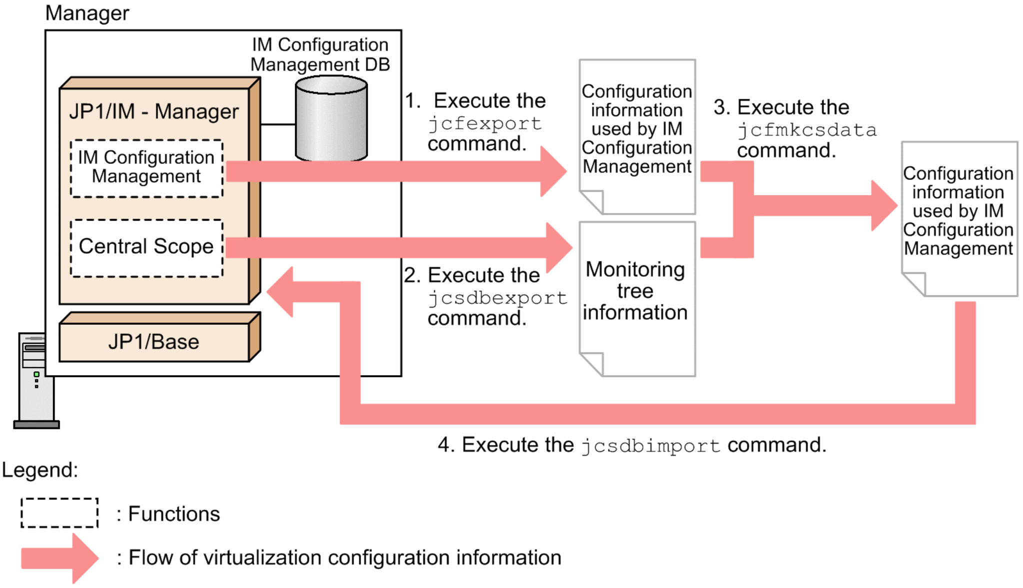
You can monitor a virtualization system configuration in the Central Scope by the following two methods.

(1) Using commands for importing virtualization configuration information into the Central Scope

You can export virtualization configuration information managed by IM Configuration Management, convert it by executing the `jcfmkcsdata` command, and then import the information into the Central Scope.

The following figure illustrates how virtualization configuration information is imported into the Central Scope.

Figure 6–22: Importing virtualization configuration information into the Central Scope


Manager
IM Configuration Management DB
JP1/IM - Manager
IM Configuration Management
Central Scope
JP1/Base
1. Execute the jcfexport command.
2. Execute the jcsdbexport command.
Configuration information used by IM Configuration Management
Monitoring tree information
3. Execute the jcfmkcsdata command.
Configuration information used by IM Configuration Management
4. Execute the jcsdbimport command.
Legend:
: Functions
: Flow of virtualization configuration information

The flow of importing virtualization configuration information into the Central Scope is described below, following the numbers in the figure:

1. Execute the `jcfexport` command to output the system hierarchy, host information, and definition information that are managed by IM Configuration Management.
2. Execute the `jcsdbexport` command to output the monitoring tree information shown in the Central Scope. (This information is saved in the monitoring object database of JP1/IM - Manager.)
3. Execute the `jcfmkcsdata` command to merge the files output in steps 1 and 2.
4. Execute the `jcsdbimport` command to import the merged file created in step 3 into the Central Scope.

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

(2) Using the IM configuration management viewer to apply virtualization configuration information to the Central Scope

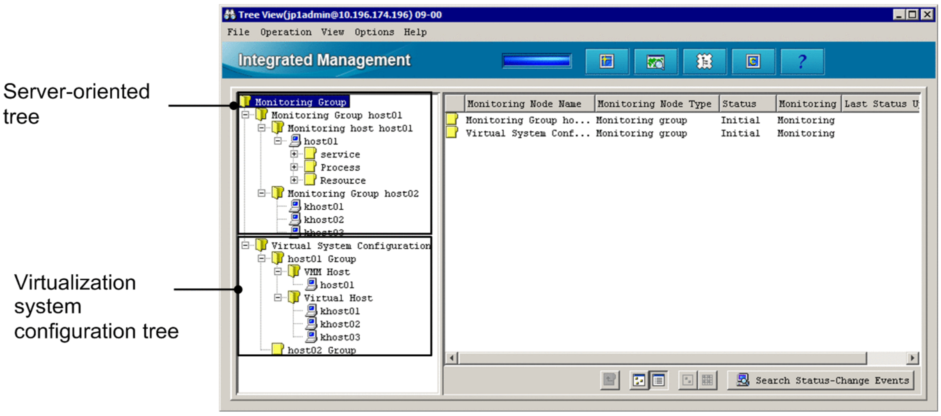
You can use the IM configuration management viewer to apply virtualization system configuration to the Central Scope. To perform this operation, the following permissions are required for the JP1 user logged in to the IM configuration management viewer:

- JP1 resource group: JP1_Console
- JP1 permission level: JP1_Console_Admin

Applying virtualization system configuration to the Central Scope updates the monitoring tree in the Central Scope.

The following figure is an example of displaying the monitoring tree in the Central Scope.

Figure 6–23: Example of displaying the monitoring tree in the Central Scope



Monitoring Node Name	Monitoring Node Type	Status	Monitoring	Last Status U
Monitoring Group ho...	Monitoring group	Initial	Monitoring	
Virtual System Conf...	Monitoring group	Initial	Monitoring	

We recommend that you use the IM configuration management viewer to apply virtualization system configuration into the Central Scope if the following condition is met:

- Monitoring is performed by using an automatically-generated or customized server-oriented tree.

6.4 Managing business groups

Using IM Configuration Management, you can monitor multiple monitored hosts by grouping them as individual business systems or as monitoring targets managed by individual system administrators. A unit of hosts grouped based on a certain objective is called a *business group*. In the Event Console window (Central Console) or the Monitoring Tree window (Central Scope), you can manage the scope of JP1 events that can be viewed and the scope of monitoring settings that can be operated on for individual business groups. These permitted scopes are called a *view permission* and *operating permission* respectively. By restricting the view permission and operating permission for business groups, you can monitor and handle individual business groups differently.

Note

Monitoring in the Event Console window and the Monitoring Tree window

Monitoring in the Event Console window

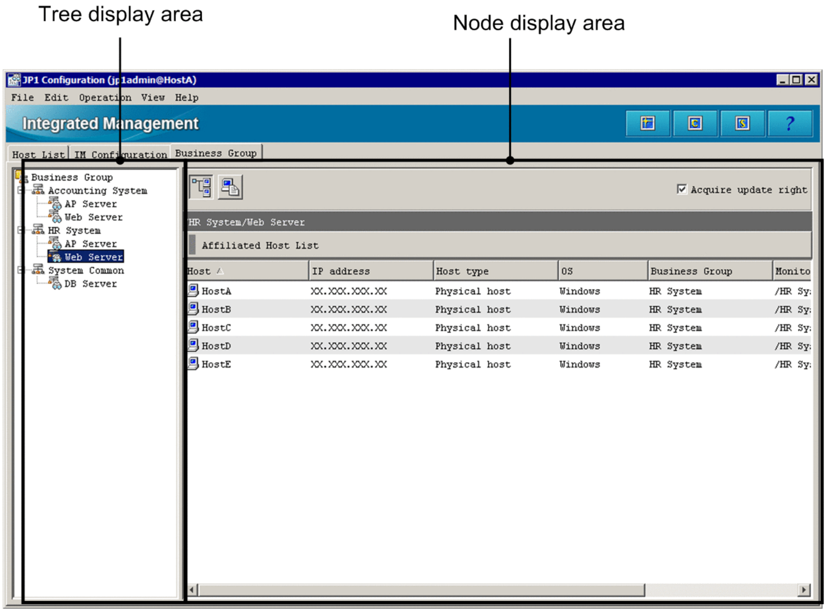
> The information settings of business groups are passed to the Event Console window (Central Console). If you enable restriction of viewing and operating business groups in the Central Console, in the Event Console window, you can view and operate only the JP1 events issued in the business group you are in charge of. For details, see *3.1.4 Restrictions on viewing and operating business groups*.

Monitoring in the Monitoring Tree window

> If you apply the setting information of business groups to the Central Scope, the hierarchical configuration of business groups and the view and operating permissions are passed to the Monitoring Tree window (Central Scope), and you will be able to view and operate on only the JP1 events issued in the business group you are in charge of.

You can check the defined business groups in the tree display area on the **Business Group** page of the IM Configuration Management window. The following figure is an example of displaying business groups.

Figure 6–24: Example of displaying business groups (on the Business Group page of the IM Configuration Management window)



Host	IP address	Host type	OS	Business Group	Monito
HostA	XX.XXX.XXX.XX	Physical host	Windows	HR System	/HR Sy:
HostB	XX.XXX.XXX.XX	Physical host	Windows	HR System	/HR Sy:
HostC	XX.XXX.XXX.XX	Physical host	Windows	HR System	/HR Sy:
HostD	XX.XXX.XXX.XX	Physical host	Windows	HR System	/HR Sy:
HostE	XX.XXX.XXX.XX	Physical host	Windows	HR System	/HR Sy:

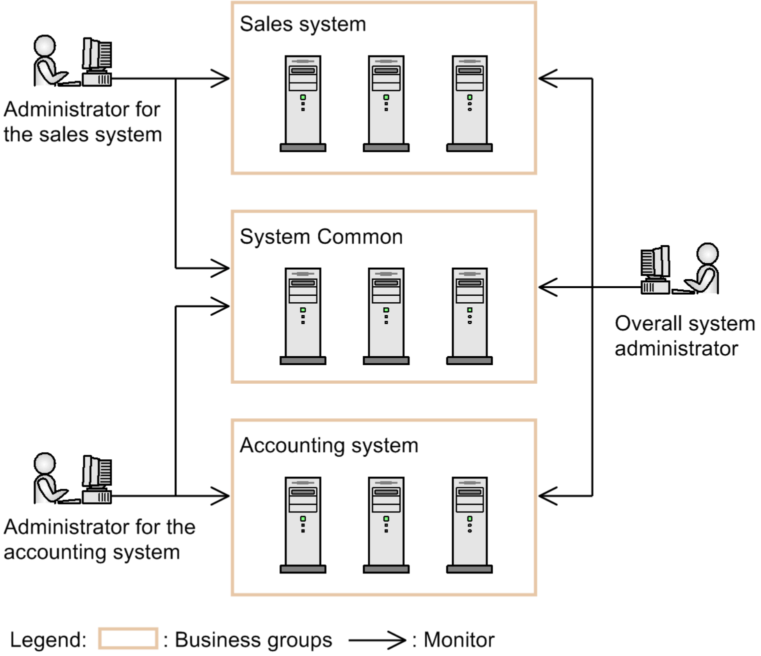
Before using this business group functionality, you need to set business groups. To set business groups, you need to acquire update rights. For details about how to set business groups, see *3.4 Setting business groups* in the *JP1/Integrated Management - Manager Configuration Guide*.

6.4.1 Overview of business groups

You can group multiple hosts by units such as business system. One host cannot belong to multiple business groups.

The following figure shows an example of monitoring systems by using business groups.

Figure 6–25: Example of monitoring systems by using business groups


Sales system
Administrator for the sales system
System Common
Overall system administrator
Accounting system
Administrator for the accounting system
Legend:
: Business groups
: Monitor

In this example, three business groups (`Sales system`, `System common`, and `Accounting system`) are defined. Business group `System common` can be commonly used from both `Sales system` and `Accounting system`.

For the administrator for the sales system, only the view and operating permissions for the business groups `Sales system` and `System common` are set. Therefore, the scope the administrator for the sales system can view and operate in is restricted to the monitoring targets within the `Sales system` and `System common` business groups. Similarly, the scope the administrator for the accounting system can view and operate in is restricted to the monitoring targets within the `Accounting system` and `System common` business groups.

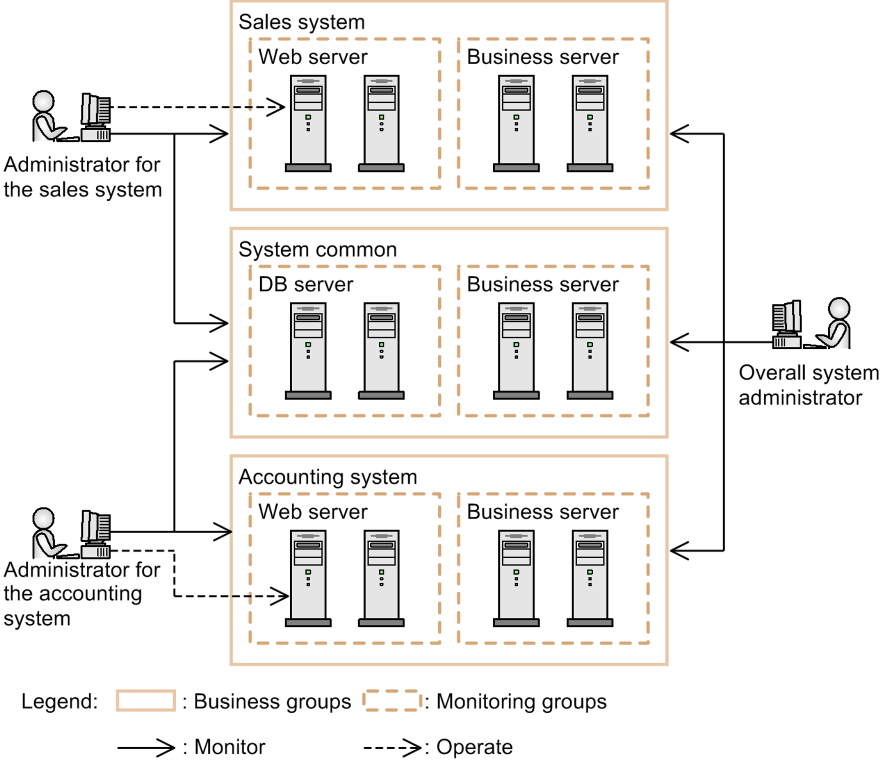
By setting the view and operating permissions for all business groups to the system administrator for the entire systems, that administrator can monitor `Sales system`, `System common`, and `Accounting system`. For monitoring of `System common`, you can set only the view permission for `System common` for the administrators of the sales system and the accounting system.

6.4.2 Monitoring groups in a business group

You can further group the hosts in a business group from the viewpoint of monitoring the business system. Such groups are called *monitoring groups*. You can also make monitoring groups in multiple tiers. A monitoring group always belongs to a business group or an upper-level monitoring group.

The following figure shows an example of monitoring systems by using monitoring groups.

Figure 6–26: Example of monitoring systems by using the functionality of monitoring groups



In this example, the business groups Sales system and Accounting system are divided into monitoring groups Web server and Business server, grouped based on the functions of the hosts.

Administrators for each business system can use the business group as a monitoring tree. Also, by specifying a monitoring group in a business group, like Business server in Accounting system, an administrator can easily operate and setup a part of the monitoring group.

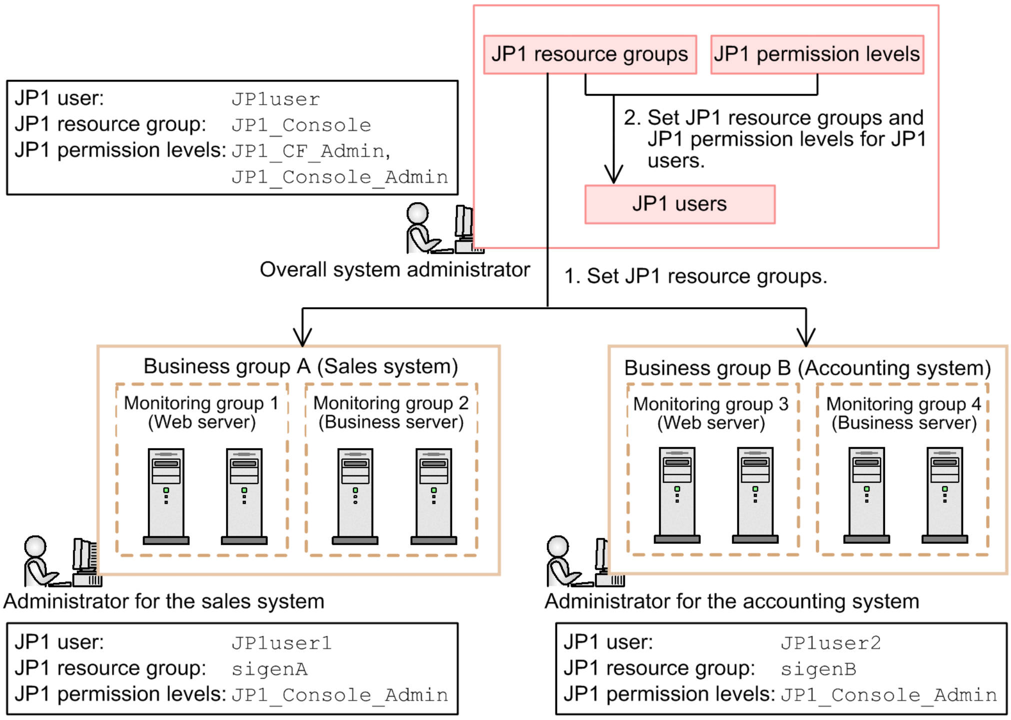
6.4.3 Viewing and operating permissions for business groups

To monitor multiple monitored hosts by grouping them into business groups, manage the JP1 users by using their JP1 resource groups and JP1 permission levels.

If restrictions on viewing and operating business groups are enabled, JP1 users who do not have permissions to the JP1_Console resource group cannot log in to the IM Configuration Management window.

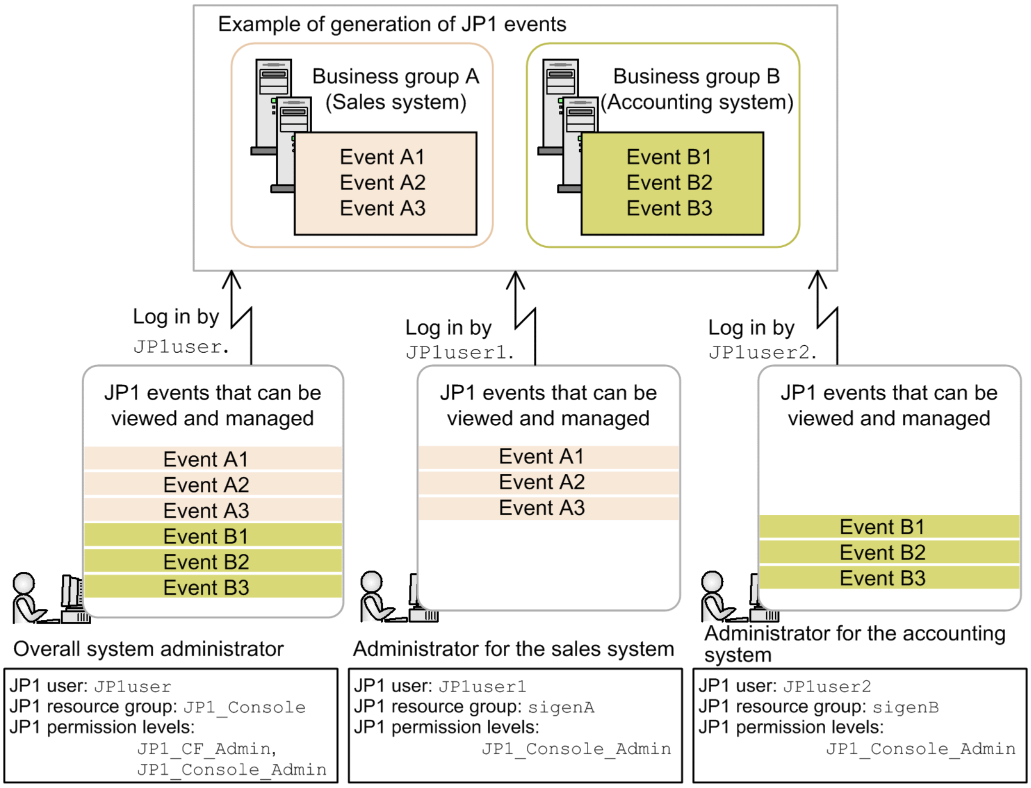
The following figure shows how JP1 resource groups are assigned to business groups, and it shows how the scope to be viewed and operated is restricted.

Figure 6–27: Assigning JP1 resource groups to business groups and restricting the scope to be viewed and operated


JP1 resource groups
JP1 permission levels
2. Set JP1 resource groups and JP1 permission levels for JP1 users.
JP1 users
JP1 user: JP1user
JP1 resource group: JP1_Console
JP1 permission levels: JP1_CF_Admin, JP1_Console_Admin
Overall system administrator
1. Set JP1 resource groups.
Business group A (Sales system)
Monitoring group 1 (Web server)
Monitoring group 2 (Business server)
Business group B (Accounting system)
Monitoring group 3 (Web server)
Monitoring group 4 (Business server)
Administrator for the sales system
Administrator for the accounting system
JP1 user: JP1user1
JP1 resource group: sigenA
JP1 permission levels: JP1_Console_Admin
JP1 user: JP1user2
JP1 resource group: sigenB
JP1 permission levels: JP1_Console_Admin

Before restricting the scope to be viewed and operated by JP1 users for each business group, assign a JP1 resource group to each business group. Then, assign JP1 resource groups and JP1 permission levels to JP1 users. As the result, you can restrict the scope a JP1 user can view and operate on to the business group that corresponds to the JP1 resource group granted to the JP1 user, according to the JP1 permission levels. The following figure shows an example of restrictions on viewing and operating business groups.

Figure 6–28: Example of restrictions on viewing and operating business groups


Example of generation of JP1 events
Business group A (Sales system)
Event A1
Event A2
Event A3
Business group B (Accounting system)
Event B1
Event B2
Event B3
Log in by JP1user.
Log in by JP1user1.
Log in by JP1user2.
JP1 events that can be viewed and managed
Event A1
Event A2
Event A3
Event B1
Event B2
Event B3
JP1 events that can be viewed and managed
Event A1
Event A2
Event A3
JP1 events that can be viewed and managed
Event B1
Event B2
Event B3
Overall system administrator
Administrator for the sales system
Administrator for the accounting system
JP1 user: JP1user
JP1 resource group: JP1_Console
JP1 permission levels: JP1_CF_Admin, JP1_Console_Admin
JP1 user: JP1user1
JP1 resource group: sigenA
JP1 permission levels: JP1_Console_Admin
JP1 user: JP1user2
JP1 resource group: sigenB
JP1 permission levels: JP1_Console_Admin

The following table describes the relationships between permissions in the IM Configuration Management window.

Table 6–26: Relationships between permissions in the IM Configuration Management window

Settings for a JP1 user		Permissions in the IM Configuration Management window
JP1 resource group	JP1 permission levels	
`JP1_Console`	JP1_CF_Admin	Permission for administrator
	JP1_CF_Manager	Permission for operator
	JP1_CF_User	Permission for monitoring person
	• JP1_Console_Admin • JP1_Console_Operator • JP1_Console_User	Permission for monitoring person
	None	Permission for monitoring person
`Other than JP1_Console`	JP1_CF_Admin	Permission for administrator#
	JP1_CF_Manager	Permission for operator#
	JP1_CF_User	Permission for monitoring person#
	• JP1_Console_Admin • JP1_Console_Operator • JP1_Console_User	Permission for monitoring person#
	None	Permission for monitoring person#
None	None	Permission for monitoring person#

#:

If restrictions on viewing and operating business groups are enabled (the `-bizmonmode` option is set to `ON` in the `jcoimdef` command), JP1 users who do not have permissions to the `JP1_Console` resource group cannot log in to the IM Configuration Management window.

6.4.4 Monitoring using the Central Scope

You can use the Central Scope to monitor a business group by the two methods below.

When you apply business group information to the Central Scope, you can apply the information only to server-oriented trees.

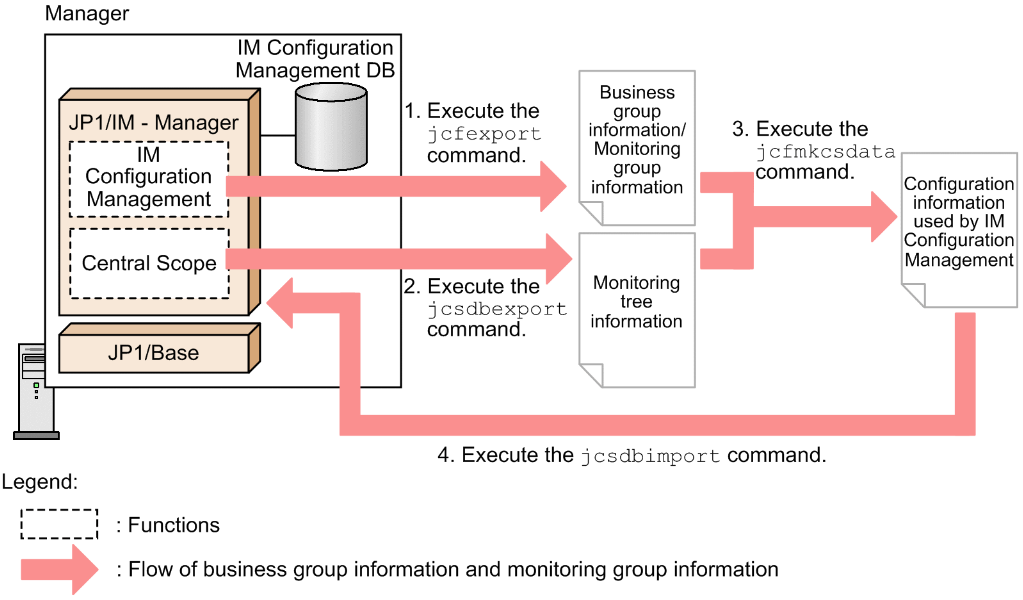
For details about the setting procedure, see *3.4.4(2) Applying business group information and monitoring group information to the Central Scope monitoring tree* in the *JP1/Integrated Management - Manager Configuration Guide*.

(1) Using commands to import information into the Central Scope

You can export business group information and monitoring group information, convert the information by using the `jcfmkcsdata` command, and import the converted information into the Central Scope.

The following figure shows how business group information and monitoring group information are imported into the Central Scope.

Figure 6–29: Importing business group information and monitoring group information into the Central Scope


Manager
IM Configuration Management DB
JP1/IM - Manager
IM Configuration Management
Central Scope
JP1/Base
1. Execute the jcfexport command.
2. Execute the jcsdbexport command.
Business group information/ Monitoring group information
Monitoring tree information
3. Execute the jcfmkcsdata command.
Configuration information used by IM Configuration Management
4. Execute the jcsdbimport command.
Legend:
: Functions
: Flow of business group information and monitoring group information

The flow of importing business group information and monitoring group information into the Central Scope is described below, following the numbers in the figure:

1. Execute the `jcfexport` command to output business group information and monitoring group information.
2. Execute the `jcsdbexport` command to output the monitoring tree information shown in the Central Scope. (This information is saved in the monitoring object database of JP1/IM - Manager.)
3. Execute the `jcfmkcsdata` command to merge the files output in steps 1 and 2.
4. Execute the `jcfmkcsdata` command with the `-a` option specified.
5. Execute the `jcsdbimport` command to import the merged file generated in step 3 into the Central Scope.

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

(2) Using the IM configuration management viewer to apply information to the Central Scope

In the IM Configuration Management window of the IM configuration management viewer, you can apply business group information and monitoring group information to the Central Scope. For details about the permissions required for the JP1 user logged in to the IM configuration management viewer to perform this operation, see *6.4.3 Viewing and operating permissions for business groups*.

Applying business group information and monitoring group information to the Central Scope updates the monitoring tree of the Central Scope. Note that the hosts placed under a business group are not displayed in the monitoring tree of the Central Scope. The hosts in a monitoring group are displayed in the tree.

6.4.5 Functions related to business groups

The following table describes what you can do with and for business groups.

Table 6–27: Functions related to business groups

Function	What you can do with and for business groups
IM Configuration Management	Set the following items in the **Business Group** page of the IM Configuration Management window. Settings for business groups • Registering, editing, deleting, and listing business groups, and displaying the basic information of business groups. To register a business group, the business group name must be set as basic information. JP1 resource group name and comments can be edited as required. • Registering a host belonging to the business group, canceling the registration, and listing hosts. Settings for monitoring groups • Registering, editing, and deleting monitoring groups, and displaying the monitoring group tree. To register a monitoring group, the monitoring group name must be set as basic information. The monitoring group name can be changed later. Comments can be edited as required. • Registering hosts belonging to the monitoring group, canceling the registration, and listing the hosts.
	Import or export the basic information of business groups by using commands. • Import: Use the `jcfimport` command. • Export: Use the `jcfexport` command.
	Automatically report a change in business groups to the Central Console#, and apply the latest business groups to the Event Console window.
	Apply the tree configuration defined for a business group to the monitoring tree of the Central Scope. To perform this, from the **Operation** menu in the IM Configuration Management window, select **Business Group** and then **Apply to Central Scope Monitoring Tree**, or execute the `jcfmkcsdata` command.
	Acquire update rights for editing and applying a business group.
Central Console	Restrict the following items for a JP1 user by using the view and operating permissions of the business group#. • Viewing and operating JP1 events • Viewing and operating action logs • The host on which commands are executed
	Specify a business group instead of a host name, which can save the time and effort of changing the host name every time the configuration is changed.

#: To restrict viewing and operating business groups in the Central Console, restrictions on viewing and operating business groups must be enabled in the Central Console. For details, see *3.1.4 Restrictions on viewing and operating business groups*.

6.5 Profile management

Using IM Configuration Management, you can centrally manage the JP1/Base profiles on the hosts in the system hierarchy (IM configuration) through the IM configuration management viewer.

To manage profiles with IM Configuration Management, the hosts must be added to the system hierarchy and JP1/Base must be active on each host.

This section describes the profiles you can manage by using IM Configuration Management, and the functionality provided for this purpose.

The supported profile management methods include the method that uses IM Configuration Management and the method that uses JP1/Base commands. If the versions of JP1/IM - Manager and of the agent's JP1/Base are both 11-10 or later, these two methods can be combined.

Some notes apply when IM Configuration Management's profile management is used together with JP1/Base's profile management. For details, see *6.5.10 Notes on using IM Configuration Management's profile management together with JP1/Base's profile management*.

The following table describes the differences in profile management according to the combination of the version of JP1/IM - Manager and the version of JP1/Base on the agent.

Table 6–28: Differences in profile management according to the combination of JP1/IM - Manager and JP1/Base on the agent

Functionality	JP1/IM - Manager 11-01 or earlier		JP1/IM - Manager 11-10 or later	
	JP1/Base on agent 11-00 or earlier	JP1/Base on agent 11-10 or later	JP1/Base on agent 11-00 or earlier	JP1/Base on agent 11-10 or later
Profile management	Profiles cannot be managed by using IM Configuration Management commands and JP1/Base commands together.			Profiles can be managed by using IM Configuration Management commands and JP1/Base commands together.
Collecting profile lists	The agent's profile lists can be collected by using IM Configuration Management.			
Collecting profiles	The agent's profiles can be collected by using IM Configuration Management.			
Collecting profiles by using a batch operation	The agent's profiles can be collected from IM Configuration Management by using a batch operation.			
Applying profiles by reload	Profiles set by using IM Configuration Management can be applied to the agent by reloading the log file trap processes.			
Applying log file trap information by restart	Log file trap information set from IM Configuration Management can be applied to the agent by restarting the log file trap processes.			
Applying log file trap information by sending a file	Log file trap information for only the cluster can be sent to the agent from IM Configuration Management.			Log file trap information can be sent to the agent from IM Configuration Management.

Functionality	JP1/IM - Manager 11-01 or earlier		JP1/IM - Manager 11-10 or later	
	JP1/Base on agent 11-00 or earlier	JP1/Base on agent 11-10 or later	JP1/Base on agent 11-00 or earlier	JP1/Base on agent 11-10 or later
Applying profiles in a batch operation	The following profile types can be applied to the agent from IM Configuration Management by using a batch operation: • Event forwarding • Event log trapping • Local action			The following profiles can be applied to the agent from IM Configuration Management by using a batch operation: • Event forwarding • Log file trapping • Event log trapping • Local action
Displaying profiles	The following information can be displayed by using IM Configuration Management: • Service activity status • Valid configuration information • Contents of configuration files			
Editing configuration files	The configuration files for the agent's profiles can be edited.			
Saving edited file contents	The contents of edited configuration files can be saved to the manager where IM Configuration Management is running.			
Adding log file trap information	Profiles of the log file traps can be added by using IM Configuration Management.			
Deleting log file trap information	The profiles of the log file traps that are saved in the IM Configuration Management database will be deleted.			The profiles of the log file traps that are saved in the IM Configuration Management database and the profiles of the agent's log file traps will be deleted.
Starting log file traps	Log file traps can be started by using IM Configuration Management.			
Stopping log file traps	The agent's log file trap information will be deleted when the log file traps are stopped by using IM Configuration Management.			The agent's log file trap information will not be deleted when the log file traps are stopped by using IM Configuration Management.
Starting log file trapping automatically	You cannot specify in IM Configuration Management whether to enable or disable the automatic start of log file trapping. When a log file trap is started, automatic start is enabled, and when a log file trap is stopped, automatic start is disabled.			You can specify in IM Configuration Management whether to enable or disable the automatic start of log file trapping.

6.5.1 Types of profiles that can be managed

Using IM Configuration Management, you can manage the profiles set for JP1/Base on the agent hosts and the profiles on the remotely monitored hosts.

You can manage the following profiles:

- Valid configuration information
  The setting information currently enabled in JP1/Base of the agent hosts and on the remotely managed hosts (information in the setting files loaded when the service is started). To manage this information, the JP1/Base on the target host must be version 9 or later.
- Configuration file contents
  The information in the definition file that is set in JP1/Base of the agent hosts and on the remotely monitored hosts. This information will differ from the valid configuration information if you made any changes to the configuration file after startup of the JP1/Base service but did not apply the edited file contents.

Using IM Configuration Management, you can manage profiles in JP1/Base version 7 or later.

Profile management can be used for the following purposes:

- To check the status of the hosts on a routine basis or in the event of an error
- To change a profile during a system upgrade or maintenance
- To apply the contents of a profile to the profiles on other hosts

(1) Types of profiles on agent hosts

The following table lists and describes the profile types on the agent hosts managed by IM Configuration Management.

Table 6–29: Profile types on the agent hosts managed by IM Configuration Management

Profile type	Description
Event Forwarding	Profile about the functionality for forwarding JP1 events to a higher-level host in accordance with the system hierarchy.
Log File Trapping	Profile about the functionality for converting information output to a log file by an application program into JP1 events. Configuration files cannot have identical file names. A different file name must be assigned to the configuration file for each process, even when the files are stored in different directories. If JP1/IM - Manager is running on a Windows host, the setting file name used on an agent host is not case sensitive.
Event Log Trapping	Profile about the functionality for converting Windows events into JP1 events.
Local Action[#1]	Profile about actions executed on an agent without going through a manager.
Authentication Server[#1]	Profile about the server for centrally managing the users of a system configured in JP1/IM or JP1/AJS.
JP1 User-Permissions Level[#1, #2]	Profile about the permission levels of JP1 users (users of a JP1 system such as JP1/IM or JP1/AJS).
Registered JP1 Users[#1, #2]	Profile about the list of JP1 users.
OS User Mapping[#1, #2]	Profile about the mapping between OS users who have permission to execute jobs and commands and JP1 users.

#1

Only information in JP1/Base version 9 or later can be managed.

#2

If the local host is used as the authentication server, information can be displayed only when the service of the authentication server is active. If the local host is used as the authentication server, the display area appears grayed when the service of the authentication server is stopped.

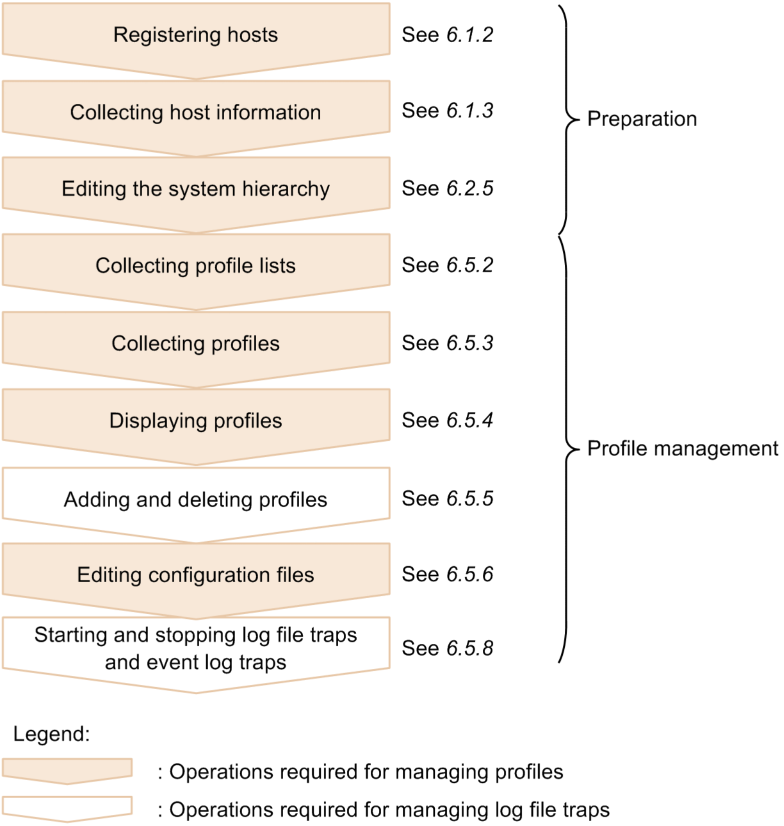
The profiles in JP1/Base that can be managed by IM Configuration Management are the contents of the configuration files stored in each host's `conf` directory. Configuration files located in other directories, such as those for log file trapping, cannot be managed by IM Configuration Management. If you want to include such files in the profile management functionality, you must move them to the `conf` directory.

IM Configuration Management manages JP1/Base event log traps and log file traps on a physical host basis, not on a logical host basis. To display or edit profiles about event log traps or log file traps in a logical host, you must do so on a physical host basis, identifying the physical host associated with the logical host.

All valid configuration information can be displayed, however, even for services that start with a configuration file located in a directory other than the `conf` directory. From the displayed information you can find out whether a service's configuration file is located in the `conf` directory.

The following figure shows the flow of operations necessary to manage profiles or log file traps in IM Configuration Management.

Figure 6–30: Flow of operations for managing profiles with IM Configuration Management


Registering hosts
See *6.1.2*
Collecting host information
See *6.1.3*
Editing the system hierarchy
See *6.2.5*
Preparation
Collecting profile lists
See *6.5.2*
Collecting profiles
See *6.5.3*
Displaying profiles
See *6.5.4*
Adding and deleting profiles
See *6.5.5*
Editing configuration files
See *6.5.6*
Starting and stopping log file traps and event log traps
See *6.5.8*
Profile management
Legend:
: Operations required for managing profiles
: Operations required for managing log file traps

If IP addresses are registered as host names when the system hierarchy (IM configuration) is applied, profiles cannot be managed in IM Configuration Management. Performing any of the operations below will display the KNAN22412-E message. This message appears when you perform any of the following operations on a host defined by its IP address:

- Open the Display/Edit Profiles window.
- Collect profiles as a batch operation in the IM Configuration Management window.

You cannot collect profiles from hosts defined by their IP addresses, but processing succeeds for the other hosts.

- Apply profiles as a batch operation in the IM Configuration Management window.
  You cannot apply profiles to hosts defined by their IP addresses, but processing succeeds for the other hosts.

(2) Types of profiles on remotely monitored hosts

The following table lists and describes the profile types on the remotely monitored hosts managed by IM Configuration Management.

Table 6–30: Profile types on the remotely monitored hosts managed by IM Configuration Management

Profile type	Description
Remote-monitoring log file trap information	Profiles related to converting the information output to the log files of application programs to JP1 events
Remote-monitoring event log trap information	Profiles related to converting Windows events to JP1 events

6.5.2 Collecting profile lists

In IM Configuration Management, before you collect profiles, you must obtain a list of profiles (called a *profile list hereafter*) that can be managed from agent hosts and remotely monitored hosts.

The collected profile list appears in the tree display area of the Display/Edit Profiles window.

If the service for which the profile is set (event log trapping service, event service, and so on) is inactive on a target host, the collected profile list is displayed as follows:

- In the tree display area of the Display/Edit Profiles window, profiles from the host where the service is inactive appear grayed and cannot be selected in the profile list.
- In the node display area of the Display/Edit Profiles window, the configuration file's **Collection status** remains unchanged.
- When you click the **Basic Information** button in the node display area of the **Host List** page or **IM Configuration** page of the IM Configuration Management window, the profile collection status is shown as **Collected**.

The service for local actions is inactive by default because there is no configuration file (`jbslcact.conf`) in the host. As a result, when you collect a profile list in the Display/Edit Profiles window, the KNAN20333-I message is displayed and **Collected** appears as the **Collection status** in the node display area.

You can start the service for local actions by creating a configuration file (`jbslcact.conf`) and applying it to the host in question.

For details about how to create a configuration file (`jbslcact.conf`) and apply it to the host in question, see *3.5.1(6) (b) Applying edited information in configuration files individually to each agent* in the *JP1/Integrated Management - Manager Configuration Guide*.

Perform one of the operations listed below to delete the profile list saved on the server, and then acquire profile lists again from hosts. For agent configuration, if the profiles have not yet applied, apply the profiles to the hosts, and then rebuild the profile tree. For a remote monitoring configuration, you do not have to rebuild the profile tree.

- In the tree display area of the Display/Edit Profiles window, click the JP1 product name (**JP1/Base**) and then choose **Operation** and **Rebuild Profile Tree**.
- In the tree display area of the Display/Edit Profiles window, right-click the JP1 product name (**JP1/Base**) and then choose **Rebuild Profile Tree**.
- On the **Host List** or **IM Configuration** page of the IM Configuration Management window, choose **Operation** and then **Batch Collect Profiles**.

If you have restarted the host or JP1/Base on the host, you must update the profile list by opening the Display/Edit Profiles window, choosing **Operation**, and then choosing **Rebuild Profile Tree**.

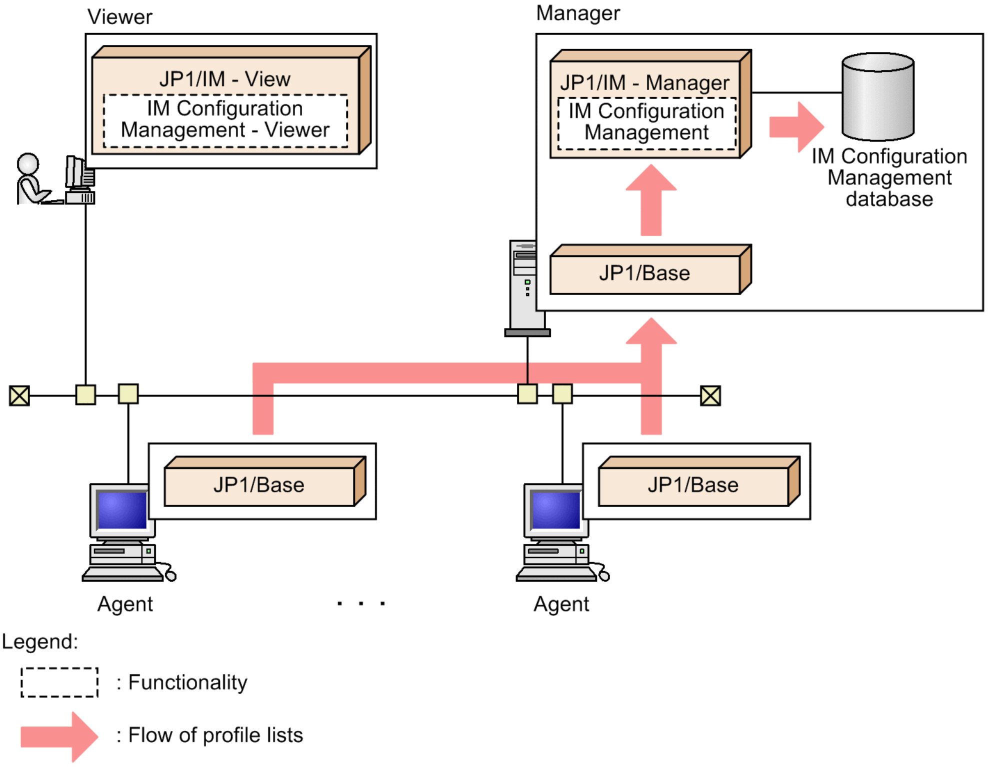
Note that the profile list is updated when host information is collected.

If you perform either of the following operations, and if the profile list does not exist in the IM Configuration Management database, a profile list is created, or the system is updated.

- Open the Display/Edit Profiles window.
- On the **Host List** page or **IM Configuration** page of the IM Configuration Management window, choose **Operation** and **Batch Collect Profiles**.

The figure below shows the flow of processing when collecting profile lists with IM Configuration Management.

Figure 6–31: Collecting profile lists with IM Configuration Management



If a host is deleted from the system hierarchy or is no longer managed by IM Configuration Management, the profile list collected from that host is deleted. Profile lists are also deleted when you perform any of the following operations:

- Collect host information on the **Host List** page or **IM Configuration** page of the IM Configuration Management window.
- Apply the system hierarchy created or edited in the Edit Agent Configuration window or in the Edit Remote Monitoring Configuration window.

- Import configuration definition information on the manager running IM Configuration Management.

The following table describes the profile lists you can collect for each version of JP1/Base on the target host.

Table 6–31: Profile lists that can be collected by JP1/Base version

JP1/Base version	Profile type	Description
Versions 7 and 8	Event Forwarding	--
	Log File Trapping	--
	Event Log Trapping	Can be collected from a Windows host only.
Version 9 or later	Event Forwarding	--
	Log File Trapping[#1]	Multiple profile configuration files can be collected.[#2]
	Event Log Trapping	--
	Local Action	--
	Authentication Server	Limited to display of valid configuration information.
	JP1 User-Permissions Level	• Limited to display of valid configuration information. • Supported only for an authentication server on the local host.
	Registered JP1 Users	• Limited to display of valid configuration information. • Supported only for an authentication server on the local host.
	OS User Mapping	Limited to display of valid configuration information.

Legend:

--: Not applicable.

#1

If the version of JP1/Base is 09-10 or later, you can collect the log-file trap action definition file and the log-file trap startup definition file. If the version of JP1/Base is earlier than 09-10, you can collect only the log-file trap action definition file.

#2

A maximum of 100 profile configuration files for log file trapping can be collected from JP1/Base on each host.

When a host is restarted, or when JP1/Base is restarted on a host, you must update the host's profile list.

You must also update the profile list in the following cases:

- When changes are made to the index file for the event forwarding settings on a host
  Unless you update the profile list, the contents of the superseded configuration file will be displayed, or an error message will appear, when you collect the host's configuration file.
- When the service for which the profile is set (event log trapping service, event service, and so on) starts or stops on the host

Unless you update the profile list, the following problems occur:

- An error message appears when you display valid configuration information, or when you collect or apply configuration files.
- In the tree display area of the Display/Edit Profiles window, the profiles that you want to view appear grayed in the profile list.
- When log file trapping starts or stops on the host, an error message appears when you display valid configuration information, or when you collect or apply configuration files.

6.5.3 Collecting profiles

Using IM Configuration Management, you can collect profiles from agent hosts and remotely monitored hosts. For agent hosts, you can collect profiles for valid configuration information and configuration files. For remotely monitored hosts, you can collect profiles for valid configuration information only.

Collect this information in the Display/Edit Profiles window.

(1) Collecting valid configuration information

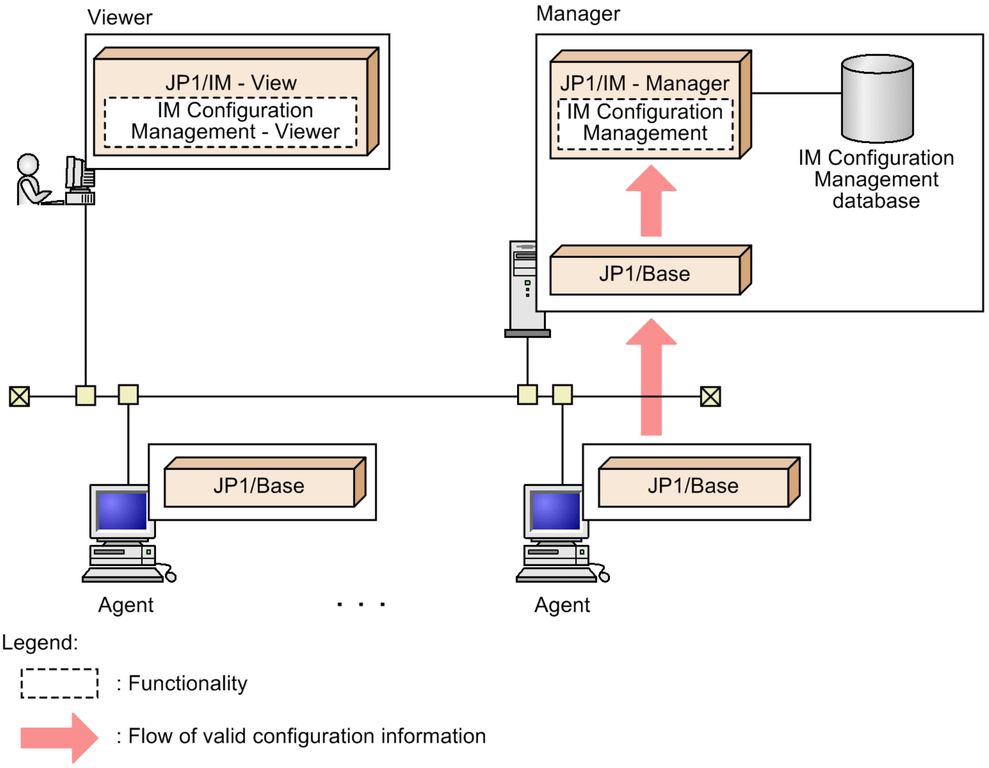
You can collect valid configuration information from the agent hosts on which JP1/Base version 9 or later is running and from the remotely monitored hosts.

To collect valid configuration information:

1. Open the Display/Edit Profiles window.
2. In the tree display area, select a profile.
3. Click the **Valid Configuration Information** button.

The figure below shows the flow of processing when collecting valid configuration information with IM Configuration Management.

Figure 6–32: Collecting valid configuration information with IM Configuration Management


Viewer
JP1/IM - View
IM Configuration Management - Viewer
Manager
JP1/IM - Manager
IM Configuration Management
IM Configuration Management database
JP1/Base
JP1/Base
JP1/Base
Agent
. . .
Agent
Legend:
: Functionality
: Flow of valid configuration information

If collection fails, the possible causes are as follows:

Table 6–32: Causes of failures to obtain valid configuration information

Status	Cause	Action
No valid configuration information could be obtained in the event forwarding, from the forwarding filter entry onward.	The possible cause is that a higher-level host is set in the forwarding setting file (`forward`) as the destination host for forwarded events, but no higher-level host exists for the source host in the system hierarchy.	Check whether the system hierarchy is correct.
No valid configuration information could be obtained in the log file trapping.	The process ID might have changed when log file trapping was restarted on the host, resulting in a mismatch with the process ID managed by IM Configuration Management. The process ID changes each time log file trapping starts.	Update the profile list: In the tree display area of the Display/Edit Profiles window, click the JP1 product name (**JP1/Base**) and then choose **Operation** and **Rebuild Profile Tree**.
No valid configuration information could be obtained in the JP1 user-permissions level or Registered JP1 Users.	The local host might not be acting as the authentication server.	Check whether the authentication service is active on the local host.
Other status	The target service might be inactive on the host.	Execute the `jbs_spmd_status` command to check whether the service started successfully. Alternatively, in a Windows system, check the service status from the Computer Management window.

(2) Collecting configuration files per Agent

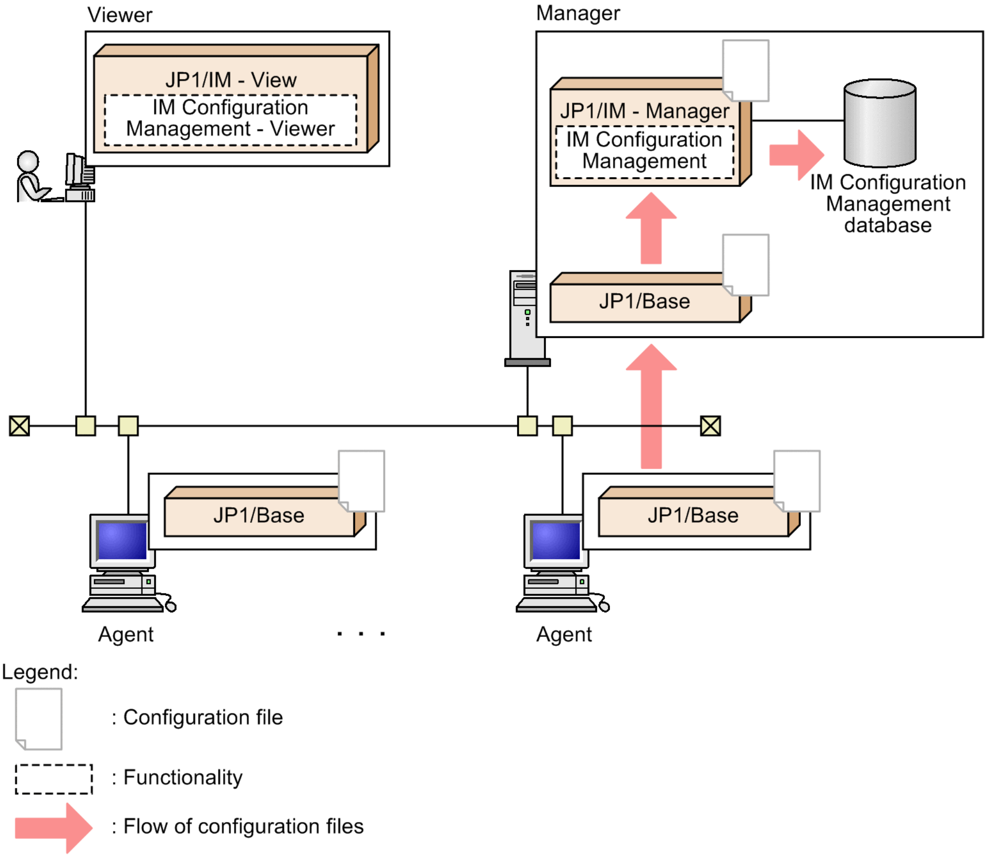
You can collect the profile configuration file for each host from the agent hosts on which JP1/Base version 9 or later is running.

To collect configuration files from a host, perform either of the following:

- In the Display/Edit Profiles window, make sure the **Exclusive Editing Settings** command is checked in the **Edit** menu, or look at the icons in the tree display area to make sure you have exclusive editing rights to the profiles on the target host. Then choose **Operation** and **Collect Profiles**.
- In the IM Configuration Management window, choose **Operation** and **Batch Collect Profiles**.

The figure below shows the flow of processing when collecting configuration files from a host with IM Configuration Management.

Figure 6–33: Collecting configuration files with IM Configuration Management (per host)


Viewer
JP1/IM - View
IM Configuration Management - Viewer
Manager
JP1/IM - Manager
IM Configuration Management
IM Configuration Management database
JP1/Base
JP1/Base
JP1/Base
Agent
. . .
Agent
Legend:
: Configuration file
: Functionality
: Flow of configuration files

For details about the configuration files that can be collected, see *6.5.3(4) Configuration files that can be collected for each version of JP1/Base*.

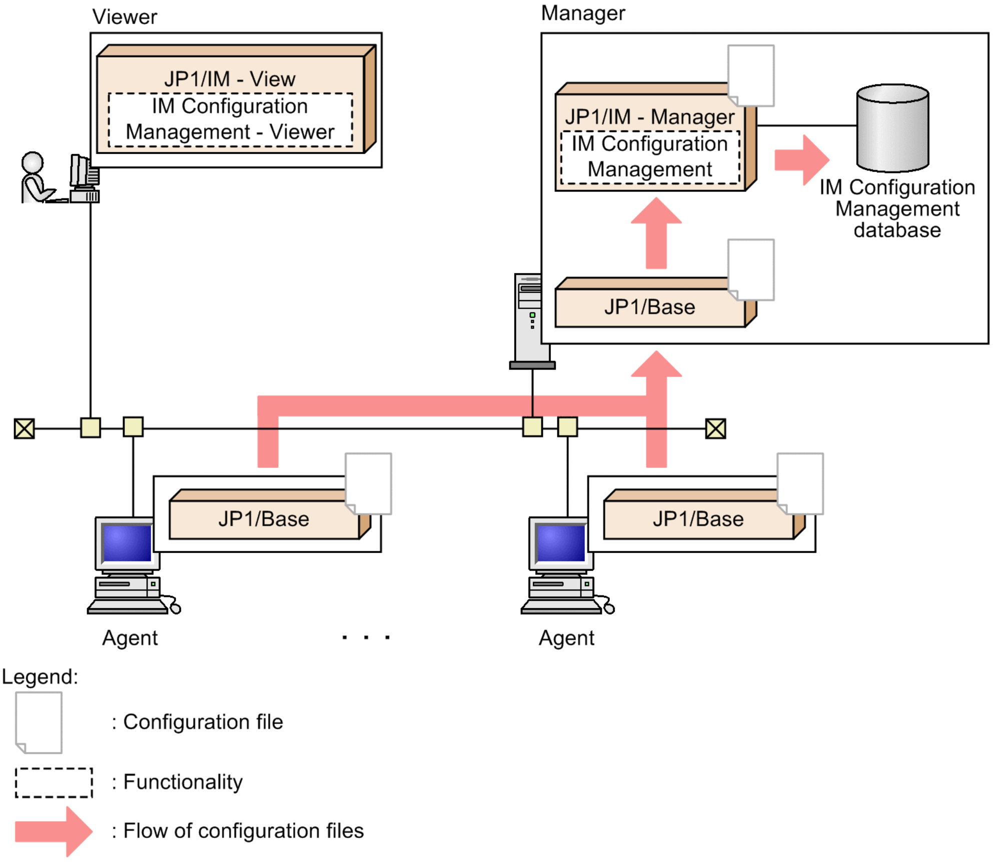
(3) Batch collection of configuration files on agent hosts

On the **Host List** page or **IM Configuration** page of the IM Configuration Management window, if you select **Batch Collect Profiles** from the **Operation** menu, configuration files on agent hosts are collected in a batch.

You cannot collect profiles in a batch if another user has exclusive editing rights to any of the configuration files. To obtain these rights, see *6.5.7 Obtaining and releasing exclusive editing rights for a configuration file*.

The figure below shows the flow of processing when collecting configuration files from all hosts as a batch operation with IM Configuration Management.

Figure 6–34: Collecting configuration files with IM Configuration Management (all hosts)


Viewer
JP1/IM - View
IM Configuration Management - Viewer
Manager
JP1/IM - Manager
IM Configuration Management
IM Configuration Management database
JP1/Base
JP1/Base
JP1/Base
Agent
. . .
Agent
Legend:
: Configuration file
: Functionality
: Flow of configuration files

For details about the configuration files that can be collected, see *6.5.3(4) Configuration files that can be collected for each version of JP1/Base*.

In the Display/Edit Profiles window, you can check whether all the configuration files were successfully collected. If any file could not be collected, **Configuration file contents** is unavailable and the file status appears in **Status** in the node display area.

On the **IM Configuration** page of the IM Configuration Management window, you can check whether the configuration files were successfully collected from all the hosts. If files could not be collected from any host, an error-status icon is displayed for the affected host in the tree display area. To view further details, click the **Basic Information** button in the node display area.

If batch collection fails for any host, processing continues and the profiles on the other hosts are collected. Also, if the maximum number of profile configuration files for log file trapping is exceeded on a host, a message appears and collection processing is canceled for that host.

At batch collection, the profile list on each host is updated automatically. For this reason, configuration files are not collected for services and processes that were inactive at the time the profile list was updated.

When batch collection is completed, a message to that effect appears.

(4) Configuration files that can be collected for each version of JP1/Base

The following table describes the configuration files that can be collected for each version of JP1/Base.

Table 6–33: Configuration files that can be collected

Profile type	Configuration file	JP1/Base version			Notes
		Earlier than version 9	Version 09-00 to 09-01	Version 09-10 or later	
Event Forwarding	Event forwarding setting file (`forward`)	Y	Y	Y	Files such as the event server index file (`index`) and event server settings file (`conf`) are not collected.
Log File Trapping	Action definition file for log file trapping (any file)#1	Y	Y	Y	The following restrictions are applied if the version of JP1/Base is earlier than 09-00: • Only batch-collection is available. • Only the setting file for a log file trap is collected. • Only the action definition file saved with the default file name (`jevlog.conf`) in the default location (the `conf` directory) is regarded as a valid definition file.
	Log-file trap startup definition file (`jevlog_start.conf`)#2	N	N	Y	Displayed as the start option, not as a profile. When a host that is a UNIX or Linux environment collects log files without the startup LANG specified, IM Configuration Management collects them by assuming that the startup LANG is `C`. The startup LANG should be specified to prevent a wrong LANG from being used for collection.
Event Log Trapping	Action definition file for event log trapping (`ntevent.conf`)	Y	Y	Y	Collected when the host environment is Windows.
Local Action	Local action execution definition file (`jbslcact.conf`)	N	N	N	--

Legend:

Y: Can be collected

N: Cannot be collected

--: Not applicable.

#1

To collect the log-file trap action definition file, one of the following agent log file trap conditions must be satisfied:

• The log file trap process is running.

• The log-file trap startup definition file has been defined.

#2

If a UNIX or Linux host collects log files without the startup LANG specified, IM Configuration Management collects them by assuming that the startup LANG is `C`. The startup LANG should be specified to prevent wrong overwriting.

(5) Saving configuration files

The configuration files collected from agents or the configuration files for agents or remotely monitored hosts edited on the IM configuration management viewer can be saved on a manager host on which IM Configuration Management is running. For the configuration files for remotely monitored hosts, only action definition files can be saved.

Configuration files are saved when you perform any of the following operations:

- In the Display/Edit Profiles window, choose **Operation** and **Collect Profiles** (provided no one has obtained exclusive editing rights to the configuration files).
- On the **Host List** page or **IM Configuration** page of the IM Configuration Management window, choose **Operation** and **Batch Collect Profiles**.
- In the node display area (settings information) of the Display/Edit Profiles window, select the **Save** check box and then click the **Execute** button.
- In the node display area (settings information) of the Display/Edit Profiles window, select the **Apply** check box and then click the **Execute** button.
- Import configuration definition information on the manager running IM Configuration Management.

IM Configuration Management stores only one configuration file per profile. The saved profile information will be overwritten if the same configuration file is collected by another user before the saved information is applied to the host.

Configuration files that could not be collected during batch collection of profiles from all hosts cannot be saved.

The file names and location of files saved by IM Configuration Management cannot be specified by the user.

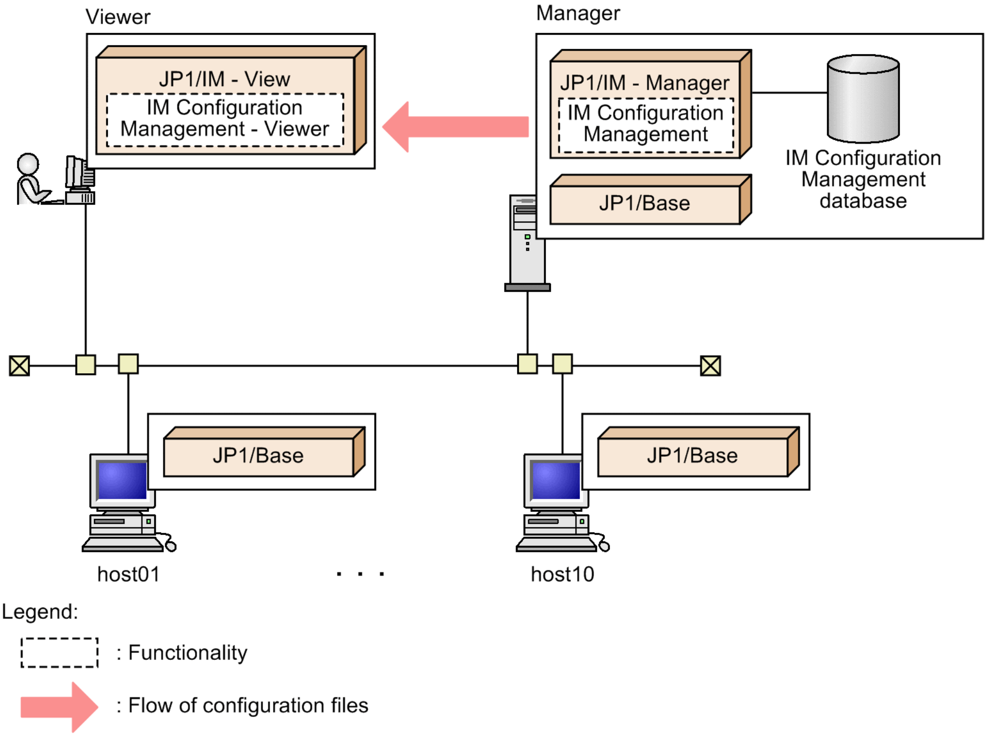
When you delete a host, the host's configuration files are also deleted from the manager running IM Configuration Management. When you delete host information on the **Host List** page of the IM Configuration Management window, the host's configuration files are also deleted.

6.5.4 Displaying profiles

Using IM Configuration Management, you can display JP1/Base profiles of agents and profiles of remotely monitored hosts in the Display/Edit Profiles window.

The figure below shows the flow of processing when displaying profiles with IM Configuration Management.

Figure 6–35: Displaying profiles with IM Configuration Management


Viewer
JP1/IM - View
IM Configuration Management - Viewer
Manager
JP1/IM - Manager
IM Configuration Management
JP1/Base
IM Configuration Management database
JP1/Base
JP1/Base
host01
. . .
host10
Legend:
: Functionality
: Flow of configuration files

(1) Profile information that can be displayed for agents according to the status of service activity

The following table describes the profile information you can display according to whether the service is active or inactive.

Table 6–34: Profile information that can be displayed according to the service's activity status (for agents)

Profile type	Service activity status	Display of valid configuration information	Display of configuration file contents
Event Forwarding	Running	Y	Y
	Stopped	N	Y
Log File Trapping	Running	Y	Y
	Stopped	N	Y
Event Log Trapping	Running	Y	Y
	Stopped	N	Y
Local Action	Running	Y	Y
	Inactive	N	Y
	Stopped	N	Y

Legend:

Y: Can be displayed.

N: Cannot be displayed.

(2) Profile information that can be displayed for remotely monitored hosts according to the status of service activity

The following profile information can be displayed:

- Remote-monitoring log file trap information
- Remote-monitoring event log trap information (for Windows only)

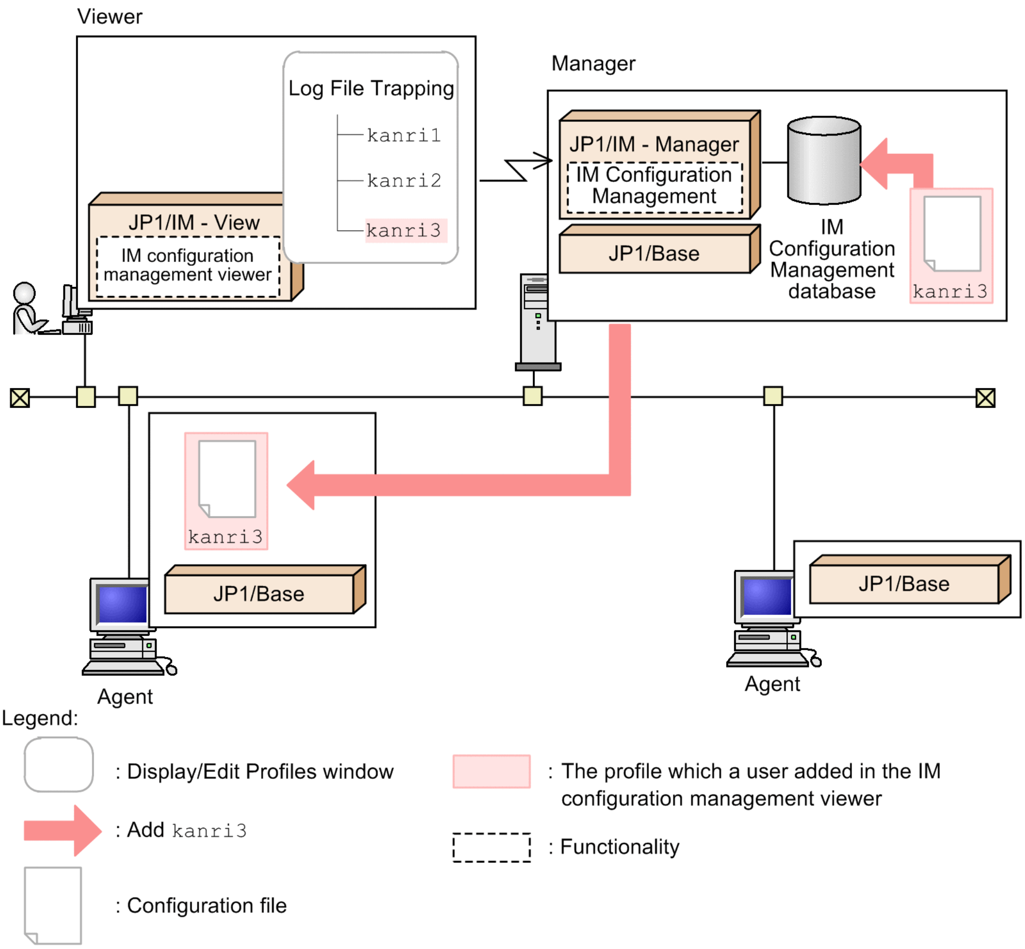
6.5.5 Adding and deleting profiles

Using IM Configuration Management, you can add or delete profiles for log file traps that were set on individual agents if the versions of JP1/Base on the agents are 09-10 or later. You can also add or delete profiles for remote-monitoring log file traps that were set on individual remotely monitored hosts.

(1) Adding profiles

The following figure illustrates the flow for adding profiles for log file traps and remote-monitoring log file traps.

Figure 6–36: Flow for adding a profile by using IM Configuration Management


Viewer
Log File Trapping
kanri1
kanri2
kanri3
JP1/IM - View
IM configuration management viewer
Manager
JP1/IM - Manager
IM Configuration Management
JP1/Base
IM Configuration Management database
kanri3
kanri3
JP1/Base
Agent
JP1/Base
Agent
Legend:
: Display/Edit Profiles window
: Add kanri3
: Configuration file
: The profile which a user added in the IM configuration management viewer
: Functionality

You can add profiles in the Add Profile window of the IM configuration management viewer. After you add profiles, the added profiles are displayed in the tree display area in the Display/Edit Profiles window.

After you add profiles, you need to edit and save or apply the following information:

- For agents:
  - Log-file trap action definition file
  - Log-file trap startup definition file
- For remotely monitored hosts:
  - Remote-monitoring log file trap action-definition file
  - Start options for remote-monitoring log file traps

For details about the procedure, see *3.5.1(5) Editing configuration files* in the *JP1/Integrated Management - Manager Configuration Guide*.

The following table describes the items that can be set when you add profiles.

Table 6–35: Items that can be set when you add profiles

Item	Description
Log file trap name	Specify the log file trap name.

Item	Description
	You cannot specify a log file trap name that is already set or that is the same as the log-file trap action definition file.
Cluster ID	Specify the cluster ID when you manage the log file on a shared disk of a logical host. For details about the cluster ID, see the *JP1/Base User's Guide*. If the cluster ID is enabled, you can specify the log file trap for a cluster.

For details about how to add profiles, see *3.5.1(4)(a) Adding profiles* in the *JP1/Integrated Management - Manager Configuration Guide*.

The following table shows the paths where the definition files are located when the log file trap information added from IM Configuration Management is applied to the monitoring target of the agent.

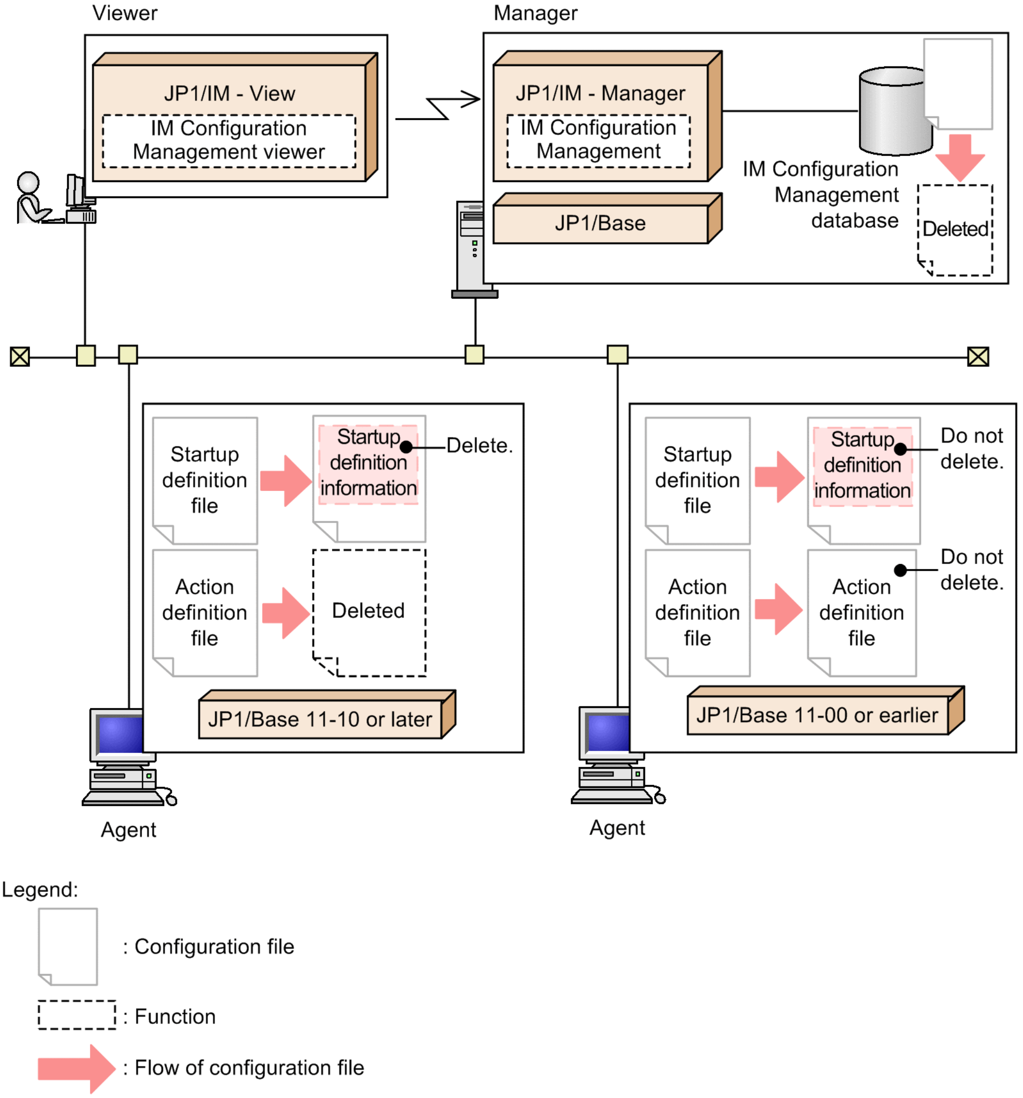
Table 6–36: Location of the definition files that are added from IM Configuration Management

Configuration file	Type of OS on agent	Location
Log-file trap action definition file	Windows	*Base-path*`\conf\cf_log_file_trap\`
	UNIX	`/etc/opt/jp1base/conf/cf_log_file_trap/`
Log-file trap startup definition file	Windows	*Base-path*`\conf\event\`
	UNIX	`/etc/opt/jp1base/conf/event/`

(2) Deleting profiles

The following figure illustrates the flow for deleting profiles for log file traps and remote-monitoring log file traps.

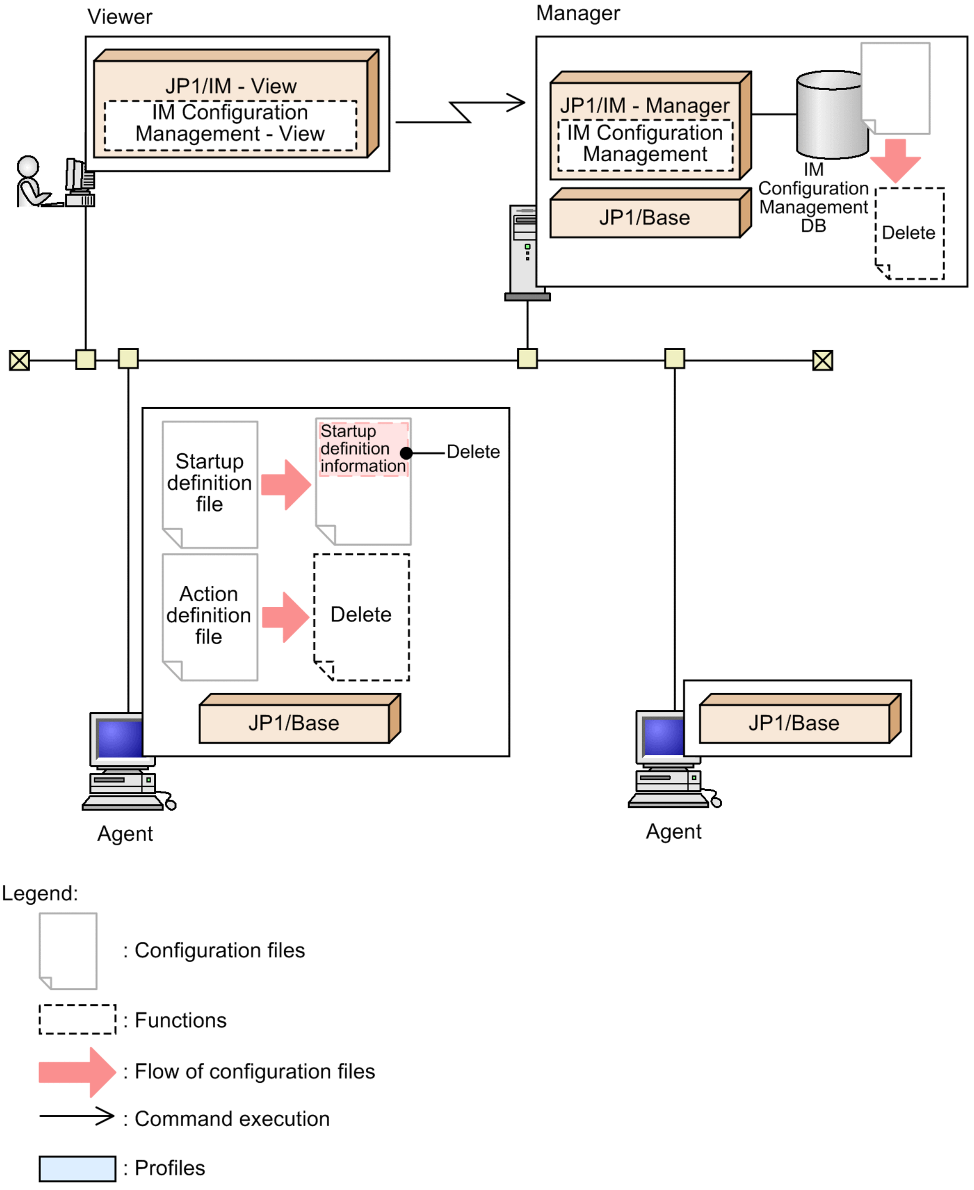
Figure 6–37: Flow for deleting profiles by using IM Configuration Management



You can delete profiles in the Display/Edit Profiles window of the IM configuration management viewer. After you delete profiles, the profiles for log file traps and remote-monitoring log file traps that are saved in the IM Configuration Management database are deleted. If the agent's JP1/Base version is 11-10 or later, the agent's log file trap information is also deleted when the profiles are deleted. If the agent's JP1/Base version is 11-00 or earlier, the agent's log file trap information is deleted when the log file trap process is stopped, not when the profiles are deleted.

When you delete profiles for log file traps for a cluster, however, the flow for deleting profiles is different as shown in the following figure.

Figure 6–38: Flow for deleting profiles for cluster by using IM Configuration Management



When you delete a profile, the profile for log file traps saved in the IM Configuration Management database is deleted.

- For agents:

  The log-file trap startup definition information is deleted from the log-file trap startup definition file, and then the log-file trap action definition file is deleted. Then, the settings of log file traps are deleted from agents.
- For remotely monitored hosts:

  The log-file trap startup definition information is deleted from the remote-monitoring log file trap startup-definition file, and then the remote-monitoring log file trap action-definition file is deleted.

Note that the profile cannot be deleted if the log file trap whose profile you want to delete is running on the agent regardless of whether it is for a cluster. First stop the log file trap whose profile you want to delete, and then delete the profile.

For details about how to delete profiles, see *3.5.1(4)(b) Deleting profiles* in the *JP1/Integrated Management - Manager Configuration Guide*.

6.5.6 Editing configuration files

Using IM Configuration Management, you can edit JP1/Base profiles on agents and profiles on remotely monitored hosts.

The following describes the functionality for editing configuration files.

(1) Editing configuration file contents

In the Display/Edit Profiles window, you can edit the contents of a displayed configuration file.

The following configuration files can be edited in IM Configuration Management:

Table 6–37: Configuration files that can be edited in IM Configuration Management

Profile type	Configuration file	Notes
Event Forwarding	Event forwarding setting file (`forward`)	--
Log File Trapping	Action definition file for log file trapping (any file)	If the version of JP1/Base on an agent host is 09-10 or later, the service must be restarted when an item other than `MARKSTR` and `ACTDEF` is edited. If the version of JP1/Base on an agent host is earlier than 09-10, do not edit any item other than `MARKSTR` and `ACTDEF`.
	Log-file trap startup definition file (`jevlog_start.conf`)	If the version of JP1/Base of an agent host is 09-10 or later, you can edit only the start options. The log-file trap startup definition file is updated based on the edited start options.
Event Log Trapping	Action definition file for event log trapping (`ntevent.conf`)	You cannot edit the event server name (`server`).
Local Action	Local action execution definition file (`jbslcact.conf`)	--
Remote-monitoring Log File Trapping	Remote-monitoring log file trap action-definition file (any file)	--
Remote-monitoring Event Log Trapping	Remote-monitoring event log trap action-definition file (any file)	--

Legend:

--: Not applicable.

You can perform the following operations on these files in the Display/Edit Profiles window.

Copy text

You can copy text from a configuration file. Exclusive editing rights are not required.

In the file contents shown in the node display area, select the text that you want to copy and then perform either of the following:

- Choose **Edit** and **Copy**.
- Right-click and choose **Copy**.

Cut text

You can cut text from a configuration file. To do so, you must first obtain exclusive editing rights.

In the file contents shown in the node display area, select the text that you want to cut and then perform either of the following:

- Choose **Edit** and **Cut**.
- Right-click and choose **Cut**.

Paste text

You can paste copied or cut text into a configuration file. To do so, you must first obtain exclusive editing rights.

In the file contents shown in the node display area, select the position where you want to paste the text and then perform either of the following:

- Choose **Edit** and **Paste**.
- Right-click and choose **Paste**.

The changes you make while editing a configuration file are not checked. If you quit or forcibly terminate IM Configuration Management - View during editing, the changes will not be saved.

(2) Saving edited file contents

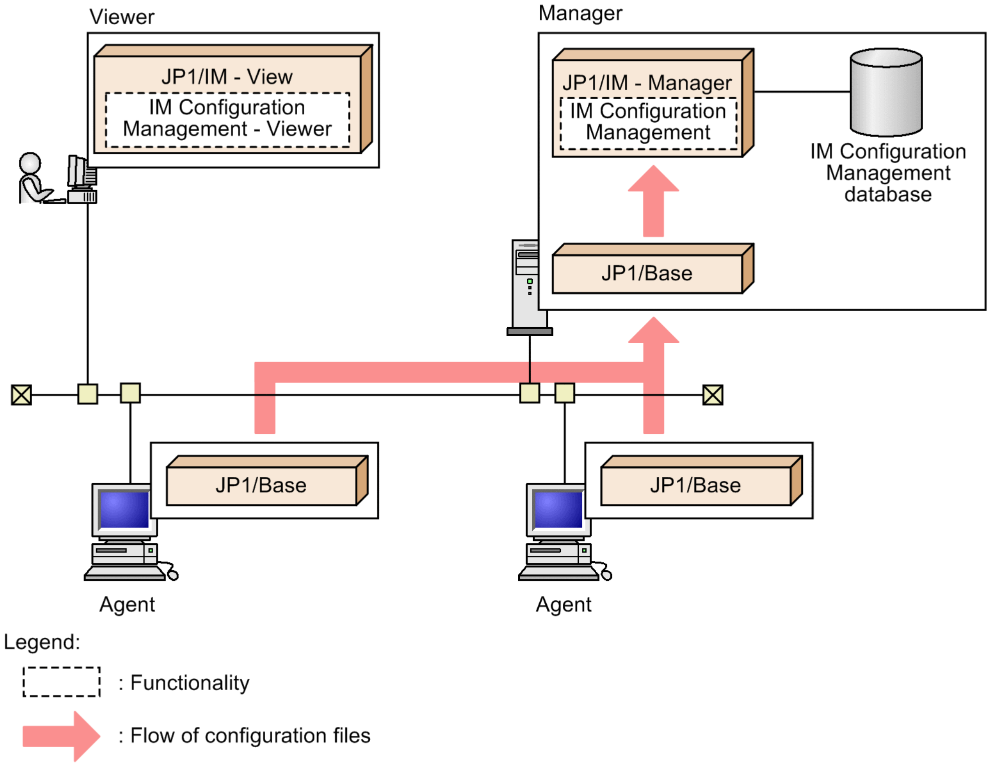
The contents of edited configuration files can be saved to the manager running IM Configuration Management.

Edited file contents are saved when you perform any of the following operations:

- In the node display area (settings information) of the Display/Edit Profiles window, select the **Save** check box and then click the **Execute** button.
- In the node display area (settings information) of the Display/Edit Profiles window, select the **Apply** check box and then click the **Execute** button.
- In the Display/Edit Profiles window, choose **Operation**, **Save/Apply Profiles**, and then **Save on the Server**.
- Import configuration files on the manager running IM Configuration Management.

The figure below shows the flow of processing when saving the contents of edited configuration files with IM Configuration Management.

Figure 6–39: Saving edited file contents with IM Configuration Management



Viewer
JP1/IM - View
IM Configuration Management - Viewer
Manager
JP1/IM - Manager
IM Configuration Management
IM Configuration Management database
JP1/Base
JP1/Base
JP1/Base
Agent
Agent
Legend:
: Functionality
: Flow of configuration files

The following configuration files can be saved:

- Event forwarding setting file
- Action definition file for log file trapping
- Log-file trap startup definition file
- Action definition file for event log trapping
- Local action execution definition file

Note that the log-file trap startup definition file can be saved only when the version of JP1/Base on the agent is 09-10 or later.

The edited file contents saved to the manager running IM Configuration Management cannot be forwarded to hosts.

Edited file contents saved to the manager will be overwritten when profiles are collected from the hosts.

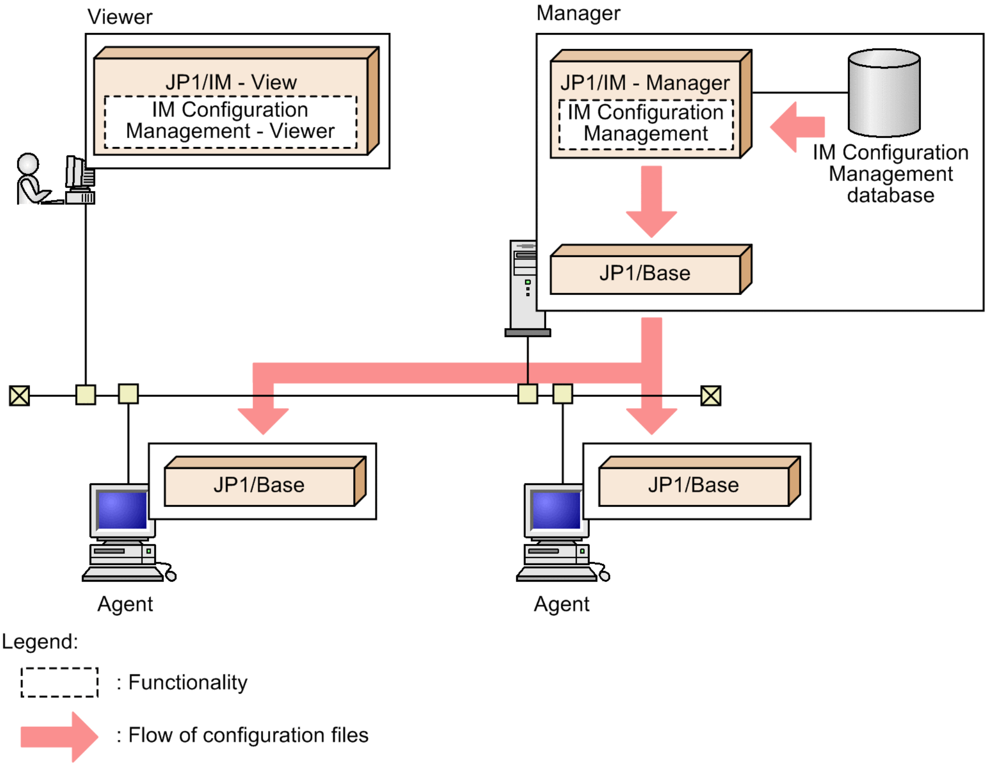
(3) Applying edited file contents

You can apply the contents of edited configuration files to JP1/Base on the agents. You can also enable the contents of the configuration files on remotely monitored hosts.

The operations for applying edited file contents differ depending on the items in the configuration file. For details about these operations, see *4.9.2 Configuration File page* in the manual *JP1/Integrated Management - Manager GUI Reference*.

The figure below shows the flow of processing when applying the contents of edited configuration files with IM Configuration Management.

Figure 6–40: Applying edited file contents with IM Configuration Management


Viewer
JP1/IM - View
IM Configuration Management - Viewer
Manager
JP1/IM - Manager
IM Configuration Management
IM Configuration Management database
JP1/Base
JP1/Base
JP1/Base
Agent
Agent
Legend:
: Functionality
: Flow of configuration files

You can apply the edited file contents per host, or batch-apply the contents to all hosts.

On the **Configuration File** page of the Display/Edit Profiles window, you can check the status of a configuration file after the edited contents are applied. If the application is successful, the status becomes **Applied**. If the application fails, the status becomes **Application failed**. If the saved configuration file is not used on the server, the status becomes a blank (not applied). If the configuration file is saved on the server, but not used on the target host, the status becomes **Saved on the server**.

If the status of the configuration file is **Application failed** or **Saved on the server**, in the tree display area on the **Configuration File** page, an icon appears indicating that the configuration file is being edited.

If the processing fails in JP1/Base version 9 or later, the configuration files on the agent are rolled back to their previous status.

On the **IM Configuration** page of the IM Configuration Management window, you can check the status of the host after the contents are applied. If there are configuration files that have the **Application failed** or **Saved on the server** status, among host icons in the tree display area, an icon appears indicating an error status. To see the details, on the **IM Configuration** page, click the **Basic Information** button in the node display area.

Apply per host

The following configuration files can be applied per host in IM Configuration Management:

- Event forwarding setting file
- Action definition file for log file trapping
- Log-file trap startup definition file
- Action definition file for event log trapping
- Local action execution definition file
- Remote-monitoring log file trap action-definition file

- Remote-monitoring event log trap action-definition file

Note that the log-file trap startup definition file can be applied only when the version of JP1/Base on the agent is 09-10 or later.

For details about how to apply the edited contents per host, see *3.5.1(6)(b) Applying edited information in configuration files individually to each agent* in the *JP1/Integrated Management - Manager Configuration Guide*.

Apply to all hosts

The following configuration files can be applied in one operation with IM Configuration Management:

- Event forwarding setting file
- Log-file trap action definition file
- Log-file trap startup definition file
- Action definition file for event log trapping
- Local action execution definition file

Note that the log-file trap startup definition file can be applied only if the agent's JP1/Base version is 11-10 or later.

For details about how to batch-apply the edited contents, see *3.5.1(6)(a) Using the batch mode to apply edited information in configuration files* in the *JP1/Integrated Management - Manager Configuration Guide*.

When batch-applying the edited contents, if the configuration file does not exist on the server, the KNAN22497-I message is displayed, and the information is not applied.

6.5.7 Obtaining and releasing exclusive editing rights for a configuration file

Before you collect or edit configuration files, you must obtain exclusive editing rights to the files so that they cannot be edited from another instance of IM Configuration Management - View.

Because exclusive editing rights are obtained for each JP1 product on a host, the exclusive editing rights for JP1/Base and the exclusive editing rights for a remotely monitored host can be obtained separately. Therefore, for example, the profiles on a remotely monitored host can be edited while JP1/Base profiles are being edited. Also, you can obtain exclusive editing rights for multiple hosts and multiple JP1 products at the same time.

This section describes how to set and release exclusive editing rights for configuration files.

(1) Obtaining exclusive editing rights

Exclusive editing rights are required to perform the following operations:

- Edit a configuration file
- Add, delete, start, or stop log file traps of JP1/Base 09-10 or later, or the profiles on a remotely monitored host
- Export or import configuration files
- Collect configuration file information from lower-level hosts
- Update information in a profile tree

To obtain exclusive editing rights for configuration files, perform either of the following:

- In the tree display area in the Display/Edit Profiles window, click the JP1 product name (JP1/Base) or the profile for remote monitoring (remote monitoring), and then select **Exclusive Editing Settings** from the **Edit** menu.

- In the tree display area in the Display/Edit Profiles window, right-click the JP1 product name (JP1/Base) or the profile for remote monitoring (remote monitoring), and then select **Exclusive Editing Settings**.

(2) Releasing exclusive editing rights

To release exclusive editing rights for configuration files, perform either of the following:

- In the tree display area in the Display/Edit Profiles window, right-click the JP1 product name (JP1/Base) or the profile for remote monitoring (remote monitoring), and then select **Release Exclusive Editing**.
- In the tree display area of the Display/Edit Profiles window, click the JP1 product name (**JP1/Base**) and then choose **Edit** and **Release Exclusive Editing**. In the tree display area in the Display/Edit Profiles window, click the JP1 product name (JP1/Base) or the profile for remote monitoring (remote monitoring), and then select **Release Exclusive Editing** from the **Edit** menu.

6.5.8 Starting and stopping log file traps and event log traps

You can manage starting and stopping of the following log file traps and event log traps:

- Log file traps (for agents)
- Remote-monitoring log file traps (for remotely monitored hosts)
- Remote-monitoring event log traps (for remotely monitored hosts)

For agents, you can start and stop log file traps only when the version of JP1/Base is 09-10 or later.

To start and stop them, use the following configuration files:

For log file traps:

  - Log-file trap action definition file
  - Log-file trap startup definition file

For remote-monitoring log file traps:

  - Remote-monitoring log file trap action-definition file

For remote-monitoring event log traps:

  - Remote-monitoring event log trap action-definition file

If both the following criteria are met for agents, you must move the log-file trap definition to the log-file trap startup definition file:

- If the version of JP1/Base is changed from a version earlier than 09-10 to version 09-10 or later;

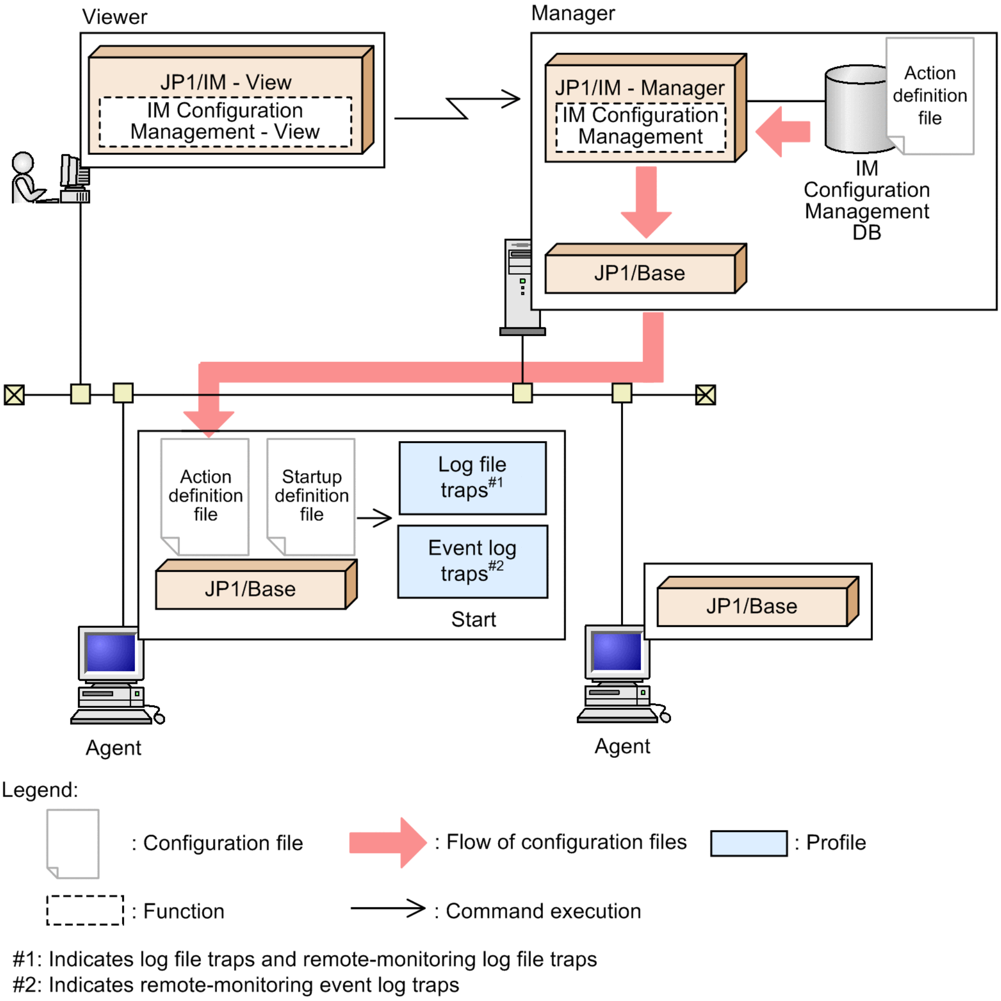
- If the setting is defined so that log file traps are started by the start sequence definition file or the `jbs_start` command.

For details about how to move the log-file trap definition, see the description in *Notes on installing and uninstalling JP1/Base* in the *JP1/Base User's Guide*.

(1) Starting log file traps and event log traps

The following illustrates the flow for starting log file traps and event log traps by using IM Configuration Management.

Figure 6–41: Flow for starting log file traps and event log traps



You can start log file traps and event log traps in the Display/Edit Profiles window of the IM configuration management viewer.

For agents:

After you start log file traps, the log-file trap action definition file saved in the IM Configuration Management database is applied to the agents. Then, the log-file trap startup definition is applied to the log-file trap startup definition file on the agents as follows:

- When the log-file trap startup definition file has been defined:
  The startup definition information is overwritten.
- When the log-file trap startup definition file has not been defined:
  The startup definition information is added.

After the definition information in the log-file trap action definition file and the log-file trap startup definition file is applied, commands are executed on the agents, and the log file traps are started.

For remotely monitored hosts:

- After you start a remote-monitoring log file trap, commands are executed on the remotely monitored hosts, and the remote-monitoring log file traps are started.
- After you start a remote-monitoring event log trap, commands are executed on the remotely monitored hosts, and the remote-monitoring event log traps are started.

In the following statuses, you cannot select **Start Process** from the **Operation** menu in the Display/Edit Profiles window.

- The log file trap or event log trap you want to start has already been started.
- A cluster ID is specified for the agent.
  If a cluster ID is specified for the agent, send the configuration files to the agent. For details about how to send the configuration files, see *3.5.1(6)(b) Applying edited information in configuration files individually to each agent* in the *JP1/Integrated Management - Manager Configuration Guide*.

If you change the Windows account information after you start a remote-monitoring log file trap and NetBIOS (NetBIOS over TCP/IP) connection is established with the monitored host, the connection is maintained until the NetBIOS (NetBIOS over TCP/IP) is disconnected. If you want to break the NetBIOS (NetBIOS over TCP/IP) connection and reconnect using the new account information, you need to restart the monitored host or the manager.

For details about how to start log file traps on agents, see *3.5.1(7)(a) Starting log file traps* in the *JP1/Integrated Management - Manager Configuration Guide*.

For details about how to start remote-monitoring log file traps and remote-monitoring event log traps, see *3.5.2(5)(a) Starting remote-monitoring log file traps* in the *JP1/Integrated Management - Manager Configuration Guide*.

(a) Starting log file trapping automatically

If the agent's JP1/Base version is 11-10 or later, you can specify in IM Configuration Management whether log file trapping is to be started automatically when an agent host is restarted or when the log file trap service is restarted.

To specify that log file trapping be started automatically, in the Display/Edit Profiles window, under **Startup options**, select the **Start the process automatically when the log file trap service starts** check box. The settings for starting log file trapping automatically that are specified by selecting the **Start the process automatically when the log file trap service starts** check box are applied to the agent's log-file trap startup definition file at the following times:

- When log file trapping starts
- When profiles are applied (**Reload**, **Restart**, or **Send a file**)
- When batch application of profiles is performed

The **Start the process automatically when the log file trap service starts** check box is displayed only when the `LOGFILETRAP_AUTO_START_CONTROL` common definition information is set to `00000001` (enabled).

If common definition information `LOGFILETRAP_AUTO_START_CONTROL` is set to `00000000` (disabled), the **Start the process automatically when the log file trap service starts** check box is not displayed. The setting for starting log file trapping automatically is changed as follows:

- When log file trapping is started, the setting for starting log file trapping automatically is enabled.
- When log file trapping is stopped, the setting for starting log file trapping automatically is disabled.

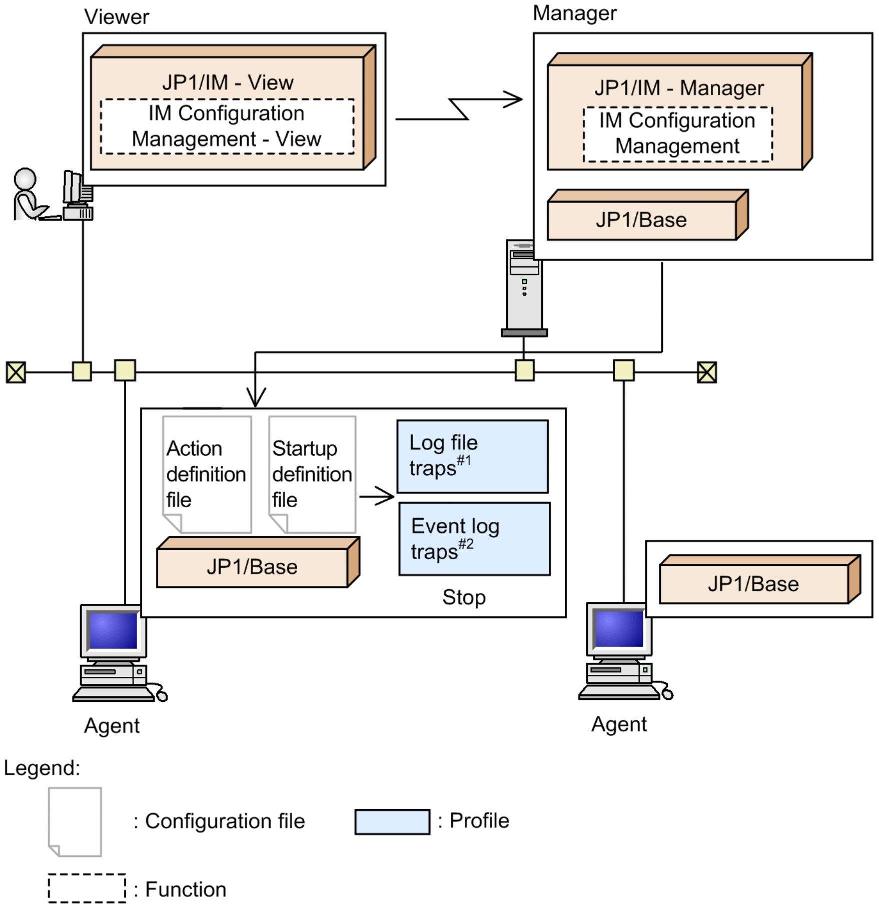
The `LOGFILETRAP_AUTO_START_CONTROL` common definition information is defined in the profile management environment definition file (`jp1cf_profile_manager.conf`). For details, see *Profile management environment definition file (jp1cf_profile_manager.conf)* in *Chapter 2. Definition Files* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

For details about **Startup options** in the Display/Edit Profiles window, see *4.9.2 Configuration File page* in the manual *JP1/Integrated Management - Manager GUI Reference*.

(2) Stopping log file traps and event log traps

The following illustrates the flow for stopping log file traps and event log traps by using IM Configuration Management.

Figure 6–42: Flow for stopping log file traps and event log traps



#1: Indicates log file traps and remote-monitoring log file traps.
#2: Indicates remote-monitoring event log traps.

You can stop log file traps and event log traps in the Display/Edit Profiles window of the IM configuration management viewer.

For agents running JP1/Base version 11-10 or later

If you stop log file traps, log file trapping stops. When log file trapping stops, the log-file trap startup definition is not deleted from the agent's log-file trap startup definition file. The agent's log-file trap action definition file is not deleted either.

For agents running JP1/Base version 11-00 or earlier

If you stop log file traps, log file trapping stops. When log file trapping stops, the log-file trap startup definition is deleted from the log-file trap startup definition file, and then the log-file trap action definition file is deleted. Also, the log-file trap action definition file is deleted on the agent, and log file trapping is stopped.

For remotely monitored hosts:

- After you stop remote-monitoring log file traps, commands are executed on the remotely monitored host, and remote-monitoring log file traps stop.
- After you stop remote monitoring event log traps, commands are executed on the remotely monitored host, and remote-monitoring event log traps stop.

In the following statuses, you cannot select **Stop Process** from the **Operation** menu in the Display/Edit Profiles window:

- The log file trap or event log trap you want to stop has not been started.
- A cluster ID is specified for the agent.

For details about how to stop log file traps on agents, see *3.5.1(7)(b) Stopping log file traps* in the *JP1/Integrated Management - Manager Configuration Guide*.

For details about how to stop remote-monitoring log file traps and remote-monitoring event log traps, see *3.5.2(5)(b) Stopping remote-monitoring log file traps* in the *JP1/Integrated Management - Manager Configuration Guide*.

6.5.9 Synchronizing profiles

If profiles are edited at an agent or at the manager (IM Configuration Management) while profile management of IM Configuration Management is being used together with JP1/Base's profile management, the profiles held by the agent will no longer match the profiles held by the manager. In this case, the profiles must be synchronized manually between the agent and the manager.

The following table describes when synchronization is needed and the synchronization methods.

Table 6–38: When profiles need to be synchronized and synchronization methods

No.	Timing	Synchronization method	Operation
1	An agent's profiles are edited.	Use IM Configuration Management to collect profiles from the agent.	In the Display/Edit Profiles window, select a profile you want to collect, and then run **Collect Profiles** from the menu.
2	Profiles were distributed to agents by the `jevdef_distrib` command.	Use IM Configuration Management to collect profiles from the agents in a batch operation.	In the IM Configuration Management window, run **Batch Collect Profiles** from the menu.
3	Profiles were edited with IM Configuration Management and then saved in the manager.	Apply the profiles from the manager to the agents.	In the Display/Edit Profiles window, on the **Configuration File** page, select the **Apply** radio button, and then select **Restart**, **Reload**, or **Send a file** to synchronize profiles.
4	Profiles were imported by the `jcfimport` command.	Apply profiles from the manager to the agents in a batch operation.	In the IM Configuration Management window, run **Batch Apply Profiles** from the menu.

When you display and apply profiles, IM Configuration Management can compare the contents of profiles that were collected previously by the manager to the contents of the most recent agent profiles and detect any inconsistencies. If the contents do not match, IM Configuration Management displays a dialog box containing a message (`KNAN21187-W`) that indicates that the configuration file for the agent's log file information might have been modified. This function is called the updated agent profile notification function.

You can use the `AGENT_PROFILE_UPDATE_NOTICE` function in the common definition information to enable or disable the updated agent profile notification function. You can define `AGENT_PROFILE_UPDATE_NOTICE` in the profile management environment definition file (`jp1cf_profile_manager.conf`). For details, see *Profile management environment definition file (jp1cf_profile_manager.conf)* in *Chapter 2. Definition Files* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

If the updated agent profile notification function is enabled, IM Configuration Management checks agent profiles to determine if the profiles have been updated when any of the operations listed in the following list is performed in the Display/Edit Profiles window. Note that this check is performed only when **Exclusive Editing Settings** is selected.

- Displaying profiles
- Applying profiles (**Reload**, **Restart**, or **Send a file**)
- Starting log file trapping

6.5.10 Notes on using IM Configuration Management's profile management together with JP1/Base's profile management

This subsection provides notes on using IM Configuration Management's profile management together with JP1/Base's profile management.

(1) Applying profiles from both JP1/Base and IM Configuration Management

Even when **Exclusive Editing Settings** is selected in the Display/Edit Profiles window, changes to profiles cannot be locked if JP1/Base's `jevdef_distrib` command is used and the definition files are edited directly. If profiles are applied from both JP1/Base and IM Configuration Management, the content applied most recently takes effect.

(2) Number of log file traps that can be specified in the log-file trap startup definition file

The maximum number of log file traps that can be specified in the JP1/Base log-file trap startup definition file is 200. The maximum number of log file traps that can be managed per host by IM Configuration Management is 100. If you will be managing all log file traps that are set for one host by IM Configuration Management, ensure that no more than 100 traps are specified in the log-file trap startup definition file when definition information is distributed by the `jevdef_distrib` command.

6.6 Managing remotely monitored hosts

Using IM Configuration Management, you can manage remotely monitored hosts by collecting the following types of remote-monitoring log information from the remotely monitored hosts:

- Remote-monitoring log file trap information
- Remote-monitoring event log trap information (for Windows only)

Only the newly acquired log information (information not previously in the log) is collected by lines.

The following remotely monitored hosts listed can be managed. Note that remotely monitored hosts are limited to hosts whose language is the same as that of the managing JP1/IM - Manager. However, only ASCII encoding is supported; multibyte characters are not supported.

- If the managing JP1/IM - Manager is running Windows, remotely monitored Windows, Linux, and UNIX hosts can be managed.
- If the managing JP1/IM - Manager is running Linux or UNIX, remotely monitored Linux and UNIX hosts can be managed.

Remote monitoring has some functional limitations compared to monitoring in an agent configuration. For details about selection of remote monitoring or monitoring using JP1/Base, see *6.2.8 Selection of agent configuration or remote monitoring configuration*.

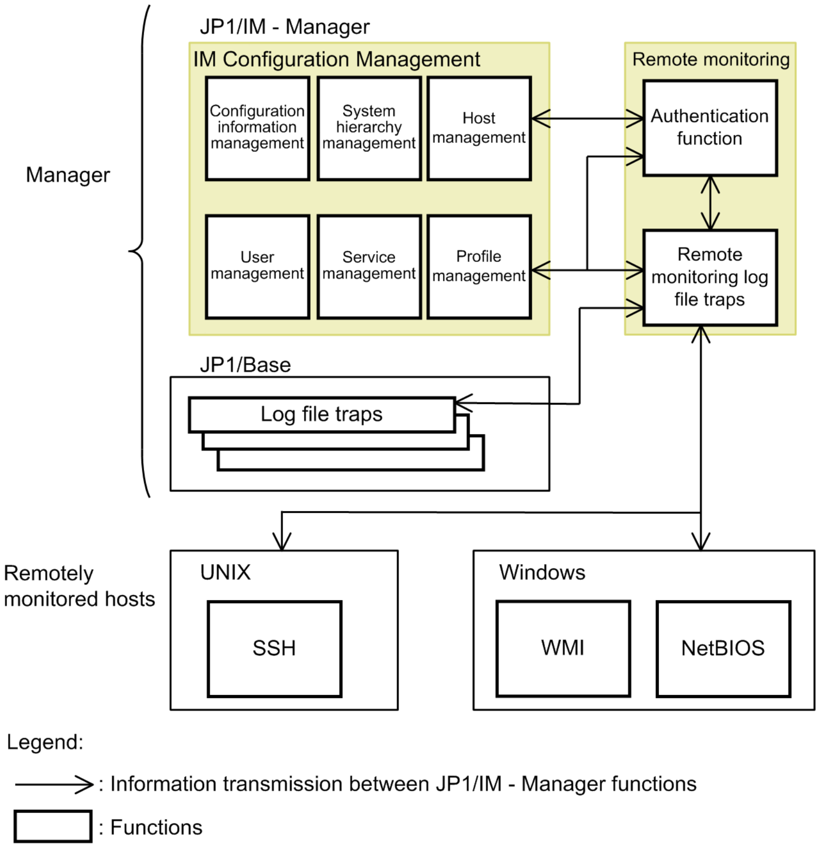
In remote monitoring, the resolution of names of monitored hosts into the IP addresses is performed by the JP1/IM - Manager host OS. When you perform remote monitoring, specify and register the host names of monitored hosts in the `hosts` file and DNS so that the JP1/IM - Manager host OS can resolve them.

6.6.1 Collecting log information

Linking with IM Configuration Management functions and JP1/Base log file trapping, authentication management for remote monitoring and the remote monitoring log file trap function collect remote monitoring log information from SSH, WMI, and NetBIOS (NetBIOS over TCP/IP) on remotely monitored hosts.

The following figure shows the relationships between the functions for collecting remote monitoring log information.

Figure 6–43: Relationships between the functions for collecting remote monitoring log information



Remote monitoring log information collection is done based on the character string for the start option or monitoring conditions for action definition that are set on the IM configuration management viewer or on a command for remote monitoring. To collect remote monitoring log information, the manager connects to the remotely monitored hosts, collects the output results of the log files or event logs at the specified monitoring interval, and passes the information to the JP1/Base log file traps.

For the character string for the start option, the contents set in the IM configuration management viewer or in the start option of a command, and the contents set in the remote-monitoring log file trap startup-definition file or the remote-monitoring event log trap action-definition file are used. For the action definition, the contents set in the remote-monitoring log file trap action-definition file and in the remote-monitoring event log trap action-definition file are used.

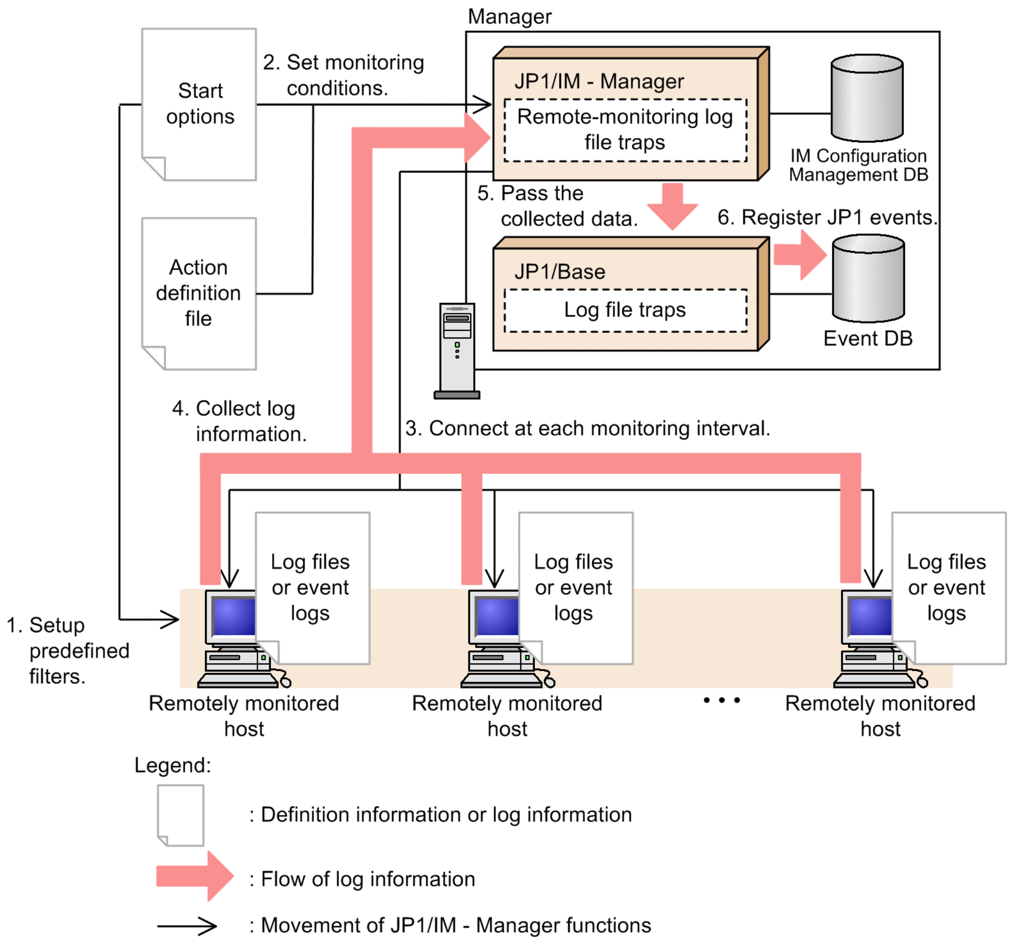
To use the remote-monitoring log file trap function, specify a log file trap name. A remote-monitoring log file trap name can be the same as the name for a remote-monitoring log file trap on another monitored host or for a JP1/Base log file trap. However, the same name cannot be specified for multiple remote-monitoring log file traps on one monitored host. Specify a unique name for a monitored host.

Note

When the remote event-log trapping function is used, the monitoring name `DEFAULT0` is used internally by the JP1/Base log file trapping function. Therefore, the name `DEFAULT0` is output by the JP1/Base log file trapping function to the log message. However, `DEFAULT0` is not set as a monitoring name for the JP1 event extended attribute. If a monitoring name is specified for `trap-name` in the `filter` parameter in the remote-monitoring event log trap action-definition file, the value specified for `trap-name` is set as the monitoring name for the JP1 event extended attribute.

The following figure shows how remote monitoring log information is collected.

Figure 6–44: Collecting remote monitoring log information



Manager
Start options
2. Set monitoring conditions.
JP1/IM - Manager
Remote-monitoring log file traps
IM Configuration Management DB
5. Pass the collected data.
6. Register JP1 events.
JP1/Base
Log file traps
Event DB
Action definition file
4. Collect log information.
3. Connect at each monitoring interval.
Log files or event logs
Log files or event logs
Log files or event logs
1. Setup predefined filters.
Remotely monitored host
Remotely monitored host
Remotely monitored host
Legend:
: Definition information or log information
: Flow of log information
: Movement of JP1/IM - Manager functions

The following describes the above figure.

1. Use JP1/IM - View or a command for remote monitoring to set a predefined filter.
   For details about predefined filters, see *6.6.5 Predefined filter*.
2. Use JP1/IM - View or a command for remote monitoring to set the character string for the start option and monitoring conditions for action definitions.
3. Connect to the remotely monitored hosts at each monitoring interval set for monitoring conditions.
4. Collect the newly acquired log information from the remotely monitored hosts.
5. Pass the collected information to the JP1/Base log file trap.
6. Register the log information items that match the monitoring conditions as JP1 events in the event database.

Before performing remote monitoring, remote communication must be set up between the manager and the monitored hosts. For details about the communication settings, see *1.17 Specifying settings for monitoring logs on remotely monitored hosts (for Windows)* (for Windows) or *2.16 Specifying settings for monitoring logs on remotely monitored hosts (for UNIX)* (for UNIX) in the *JP1/Integrated Management - Manager Configuration Guide*. For details about how to configure the settings for collecting remote monitoring log information, see *Chapter 3. Using IM Configuration Management to Set the System Hierarchy* in the *JP1/Integrated Management - Manager Configuration Guide*.

6.6.2 Collectable log information and connection methods for remote monitoring

The following table describes remote monitoring log information that can be collected from the remotely monitored hosts, and the connection methods for remote monitoring.

For collecting host information, WMI and NetBIOS (NetBIOS over TCP/IP) connections are used to check connection and collect host information. Therefore, the agents on remotely monitored hosts operate on the premise that they can connect to WMI and NetBIOS (NetBIOS over TCP/IP). Even if you intend to collect only event logs, enable not only WMI connection but also NetBIOS (NetBIOS over TCP/IP) connection.

Table 6–39: Log information and connection methods for remote monitoring

OS on the host on which JP1/IM - Manager has been installed	OS on the monitored host	Log information	Connection method
Windows	Windows	Log file	NetBIOS (NetBIOS over TCP/IP)
		Event log	WMI
	UNIX	Log file	SSH
UNIX	Windows	--	--
	UNIX	Log file	SSH

Legend:

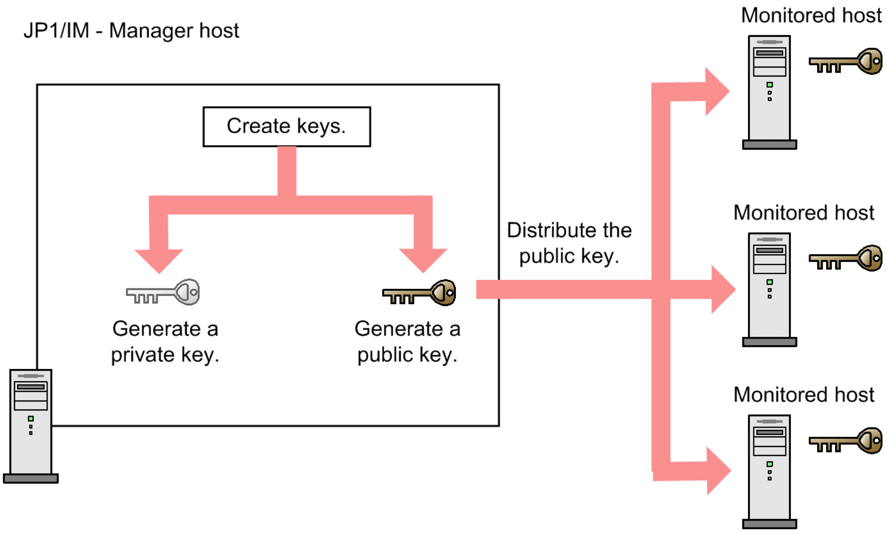
--: Not applicable.

SSH authentication

The public key authentication method is used for SSH authentication.

The figure below illustrates the concept of public key authentication. When JP1/IM - Manager is running on Windows, the keys are actually created on UNIX monitored hosts. This explanation is omitted in the figure.

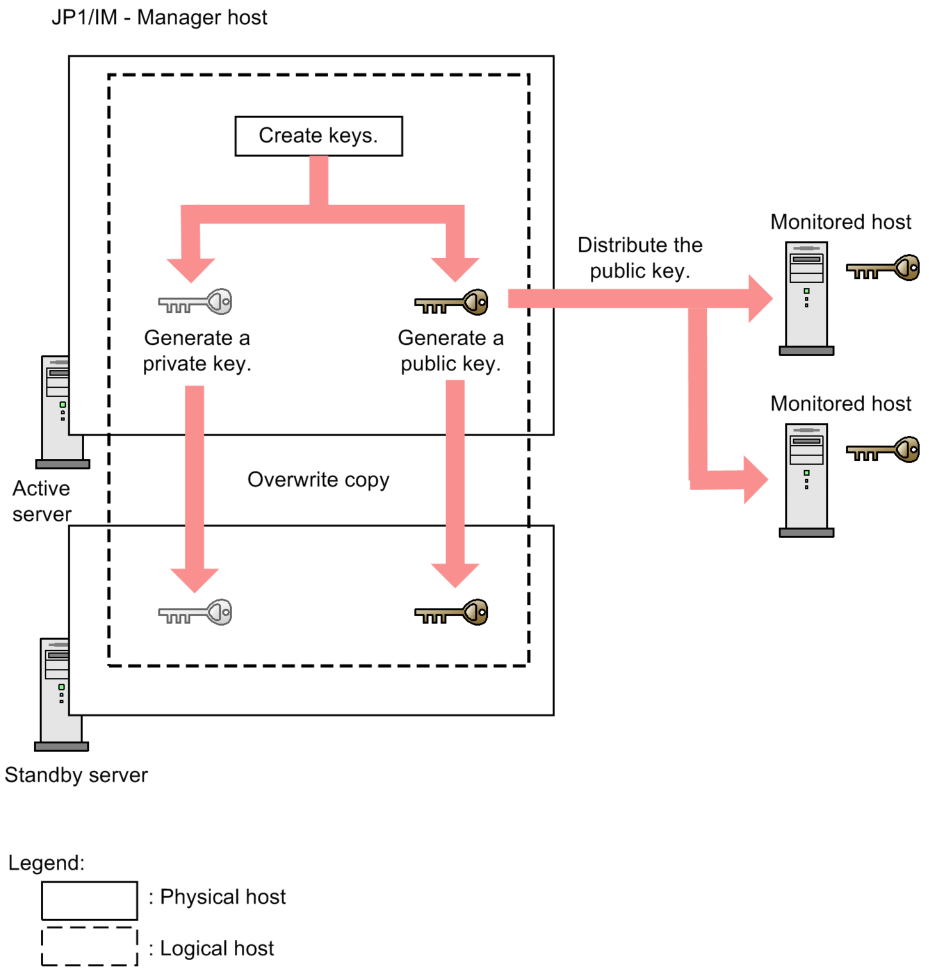
Figure 6–45: Concept of public key authentication



There are two methods of public key authentication on a cluster system. One method uses a common key on both the primary node and the standby node. The other method uses different keys on the primary node and the standby node.

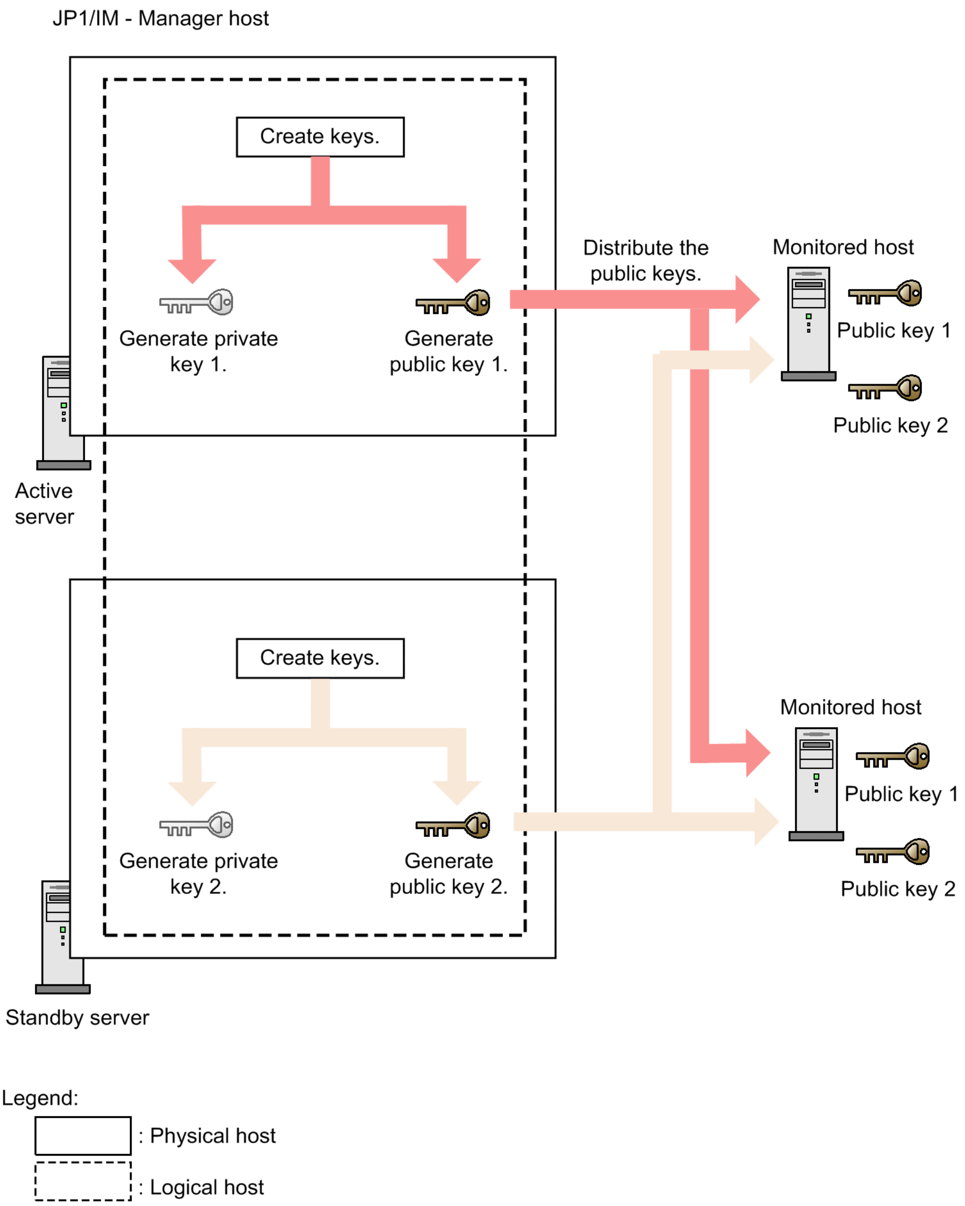
To use a common key on both the primary node and the standby node, overwrite-copy the key file on the primary node to the key file on the standby node. The following figure illustrates the concept when a common key is used.

Figure 6–46: Concept of public key authentication (when a common key is used on the primary node and the standby node)



To use different keys on the primary node and the standby node, register both key files on the primary node and the standby node in the remotely monitored hosts. The following figure illustrates the concept when different keys are used.

Figure 6–47: Concept of public key authentication (when different keys are used on the primary node and the standby node)



6.6.3 Log information that can be monitored

The following describes log file trap information and Windows event log information that can be monitored.

(1) Output formats of log file trap information

The following shows the output formats of log file trap information that can be monitored by the remote-monitoring log file trap function. Note that if a new log file is output while another log file is being collected, the same log file might be trapped twice.

- SEQ
  In this format, log data is repeatedly added to a log file. When the log file reaches a certain size, a new log file with another file name is created and further log data is written to the new log file.

- SEQ2

  In this format, when a log file reaches a certain size, the log file is renamed as a backup file and saved in the same directory or under a subdirectory. Then a new log file is created with the same name as the old log file and further log data is written to the new log file.

  The created backup file must not be deleted until the log file is trapped next time.

  If the log file is switched during the monitoring interval, the data that was stored in the old log file since the last reading of the old log file is read from the most recently saved backup file. After that, data is read from the new log file. Other data is not read. Therefore, when you monitor a SEQ2-format log file, you need to set the monitoring interval appropriately so that the log file will not be switched twice or more during the monitoring interval.

  To set the monitoring interval, specify the `-t` option in the `jcfallogstart` command or, in the Display/Edit Profiles window, specify the `-t` option in the **Additional Options** field for **Startup Options**.

- WRAP2

  In this format, when a log file reaches a certain size and is wrapped, the log data in the log file is all deleted first, and then log data is written from the beginning of the log file.

  In the case of a WRAP2-format file, if the file is wrapped around and data is deleted before all data is read from the file, some data cannot be read from the file.

  Because a long monitoring interval might increase the size of the data to be read at a time, the monitoring interval must be set carefully.

  To set the monitoring interval, specify the `-t` option in the `jcfallogstart` command or, in the Display/Edit Profiles window, specify the `-t` option in the **Additional Options** field for **Startup Options**.

The following table describes the conditions for log files.

Table 6–40: Conditions for log files

Item	Conditions
File name	When the monitored host is a UNIX host, alphanumeric characters, hyphens (`-`), underscores (`_`), periods (`.`), and slashes (`/`) can be included in the path to the monitored files. A file path that includes a character other than above might not be normally monitored.
File output destination	If the monitored host is in a cluster configuration, and a logical name is specified for the monitored host, you can monitor the log files on a shared disk only. Network files cannot be monitored. You cannot monitor the files on a physical disk by using a logical host name because the information in the files on physical disks is managed by the executing host and the standby host. To monitor the files on a physical disk, specify the physical host names of the executing host and the standby host for the monitored host names.
File size	No more than 64 megabytes
Character string	Within the scope of JIS X 0208 If you use a character string outside the scope of JIS X 0208, the character string might not be normally monitored.
Acquisition limit	The total size of collected logs is within the maximum size of obtainable logs that is specified in the remote log trap environment definition file (`jp1cf_remote_logtrap.conf`).# If the specified size is exceeded, log files are not trapped. If the monitored host is a UNIX host and a predefined filter is used, the difference information of a log file is the size after the predefined filter is applied.
Monitoring start position at startup	The character next from the linefeed code that is output at the end of the log file If the monitored host is a Windows host and there is no linefeed code within the specified maximum amount of log data that can be acquired (or 10 kilobytes if not specified) from the end of the log file, the monitoring start position is the next character following the end of the file.

#: For details about the remote log trap environment definition file (`jp1cf_remote_logtrap.conf`), see *Remote log trap environment definition file (jp1cf_remote_logtrap.conf)* (*Chapter 2. Definition Files*) in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

(2) Types of Windows event log information

The following are types of Windows event log information that can be monitored by the remote-monitoring event log trap function:

- Application
- Security
- System
- DNS Server
- Directory Service
- File Replication Service
- DFS Replication

The log types `Critical` and `Verbose`, which were added in Windows Server 2008 R2, are not supported. A `Critical` or `Verbose` event log is collected as a JP1 event with an event level of `Error` or `Information` respectively.

If remote-monitoring event log traps are used, set the date and time on the manager host and on the monitored host to the correct current date and time.

If there is a difference between the date and time on the manager host and on the monitored host, monitoring might not be performed successfully. In addition, if the timestamp of an event log on the monitored host indicates a future time based on the time on the monitored host, monitoring might not be normally performed.

If the monitored host is in a cluster configuration and you specify a logical host name for the monitored host, Windows event log cannot be monitored.

The Windows event log is held by the executing host and the standby host. Therefore, specify a physical host name of the executing host and the standby host for the monitored host name.

The following table describes the conditions for Windows event logs.

Table 6–41: Conditions for Windows event logs

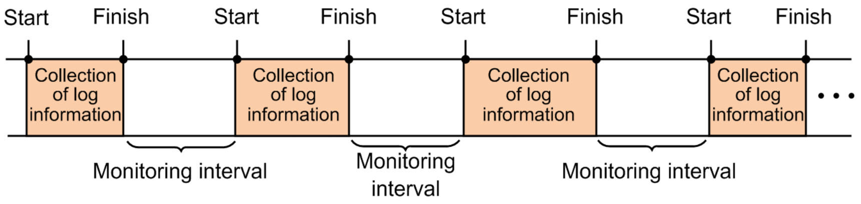
Item	Conditions
Character string	Within the scope of JIS X 0208 If you use a character string outside the scope of JIS X 0208, the character string might not be normally monitored.
Acquisition limit	The total size of collected Windows event logs is within the maximum obtainable size specified in the remote log trap environment definition file (`jp1cf_remote_logtrap.conf`)# If the specified size is exceeded, Windows event logs are not trapped. If a predefined filter is used, the difference information of the Windows event log is the size after the predefined filter is applied.
Monitoring start position at startup	Windows event logs that are generated on the monitored host after remote-monitoring event log trapping has started If logs generated while remote monitoring is stopped are set to be collected, they are treated as Windows event logs that are monitored while remote monitoring is stopped. You can specify whether to collect logs that are generated while remote monitoring is stopped in the remote log trap environment definition file (`jp1cf_remote_logtrap.conf`).#

#: For details about the remote log trap environment definition file (`jp1cf_remote_logtrap.conf`), see *Remote log trap environment definition file (jp1cf_remote_logtrap.conf)* (*Chapter 2. Definition Files*) in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

6.6.4 Monitoring interval for log information

Monitoring interval is the interval from when collection of log information finishes until when the next collection starts.

The following figure overviews the monitoring interval.

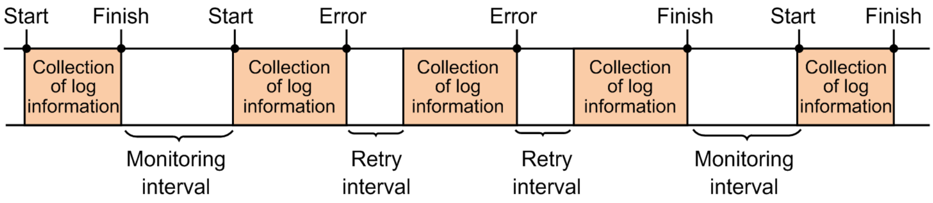

Start
Finish
Start
Finish
Start
Finish
Start
Finish
Collection of log information
Collection of log information
Collection of log information
Collection of log information
Monitoring interval
Monitoring interval
Monitoring interval

After a log that will be monitored is generated on a monitored host, the maximum time you might need to wait until a JP1 event is issued is the sum of the monitoring interval and the time it takes until the log information is collected.

If collection of log information fails, log information will be recollected based on the retry interval, which is from when a collection error occurs until collection starts. If log information cannot be collected within the maximum number of retries, monitoring stops. If JP1/IM - Manager is stopped, log information is not collected.

- For a remote monitoring log file trap:

  The following figure overviews the retry interval for a remote-monitoring log file trap.

  
  Start
Finish
Start
Error
Error
Finish
Start
Finish
Collection of log information
Collection of log information
Collection of log information
Collection of log information
Collection of log information
Monitoring interval
Retry interval
Retry interval
Monitoring interval

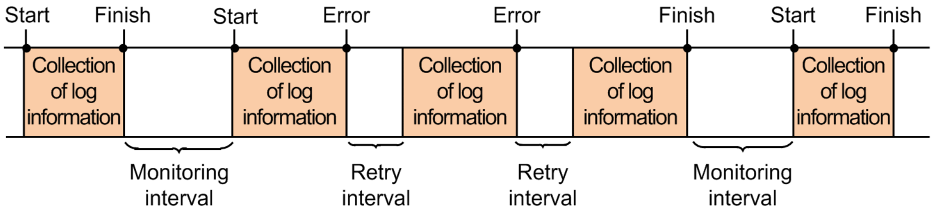
  Retry for a remote-monitoring log file trap is performed based on the number of times and the interval that have been specified in the following items in the remote-monitoring log file trap action-definition file:

  - Number of times specified by `open-retry-times` (if `open-retry-times` is omitted, the retry count is 1)
  - Interval specified by `open-retry-interval` (if `open-retry-interval` is omitted, the retry interval is 3 seconds)

  However, if you execute the `jcfallogdef` or `jcfallogstart` command with the `-r` option specified, log collection continues using the usual monitoring interval without performing retry operations.

- For a remote monitoring event log trap:

  The following figure provides an overview of a retry interval for remote monitoring event log traps.

  
  Start
Finish
Start
Error
Error
Finish
Start
Finish
Collection of log information
Collection of log information
Collection of log information
Collection of log information
Collection of log information
Monitoring interval
Retry interval
Retry interval
Monitoring interval

  Remote-monitoring event log trapping is retried based on the count and interval specified for the following items in the remote-monitoring event log trap action-definition file:

  - Number of retries specified for `open-retry-times` (if `open-retry-times` is omitted, the retry count is 3)

- Interval specified for `open-retry-interval` (if `open-retry-interval` is omitted, the `trap-interval` value is used. If `open-retry-interval` and `trap-interval` are both omitted, the retry interval is 300 seconds)

Note

- If wrap around occurs frequently, or if a long monitoring interval or a long retry interval for a remote-monitoring log file trap is specified, the log file might be overwritten before the log file trap loads the data, and some data might not be loaded. To avoid this, set an appropriate monitoring interval. Use the following formula to estimate an appropriate monitoring interval:

  log file size (byte) × *number of log files* > *output size per second (byte)* × *monitoring interval (second) or retry limit for a remote monitoring log file trap (second)*
- If connection to the monitoring target fails, errors such as connection errors might be output to the Windows event log on the manager host. Therefore, if there are multiple consecutive retries, a large amount of error log data might be output to the Windows event log. Specify the retry interval and the retry count taking into account the errors that might be output to the Windows event log during retry operations.

For details about each action definition file, see *Remote-monitoring log file-trap action definition file* in *Chapter 2. Definition Files* and *Remote-monitoring event log trap action-definition file* in *Chapter 2. Definition Files* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

6.6.5 Predefined filter

A predefined filter filters the log files and event logs acquired from the remotely monitored hosts. If you set such a filter, only the log files and event logs that match the specified conditions are transferred to the server, so you can control the amount of transferred data.

If no filter is set, more data than can be monitored in an action definition file might be collected from the monitored server. If this occurs, the maximum size of data that can be collected during the collection period might be exceeded and a warning might appear when the file is trapped. In cases such as this, consider whether you can use a predefined filter.

The following profiles can be filtered by predefined filters.

- Remote-monitoring log file traps when an SSH connection is used
- Remote-monitoring event log traps when a WMI/NetBIOS (NetBIOS over TCP/IP) connection is used

You can set predefined filters in the Display/Edit Profiles window or using the `-filter` option of a command for remote monitoring (`jcfallogstart`, `jcfallogdef`, `jcfaleltstart`, and `jcfaleltdef`). The settings are applied when a remote-monitoring log file trap or remote-monitoring event log trap is started. For details, see the following:

- Display/Edit Profiles window

  4.9 Display/Edit Profiles window in the manual *JP1/Integrated Management - Manager GUI Reference*
- `Jcfallogstart` command

  jcfallogstart in *Chapter 1. Commands* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*
- `Jcfallogdef` command

  jcfallogdef in *Chapter 1. Commands* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*

- `Jcfaleltstart` command

  jcfaleltstart (Windows only) in *Chapter 1. Commands* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*

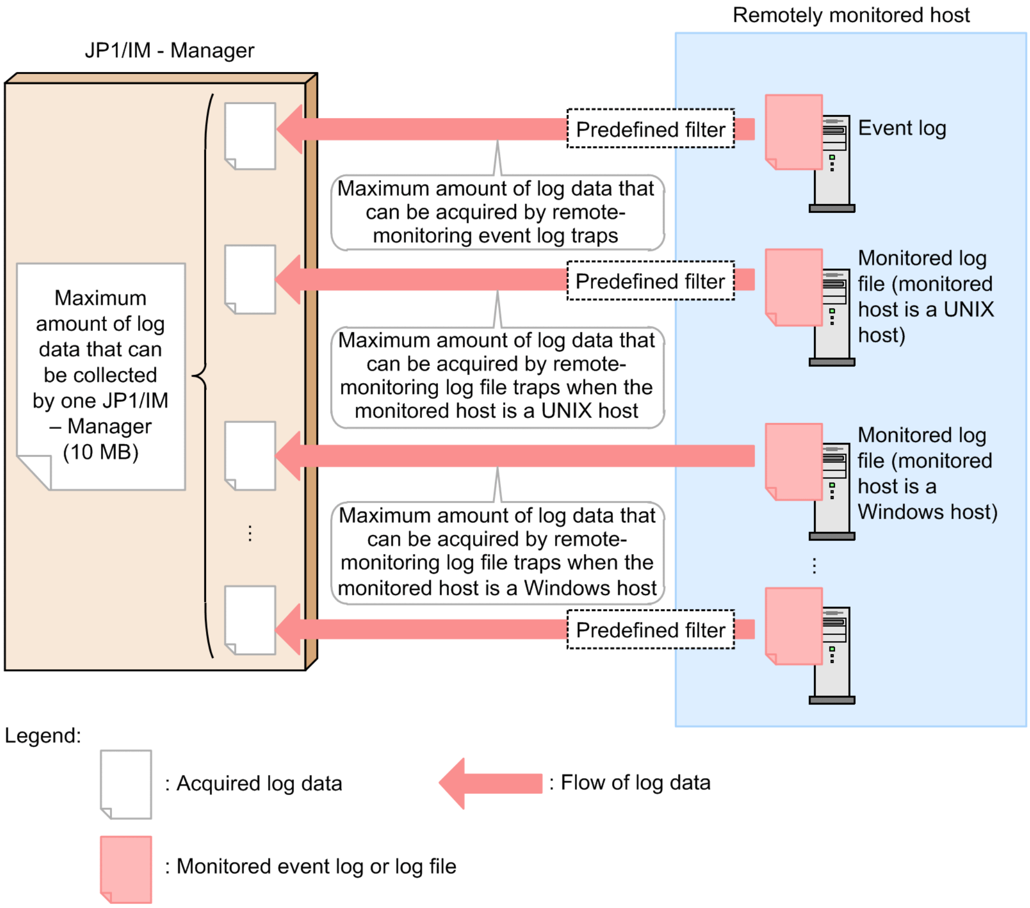
- `Jcfaleltdef` command

  jcfaleltdef (Windows only) in *Chapter 1. Commands* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*

6.6.6 Maximum amount of log data that can be collected by one JP1/IM - Manager

In remote monitoring, the maximum amount of log data that can be collected by one JP1/IM - Manager is 10 MB.

Figure 6–48: Maximum amount of log data that can be collected by one JP1/IM - Manager


Remotely monitored host
JP1/IM - Manager
Predefined filter
Event log
Maximum amount of log data that can be acquired by remote-monitoring event log traps
Predefined filter
Monitored log file (monitored host is a UNIX host)
Maximum amount of log data that can be collected by one JP1/IM – Manager (10 MB)
Maximum amount of log data that can be acquired by remote-monitoring log file traps when the monitored host is a UNIX host
Monitored log file (monitored host is a Windows host)
Maximum amount of log data that can be acquired by remote-monitoring log file traps when the monitored host is a Windows host
Predefined filter
Legend:
: Acquired log data
: Flow of log data
: Monitored event log or log file

If the maximum amount of log data that can be collected by one JP1/IM - Manager exceeds 10 MB, the workload increases on the machine on which JP1/IM - Manager is running. As a result, log files and Windows event logs might not be trapped.

The maximum amount of log data that can be collected by one JP1/IM - Manager is determined by the maximum amount of log data that can be acquired, the number of monitored hosts, the number of monitored log files, and the number of monitored event logs. For details about the maximum amount of log data that can be acquired, see *6.6.3 Log information that can be monitored*.

The following shows the formula for determining the maximum amount of log data that can be collected by one JP1/IM - Manager:

a **x** *b* + *c* **x** *d* + *e* **x** *f* (bytes)

Legend:

a: Maximum amount of log data that can be acquired by remote-monitoring event log traps

b: Total number of remote-monitoring event log traps that are run

c: Maximum amount of log data that can be acquired by remote-monitoring log file traps when the monitored host is a UNIX host

d: Total number of log files that are monitored by remote-monitoring log file traps that are run (when the monitored host is a UNIX host)

e: Maximum amount of log data that can be acquired by remote-monitoring log file traps when the monitored host is a Windows host

f: Total number of log files that are monitored by remote-monitoring log file traps that are run (when the monitored host is a Windows host)

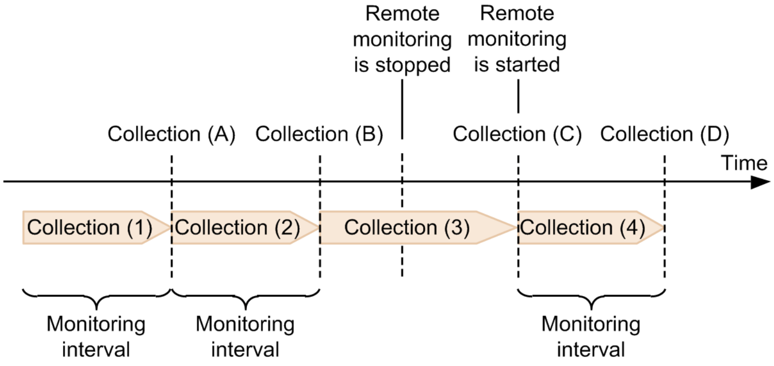
6.6.7 Event-source-host mapping

The source event server name for the JP1 events issued by remote monitoring is the name of the integrated manager host, not the monitored host name. To display and define the monitored host name as the event source host name for the JP1 events issued in remote monitoring, the monitored host name must be stored as the event source host name (`E.JP1_SOURCEHOST`). Note that event source host names (monitored host names) for JP1 events issued in remote monitoring are not displayed on the event list when the event-source-host mapping is disabled. To display the names on the event list, the event-source-host mapping must be enabled (`jcoimdef -hostmap ON`). For details about JP1 events issued in remote monitoring, see *3.2.2 Details of JP1 events* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*. Additionally, note that the common definition `ATTR_EVENT_LOGTRAP_SOURCEHOST` is set to `0`, the event source host name is not set in remote-monitoring event log trapping.

6.6.8 Monitoring logs that are generated while remote monitoring is stopped

The remote monitoring function enables you to collect logs that are generated while remote monitoring is stopped by saving the location of collected logs and then restoring the previous collection status when remote monitoring is restarted.

Figure 6–49: Operation for monitoring logs that are generated while remote monitoring is stopped



If remote monitoring is stopped and then restarted, this function executes *Collection (3)* shown in the figure when the function's processing starts. *Collection (3)* involves collection of logs that occurred from *Collection (B)* to *Collection (C)*.

The previous collection status can be inherited when remote monitoring is restarted by using remote-monitoring log file traps and remote-monitoring event log traps. When the collection status of remote-monitoring log file traps is inherited, the function collects logs starting at the line that immediately follows the last line collected. When the collection status of remote-monitoring event log traps is inherited, the function collects logs that are generated subsequent to the time of the last event log that was collected.

You specify whether to monitor logs that are generated while remote monitoring is stopped with the `START_OPTION` parameter in the remote log trap environment definition file (`jp1cf_remote_logtrap.conf`). For details about the remote log trap environment definition file (`jp1cf_remote_logtrap.conf`), see *Remote log trap environment definition file (jp1cf_remote_logtrap.conf)* (*Chapter 2. Definition Files*) in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

(1) Notes

The remote-monitoring function might not be able to inherit the collection status depending on the operations performed with IM Configuration Management between the time remote monitoring was stopped and the time remote monitoring is restarted.

Cases where the collection status cannot be inherited (for remote-monitoring log file traps)

- Settings for the monitored log file names were added or changed since the last time remote monitoring was stopped.[#1]
- A profile was deleted and then another profile was created with the same name.
- Monitored hosts were removed from the remote monitoring configuration and then were added back again to the remote monitoring configuration.
- When host information for the monitored hosts was collected, the OS names for the monitored hosts had changed.
- When remote monitoring settings were changed for the monitored hosts, the communication type (WMI/NetBIOS, SSH) was changed.
- Monitored hosts were removed from the host list in IM Configuration Management and were then added to the list again.
- While log files with log file format SEQ, SEQ2, or WRAP2 were being monitored, a `KNAN26095-E` error message was output and remote monitoring was stopped.[#2]

#1: The file names are case sensitive.

#2: For details about the errors, see *2.13 Messages related to IM Configuration Management (KNAN22000 to KNAN26999)* in the manual *JP1/Integrated Management - Manager Messages*.

Cases where the collection status cannot be inherited (for remote-monitoring event log traps)

- Monitored hosts were removed from the remote monitoring configuration and then were added back to the remote monitoring configuration.
- When host information for the monitored hosts was collected, the OS names for the monitored hosts had changed.
- Monitored hosts were removed from the host list in IM Configuration Management and were then added to the list again.

6.7 Management of service activity information

Using IM Configuration Management - View, you can check whether services are active on the managed hosts.

This functionality allows you to monitor service activity on each host, and to investigate the service status if an error occurs on a host.

This section describes the service activity information you can manage using IM Configuration Management, and the functionality provided for checking the status of JP1 services.

6.7.1 Services whose activity information can be obtained

Using IM Configuration Management, you can check activity information on services related to the system hierarchy (IM configuration) among the JP1 product services running on the target host.

When you collect service activity information with IM Configuration Management, a collection command is executed on the target host. The command outputs an execution log on the host.

The table below lists the services whose activity information you can view in IM Configuration Management, and the corresponding status collection command.

Table 6–42: Services and commands for viewing service activity information

Product name	Service name	Status collection command
JP1/Base	JP1/Base	`jbs_spmd_status`
	Event service	`jevstat`
	Log file trapping	`jevlogstat ALL`
JP1/IM - Manager	JP1/IM-Manager	`jco_spmd_status`

For remote monitoring configuration, you can check the following types of activity information by using the command for checking the operating status:

- Remote-monitoring log file trapping
  Specify as follows:
  `jcfallogstat -o` *target-host-name* `[-h` *logical-host-name*`]`
- Remote-monitoring event log trapping
  Specify as follows:
  `jcfaleltstat -o` *target-host-name* `[-h` *logical-host-name*`]`

6.7.2 Collecting service activity information

Using IM Configuration Management, you can collect service activity information from any of the managed hosts.

To collect service activity information, the target host must be registered in the IM Configuration Management database and its host information must have been collected. In addition, JP1/Base must be active on the target host. Service activity information cannot be collected from a host running a version of JP1/Base earlier than version 9.

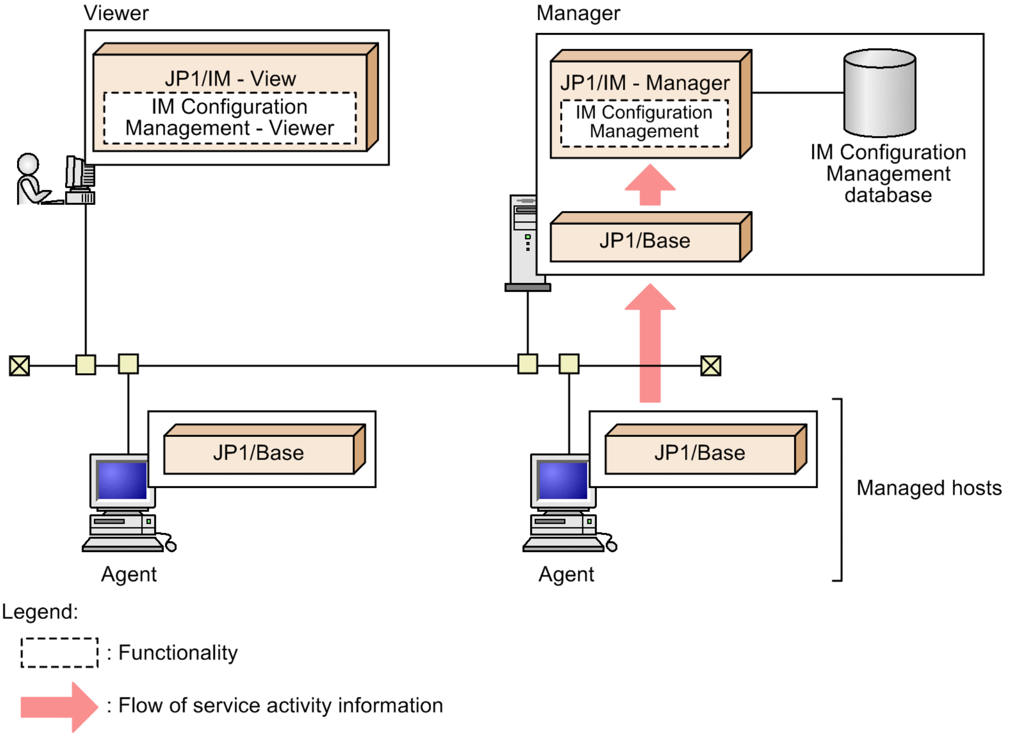
(1) Procedure for collecting service activity information

To collect service activity information, perform either of the following operations in IM Configuration Management - View:

- On the **Host List** page or **IM Configuration** page of the IM Configuration Management window, select a host and then click the **Service Information** button.
- On the **IM Configuration** page, click the **Refresh** button (to refresh the displayed information).

The figure below shows the flow of processing when collecting service activity information.

Figure 6–50: Collecting service activity information


Viewer
JP1/IM - View
IM Configuration Management - Viewer
Manager
JP1/IM - Manager
IM Configuration Management
IM Configuration Management database
JP1/Base
JP1/Base
JP1/Base
Managed hosts
Agent
Agent
Legend:
: Functionality
: Flow of service activity information

The collected service activity information is saved to memory on the manager running IM Configuration Management, not to the manager's IM Configuration Management database.

(2) Hosts from which service activity information can be collected

You can collect service activity information from only one host at a time. The range of hosts from which you can collect activity information depends on which host IM Configuration Management is installed on.

The following table describes the range of hosts whose service activity information you can collect from the integrated manager.

Table 6–43: Range of hosts whose service activity information can be collected from the integrated manager

Host type	Collect
Local host	Y
Relay manager	Y
Base manager	Y

Host type		Collect
Agent	Directly under the local host	Y
	Under a relay manager	Y
	Under a base manager	N#
Remotely monitored host	Directly under the local host	N
	Under a base manager	N

Legend:

Y: The information can be collected.

N: The information cannot be collected.

#

An agent under a base manager might not be reachable from the integrated manager if it is behind a firewall. For this type of agent, collect the service activity information from the base manager.

The following table describes the range of hosts whose service activity information you can collect from a base manager.

Table 6–44: Range of hosts whose service activity information can be collected from a base manager

Host type		Collect
Local host		Y
Parent host		N#1
Relay manager		Y#2
Base manager		Y#2
Agent	Directly under the local host	Y
	Under a relay manager	Y#2
	Under a lower-level base manager	N#3
Remotely monitored host	Directly under the local host	N
	Under a base manager	N

Legend:

Y: The information can be collected.

N: The information cannot be collected.

#1

You cannot collect service activity information from a parent host because its host information cannot be collected.

#2

Not recommended because the system configuration, including the integrated manager, would be more than three tiers.

#3

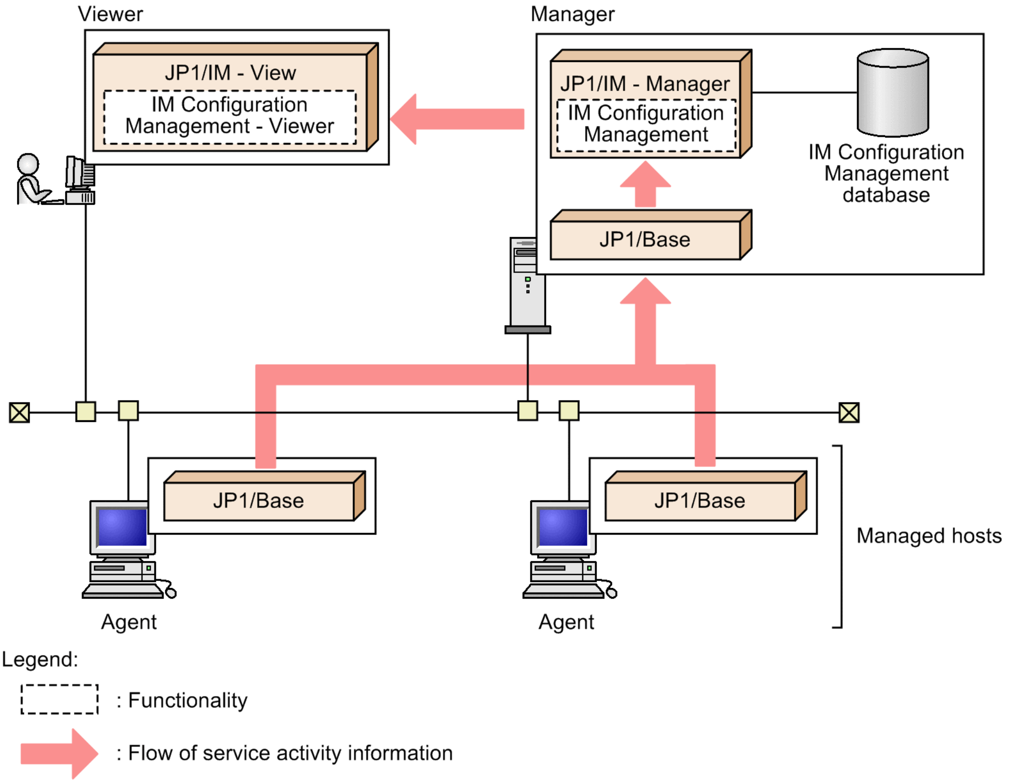
Collect service activity information on a lower-level base manager because the integrated manager might not be able to connect to the agent under the lower-level base manager via a firewall.

6.7.3 Displaying service activity information

You can display service activity information collected from a managed host on the **IM Configuration** page (service information) of the IM Configuration Management window.

The figure below shows the flow of processing when displaying service activity information with IM Configuration Management.

Figure 6–51: Displaying service activity information with IM Configuration Management


Viewer
JP1/IM - View
IM Configuration Management - Viewer
Manager
JP1/IM - Manager
IM Configuration Management
IM Configuration Management database
JP1/Base
JP1/Base
JP1/Base
Agent
Agent
Managed hosts
Legend:
: Functionality
: Flow of service activity information

6.8 Exporting and importing IM Configuration Management information

Using IM Configuration Management, you can export information managed by IM Configuration Management and import management information that has been exported.

The import/export functionality can be used for the following purposes:

- To move the system hierarchy (IM configuration) from the test environment to the operational environment, or from the environment before change to the environment after change
- To import management information from another manager server on which IM Configuration Management is installed
- To temporarily or periodically change the system hierarchy
- To change settings back to a previous status after a failure

This section describes the information you can import or export using IM Configuration Management, and the functionality provided for this purpose.

6.8.1 Types of information that can be imported or exported

The following table describes the range of information managed by IM Configuration Management that can be imported or exported.

Table 6–45: Range of IM Configuration Management information that can be imported or exported

Information managed by IM Configuration Management		Export	Import
Host information	User-specified items	Y	Y
	OS information	Y	N
	Product information	Y	N
	Virtualization configuration information	Y	Y
	Remote communication method	Y	Y
	User name/password information	Y	Y
System hierarchy	Agent configuration information	Y	Y
	Remote monitoring configuration information	Y	Y
Remote authentication information	WMI authentication information	Y	Y
	SSH authentication information output	Y	Y
Business group information		Y	Y
Monitoring group information		Y	Y
Profiles#1	Event forwarding setting file	Y	Y
	Action definition file for event log trapping	Y	Y
	Action definition file for log file trapping#2	Y	Y
	Log-file trap startup definition file#2	Y	Y
	Local action execution definition file	Y	Y

Information managed by IM Configuration Management		Export	Import
	Authentication server settings file	N	N
	JP1 user settings file	N	N
	User mapping settings file	N	N
	Remote-monitoring log file trap action-definition file	Y	Y
	Remote-monitoring log file trap startup-definition file	Y	Y
	Remote-monitoring event log trap action-definition file	Y	Y
Service activity information		N	N

Legend:

Y: Can be imported or exported.

N: Cannot be imported or exported.

#1

If the host does not collect profile settings files, there is no data to be exported (no directory is created).

#2

Information is imported as follows:

When a log file trap having the same name as the log file trap corresponding to the imported profile exists and is running on the host to which the information was imported:

Information is imported when the log file trap is running, and the edited contents of the imported profile have not been applied. To apply the edited contents of the imported profile, restart the log file trap after importing the profile. For details about how to restart a log file trap to apply the profile, see *3.5.1(6)(b) Applying edited information in configuration files individually to each agent* in the *JP1/Integrated Management - Manager Configuration Guide*.

When a log file trap having the same name as the log file trap corresponding to the imported profile exists and is stopped on the host to which the information was imported:

Information is imported when the log file trap is stopped, and the edited contents of the imported profile have not been applied. To apply the edited contents of the imported profile, start the log file trap after importing the profile. For details about how to start a log file trap, see *3.5.1(7)(a) Starting log file traps* in the *JP1/Integrated Management - Manager Configuration Guide*.

When a log file trap having the same name as the log file trap corresponding to the imported profile does not exist on the host to which the information was imported:

Information is imported when the log file trap is stopped. After importing the profile, start the log file trap. For details about how to start a log file trap, see *3.5.1(7)(a) Starting log file traps* in the *JP1/Integrated Management - Manager Configuration Guide*.

For details about the IM Configuration Management information that can be exported and imported, see *8.7 Exporting and importing management information of IM Configuration Management* in the *JP1/Integrated Management - Manager Administration Guide*.

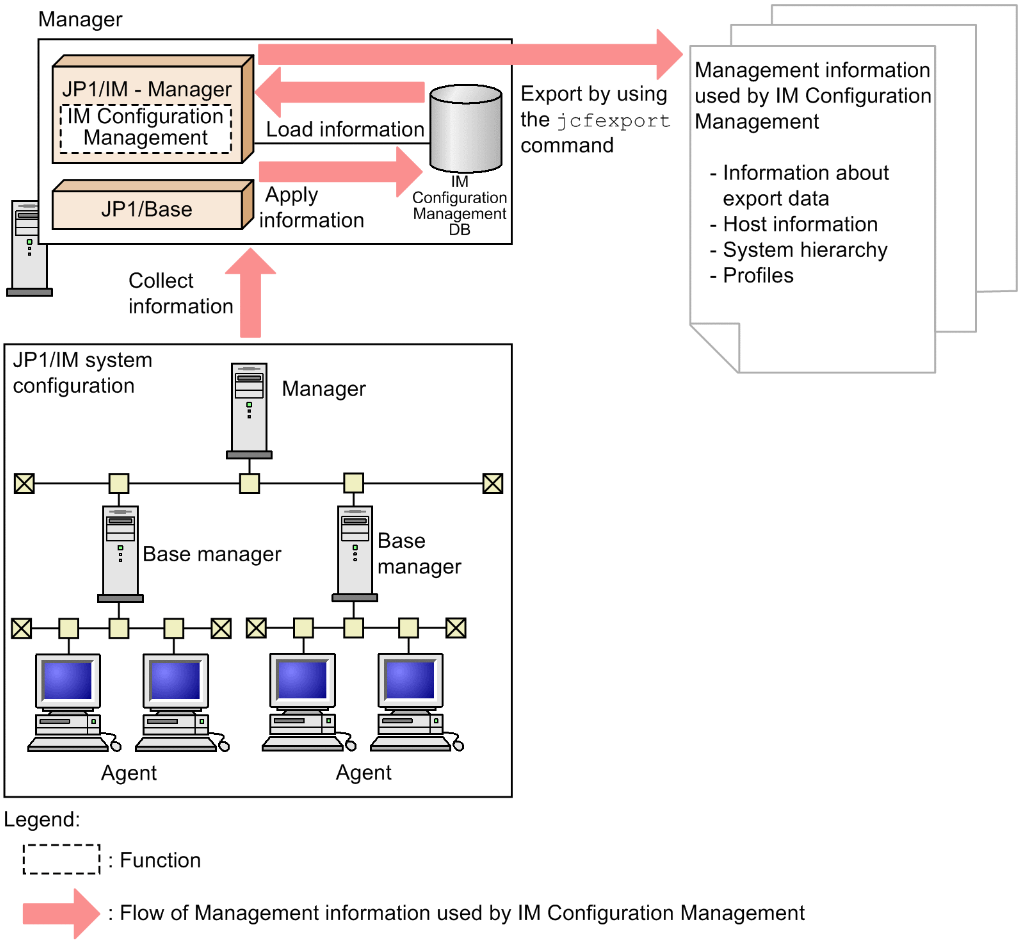
6.8.2 Exporting IM Configuration Management information

Using IM Configuration Management, you can export information held in the IM Configuration Management database to multiple files.

To export management information, execute the `jcfexport` command on the manager running IM Configuration Management.

The figure below shows the flow of processing when exporting management information with IM Configuration Management.

Figure 6–52: Exporting management information with IM Configuration Management


Manager
JP1/IM - Manager
IM Configuration Management
Load information
JP1/Base
Apply information
IM Configuration Management DB
Export by using the jcfexport command
Management information used by IM Configuration Management
- Information about export data
- Host information
- System hierarchy
- Profiles
Collect information
JP1/IM system configuration
Manager
Base manager
Base manager
Agent
Agent
Legend:
: Function
: Flow of Management information used by IM Configuration Management

Before executing the command, make sure you check the information to be exported in case the IM Configuration Management database contains management information that has not been applied in the actual system.

You can specify options in the `jcfexport` command to select the types of management information to export. For the command syntax, see *jcfexport* in *Chapter 1. Commands* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

The following table describes the range of information you can specify for export.

Table 6–46: Range of specifiable management information for export

Type of management information (for export)		Export				
		Host information (`-m` option)	Remote authentication information (`-r` option)	System hierarchy (`-c` option)	Profiles (all hosts) (`-a` option)	Business group information (`-g` option)
Information about exported data		Y	Y	Y	Y	Y
Host information		Y	Y	Y	Y	Y
Remote authentication information		N	Y	N	Y	N
System hierarchy		N	N	Y	Y	N
Profile information#	Event forwarding setting file	N	N	N	Y	N

Type of management information (for export)		Export				
		Host information (`-m` option)	Remote authentication information (`-r` option)	System hierarchy (`-c` option)	Profiles (all hosts) (`-a` option)	Business group information (`-g` option)
	Log-file trap action definition file	N	N	N	Y	N
	Log-file trap startup definition file	N	N	N	Y	N
	Action definition file for event log trapping	N	N	N	Y	N
	Local action execution definition file	N	N	N	Y	N
Business group information		N	N	N	Y	Y
Monitoring group information		N	N	N	Y	Y

Legend:

Y: Can be specified.

N: Cannot be specified.

#

If the host does not collect profile settings files, there is no data to be exported (no directory is created).

The following table describes the output formats of exported management information.

Table 6–47: Output formats of exported management information

Management information	Output format
Information about exported data	Information about exported data is output to one file.
Host information	Information about managed hosts is output to two files.
System hierarchy	Information about the system hierarchy is output to one file.
Profiles	• For agents: JP1/Base profiles on the agents are output to multiple files. • For remotely monitored hosts: Profiles on the hosts are output to multiple files.
Business group information	Business group information is output to two files.
Monitoring group information	Monitoring group information is output to two files.

Information cannot be exported while import is in progress.

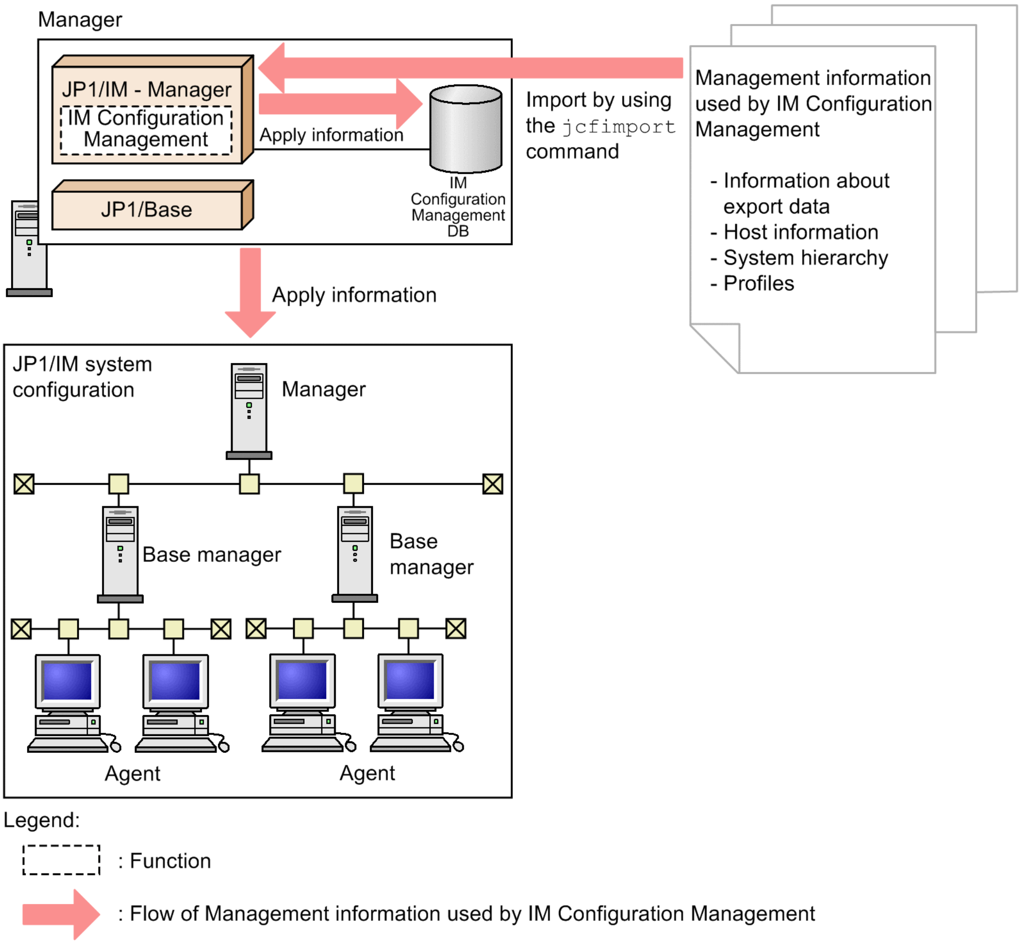
6.8.3 Importing IM Configuration Management information

Using IM Configuration Management, you can import exported management information.

To import management information, execute the `jcfimport` command on the manager running IM Configuration Management. When you execute this command, host information about the manager on which the `jcfimport` command is executed is overwritten. (This information is registered in the IM Configuration Management database.)

The figure below shows the flow of processing when importing management information with IM Configuration Management.

Figure 6–53: Importing management information with IM Configuration Management


Manager
JP1/IM - Manager
IM Configuration Management
JP1/Base
Apply information
IM Configuration Management DB
Import by using the jcfimport command
Management information used by IM Configuration Management
- Information about export data
- Host information
- System hierarchy
- Profiles
Apply information
JP1/IM system configuration
Manager
Base manager
Base manager
Agent
Agent
Legend:
: Function
: Flow of Management information used by IM Configuration Management

Because importing information changes the data held by the IM Configuration Management database, we recommend that you back up the existing data in the database before performing an import operation. If an error occurs during import, the data will be rolled back to its previous state.

When importing information, you can select the management information to be imported by specifying options in the `jcfimport` command. For the command syntax, see *jcfimport* in *Chapter 1. Commands* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

The following table describes the range of information you can specify for import.

Table 6–48: Range of specifiable management information for import

Type of management information (for import)		Import				
		Host information (`-m` option)	Remote authentication information (`-r` option)	System hierarchy (`-c` option)	Profiles (all hosts) (`-a` option)	Business group information (`-g` option)
Information about exported data		N	N	N	N	N
Host information		Y	Y	Y	Y	Y
Remote authentication information		N	Y	N	Y	N
System hierarchy information		N	N	Y	Y	N
Profile information	Event forwarding setting file	N	N	N	Y	N
	Log-file trap action definition file	N	N	N	Y	N
	Log-file trap startup definition file	N	N	N	N	N
	Action definition file for event log trapping	N	N	N	Y	N
	Local action execution definition file	N	N	N	Y	N
Business group information		N	N	N	Y	Y
Monitoring group information		N	N	N	Y	Y

Legend:

Y: Can be specified.

N: Cannot be specified.

To apply the imported management information for IM Configuration Management to an actual system, you need to apply the system hierarchy in the Edit Agent Configuration window or the Edit Remote Monitoring Configuration window. For details about how to apply the system hierarchy, see *3.2.4(3) Applying a system hierarchy to a system managed by IM Configuration Management* in the *JP1/Integrated Management - Manager Configuration Guide*.

Management information cannot be imported while any of the following operations are in progress in IM Configuration Management:

- Collect, verify, synchronize, or apply the system hierarchy; obtain or release update rights to the system hierarchy
- Collect, edit, or delete host information
- Collect, edit, save, apply, or batch-distribute profiles
- Export or import management information

7 JP1/IM Operation Control

This chapter describes the operation control in JP1/IM, and the communication that takes place in the JP1/IM system environment.

7.1 JP1/IM - Manager process management

Process management is a core functionality of JP1/IM - Manager, used to control startup and termination of the manager functions. Another responsibility of process management is to issue instructions for checking the status of JP1/IM - Manager functions.

JP1/IM - Manager provides the following functions, the processes of which are controlled by process management:

- Event console service (`evtcon`)
- Event base service (`evflow`)
- Automatic action service (`jcamain`)
- Event generation service (`evgen`)#1, #2
- Central Scope service (`jcsmain`)#2
- IM Configuration Management service (`jcfmain`)#2
  #1: Applicable when not using the integrated monitoring database.
  #2: Not started by default.

Process management is realized by the following commands:

Table 7–1: Process management commands

Functionality	Command	Description
Start JP1/IM - Manager# (UNIX only)	`jco_start`	Controls JP1/IM - Manager startup and termination.
Stop JP1/IM - Manager# (UNIX only)	`jco_stop`	
JP1/IM - Manager status check	`jco_spmd_status`	Checks the activity status of JP1/IM - Manager.
Reload JP1/IM - Manager definition information	`jco_spmd_reload`	When definition information is updated in JP1/IM - Manager, this command reloads and applies the new definitions.

#: In Windows, JP1/IM - Manager is started and stopped by a Windows service registered under the service name JP1/IM-Manager. Use this service to start and stop JP1/IM - Manager.

For details about the commands in the table, see *Chapter 1. Commands* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

JP1/IM - Manager process management can also detect and troubleshoot abnormal process startup and termination using the following functionality:

- Automatically restarting an abnormally ended process
- Issuing a JP1 event when an error is detected at process startup or termination

For details about this functionality, see *7.1.1 Restarting abnormally ended processes* and *7.1.2 Issuing JP1 events at detection of process errors*.

7.1.1 Restarting abnormally ended processes

When a process that provides a function in JP1/IM - Manager ends abnormally, JP1/IM - Manager can attempt to recover the process.

JP1/IM processes are controlled by the process management, which detects when a process terminates abnormally and automatically restarts it. This allows JP1/IM - Manager to recover automatically from some temporary errors.

Process restarting is not enabled at installation. To enable process restarting, enable the restart parameter in the extended startup process definition file (`jp1co_service.conf`).

The operation of process restarting is described below. This example is based on settings for the `jcamain` process (automatic action service) being made in the extended startup process definition file. For details about the definition file, see *Extended startup process definition file (jp1co_service.conf)* in *Chapter 2. Definition Files* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

Setting example

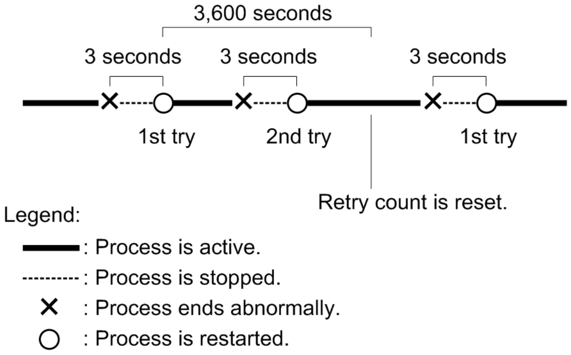
```
jcamain||1|3|3|3600|
```

Explanation

```
Process name: jcamain
Restart: 1 (1: Restart; 0: Do not restart (default))
Retry count: 3 (default)
Retry interval: 3 seconds (default)
Retry count reset time: 3,600 seconds (default)
```

In this definition, only the restart parameter is changed. There is typically no need to change the other values as the defaults will be suitable in most situations. With these settings, process restarting operates as follows:

Figure 7–1: Behavior when a process ends abnormally



In this example, if the process does not end abnormally within 3,600 seconds of restarting as specified by the retry count reset time, the retry count is reset. On the other hand, if the process terminates within 3,600 seconds of restarting, the retry count is incremented by one. No more attempts are made to restart the process after the retry count reaches the specified number.

In Windows, a Windows dialog box for reporting the error to Microsoft appears when a process results in an application error. Because these dialog boxes wait for user input, they can prevent processes from restarting automatically. For this reason, you must disable error reporting using dialog boxes.

Important

If you are using JP1/IM - Manager in a cluster system, do not set up process management to restart abnormally ended processes because the error in the JP1/IM - Manager process might also affect the function that restarts processes. To ensure a more reliable restart, restart JP1/IM - Manager processes under the control of the clustering software.

7.1.2 Issuing JP1 events at detection of process errors

When JP1/IM - Manager detects an error in process startup or shutdown processing, it outputs an error message to the integrated trace log. However, this error message can also be issued as a JP1 event.

By default, JP1 events are not issued when a process error is detected. To enable this feature, enable the relevant parameters (`SEND_PROCESS_TERMINATED_ABNORMALLY_EVENT` and `SEND_PROCESS_RESTART_EVENT`) in the IM parameter definition file (`jp1co_param_V7.conf`). For details about the definition file, see *IM parameter definition file (jp1co_param_V7.conf)* in *Chapter 2. Definition Files* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

If JP1 event issuance is enabled, a JP1 event is issued when:

- A process ends abnormally.
- No startup notification is received and a timeout occurs at process startup.
- Restart of a process that ended abnormally is completed (if process restarting is enabled).

7.2 JP1/IM - Manager health check function

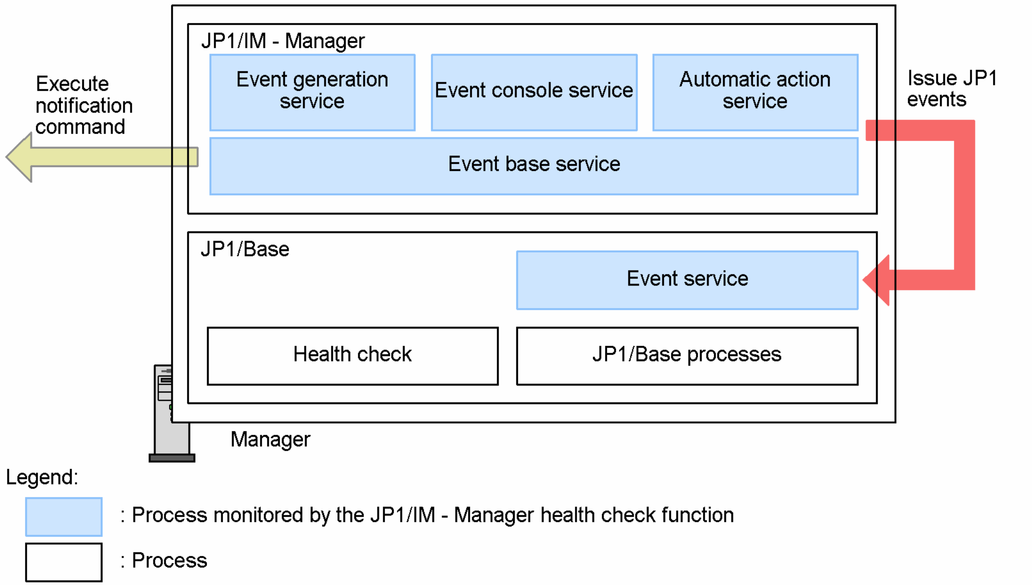
JP1/IM - Manager provides a feature to detect when a process goes into an infinite loop or deadlock (hangup#) and ceases processing, and to notify the operator by issuing a JP1 event or executing a notification command. In JP1/IM - Manager, this is called the *health check function*.

#: Hangups are caused by a deadlock or infinite loop. This means that the process can no longer accept processing requests.

Use of the health check function enables early detection and response to process errors that can often go unnoticed, such as deadlocks and infinite loops, by issuing a message or JP1 event to report the error and prompt the operator to take recovery action.

The following figure gives an overview of the JP1/IM - Manager health check function.

Figure 7–2: Overview of process monitoring using the JP1/IM - Manager health check function



If enabled, the health check function outputs message information to the OS log (the Windows event log or UNIX syslog) and the integrated trace log when a process hangs. By making the appropriate settings in the health check definition file (`jcohc.conf`), you can also have the health check function issue a JP1 event or notification command when a process hangs.

JP1/Base also provides a health check function for monitoring the various JP1/Base processes. Used in conjunction, the JP1/IM - Manager and JP1/Base health check functions enable early detection and response for process errors in JP1/IM - Manager and instances of JP1/Base in the JP1/IM system.

The following describes the processes monitored by the health check function, how to enable and disable the function, and how the function monitors processes.

7.2.1 Processes monitored by the health check function

The following table shows which processes are monitored by the JP1/IM - Manager health check function.

Table 7–2: Processes monitored by the health check function

Product	Process	Process name	Monitor
JP1/IM - Manager	Event console service	`evtcon`	Y
	Automatic action service	`jcamain`	Y
	Event base service	`evflow`	Y
	Event generation service#1	`evgen`	Y
	Central Scope service#2	`jcsmain`	--
	Process management#2	`jco_spmd`	--
	Windows service control#2	`jco_service`	--
	IM Configuration Management service	`jcfmain`	--
JP1/Base	Event service#3	`jevservice`	Y
	Functions other than the event service	`jbsplugin` and others	--

Legend:

Y: Monitored by the health check function.

--: Not monitored by the health check function.

#1

The event generation service is disabled by default. It is applicable in a system that does not use the integrated monitoring database, and is not monitored otherwise. To monitor this process, enable the event generation service and the health check function (use the `jcoimdef` command to enable or disable the service).

#2

The Central Scope service (`jcsmain`) and IM Configuration Management service (`jcfmain`) do not support the health check function. The process management (`jco_spmd`) is not monitored because it does not affect JP1/IM - Manager services. The process that starts and stops JP1/IM - Manager (`jco_service`) is not monitored because its role is limited to starting and stopping services.

#3

The JP1/IM - Manager health check function monitors the event service on the manager. All other JP1/Base processes are the responsibility of the health check function provided by JP1/Base.

Note

The other JP1/Base processes on the manager can be monitored by the JP1/Base health check function. JP1/Base processes on agents are also monitored for errors by the JP1/Base health check function, through the forwarding and registration of error information to the manager as JP1 events.

For details, see the chapter on setting the health check function in the *JP1/Base User's Guide*.

7.2.2 Enabling and disabling the health check function

The health check function is not enabled at installation.

In the health check definition file, set the parameter that enables or disables health checking (`ENABLE`) to true. To issue a JP1 event or execute a notification command when a process hangs, enable the `EVENT` parameter, and specify the command to be executed using the `COMMAND` parameter.

To initiate a failover in a cluster system when the health check function detects a process error, you must enable the FAILOVER parameter in the health check setup file. When this setting is enabled, JP1/IM - Manager is stopped when the health check function detects a process error, allowing failover to take place.

For details about the definition file, see *Health check definition file (jcohc.conf)* in *Chapter 2. Definition Files* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

7.2.3 How the health check function works

The JP1/IM - Manager health check function is realized by having processes monitor one another.

The following table describes the correspondence between the processes that perform monitoring in the JP1/IM - Manager health check function, and the processes they monitor.

Table 7–3: Correspondence between monitoring processes and monitored processes

Monitoring processes	Monitored processes
Event base service (evflow)	Event console service (evtcon)
	Automatic action service (jcamain)
	Event generation service (evgen)#1
	Event service (jevservice)#2
Event console service (evtcon)	Event base service (evflow)

#1: Applicable when not using the integrated monitoring database.

#2: A JP1/Base service that runs on the manager.

(1) Detecting process errors

In the JP1/IM - Manager health check function, a process that performs monitoring communicates over the network with the processes it monitors, to check whether the processes are working normally.

To detect process errors, the health check function sends polling signals to the monitored processes at regular intervals. If a process has not responded to the signal within a set time, the health check function regards the process as being in an abnormal state.

The interval at which processes are polled, and the number of non-responses for a process to be judged abnormal, differ according to the monitored process, as follows:

Table 7–4: Differences in non-response count

Monitored process	Polling interval#	Non-response count#
Event service (jevservice)	60 to 3,600 seconds	1 to 60
Process other than the event service	60 to 3,600 seconds	1 to 60

#: For details about the definition, see *Health check definition file (jcohc.conf)* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

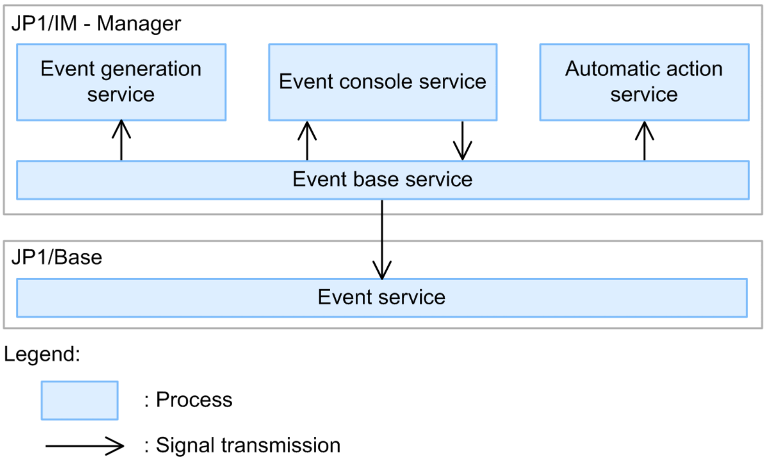
The following describes the JP1/IM - Manager operation after a non-response is detected:

- When a non-response is detected, the JP1/IM - Manager outputs the KAVB8064-W message until an error is detected.

- When the maximum non-response count is reached, the JP1/IM - Manager outputs the `KAVB8060-E` or `KAVB8062-E` message.
- If a non-response is detected but recovered later, JP1/IM - Manager resets the non-response count.
- If a non-response is detected and is not recovered, JP1/IM - Manager does not output the `KAVB8064-W`, `KAVB8060-E`, or `KAVB8062-E` message.

The figure below shows in diagrammatic form how process errors are detected.

Figure 7–3: Communication between processes



(2) Reporting process errors

When the JP1/IM - Manager health check function is enabled, on detection of a process error, JP1/IM - Manager executes the following processing to report that an error has occurred:

- If the error occurred in a process being monitored by JP1/IM - Manager (*evtcon*, *jcamain*, *evflow*, or *evgen*), message KAVB8060-E is output to the integrated trace log and to the Windows event log or UNIX syslog.
- If the error occurred in the JP1/Base event service, message KAVB8062-E is output to the integrated trace log and to the Windows event log or UNIX syslog.
- If a notification command has been set, the command is executed.
- If the `FAILOVER` parameter is enabled, any process for which an error has been detected ends abnormally. The abnormality of JP1/IM - Manager is then reported to the cluster system. The cluster system can initiate a failover when the health check function detects a process error if you set it to initiate a failover when an error in JP1/IM - Manager occurs in the cluster system.

When the failed process has been restored to normal status, message KAVB8061-I for a monitored process of JP1/IM - Manager or message KAVB8063-I for an event service of JP1/Base is output to the integrated trace log and to the Windows event log or UNIX syslog. If JP1 event issuance is enabled, a JP1 event (event ID: 00002014) is issued.

Note

- **The JP1 event with event ID 000020**13 is a dummy event (an event not registered in the event database) issued to JP1/IM - View. A dummy event is issued when an error occurs in the event service in which JP1 events are registered.
- We recommend that you set up the functionality for executing a notification command when using the JP1/IM - Manager health check function.

Execution of a notification command is recommended because if errors are reported only by issuing JP1 events, the user might fail to respond promptly when not monitoring services in JP1/IM - View or if a problem occurs in the event console service (that is, the user is not made aware that an error has been detected by JP1/IM).

7.3 Communication performed in the JP1/IM system environment

When you monitor the system operation using JP1/IM, communication based on the TCP/IP protocol takes place between the hosts in the system, using port numbers and IP addresses. The port numbers used by JP1/IM and JP1/Base are registered in the `services` file automatically when the product is installed. For details about the port numbers registered at JP1/IM installation, see *Appendix C. Port Numbers*. For details about the port numbers registered at JP1/Base installation, see the appendixes in the *JP1/Base User's Guide*. For details about the concept of communication in JP1 series products, see the section on the communication protocol of JP1/Base in the overview chapter in the *JP1/Base User's Guide*.

7.3.1 Communication between the viewer and manager

Typically, communication is established between the viewer and manager when a user logs in to JP1/IM - Manager from JP1/IM - View, and is terminated when the user logs out. Communication is also terminated according to the timeout period set in JP1/IM when communication processing between the viewer and manager takes too long or the manager goes down and fails to respond to requests. For details about the timeout period, see *Communication environment definition file (console.conf.update)* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*. To change the communication timeout period, you must change settings for the viewer (JP1/IM - View) and the manager (JP1/IM - Manager (Central Console)). You do not need to do this for JP1/IM - Manager (Central Scope).

The following table lists the ports used for communication between JP1/IM - View and JP1/IM - Manager.

Table 7–5: Ports used for communication between JP1/IM - View and JP1/IM - Manager

Service	Port number	Description
`jp1imevtcon`	20115/tcp	Used to connect to JP1/IM - Manager (event console service) from JP1/IM - View.
`jp1imcmda`	20238/tcp	Used to execute commands from JP1/IM - View.
`jp1imcss`	20305/tcp	Used to connect to JP1/IM - Manager (Central Scope service) from JP1/IM - View.
`jp1imcf`	20702/tcp#	Used to connect to JP1/IM - Manager (IM Configuration Management service) from JP1/IM - View.

#

Port used for communication between JP1/IM - View and JP1/IM - Manager when using IM Configuration Management.

If you use the Web-based JP1/IM - View, the following ports are used for communication between the viewer and manager.

Table 7–6: Ports used for communication between the viewer and manager when using the Web-based JP1/IM - View

Service	Port number	Description
`http`	80/tcp#	Used to connect to the Web server (to download `console.html` from JP1/IM - Manager).
`jp1imevtcon`	20115/tcp	Used to connect to JP1/IM - Manager (event console service) from the Web-based JP1/IM - View (through a Web browser).

#: The port number might differ depending on how the Web server is set up.

7.3.2 Communication between the manager and authentication server

Communication takes place between the manager and authentication server when a user logs in to JP1/IM - Manager from JP1/IM - View.

The following table lists the ports used for communication between the manager and the authentication server.

Table 7–7: Ports used for communication between the manager and authentication server

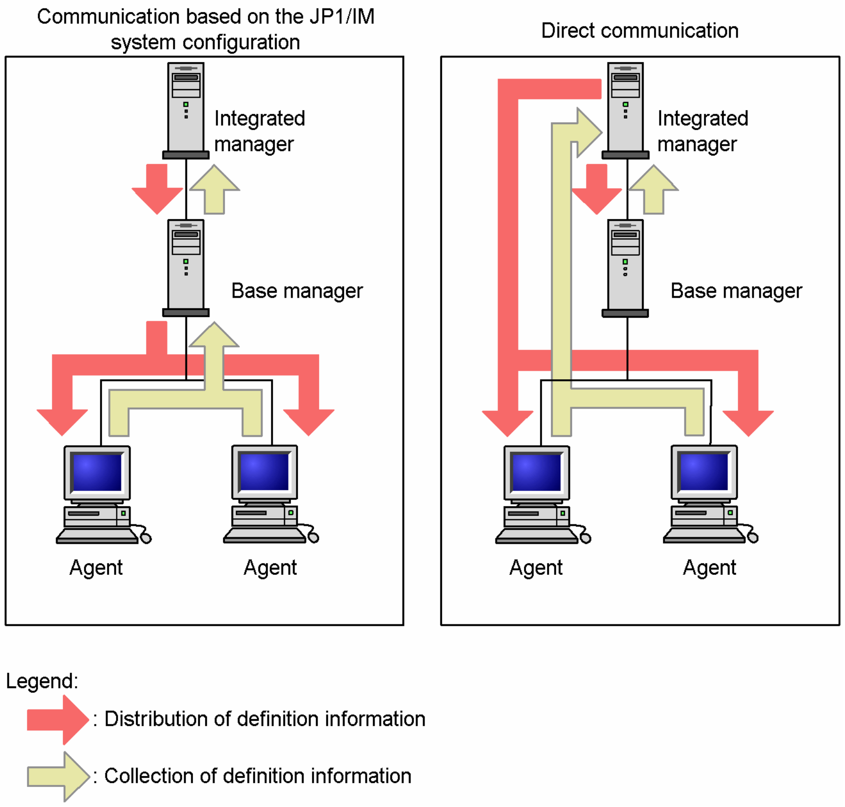
Service	Port number	Description
jp1bsuser	20240/tcp	Used for user authentication.

7.3.3 Communication between the manager and agent

Communication takes place between the manager and agent when the manager sends an instruction to the agent, or the agent sends processing results to the manager.

There are two types of communication that take place between the manager and agents: communication that takes place according to the management hierarchy defined by the system hierarchy (IM configuration) and direct communication with the target hosts. For this reason, take care when using JP1/IM and JP1/Base in a firewall environment or a system made up of multiple LANs.

Figure 7–4: Types of communication between manager and agent


Communication based on the JP1/IM system configuration
Integrated manager
Base manager
Agent
Agent
Direct communication
Integrated manager
Base manager
Agent
Agent
Legend:
: Distribution of definition information
: Collection of definition information

The communication that takes place between manager and agent is described below, categorized according to the form of communication involved.

Communication based on the system hierarchy

- Distributing configuration definitions

  Configuration definition information is distributed to each host in the system, according to the hierarchy defined in the configuration definition file.

- Executing commands from JP1/IM - View

  Command execution requests are sent down through lower-level hosts according to the system hierarchy, and the execution results are forwarded through higher-level hosts as defined in the hierarchy.

- Executing commands by automated action

  Command execution requests are sent down through lower-level hosts according to the system hierarchy, and the execution results are forwarded through higher-level hosts as defined in the hierarchy.

- Forwarding JP1 events

  Under the default settings, JP1 events are forwarded through higher-level hosts according to the system hierarchy.

The following table lists the ports used when communication is based on the system hierarchy.

Table 7–8: Port numbers used for communication based on the system hierarchy

Service	Port number	Description
`jp1imrt`	20237/tcp	Used to distribute configuration definitions.
`jp1imcmdc`	20239/tcp	Used for the following tasks: • Executing commands from JP1/IM - View • Executing commands by automated action
`jp1imevt`	20098/tcp	Used to forward JP1 events.

Communicating directly with the target host

- Searching for events

  The manager communicates directly with the target host.

- Collecting and distributing event service definitions

  Definition information is collected and distributed by communicating directly with all the hosts in the configuration definition file.

- Auto-generating a monitoring tree

  Definition information is collected from all products that support the auto-generation function of JP1/IM - Manager (Central Scope), by communicating directly with each host.

- Using the `jcochstat` command

  The manager communicates directly with the host specified as the command argument.

- Canceling an automated action from JP1/IM - View or using the `jcacancel` command

  The manager communicates directly with the host where the action is to be canceled.

- Using the `jcocmdshow` and `jcocmddel` commands

  The manager communicates directly with the host specified as the command argument.

The following table lists the ports used for direct communication with a target host.

Table 7–9: Ports used for direct communication with target hosts

Service	Port number	Description
`jp1imevtapi`	20099/tcp	Used to conduct an event search.
`jp1bsplugin`	20306/tcp	Used for the following tasks: • Collecting and distributing event service definitions

Service	Port number	Description
		- Auto-generating a monitoring tree - Canceling an automated action from JP1/IM - View - `jcacancel` command - `jcocmdshow` and `jcocmddel` commands
`jp1imevtcon`	20115/tcp	Used by the `jcochstat` command.

7.3.4 Communicating within a local host

JP1/IM and JP1/Base use ports to communicate even when the communication takes place within a local host (between the processes on that host).

The following table lists the ports used for communication within a local host.

Table 7–10: Ports used for communication within a local host

Service	Port number	Description
`jp1imevtapi`	20099/tcp	Used to acquire JP1 events from JP1/Base and to register JP1 events in JP1/Base.
`jp1imevtcon`	20115/tcp	Used by JP1/IM - Manager internal processing.
`jp1imfcs`	20701/tcp	Used by JP1/IM - Manager internal processing.
`jp1imcmda`	20238/tcp	Used to execute automated actions.
`jp1imegs`	20383/tcp	Used by JP1/IM - Manager (event generation service) internal processing.
`jp1imcss`	20305/tcp	Used by JP1/IM - Manager (Central Scope service) internal processing.
`JP1/IM-Manager DB Server`	20700/tcp#	Used by JP1/IM - Manager (IM database) internal processing.
`jp1imcf`	20702/tcp	Used by JP1/IM - Manager (IM Configuration Management service) internal processing.

#

You do not have to write the port number for the JP1/IM-Manager DB Server in the `services` file. The port number increases with each logical host configured in the system. The port number for the IM database is set in the setup information file. For details, see *Setup information file (jimdbsetupinfo.conf)* in *Chapter 2. Definition Files* and *Cluster setup information file (jimdbclustersetupinfo.conf)* in *Chapter 2. Definition Files* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

7.3.5 Communicating with JP1/IM - Rule Operation

When linking with JP1/IM - Rule Operation, communication takes place according to the system hierarchy (IM configuration). Communication takes place on the following occasions:

- When a rule startup request is sent automatically

  The rule startup request is sent from the JP1/IM - Manager (Central Console) host to the JP1/IM - Rule Operation host.

The following table lists the ports used for communication between the JP1/IM - Manager (Central Console) host and JP1/IM - Rule Operation.

Table 7–11: Ports used for communication between the JP1/IM - Manager (Central Console) host and JP1/IM - Rule Operation

Service	Port number	Description
jp1imcmdc	20239/tcp	Used to send rule startup requests to JP1/IM - Rule Operation by automated action.
jp1imevt	20098/tcp	Used to forward JP1 events issued by JP1/IM - Rule Operation.

7.4 Core functionality provided by JP1/Base

JP1/Base is a prerequisite product for JP1/IM - Manager, providing the core functionality for monitoring the system operation using JP1/IM. This section describes the role of JP1/Base in the JP1/IM system environment.

7.4.1 Managing JP1 users

JP1/IM performs user authentication and access control based on dedicated **JP1 user** accounts, designed to allow JP1/IM to operate securely in a multi-platform environment. JP1 users are managed via JP1/Base user management.

The following are the details about the user management functionality.

(1) User authentication

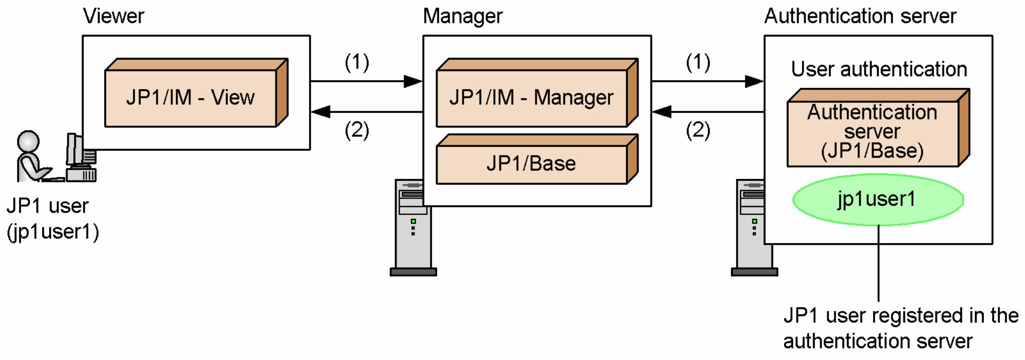
JP1/IM monitors the system by accessing JP1/IM on the manager from JP1/IM - View on the viewer. To prevent access by unauthorized users, user authentication is performed by a login processing when JP1/IM is accessed from JP1/IM - View.

In JP1/IM, user authentication is carried out by the JP1/Base user authentication function when a user attempts to log in to JP1/IM from JP1/IM - View. The JP1/Base that performs this user authentication is called an *authentication server*.

At login, the JP1 user is authenticated by the authentication server assigned to the JP1/IM host.

The following figure shows the flow of user authentication when a user logs in to the JP1/IM host from JP1/IM - View.

Figure 7–5: Flow of processing for user authentication



The flow of processing is described below, following the numbers in the figure:

1. When a user logs in to the JP1/IM host from JP1/IM - View, user authentication is carried out by the authentication server associated with JP1/Base on the JP1/IM host.

   The authentication server used by the JP1/IM host is set up in JP1/Base on that host.

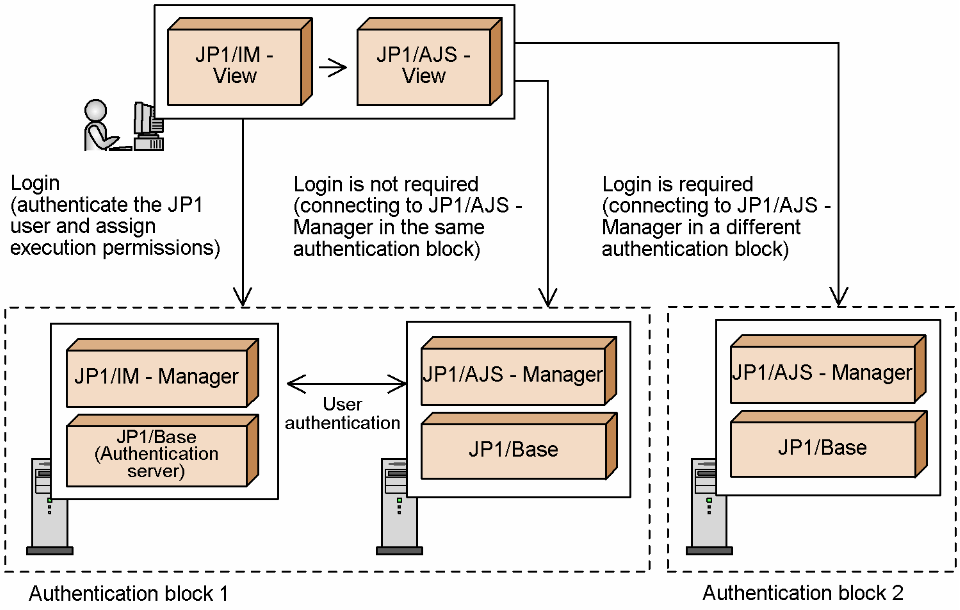
   When the authentication server is installed on a host that is not the JP1/IM - Manager host, login from JP1/IM - View fails if the authentication server is not already running.

2. The authentication server checks whether the JP1 user who made the login attempt is registered. If the JP1 user is registered, information about the operating permissions for that JP1 user is returned to JP1/IM - View via the JP1/IM host. (For details about operating permissions for JP1 users, see *7.4.1(2) Access control*.)

   JP1 users must be registered in the authentication server in advance.

A group of hosts that use the same authentication server for JP1 user authentication is called an *authentication block*. Users can access JP1/AJS - View windows from JP1/IM - View without needing to log in to JP1/AJS - View if the associated JP1/AJS - Manager is in the same authentication block as JP1/IM - View, as shown in the following figure. (In a system that switches between authentication servers, login will be required after a switch has taken place.) If the JP1/AJS - Manager is in a different authentication block, login is required.

Figure 7–6: Authentication blocks


JP1/IM - View
JP1/AJS - View
Login (authenticate the JP1 user and assign execution permissions)
Login is not required (connecting to JP1/AJS - Manager in the same authentication block)
Login is required (connecting to JP1/AJS - Manager in a different authentication block)
JP1/IM - Manager
JP1/Base (Authentication server)
User authentication
JP1/AJS - Manager
JP1/Base
JP1/AJS - Manager
JP1/Base
Authentication block 1
Authentication block 2

You can set up two authentication servers in the same authentication block. If connection to one authentication server fails, the JP1 user can connect to and be authenticated by the other authentication server. This prevents any interruption of job processing due to an authentication server error or other such problem. The authentication server used routinely is called the *primary authentication server*, and the authentication server in reserve is called the *secondary authentication server*. Both servers must be running the same JP1/Base version.

(2) Access control

Only users authenticated by the authentication server are able to log in to JP1/IM. However, there are problems inherent in giving all logged-in users unrestricted access to reference or operate on the management information of JP1/IM. For this reason, JP1/IM allows you to assign access permissions and operating permissions to individual JP1 users that restrict the operations and information available to them in JP1/IM - View.

The access permissions and operating permissions for JP1 users are managed by the authentication server. When user authentication is performed at login, information about the access permissions and operating permissions of the logged-in user (JP1 user) is returned to JP1/IM. JP1/IM uses this information to control what information is displayed and what operations the user might perform in JP1/IM - View.

Access permissions and operating permissions are set when JP1 users are registered in the authentication server. The access permission for a JP1 user is called a *JP1 resource group*, and the operating permission is called a *JP1 permission level*. The range of tasks a JP1 user can perform in JP1/IM - View is determined by assigned JP1 resource group and JP1 permission level.

The JP1 resource group for JP1/IM is `JP1_Console`. You do not have to change this if you use IM Configuration Management. If you want to restrict viewing of and operating on business groups for individual JP1 users in the Central Console, or if you want to control the display range of the monitoring tree in the Central Scope, you need to change the JP1 resource groups set on the authentication server. For details, see *3.1.4 Restrictions on viewing and operating business groups* and *4.4.3 Setting the monitoring range of a monitoring tree*.

JP1/IM and IM Configuration Management provide three JP1 permission levels, as listed below. To each JP1 user, assign the permission level that matches their responsibilities (the range of tasks the user performs in JP1/IM - View).

Table 7–12: JP1 permission levels

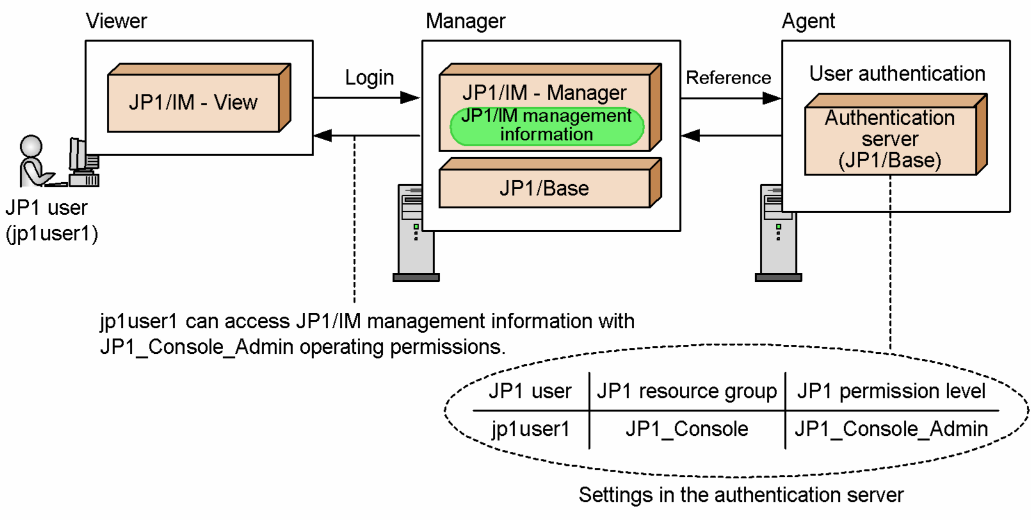
JP1/IM - Manager component	Permission level	Permitted operations
JP1/IM	`JP1_Console_Admin`	• Use the Central Console and Central Scope (set the system environment, perform system operations, reference information, set the user environment, and start linked products). • Reference the system hierarchy and host information in IM Configuration Management.
	`JP1_Console_Operator`	• Use the Central Console and Central Scope, reference information, set the user environment, and start linked products. • Reference the system hierarchy and host information in IM Configuration Management.
	`JP1_Console_User`	• Perform reference operations in the Central Console and Central Scope, set the user environment, and start linked products. • Reference the system hierarchy and host information in IM Configuration Management. • Cannot execute commands.
IM Configuration Management	`JP1_CF_Admin`	Perform all operations in IM Configuration Management, including changing the system hierarchy, changing profiles, and so on.
	`JP1_CF_Manager`	Reference the system hierarchy, and reference and collect host information.
	`JP1_CF_User`	Reference and collect the system hierarchy and host information.

Users who work with IM Configuration Management must have both a JP1/IM permission level and an IM Configuration Management permission level.

For details about the operations that the different JP1 permission levels allow JP1 users to perform in JP1/IM - View, see *Appendix E. Operating Permissions*.

The following figure shows an example of controlling a JP1 user's access.

Figure 7–7: Example of JP1 user access control



jp1user1 can access JP1/IM management information with JP1_Console_Admin operating permissions.

JP1 user	JP1 resource group	JP1 permission level
jp1user1	JP1_Console	JP1_Console_Admin

Settings in the authentication server

(3) User mapping

When a command is executed from JP1/IM, either by automated action or from JP1/IM - View, the OS user permissions for the target host are required to actually execute the command on that host. For this reason, the OS user permissions associated with the JP1 user are acquired at command execution.

The functionality that associates JP1 users with OS users is called *user mapping* and is provided by JP1/Base.

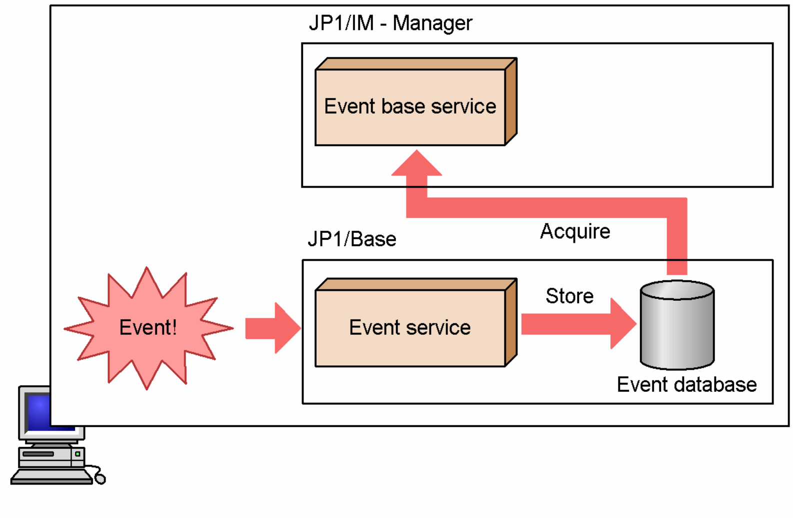
User mapping must be defined on all target hosts at which commands are to be executed.

To use IM Configuration Management, you do not need to define user mapping on the manager running IM Configuration Management or on its managed hosts.

7.4.2 Managing JP1 events using JP1/Base

JP1 events are controlled by the JP1 event service and recorded in an event database unique to JP1/Base.

Figure 7–8: Overview of JP1 event management



The information recorded in a JP1 event is categorized by attribute as follows:

- Basic attributes (held by all JP1 events)
- Extended attributes (optionally set by the program that issued the JP1 event, and consisting of common information and program-specific information)
  - Common information (information in a format shared by all JP1 programs)
  - Program-specific information (other information in a format specific to the program issuing the event)

To distinguish between attribute types, basic attribute names begin with `B.` (for example, `B.ID`), and extended attribute names begin with `E.` (for example, `E.SEVERITY`).

Information is recorded for each attribute type as follows:

Example: JP1 event generated when execution of an automated action is requested (partial only)

Basic attributes

`Event ID (B.ID): 000020E0`

- `Message (B.MESSAGE):`

  `KAVB4430-I Execution of the action for an event was requested.`

  `:`

Extended attributes - Common information

- `Event ID (E.SEVERITY): Information`
- `Product name (E.PRODUCT_NAME): /HITACHI/JP1/IM/JCAMAIN`

  `:`

Extended attributes - Program-specific information

- `Executing host (E.EXECHOST): jp1-manager`

  `:`

In this manner, events generated in the system are recorded as JP1 events.

For details about JP1 events, see *Chapter 3. JP1 Events* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*. See also the description of JP1 events in the *JP1/Base User's Guide*.

(1) Centrally managing events using JP1 events

JP1/Base manages events occurring in the system as JP1 events.

Events being managed outside JP1, such as by log files and SNMP traps, can be converted into JP1 events and handled in JP1/Base.

By using JP1 events in this manner, events handled by a wide variety of products can be managed by JP1/Base in the same way as events issued by products in the JP1 series.

Events issued as JP1 events

- JP1 events (issued by JP1 products)

  The products in the JP1 series enable system operation management from a variety of angles. By managing the JP1 events that each product issues, you can comprehensively manage the events occurring in the system.

  For details about the JP1 events issued by individual products in the JP1 series, see the relevant manual.
- JP1 events (issued by commands)

JP1/Base provides commands for issuing JP1 events (`jevsend` and `jevsendd`). By placing these commands in a shell script or similar, users can use the issued JP1 events to monitor system operation. Since JP1/IM only monitors JP1 events that have an event level, specify the event level in the command arguments (for example `-e SEVERITY=Error`).

For details, see the chapter about commands in the *JP1/Base User's Guide*.

- Events in JP1/SES format

  JP1/Base can manage events in JP1/SES format (events that can be acquired by the programs JP1/SES and JP1/AJS provided in version 5 and earlier of the JP1 series.)

  In its default state, JP1/IM cannot monitor events in the JP1/SES format. This is because JP1/IM uses the event level, an extended attribute, in monitoring events; events in the JP1/SES format have basic attributes only.

  To allow JP1/IM to monitor events in the JP1/SES format, either set up an event acquisition filter to acquire JP1/SES format events, or use the extended functions provided by JP1/Base to enable extended attributes for JP1/SES-format events.

  See *3.2 Filtering of JP1 events*.

  See the description of JP1/SES event conversion in the manual *JP1/Base Function Reference*.

  JP1/SES-format events do not include any character code set. Therefore, to monitor JP1/SES-format events, the character code for JP1/SES-format events must be defined as a unified character code in the language environment of the whole system.

- JP1 events (using the event issuing function)

  JP1/Base provides functions that allow user application programs to issue JP1 events directly.

  See the description of user-defined events in the manual *JP1/Base Function Reference*.

Events converted to JP1 events by the event converters

- Log file information

  The JP1/Base log file trapping function converts the information that application programs output to log files into JP1 events for management by JP1/Base.

- Windows event log information

  The JP1/Base event log trapping function converts the information output to the Windows event log into JP1 events for management by JP1/Base.

- SNMP traps

  The JP1/Base SNMP trap converter converts SNMP traps managed by HP NNM version 7.5 or earlier into JP1 events for management by JP1/Base.

  See the chapter on setting the event converters in the *JP1/Base User's Guide*.

Note

For details about NNMi incident conversion in HP NNMi, see the manual *Job Management Partner 1/Integrated Management - Event Gateway for Network Node Manager i Description, User's Guide and Reference*.

(2) Using JP1 event forwarding to centralize event management

JP1/IM monitors the system by acquiring from JP1/Base the JP1 events recorded in the event databases on the managers.

Of the JP1 events generated at each host in the system, important events that need to be addresses can be forwarded to the JP1/IM manager by the event forwarding function of JP1/Base. In this manner, JP1/IM can centrally manage the events occurring in the system (important events needing management follow-up).

(a) Forwarding JP1 events

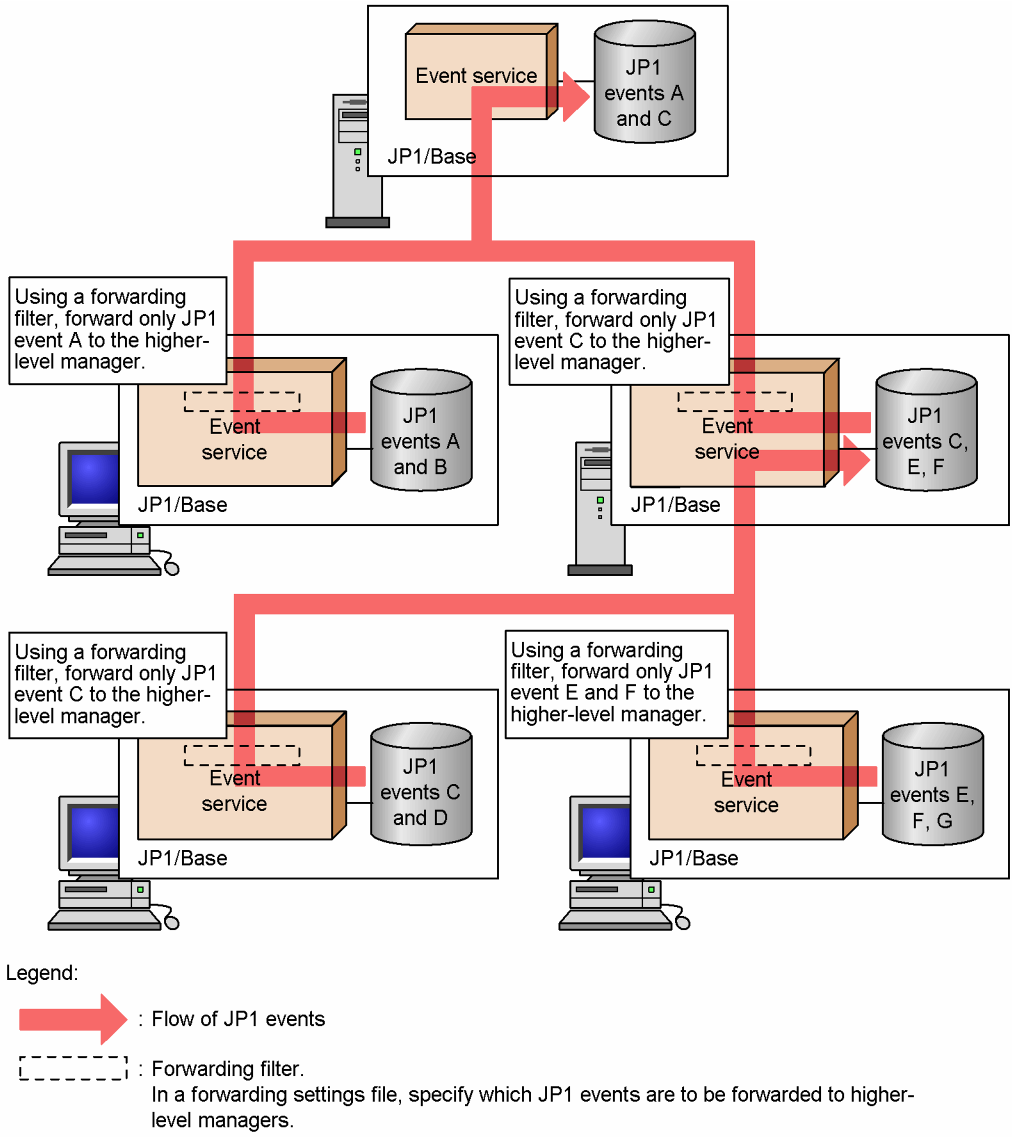
The JP1/Base event forwarding function forwards JP1 events from one host to another. By using this function, JP1/IM can forward JP1 events to a manager where they can be centrally managed.

To define which JP1 events to forward, use the forwarding settings file (`forward`) of the JP1/Base event service. This file is called a *forwarding filter* in JP1/IM.

Only important JP1 events needing management follow-up should be forwarded to a manager. Do not set up event forwarding to send all JP1 events that occur in the system. Under the default settings, JP1 events whose event level is `Emergency`, `Alert`, `Critical`, `Error`, or `Warning` are forwarded to higher-level managers according to the hierarchy defined in the configuration definition.

The following figure shows an example of how JP1 events are forwarded to higher-level managers.

Figure 7–9: JP1 event forwarding


Event service
JP1 events A and C
JP1/Base
Using a forwarding filter, forward only JP1 event A to the higher-level manager.
Event service
JP1 events A and B
JP1/Base
Using a forwarding filter, forward only JP1 event C to the higher-level manager.
Event service
JP1 events C, E, F
JP1/Base
Using a forwarding filter, forward only JP1 event C to the higher-level manager.
Event service
JP1 events C and D
JP1/Base
Using a forwarding filter, forward only JP1 event E and F to the higher-level manager.
Event service
JP1 events E, F, G
JP1/Base
Legend:
: Flow of JP1 events
: Forwarding filter.
In a forwarding settings file, specify which JP1 events are to be forwarded to higher-level managers.

You can change the forwarding settings by editing the forwarding settings file directly on each host. Alternatively, by using the JP1/Base functionality for collecting and distributing definitions, you can distribute the new settings from a higher-level host in a batch operation.

(b) Retry setting for JP1 event forwarding

The JP1/Base event service can automatically retry forwarding a JP1 event if transmission fails because of a network error or because the destination event server has stopped. Enter this setting in the JP1/Base event server settings file (`conf`).

See the chapter on setting the event service environment in the *JP1/Base User's Guide*.

(c) Event forwarding according to configuration management

When you define the hierarchy of managers and agents using the JP1/Base configuration management functions, each host is automatically set up to forward JP1 events to the higher-level manager according to the resulting configuration definition. When you change a definition in the configuration definition file, the JP1 event forwarding settings are updated automatically on each host.

See *7.4.3 Managing the system hierarchy*.

(d) Using the definition collection and distribution function

By using the definition collection and distribution function, you can distribute JP1 event forwarding settings from a higher-level host defined in the system hierarchy to lower-level hosts (for an overview of configuring a system hierarchy, see *7.4.3 Managing the system hierarchy*). You can use this function to halt event forwarding from another host when you need to temporarily stop a host for maintenance, for example, or you do not want a flood of events sent from a host on which numerous errors have occurred. By distributing the settings from the manager using a JP1/Base command, you can update the forwarding settings file (`forward`) at all the lower-level hosts. The forwarding settings are reloaded at each host when distribution is successful, and events are forwarded thereafter based on the updated information.

See *7.4.5 Collecting and distributing definition information*.

(3) Using JP1 events as historical and statistical information by CSV file output

You can check the JP1 events stored in an event database by outputting the database contents to a CSV file using the JP1/Base `jevexport` command.

JP1/IM manages the system operation by collecting important JP1 events that require urgent attention on a manager where they can be monitored from JP1/IM - View. Non-urgent JP1 events, on the other hand, are recorded in the event databases of their respective hosts, but are not forwarded to a manager or displayed in JP1/IM - View.

However, information about non-urgent JP1 events (indicating that a job has ended normally, for example) might occasionally be required in order to compile statistical information or an operating history. In this case, use the JP1/Base command `jevexport` to output the database contents to a CSV file.

For details about the `jevexport` command, see the chapter on commands in the *JP1/Base User's Guide*.

When you use the integrated monitoring database, you can output the JP1 events stored in the integrated monitoring database by using the JP1/IM `jcoevtreport` command.

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

7.4.3 Managing the system hierarchy

When you do not use IM Configuration Management, you can use the configuration definition function provided by JP1/Base to handle the system hierarchy (IM configuration) managed by JP1/IM. On the manager, define the host relationships in a configuration definition file (`jbs_route.conf`), and then apply the configuration definitions by executing the `jbsrt_distrib` command.

By defining the system hierarchy, you can perform the following operations in JP1/IM:

- Forward JP1 events to a higher-level host
- Execute commands from JP1/IM - View
- Execute automated actions from JP1/IM
- Collect and distribute definition information

If you wish to use IM Configuration Management to centrally manage the system hierarchy from JP1/IM - Manager, see *Chapter 6. System Hierarchy Management Using IM Configuration Management*.

(1) System hierarchy defined with the configuration definition functions

In a 3-tier configuration defined using the JP1/Base configuration management functions, the managers in the middle tier operate as base managers.

You can define the system hierarchy in one operation on the top-level manager, or divide it into a number of parts and define them separately on the respective managers.

Figure 7-10 to Figure 7-12 show examples of a system hierarchy defined by using the configuration management functions.

Figure 7–10: System hierarchy example (physical configuration)

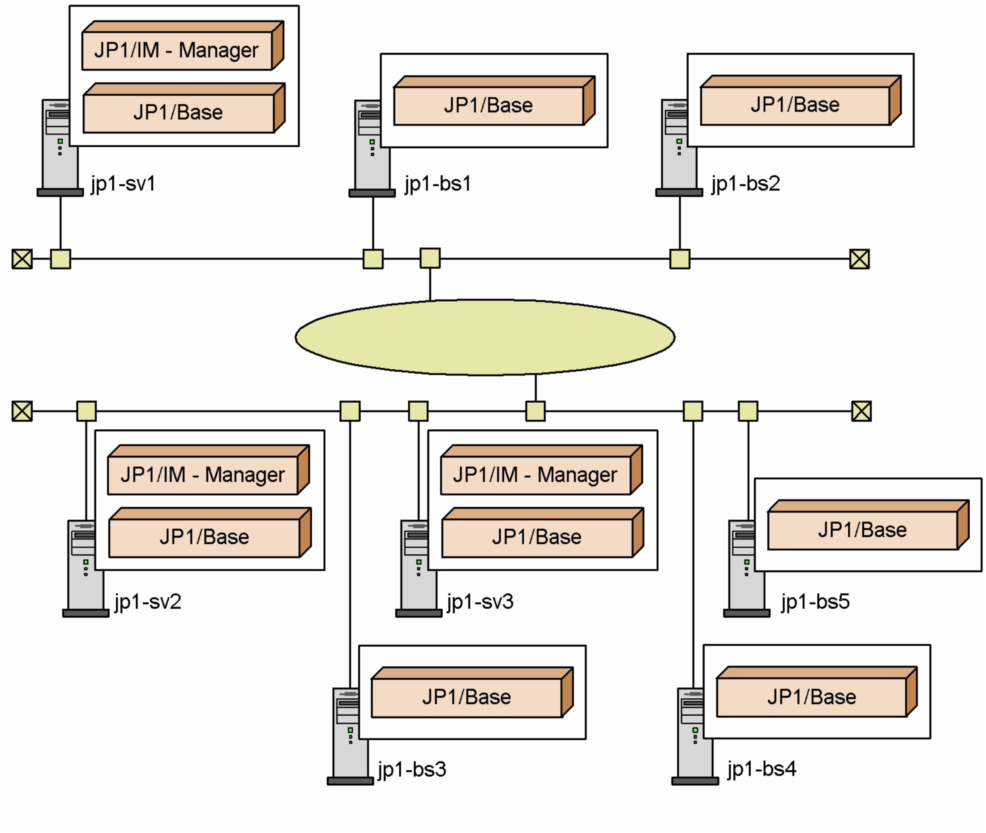


Figure 7–11: System hierarchy example (hierarchical relationships defined in one operation)

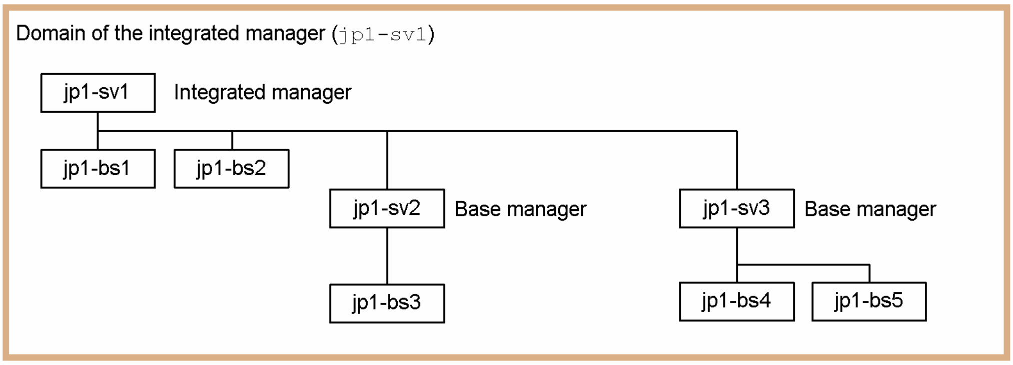
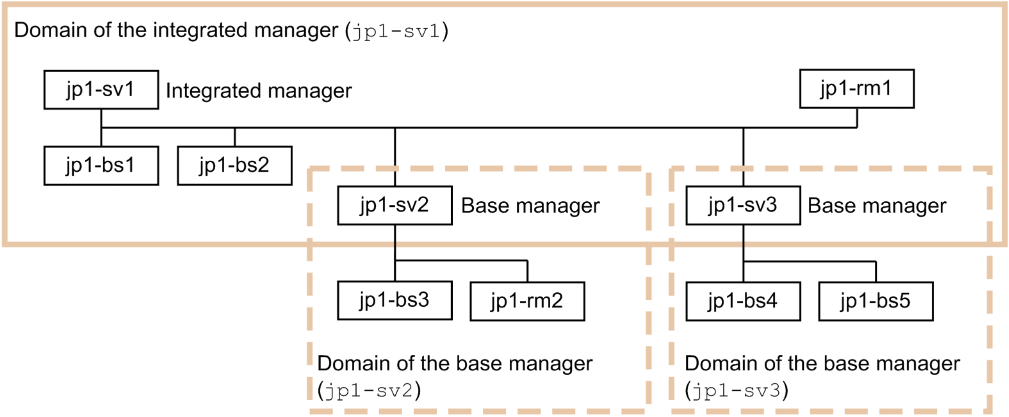
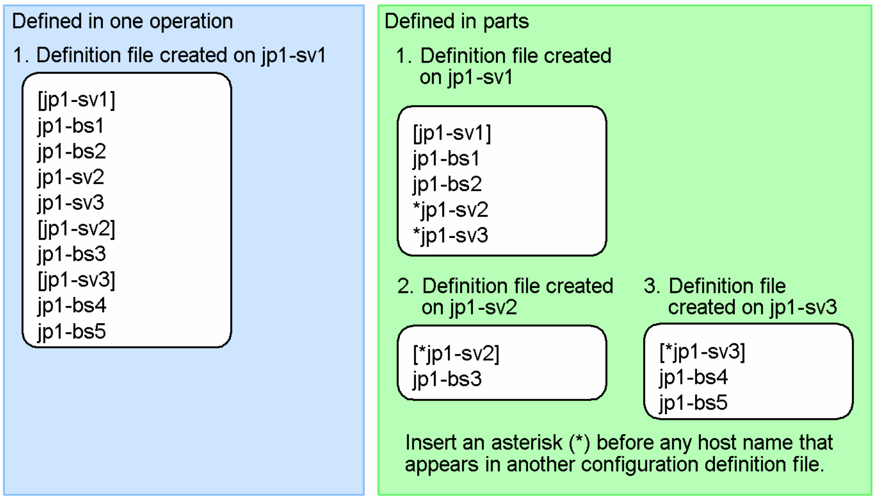


Figure 7–12: System hierarchy example (hierarchical relationships defined in parts)


Domain of the integrated manager (jp1-sv1)
jp1-sv1
Integrated manager
jp1-rm1
jp1-bs1
jp1-bs2
jp1-sv2
Base manager
jp1-sv3
Base manager
jp1-bs3
jp1-rm2
jp1-bs4
jp1-bs5
Domain of the base manager (jp1-sv2)
Domain of the base manager (jp1-sv3)

Define the system hierarchy in the above example in the configuration definition file (`jbs_route.conf`) as follows:

Figure 7–13: System hierarchy definition example



Defined in one operation

1. Definition file created on jp1-sv1

```
[jp1-sv1]
jp1-bs1
jp1-bs2
jp1-sv2
jp1-sv3
[jp1-sv2]
jp1-bs3
[jp1-sv3]
jp1-bs4
jp1-bs5
```

Defined in parts

1. Definition file created on jp1-sv1

```
[jp1-sv1]
jp1-bs1
jp1-bs2
*jp1-sv2
*jp1-sv3
```

2. Definition file created on jp1-sv2

```
[*jp1-sv2]
jp1-bs3
```

3. Definition file created on jp1-sv3

```
[*jp1-sv3]
jp1-bs4
jp1-bs5
```

Insert an asterisk (*) before any host name that appears in another configuration definition file.

(2) Procedure for defining a system hierarchy with the configuration management functions

The following is an overview of defining a system hierarchy using the configuration management functions:

1. Define the configuration definition file on the manager.

In the configuration definition file (`jbs_route.conf`), define the system configuration from the manager down to the lower-level managers and agents.

To define the system hierarchy in one operation, define the entire system configuration in the definition file. To define the system hierarchy in parts, write the configuration for each of the base managers and their lower-level hosts.

2. Execute the `jbsrt_distrib` command on the manager.

   This command distributes the definition information to the hosts defined in the configuration definition file, and applies the configuration definition.

To define the system hierarchy in parts, perform steps 1 and 2 on each manager. Then, perform the following procedure at the top-level manager to create the definition for the entire system:

1. Define the configuration definition file on the top-level manager.

   Create a configuration definition file (`jbs_route.conf`) that includes the top-level manager host and the managers directly below it in the hierarchy.

2. Execute the `jbsrt_sync` command on the top-level manager.

   This command collects the configuration information from all managers defined in the configuration definition file, and creates configuration information for the entire system.

To check the system configuration definitions, execute the `jbsrt_get` command on each host.

For details about the format of the configuration definition file, see *Configuration definition file (jbs_route.conf)* in *Chapter 2. Definition Files* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*. For details about how to set configuration definition information, see *1.9 Setting the system hierarchy (when IM Configuration Management is not used) (for Windows)* (for a Windows system) or *2.8 Setting the system hierarchy (when IM Configuration Management is not used) (for UNIX)* (for a UNIX system) in the *JP1/Integrated Management - Manager Configuration Guide*.

7.4.4 Managing command execution

The JP1/Base command execution function controls the following modes of command execution in JP1/IM:

- Command execution from the Execute Command window of JP1/IM - View
- Command execution by automated action

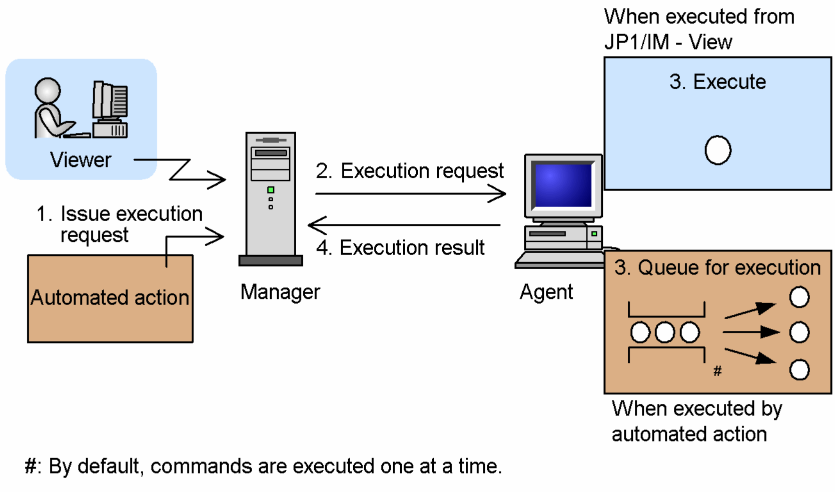
The following describes the JP1/Base command execution function.

(1) Executing commands

When you execute a command in JP1/IM, JP1/IM on the manager directs the JP1/Base command execution function to execute the command. The command execution function then executes the command by sending a request to the agent specified as the execution target.

Commands executed by the user from JP1/IM - View or by an automated action are both processed by the command execution function. However, they differ in how the execution request is controlled (whether the request is queued or not queued).

Figure 7–14: Command execution


When executed from JP1/IM - View
3. Execute
Viewer
1. Issue execution request
Automated action
Manager
2. Execution request
4. Execution result
Agent
3. Queue for execution
#
When executed by automated action
#: By default, commands are executed one at a time.

As shown in the above figure, when you execute a command from JP1/IM - View, the command is executed immediately without being queued. When you execute multiple commands, each command is executed without any controls being placed on the execution order or the number of commands that can be executed concurrently.

Commands executed by automated actions are queued up to the specified *command-queue-count*. Also, the system does not execute more commands at any one time than the specified *command-concurrent-execution-count*.

The flow of processing is described below, following the numbers in the figure:

1. A command is executed.
   - By an operation from JP1/IM - View

     When you execute a command from JP1/IM - View, a request for command execution is sent to JP1/IM on the manager that you are logged in to. That instance of JP1/IM then passes the request to the command execution function of JP1/Base on the local host.
   - By automated action

     The automated action function of JP1/IM automatically executes an action upon receiving a JP1 event specified as a condition in an action definition. When this occurs, the command defined as the action in the action definition is passed by JP1/IM as an execution request to the command execution function of JP1/Base on the local host.
2. The manager requests the agent to execute the command.

   The JP1/Base on the manager sends a request to the JP1/Base on the agent specified as the execution target, directing it to execute the command. If there is no response from the agent within the time period specified by *response-monitoring-time*, an error is returned to JP1/IM indicating that the host is unreachable.
3. The command is executed by JP1/Base on the agent.

   The command execution function of JP1/Base on the agent executes the command using the OS shell or `cmd.exe`. The command is handled differently depending on how the command execution was requested:
   - By an operation from JP1/IM - View

     The command is executed immediately.
   - By automated action

     Command execution requests are queued by the command execution control of JP1/Base on the agent, and executed in order. The maximum number of commands in the queue is determined by the specified *command-queue-count*, and the number of commands that are executed in parallel is determined by the specified *command-concurrent-execution-count*. Although the number of commands being executed at any one time differs according to the duration of commands and the execution environment, it will never exceed *command-*

concurrent-execution-count (under the default setting, *command-concurrent-execution-count* is set to 1, and commands are executed one at a time.)

Command execution might be delayed when a command executed by an automated action takes a long time to execute and commands are set to be executed serially (the default setting). In this case, you can reduce delays by setting the command execution function to execute commands in parallel.

Delays can also be introduced when a large number of commands are executed by automated actions, leading to a backlog of commands in the queue. You can gain advance notice of execution delays by setting the *command-queue-count-threshold* parameter (supported in JP1/Base 07-11). Under the default settings, a warning event is issued when the number of commands in the queue reaches 10, and a recovery event is issued when the number returns to 0.

4. The command execution result is sent from the agent to the manager.

   JP1/Base on the agent sends the command execution result (command output) to the JP1/Base on the manager. When the command finishes executing, JP1/Base on the agent reports the execution results to JP1/IM via JP1/Base on the manager.

   At this time, log information for the command is recorded in a command execution log file on the manager. The maximum number of records that can be contained in the execution log is defined by the `-record` option of the `jcocmddef` command.

   You can view these command execution logs in the Execute Command window if the command was executed from JP1/IM - View, or in the Action Log Details window if the command was executed by an automated action.

In the description above, *response-monitoring-time*, *command-queue-count*, *command-concurrent-execution-count*, and *command-queue-count-threshold* are parameters of the JP1/Base command execution function. You can set these parameters using the `jcocmddef` command.

The flow of this processing task is described in *3.19.3 Executing commands on managed hosts from JP1/IM - View* and *Chapter 5. Command Execution by Automated Action*. See also these descriptions as required.

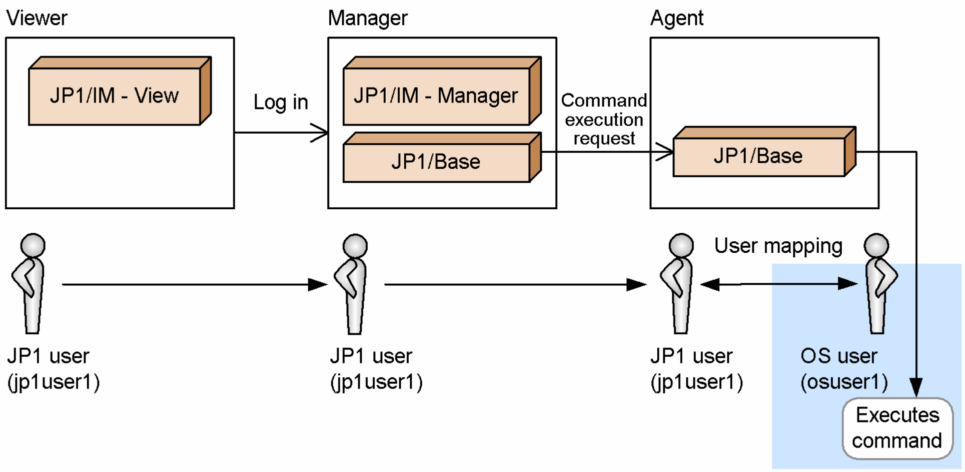
(2) Users permitted to execute commands

To execute commands in the OS environment of the agent, you must have the appropriate OS user permissions.

At command execution, user mapping associates the JP1 user with an OS user on the agent, and the command is executed under the OS user permission associated with that JP1 user account.

If the target host is a Windows host, the OS user subject to user mapping must have Windows-specific user permissions. For details about the user permissions required for an OS user subject to user mapping, see the chapter on granting user permissions to OS users in the *JP1/Base User's Guide*.

Figure 7–15: Command execution and user mapping



The command execution function directs the agent to use the following JP1 user accounts when executing commands:

- Command execution from JP1/IM - View
  The JP1 user who is currently logged in to JP1/IM - View
- Command execution by automated action
  The JP1 user specified in a definition with the highest priority based on the following ranking:
  1. The JP1 user specified in `u=` in the automated action definition file (`actdef.conf`) (for compatibility) or in `usr` in the automated action definition file (`actdef.conf`)
  2. The JP1 user specified by the `ACTIONEXECUSER` parameter in the automated action environment definition (`action.conf`) The JP1 user specified by the `ACTIONEXECUSER` parameter of the common definition information in the automated action environment definition file (`action.conf.update`)
  3. `jp1admin`

At command execution, the JP1 user is mapped to the OS user defined in the user mapping at the agent where the command is to be executed.

(3) OS-based command execution

The JP1/Base command execution function uses the following methods for command execution requested by JP1/IM - View or an automated action.

(a) Users permitted to execute commands

The command is executed by the OS user mapped to the JP1 user.

(b) Method of command execution

The command execution function uses the following methods to execute commands:

- In Windows
  The command execution function executes `cmd.exe /c` *command*.
- In UNIX
  The command execution function uses the login shell of the OS user to execute the command, for example `/bin/sh -c` *command* (where the login shell is `/bin/sh`).

When you execute a command that creates a child process, JP1/Base will be unable to process the next command until the child process has terminated. This is because command execution management recognizes the command as still running.

(c) Environment for command execution

The environment used for command execution is described below.

- Environment variables

  You can use an environment variable file in JP1/IM to specify the environment variables used at command execution. Specify the environment variable file in the Execute Command window of JP1/IM - View or in the automated action definition file (`actdef.conf`).

  See *Environment variable file* in *Chapter 2. Definition Files* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

  If you do not set up an environment variable file, the following environment variables are used.

  - In Windows

    The Windows system environment variables are used at command execution.

  - In UNIX

    The environment variables of the command execution process (the environment variables specified in the JP1/Base start command `jbs_start`, for example) are used at command execution. The OS user profile is not loaded in UNIX systems.

- OS user profile (Windows only)

  You can load the OS user profile when you execute a command on the target host. You can enable this function using the `-loaduserprofile` option of the `jcocmddef` command (it is disabled by default).

> **Important**
>
> The environment on the target host must allow the commands to execute normally. Note the following, for example:
>
> - Each command requires a certain amount of resources, such as memory, to execute. When you execute a large number of commands concurrently, the system might have insufficient resources to execute the commands. When there are insufficient system resources in Windows, for example, a dialog box is displayed with the message **cmd.exe - DLL initialization failed**.
>
>   If this occurs, adjust the number of commands that are executed concurrently to ensure that sufficient resources are available for each command.
>
> - When you execute a command or shell script that processes 2-byte code, an appropriate language code must be set as an environment variable, and a shell that supports 2-byte code such as the C shell must be used.
> - Commands that cannot be executed in the format `cmd.exe /c` *command* or `shell -c` *command* cannot be executed by the JP1/Base command execution function.
> - If the login shell of the OS user is the C shell, use the C shell for executing an automated action.

(d) Command execution results

The execution results for commands executed by the command execution control are handled as follows:

Outputting command execution results

Command execution results (such as messages) are recorded# in a command execution log file managed by the command execution control on the manager. Log information for commands executed from JP1/IM - View appears in the Execute Command window, and log information for commands executed by automated actions appears in the Action Log Details window.

When multiple commands are executed, the results might be output in a different order from the execution order. The result output timing is affected by such things as the time required to execute each command, performance and workload differences among the hosts on which the commands are executed, and retry after a communication error.

#

By changing settings in JP1/Base, you can limit the amount of execution result data output to the command execution log file when commands are executed from JP1/IM - View or by automated actions. You can either restrict the amount of transferred data or prevent registration of detailed information. Both are performed by specifying options in the `jcocmddef` command. Choose whichever method best suits your system operation.

- Restricting the amount of transferred data

  You can restrict the amount of execution log data by setting an upper limit (as a number of lines) for the amount of data that can be transferred from the execution-target host to the manager. This helps control the size of the command execution log file and reduces congestion on the communication lines between the hosts.

  You can set separate limits for the execution results of commands executed from JP1/IM - View and for those executed by automated actions.

  If you performed a new installation of version 8 of JP1/Base, data transfer will be restricted to a maximum of 1,000 lines by default.

- Preventing registration of detailed information (applies to commands executed by automated actions only)

  For the execution results of commands executed by automated actions, you can choose to register only information indicating the success or failure of the command, and discard detailed information such as message information. By doing so, you can improve the processing speed of the underlying JP1/Base components (and hence the speed with which automated actions are processed). However, when you prevent registration of detailed information, the message `KAVB2401-I` appears in the **Message** area of the Action Log Details dialog box, and no detailed log information is displayed (the **Log** area is unaffected). Do not enable this setting if you need to view detailed information (the setting is disabled by default).

The execution results of automated actions are managed by the action information file and the command execution log file.

If an automated action in which commands for the action have been omitted is executed, the execution results are not written to the command execution log file because no command is executed.

If a large number of actions are issued, only the action information file is wrapped. As a result, the execution results in the command execution log file and action information file might become inconsistent. In such a case, the execution results for another automated action that was executed in the past might be displayed.

To avoid this, do not define automated actions in which commands are omitted. Also, define commands that do not have a negative impact on the system, such as the `echo` command, in the automated action. If a large number of actions in which commands are omitted are issued and the execution results of other automated actions executed in the past are displayed, the command execution log file is also wrapped, and then inconsistency between the action information file and the command execution log file is resolved.

Command execution results (return code)

The following return codes appear in the command execution results:

- In Windows

  The return code passed to the command execution function by `cmd.exe`.

- In UNIX

The return code passed to the command execution function by the shell that executed the command.

The command will not execute if an error occurs leading up to command execution (for example user mapping fails or the target host cannot be contacted).

> **Important**
>
> After command execution has terminated, the termination code reported in the JP1 event might differ from the actual termination code depending on when the termination code is finalized. After you have received a JP1 event notification, check the details of the command's execution results in the Action Log Details window.

(4) Using host groups to execute commands on multiple hosts

You can define a number of hosts together as a single group.

You can specify a host group as the target host at command execution. By doing so, you can execute the command on all the hosts in that group in a single operation.

For details about defining host groups, see *Host group definition file* in *Chapter 2. Definition Files* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

(5) Issuing JP1 events based on the command execution status

You can issue JP1 events that indicate the execution status of commands, such as when command execution starts and stops. JP1 events can be issued in the following cases:

- Command execution from JP1/IM - View

  When a command starts executing, finishes executing, or terminates abnormally.

- Action (command) execution by automated action

  When a command starts executing, finishes executing, terminates abnormally, or fails to execute (due to a failed request).

By enabling this functionality, you can use JP1 events to manage information about when commands are executed, by which users, and on which hosts. You can then display and monitor this information in the Event Console window of JP1/IM - View.

Use the `jcocmddef` command to set up issuing of these JP1 events.

The JP1/Base command execution function also provides for other JP1 events, examples of which are given below. These JP1 events do not require setup as above.

- JP1 events issued based on how long a command takes to execute

  This function is supported from version 07-10 of JP1/Base. A JP1 event is issued when a command has not finished executing within a predetermined period of time. This JP1 event helps you to identify hangups or undue delays in commands executed from JP1/IM - View or by automated action.

  By default, this JP1 event is issued at 10-minute intervals. You can change this setting using the `jcocmddef` command.

- JP1 events issued when the queuing threshold is exceeded

  This function is supported from version 07-11 of JP1/Base. A JP1 event is issued when the number of commands in the queue reaches or exceeds a predetermined number, and another event is issued when the number returns to an acceptable level. These JP1 events allow you to gain advance notice of execution delays when a large number of commands are executed by automated actions, and let you know when the situation has recovered.

Under the default settings, a warning event is issued when the number of commands in the queue reaches 10, and a recovery event is issued when the number returns to 0. Use the `jcocmddef` command to modify these settings.

(6) Commands for troubleshooting

You might encounter the following problems when using the JP1/Base command execution function from JP1/IM.

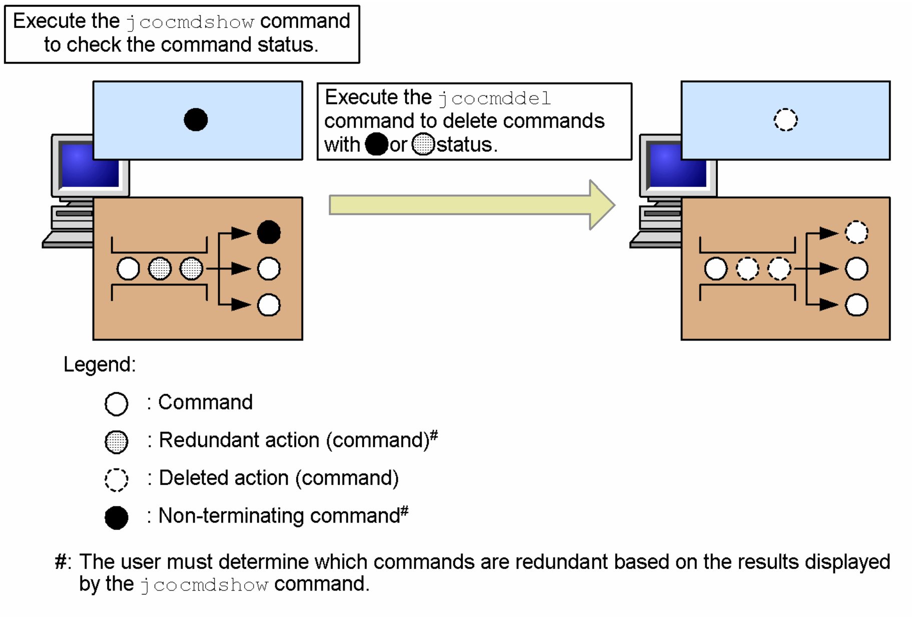
- A command that cannot be executed from JP1/IM - View (see *3.19.3(1) Executable commands*) is executed accidentally and remains stuck in executing status.
- A greater number of automated actions occur than was anticipated at the design stage, leading to a massive backlog of redundant actions in the queue.
- A command executed by an automated action hangs or takes longer than expected to execute, preventing succeeding commands (actions) from executing.

To allow you to recover quickly from these errors, JP1/Base provides a command for checking the status of queuing or executing commands (`jcocmdshow`), and a command for deleting queuing or executing commands (`jcocmddel`)#.

#

JP1/IM can cancel automated actions when command execution results in an error. When an error occurs in a command executed by an automated action, use this function where possible (for details, see *5.7 Canceling automated actions*).

Figure 7–16: Overview of jcocmdshow and jcocmddel commands


Execute the jcocmdshow command to check the command status.
Execute the jcocmddel command to delete commands with ● or ◌ status.
Legend:
○ : Command
◍ : Redundant action (command)#
◌ : Deleted action (command)
● : Non-terminating command#
#: The user must determine which commands are redundant based on the results displayed by the jcocmdshow command.

The `jcocmdshow` command displays the following information. Based on this information, determine which commands need to be deleted, and then delete them using the `jcocmddel` command.

Table 7–13: Information displayed by the jcocmdshow command

Display item	Description
`ID`	The unique ID assigned to commands that are executing or queuing in the command execution function. When you use the `jcocmddel` command to delete a command, use this ID as the key.

Display item	Description
STATUS	The execution status of the command in the command execution function, shown as either Running or Queuing.
TYPE	Whether the command was executed by JP1/IM - View or an automated action.
USER	The name of the JP1 user who issued the command execution request.
STIME	The time at which the command execution function received the instruction from JP1/IM to execute the command.
ETIME	The length of time that has elapsed since the command started execution.
COMMAND	The name of the executing or queuing command.

The `jcocmdshow` and `jcocmddel` command functionality is provided by JP1/Base and might not be supported depending on the version of JP1/Base on the host where the problem occurred. For details, see the *JP1/Base User's Guide*.

The `jcocmdshow` and `jcocmddel` commands can be executed in any of three ways:

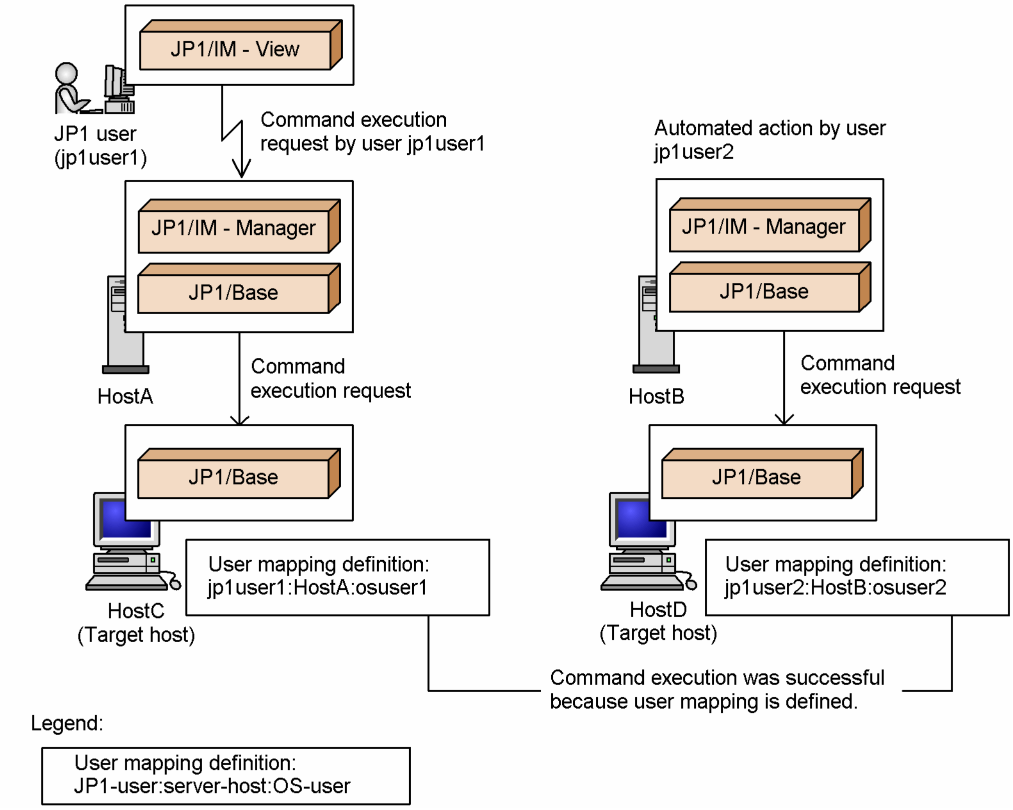
- From JP1/IM - View
  You must specify the `-f` option when you execute the `jcocmddel` command from JP1/IM - View.
- From the manager to an agent target host
  You must specify the `-s` option. Note that in order to execute these commands, the manager must also be running JP1/Base version 07-10 or later.
  Take care when using this option, as communication will take place directly between the manager and agent (using the same communication path as the definition collection and distribution function).
- Directly on the host where the problem occurred

For details about these commands, see the command descriptions in the *JP1/Base User's Guide*.

(7) Conditions for command execution

The following figure summarizes the conditions for executing commands from JP1/IM - View and by automated actions.

Figure 7–17: Conditions for executing commands and automated actions



Conditions for executing commands from JP1/IM - View:

1. The logged-in JP1 user has permission to execute commands.

   JP1 users with `JP1_Console_Admin` or `JP1_Console_Operator` permissions are permitted to execute commands.

2. User mapping is defined on the target host.

   User mapping is defined as follows:

   JP1-user:*server-host*:*OS-user*

   JP1-user is the user who is operating JP1/IM - View, *server-host* is the name of the server host the JP1 user is logged in to, and *OS-user* is the user name of a user or domain user registered on the target host.

3. The system configuration definition is set up (when executing commands on another host).

   If the system configuration is not defined, you will be unable to execute commands on another host from JP1/IM - View.

Conditions for executing commands by automated action from the manager:

1. User mapping is defined on the target host.

   User mapping is defined as follows:

   JP1-user:*server-host*:*OS-user*

   JP1-user is the user who executes the automated action, *server-host* is the name of the server host that issues the instruction to execute the automated action, and *OS-user* is the user name of a user or domain user registered on the target host.

2. The system configuration definition is set up (when executing commands on another host).

   If the system configuration is not defined, you will be unable to execute a command on another host by automated action.

7.4.5 Collecting and distributing definition information

Definition collection and distribution functions provided by JP1/Base are used to collect and distribute information on the hosts that is defined in JP1/Base. Using these functions, you can perform the following operations:

- Collect and distribute event service definitions
- Auto-generate a monitoring tree (by collecting definition information)

Definition collection and distribution is functionality specific to JP1/IM - Manager and provided through JP1/Base. Depending on the JP1/Base version, this functionality might not be supported. For details, see the *JP1/Base User's Guide*.

Note that these definition collection and distribution functions are sometimes called plug-in functions. When you use the JP1/Base `jbs_spmd_status` command to verify the status of the service, look for the displayed name `jbsplugin`.

(1) Collecting and distributing event service definitions

When using JP1/IM to monitor the system operation, you must consider, for each host, which events should be managed as JP1 events and which events should be forwarded to higher-level hosts, and define the event service accordingly. Although you can check and modify definitions in JP1/Base on each host individually, this is highly inefficient and can lead to mistakes in the definitions.

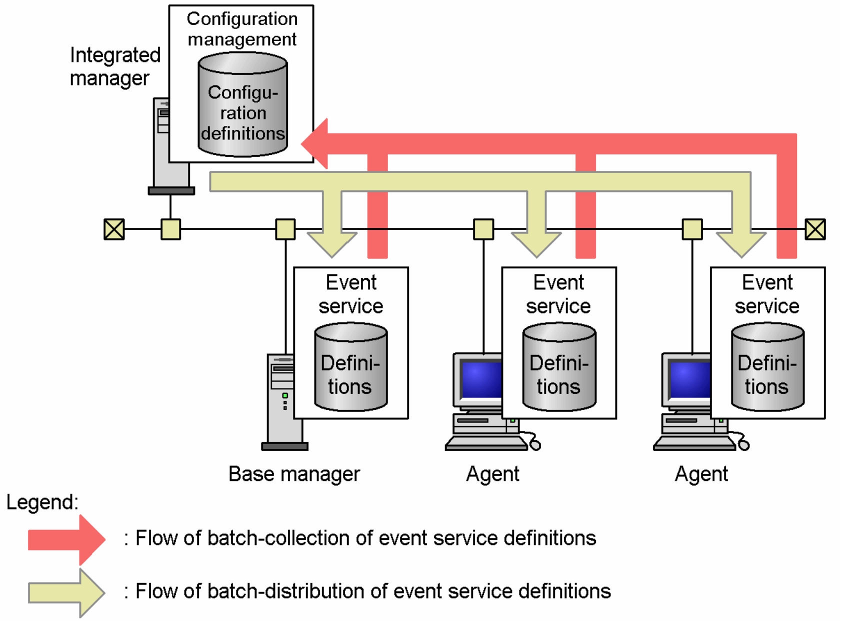
Using the definition collection and distribution functions of JP1/Base, you can batch-collect information defined in JP1/Base on the hosts, and manage the information on the manager. You can also update the definition information on each host by editing and distributing the definition information from the manager. Hence, these functions provide an efficient way of centrally managing definitions related to the event service.

You can collect and distribute definitions from the following files:

- Forwarding setting file (`forward`)
- Action definition file for log file trapping (any file)
- Action definition file for event log trapping (`ntevent.conf`)

The following figure shows the flow of processing when event service definitions are collected from or distributed to all the hosts in the system as a batch operation.

Figure 7–18: Batch-collection and batch-distribution of event service definitions



Working in conjunction with configuration management, the definition collection and distribution functions collect and distribute definitions to the hosts defined in the configuration definition as a batch operation (for details about defining the system configuration, see *7.4.3 Managing the system hierarchy*). When the manager collects definitions from or distributes definitions to managed hosts, it communicates with the hosts directly without regard to the system hierarchy defined in the configuration definition. For this reason, take care when using these functions in a firewall environment.

To collect and distribute event service definitions as a batch operation, use the commands provided by JP1/Base. For details about the procedures and a description of the batch-collection and batch-distribution commands, see the chapter on collecting and distributing event service definitions (JP1/IM only) in the *JP1/Base User's Guide*.

(2) Auto-generation of monitoring trees (Central Scope)

JP1/IM provides the Monitoring Tree window and Visual Monitoring window to allow objective-oriented system monitoring in accordance with the needs of the system administrator. When you create a Monitoring Tree window, you can use the auto-generation function to generate a monitoring tree automatically, and then customize the tree to suit your needs.

The auto-generation function collects definitions relating to specific linked products from each server, and uses a template to create a monitoring tree from the collected information. The collection of definitions is performed as functionality specific to JP1/IM - Manager, realized through the definition collection and distribution functions provided by JP1/Base.

When directed by JP1/IM - Manager to collect definitions from linked products, JP1/Base collects the definitions from the linked products on that host, and passes the information to JP1/IM. This functionality is supported from JP1/Base version 07-00. To collect definitions, the Central Scope service of JP1/IM - Manager must be active (ON).

The following are examples of the definition information that can be collected and distributed:

- Information about jobs that are being executed automatically by JP1/AJS
- Category information and application information that are monitored by JP1/Cm2/SSO version 8 or earlier
- Performance data being monitored by JP1/PFM
- System information in a Cosminexus environment (logical servers, J2EE applications, and so on)

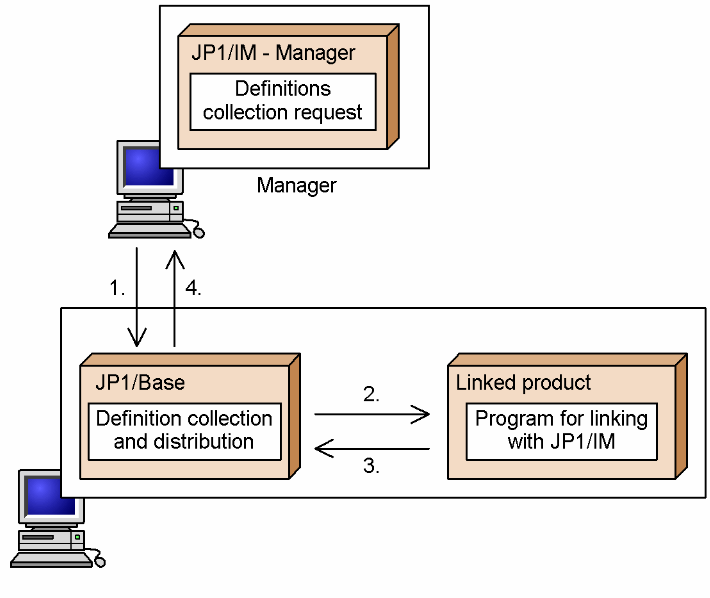
A monitoring tree is created automatically from this information collected from the hosts defined in the system hierarchy.

The collection of definition information from linked products is realized by interaction between the JP1/IM functionality and the configuration management and definition collection and distribution functions of JP1/Base. How these functions interact with each other is explained in *4.11.4 Automatic generation of a monitoring tree*.

The behavior of JP1/Base on a target host when directed by JP1/IM to collect definition information is described below.

The following figure shows the flow of the processing to collect definition information within each host.

Figure 7–19: Collection of definition information within a host


JP1/IM - Manager
Definitions collection request
Manager
1.
4.
JP1/Base
Definition collection and distribution
2.
3.
Linked product
Program for linking with JP1/IM

The flow of processing is described below, following the numbers in the figure:

1. The host receives a definitions collection request from the manager.
2. On receiving the request, JP1/Base requests definition information from any linked product on that host that supports the JP1/IM definition collection and distribution functions.
3. The linked product that receives the request starts the JP1/IM linkage program to send back the relevant information to JP1/Base.

   To start the JP1/IM linkage program, a command that sets up JP1/IM linkage must have been executed on the linked product. For details about the command that sets up JP1/IM linkage, see the documentation for the linked product.
4. On receiving the definitions from the linked product, JP1/Base passes the information back to the manager that issued the request.

7.4.6 Managing service startup (Windows only)

JP1/Base provides startup control for services.

In Windows, the functions of JP1/IM - Manager and JP1/Base are registered as Windows services at installation. By using the Windows service control manager, you can set services to start automatically when the OS starts. However, you cannot set services to start in a particular order (for example, JP1/Base before JP1/IM - Manager) because Windows does not monitor service dependencies. In some cases, a product that issues JP1 events might start before JP1/Base starts. Because JP1/Base is inactive, such JP1 events cannot be managed. To avoid such situations, use the startup control provided by JP1/Base in Windows systems.

For details about JP1/Base startup control, see the chapter on setting the service start and stop sequences (for Windows only) in the *JP1/Base User's Guide*.

In UNIX-based operating systems, you can use an OS function to control the sequence in which services such as JP1/Base and JP1/IM - Manager start and stop, by registering the services in scripts.

7.4.7 Hitachi Network Objectplaza Trace Library (HNTRLib2)

JP1/Base and JP1/IM provide the Hitachi Network Objectplaza Trace Library (HNTRLib2) to help investigate the cause of errors.

The Hitachi Network Objectplaza Trace Library (HNTRLib2) outputs trace information from the various functions of JP1/Base and JP1/IM to a single *integrated trace log*. The collection of trace information for related products in a coherent manner allows you to gain an overview of what is happening throughout the system, which is of particular value in the initial stages of tracking down a problem. As follows are potential applications of the trace library:

1. Investigating the entire system
   Investigate each host machine based on entries in the Windows event log or UNIX syslog.

2. Investigating JP1 products in the JP1 series
   Investigate JP1 products by checking the flow of operations in the Hitachi Network Objectplaza Trace Library (HNTRLib2).

Each of the JP1 product functions make use of an internal log in addition to the integrated trace log. In combination, these logs allow you to investigate problems in detail. To facilitate the collection of this data in the event of a problem, prepare the JP1/Base and JP1/IM data collection tools when you set up the system.

The Hitachi Network Objectplaza Trace Library (HNTRLib2) is installed when you install JP1/Base or JP1/IM - View, but is also used by JP1/AJS and other Hitachi products. For details about whether a product uses the Hitachi Network Objectplaza Trace Library (HNTRLib2), see the relevant product manual.

7.4.8 JP1/Base health check function

The JP1/Base health check function monitors JP1/Base processes for hangups#, abnormal termination, and other problems, and issues a message or JP1 event to report the error and prompt the operator to take recovery action. By using this function, JP1/IM can check whether the instances of JP1/Base in the JP1/IM system are operating normally. The health check function is disabled by default. Enable the function by changing the setting in the common definition information.

#: Hangups are caused by a deadlock or infinite loop, and mean that the process can no longer accept processing requests.

This subsection gives an overview of the JP1/Base health check function. For details about how the function works and how to set it up, see the chapter on setting the health check function in the *JP1/Base User's Guide*.

Broadly classified, the JP1/Base health check function has two roles:

- Monitoring the status of JP1/Base processes on the local host
- Monitoring the status of JP1/Base processes on remote hosts

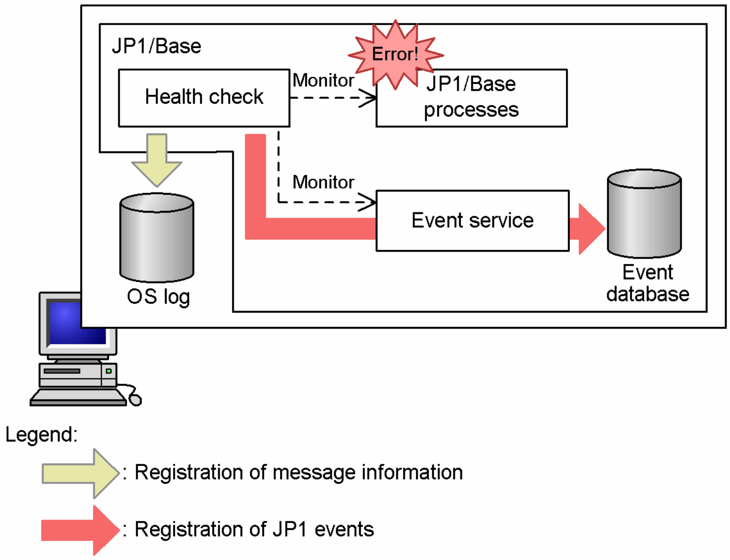
Depending on the JP1/Base version, this functionality might not be supported. For details, see the *JP1/Base User's Guide*.

(1) Monitoring the status of JP1/Base processes on the local host

By enabling the health check function, you can detect hangups and abnormal terminations in JP1/Base processes on the local host. This information is registered in the operating system's log (the Windows event log or UNIX syslog) as message information, or in the event database as JP1 events, depending on how JP1/Base is set up.

The figure below shows how JP1/Base processes are monitored on the local host.

Figure 7–20: Monitoring the status of JP1/Base processes on the local host



By recording errors that affect JP1/Base as JP1 events in the event database, you can use JP1/IM to monitor JP1/Base for errors.

The health check function is unable to monitor the status of other processes if the function itself hangs or terminates abnormally. Also, JP1 events cannot be registered if an error occurs in the event service.

To avoid this type of situation, the health check function and the event service must be monitored by the health check function of JP1/Base on a remote host.

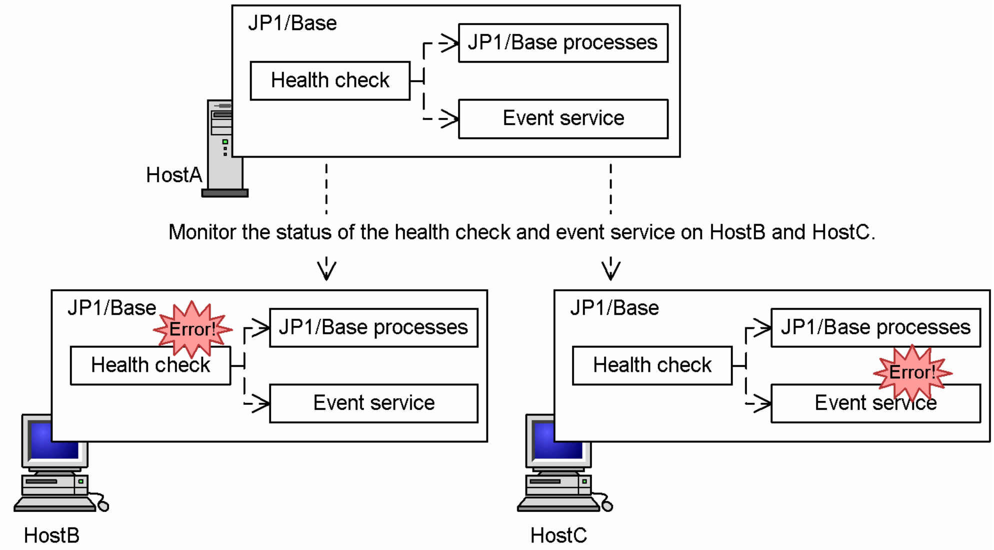
(2) Monitoring the status of JP1/Base processes on remote hosts

The JP1/Base health check function can monitor the status of the JP1/Base health check function and the event service on remote hosts, as well as the JP1/Base processes on the local host. Thus, you can prevent situations in which errors in JP1/Base processes are overlooked because of an error in the health check function, or JP1 events are not registered because of an error in the event service.

If you are using JP1/Base version 09-00 or later, you can suppress monitoring when the monitoring target stops normally. For details, see the *JP1/Base User's Guide*.

The figure below shows how JP1/Base processes are monitored on remote hosts.

Figure 7–21: Monitoring the status of JP1/Base processes on remote hosts



The above figure shows a configuration in which the health check functions and event services of HostB and HostC are monitored from HostA. When an error occurs in the health check function on HostB, HostA detects the error and records the particulars in its own OS log or event database. When an error occurs in the event service on HostC, HostA detects the error and records the particulars in its own OS log or event database#.

#: In this situation, JP1 events cannot be registered in the event database on HostC. However, log information can still be registered in the OS log provided that the health check function is working normally.

In this manner, JP1/Base detects errors in JP1/Base processes.

7.4.9 JP1/Base process management

Process management is a core functionality of JP1/Base that starts and stops the processes that make up JP1/Base. Another responsibility of process management is to issue instructions for checking the status of JP1/Base functions and reloading definition information.

JP1/Base process management controls the following functions:

- User management (`jbssessionmgr`) (also referred to as the authentication server)
- Configuration management (`jbsroute`)
- Command execution (`jcocmd`)
- Definition collection and distribution (`jbsplugin`)
- Health check (`jbshcd` and `jbshchostd`)

The event service, event converters, and Hitachi Network Objectplaza Trace Library (HNTRLib2) operate independently of the process management functionality. For details, see the *JP1/Base User's Guide*.

Process management is realized by the following commands:

Table 7–14: Process management commands

Functionality	Command	Description
Start JP1/Base (internal command)	`jbs_spmd` (For UNIX only)	Internal commands used to start and stop JP1/Base processes. These commands apply to the processes managed by process management. Do not execute these commands directly to start or stop JP1/Base process management. In Windows, JP1/Base process management is started and stopped by the Windows service control manager. In UNIX, use the start and stop commands (`jbs_start` and `jbs_stop`).
Stop JP1/Base (internal command)	`jbs_spmd_stop`	
JP1/Base status check	`jbs_spmd_status`	Checks the activity status of the processes managed by process management.
Reload JP1/Base definition information	`jbs_spmd_reload`	When definition information is updated for a process managed by process management, this command reloads and applies the new definitions.

Process management also provides the following functionality to help detect and deal with errors in JP1/Base.

- Automatically restarting an abnormally ended process
- Issuing a JP1 event when a process error is detected

This functionality applies to the processes under the control of process management, and is supported from JP1/Base version 07-00.

Important

If you are using JP1/Base in a cluster system, do not set up process management to restart processes at abnormal termination, as the error in the JP1/Base process might also affect the function that restarts processes. To ensure a more reliable restart, restart JP1 under the control of the clustering software.

For details about the commands in the table and how to deal with process management errors, see the description of the settings for dealing with JP1/Base errors in the chapter on installation and setup in the *JP1/Base User's Guide*.

8 Linking with Other Products

JP1/IM collects and centrally manages the management information of other software products and the events that occur in the system. JP1/IM also provides a function that enables JP1/IM management information to be used by other integrated management software products, JP1/Service Support, JP1/Navigation Platform, JP1/IM - Rule Operation, VMware vCenter Operations Manager, JP1/AJS, and JP1/PFM.

JP1/Service Support registers and manages an incident when the system generates a JP1 event that is monitored by JP1/IM (the operator troubleshoots the registered and managed incident).

JP1/Navigation Platform displays application information (operating procedures) applicable to the JP1 events monitored by JP1/IM.

JP1/IM - Rule Operation executes troubleshooting processes automatically. When the system generates a JP1 event being monitored by JP1/IM, JP1/IM - Rule Operation judges the JP1 event against a rule startup condition. If the condition is met, JP1/IM - Rule Operation invokes the rule and executes the process prescribed in the rule definition.

VMware vCenter Operations Manager displays details of those alerts on the virtualization platform that correspond to the JP1 events being monitored by JP1/IM.

JP1/AJS can display from JP1/IM such JP1/AJS windows as the monitor windows of jobs corresponding to JP1 events.

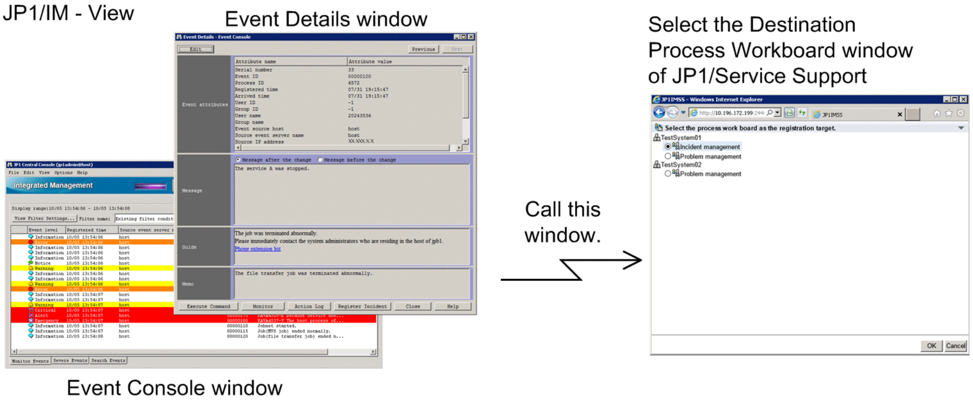
JP1/PFM can display from JP1/IM such JP1/PFM windows as those for displaying the performance reports of event-source hosts corresponding to JP1 events.

This chapter describes the functionality provided by JP1/IM for linking with these products.

8.1 Linking with JP1/Service Support

The Central Console provides a linkage function that enables you to manually register the JP1 events displayed in the event list of JP1/IM - View as incidents in JP1/Service Support. To register a JP1 event as an incident, choose **Register Incident** from the pop-up menu or click the **Register Incident** button in the Event Details window to call the Select the process work board as the registration target window. You can register the incident in this window.

Figure 8–1: Open the Select the process work board as the registration target window from JP1/IM - View



Attribute name	Attribute value
Serial number	33
Event ID	00000100
Process ID	6572
Registered time	07/31 19:15:47
Arrived time	07/31 19:15:47
User ID	-1
Group ID	-1
User name	20243536
Group name	
Event source host	host
Source event server name	host
Source IP address	XX.XXX.X.X

● Message after the change ○ Message before the change

The service A was stopped.

The job was terminated abnormally.
Please immediately contact the system administrators who are residing in the host of jpb1.
Phone extension list

The file transfer job was terminated abnormally.

http://10.196.172.199:244

Select the process work board as the registration target.

TestSystem01
- ● Incident management
- ○ Problem management

TestSystem02
- ○ Problem management

For the settings for calling the Select the process work board as the registration target window in JP1/Service Support, see *9.1.1 Enabling calling the JP1/Service Support window* in the *JP1/Integrated Management - Manager Configuration Guide*. For details about JP1/Service Support, see the *JP1/Service Support Configuration and Administration Guide*.

Note

You can use the functionality for command execution by automated actions in JP1/IM to automatically register JP1 events as incidents in JP1/Service Support.

8.1.1 Attributes of a JP1 event registered as an incident in JP1/Service Support during linkage

When a JP1 event displayed in JP1/IM - View is registered as an incident in JP1/Service Support, the incident automatically inherits attributes of the JP1 event.

In JP1/Service Support, you can register only JP1 events that are registered in the event database of the manager host to which you have logged in from JP1/IM - View or in the integrated monitoring database. You cannot register as incidents either JP1 events that are registered in the event database of an agent host or dummy events, which are events displayed only in JP1/IM - View.

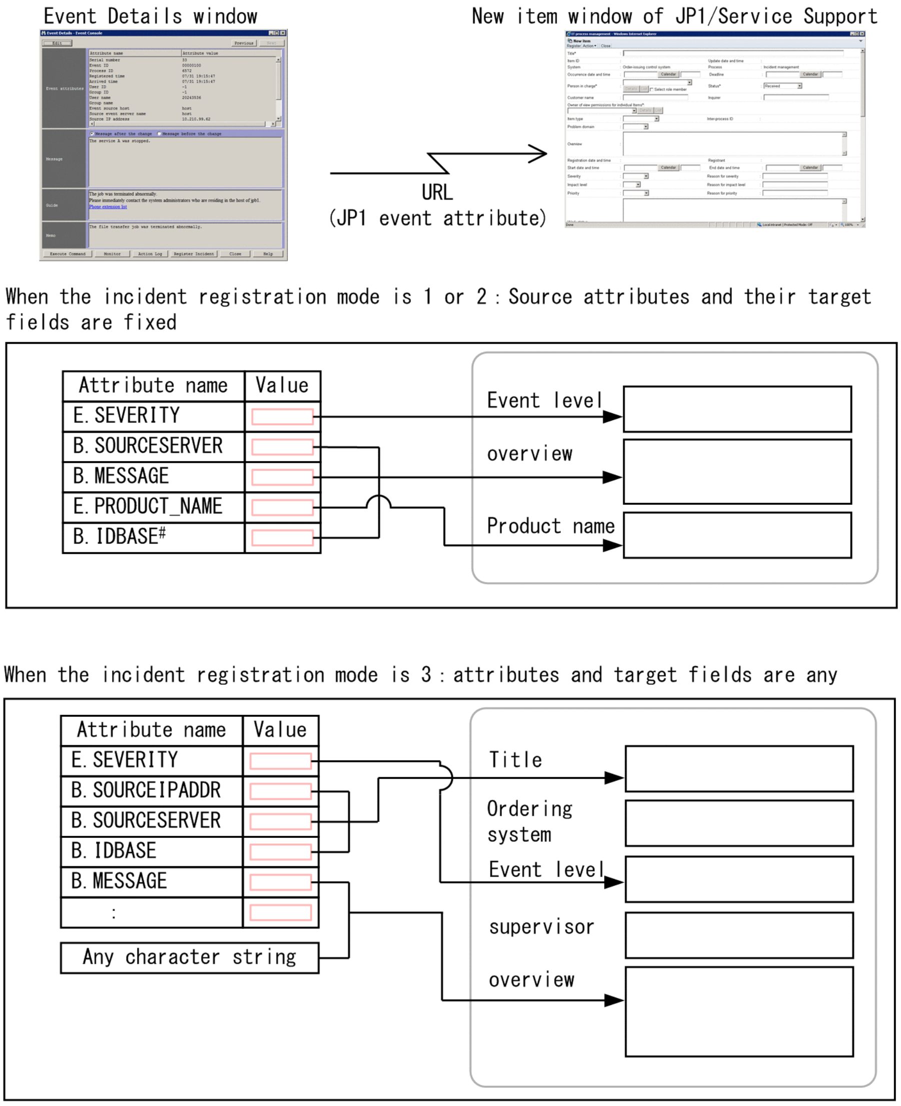
You can select an incident registration mode to control which information to be registered as an incident in JP1/Service Support. The following table describes available incident registration modes and when each mode should be used.

Table 8–1: Incident registration modes and when to use each of them

Incident registration mode	Description	When to use	Supported version of JP1/IM - Manager, JP1/IM - View, and JP1/ Service Support
SS_MODE=1	Source attributes and their target fields are fixed.	The specification of JP1/IM - Manager 10-00 or earlier must be used for linkage with JP1/Service Support.	09-50 or later
SS_MODE=2	• Source attributes and their target fields are fixed. • The event ID (B.IDBASE) is inherited in addition to the attributes that are inherited when SS_MODE=1.	• The event ID is required to be registered. • Linkage with JP1/IM - Manager, JP1/ Service Support, and JP1/Navigation Platform is required.	10-10 or later
SS_MODE=3	• The mapping between source attributes and target fields is configurable. • Multiple attributes can be mapped to one target field. • Any character string you want can be inherited.	• Any attribute or character string you want is required to be registered. • This mode also allows linkage with JP1/IM - Manager, JP1/Service Support, and JP1/Navigation Platform.	11-50 or later

The following figure shows an overview of incident registration modes.

Figure 8–2: Overview of incident registration modes



# This is not inherited when the incident registration mode is 1.

To change the incident registration mode, edit the definition file for manually registering incidents to set the `SS_MODE` parameter to a desired value. When the `SS_MODE` parameter is not set, the incident registration mode is considered to be `1`. For details about the definition file for manually registering incidents (`incident.conf`), see *Definition file for manually registering incidents (incident.conf)* in *Chapter 2. Definition Files* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

(1) JP1 event attributes inherited when the incident registration mode is 1 or 2

The following table describes the JP1 event attributes that are inherited by incidents and the items displayed in the New item window of JP1/Service Support when the incident registration mode is 1 or 2.

Table 8–2: JP1 event attributes inherited by incidents from JP1/IM - View (when the incident registration mode is 1 or 2)

Incident	JP1 event attributes
Event serial number (JIMSD_FORM_IMEVENTNO)	The event serial number (B.SEQNO) of JP1 event is inherited.
JP1/IM - Manager host name (JIMSD_FORM_IMHOSTNAME)	The host name of the JP1/IM - Manager to which you have logged in from JP1/IM - View is inherited. The maximum size of the host name is 255 bytes.
Summary (JIMSD_FORM_SUMMARY)	The following information is inherited: • The event ID of the JP1 event (B.IDBASE)#1 The format is the same as that of the event ID displayed in the Event Details window. • JP1 event message (B.MESSAGE) Maximum of 1,023 bytes • Source event server name (B.SOURCESERVER)#2 Maximum of 255 bytes
Event level (JIMSD_FORM_SEVERITYCODE)	The event level (E.SEVERITY) of the JP1 event is inherited. Event levels are inherited as the following codes: Emergency = 1, Alert = 2, Critical = 3, Error = 4, Warning = 5, Notice = 6, Information = 7, and Debug = 8. Event levels other than these eight are inherited as Information.
Product name (JIMSD_FORM_JP1PRODUCTNAME)	The product name (E.PRODUCT_NAME) of the JP1 event is inherited. The maximum size of the product name is 255 bytes.

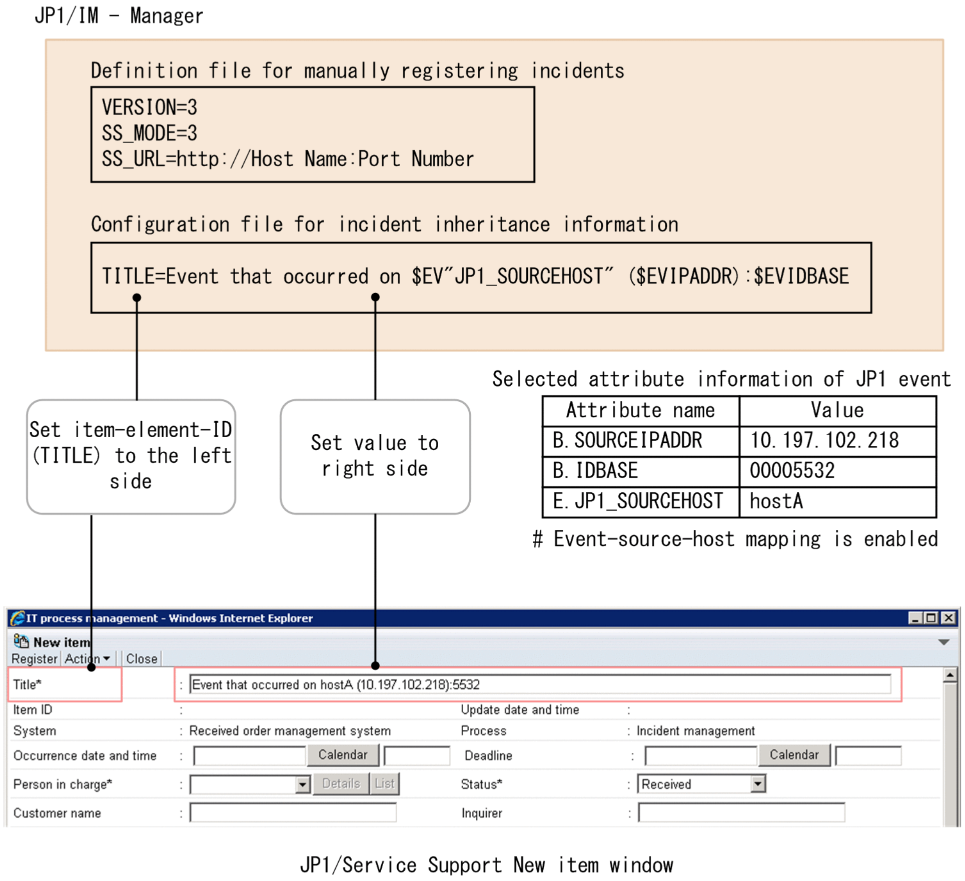
#1: This is not inherited when the incident registration mode is 1.

#2: If mapping is enabled on the source host, the source host name (E.JP1_SOURCEHOST) is inherited instead of the source event server name (B.SOURCESERVER).

(2) JP1 event attributes inherited when the incident registration mode is 3

When the incident registration mode is 3, an incident can inherit any JP1 event attributes and character strings. You can use a configuration file for incident inheritance information (incident_info.conf) to define the mapping between attributes and character strings in JP1 events and the item elements in JP1/Service Support.

Figure 8–3: Relationship between a configuration file for incident inheritance information and the New item window in JP1/Service Support


JP1/IM - Manager
Definition file for manually registering incidents
Configuration file for incident inheritance information
Set item-element-ID (TITLE) to the left side
Set value to right side
Selected attribute information of JP1 event
JP1/Service Support New item window

```
VERSION=3
SS_MODE=3
SS_URL=http://Host Name:Port Number
```

```
TITLE=Event that occurred on $EV"JP1_SOURCEHOST" ($EVIPADDR):$EVIDBASE
```

Attribute name	Value
B.SOURCEIPADDR	10.197.102.218
B.IDBASE	00005532
E.JP1_SOURCEHOST	hostA

Event-source-host mapping is enabled

IT process management - Windows Internet Explorer

New item

Register | Action | Close

Title*	: Event that occurred on hostA (10.197.102.218):5532		
Item ID	:	Update date and time	:
System	: Received order management system	Process	: Incident management
Occurrence date and time	: Calendar	Deadline	: Calendar
Person in charge*	: Details List	Status*	: Received
Customer name	:	Inquirer	:

For details, see *Configuration file for incident inheritance information (incident_info.conf)* in *Chapter 2. Definition Files* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

(3) Matrix of versions for incident registration

The following matrix describes which combinations of versions allow incident registration.

Table 8–3: Matrix of versions for incident registration (Connectivity between JP1/IM - Manager and JP1/IM - View)

Version of JP1/IM - Manager	Incident registration mode	Version of JP1/IM - View			
		Earlier than 09-10	09-50 to 10-00	10-10 to 11-10	11-50 or later
Earlier than 09-10	--	--	--	--	--
09-50 to 10-00	1	--	Y	Y	Y
10-10 to 11-10	1	--	Y	Y	Y
	2	--	R	Y	Y
11-50 or later	1	--	Y	Y	Y
	2	--	R	Y	Y
	3	--	N	N	Y

Legend:

Y: An incident can be registered according to SS_MODE you specified.

R: An incident can be registered but the functionality is limited to the scope of SS_MODE of 1.#

N: Linkage with JP1/Service Support is disabled (neither the **Register Incident** menu nor the **Register Incident** button appears).

--: There is no function to link with JP1/Service Support.

#:

For details about differences between incident registration modes, see *Table 8-1 Incident registration modes and when to use each of them*.

For details about connectivity between JP1/IM - View and JP1/Service Support, see the manual *JP1/Service Support Configuration and Administration Guide*.

(4) Notes on switching the incident registration mode

The maximum length of a URL that is used to call JP1/Service Support is 2,046 characters. The message inherited when the incident registration mode is 2 is shorter than the message inherited when the incident registration mode is 1. This is because the event ID is inherited when the incident registration mode is 2. If an inherited message is truncated before the end, copy the full message displayed in the Event Details window, and then paste it into JP1/Service Support.

8.1.2 Permissions required to manually register incidents in JP1/Service Support

To manually register incidents in JP1/Service Support, you must be one of the following JP1 users:

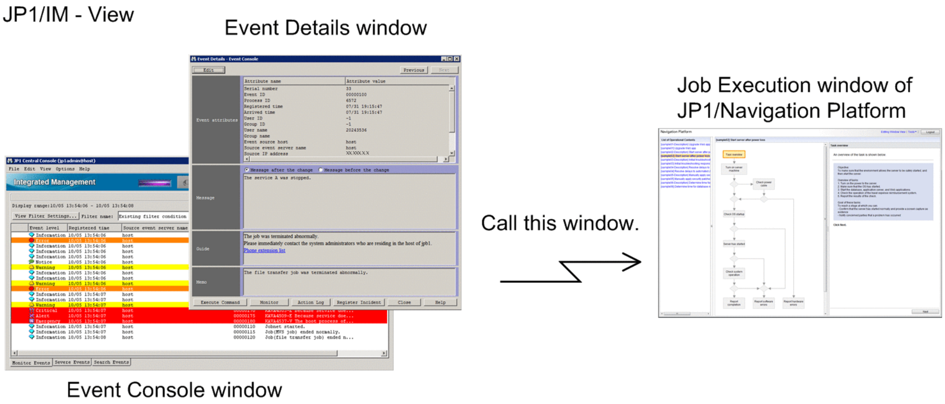
- JP1 user who has JP_Console_Admin permission
- JP1 user who has JP_Console_Operator permission

Also, to use the Select the process work board as the registration target window of JP1/Service Support to register incidents, you must have the view permission and the item creation permission for the process workboard on which items have been registered in JP1/Service Support.

8.2 Linking with JP1/Navigation Platform

The Central Console lets you to view the application information (operating procedure) applicable to a JP1 event displayed in the event list of JP1/IM - View. To view the information, specify the URL of JP1/Navigation Platform in an event-guide message file provided by the event guide functionality.

Figure 8–4: Calling, from JP1/IM - View, the window of JP1/Navigation Platform where work tasks are executed



Display range:10/05 13:54:06 - 10/05 13:54:08

Filter name: Existing filter condition

Attribute name	Attribute value
Serial number	33
Event ID	00000100
Process ID	6572
Registered time	07/31 19:15:47
Arrived time	07/31 19:15:47
User ID	-1
Group ID	-1
User name	20243536
Group name	
Event source host	host
Source event server name	host
Source IP address	XX.XXX.X.X

● Message after the change ○ Message before the change

The service A was stopped.

The job was terminated abnormally.
Please immediately contact the system administrators who are residing in the host of jpb1.
Phone extension list

The file transfer job was terminated abnormally.

```
Event level  Registered time  Source event server name
Information  10/05 13:54:06   host
Error        10/05 13:54:06   host
Information  10/05 13:54:06   host
Information  10/05 13:54:06   host
Information  10/05 13:54:06   host
Notice       10/05 13:54:06   host
Warning      10/05 13:54:06   host
Information  10/05 13:54:06   host
Information  10/05 13:54:06   host
Warning      10/05 13:54:06   host
Error        10/05 13:54:06   host
Information  10/05 13:54:07   host
Information  10/05 13:54:07   host
Warning      10/05 13:54:07   host
Critical     10/05 13:54:07   host   00000170  KAVA4505-E Because service doe...
Alert        10/05 13:54:07   host   00000175  KAVA4509-E Because service doe...
Emergency    10/05 13:54:07   host   00000180  KAVA4537-V The boot process of...
Information  10/05 13:54:07   host   00000110  Jobnet started.
Information  10/05 13:54:07   host   00000115  Job(MVS job) ended normally.
Information  10/05 13:54:08   host   00000120  Job(file transfer job) ended n...
```

To view the application information (operating procedure) by single sign-on, configure the system so that the same authentication server is used for JP1/IM - Manager and JP1/Navigation Platform. Also, on the authentication server, specify 10-10 or later as the JP1/Base version.

The following table lists the combinations of JP1 product versions that permit you to view application information (operating procedures) by single sign-on.

Table 8–4: Combinations of JP1 product versions that permit access to operational content (operating procedures) with a single sign-on

Version	JP1/IM - View 10-00 or earlier			JP1/IM - View 10-10 or later		
	JP1/IM - NP 10-00 (uCNP09-50)	JP1/IM - NP 10-10 (uCNP09-60)	JP1/IM - NP 10-50 or later#1 (HNP10-00 or later)	JP1/IM - NP 10-00 (uCNP09-50)	JP1/IM - NP 10-10 (uCNP09-60)	JP1/IM - NP 10-50 or later#1 (HNP10-00 or later)
JP1/IM - Manager 10-00 or earlier	N			N		
JP1/IM - Manager 10-10 or later	N			N	Y#2	

Legend:

Y: Application information (operating procedures) can be displayed by single sign-on.

N: Application information (operating procedures) cannot be displayed by single sign-on (The JP1/IM - Navigation Platform login window appears).

#1: The product name of JP1/IM - NP will be changed to JP1/Navigation Platform in version 11-00 and later.

#2: Specify the URL for single sign-on in the event-guide message file on the Central Console.

For details about the settings for calling JP1/Navigation Platform's Operational Content Execution window, see the section on the URL for calling Navigation Platform from JP1 products.

Using Navigation Platform and event guide function separately for a specific purpose

To reference a complex operating procedure that is difficult to understand from text alone, link with JP1/Navigation Platform and call the window of JP1/Navigation Platform where work tasks are executed, to view the procedure in an easy-to-understand format. To reference a simple operating procedure, for example, "Contact the system administrator," use the event guide function to directly display the procedure in the **Guide** field of the Event Details window.

8.2.1 JP1 events that can be referenced as application information (operation procedures) when JP1/Navigation Platform is linked

The following JP1 events can be viewed to reference application information (operation procedures):

- JP1 events registered in the integrated monitoring database on the manager host
- JP1 events registered in the event database on the manager host
- JP1 events registered in the event database on agent hosts

The following JP1 events cannot be viewed to reference application information (operating procedures):

- Dummy events displayed only in JP1/IM - View

8.2.2 Permission required to view application information (operating procedures) in JP1/Navigation Platform

If you try to access JP1/Navigation Platform without having the JP1/Navigation Platform user permission, the login window of JP1/Navigation Platform appears.

8.3 Linking with JP1/IM - Rule Operation

The Central Console provides the following functionality used for linking with JP1/IM - Rule Operation:

- Automatically sending rule startup requests to JP1/IM - Rule Operation
- Checking the notification progress and result of such rule startup requests

This functionality is used only for linking with JP1/IM - Rule Operation, and is thus disabled by default.

This section describes this functionality. For details on JP1/IM - Rule Operation, see the *Job Management Partner 1/ Integrated Management - Rule Operation System Configuration and User's Guide*.

Important

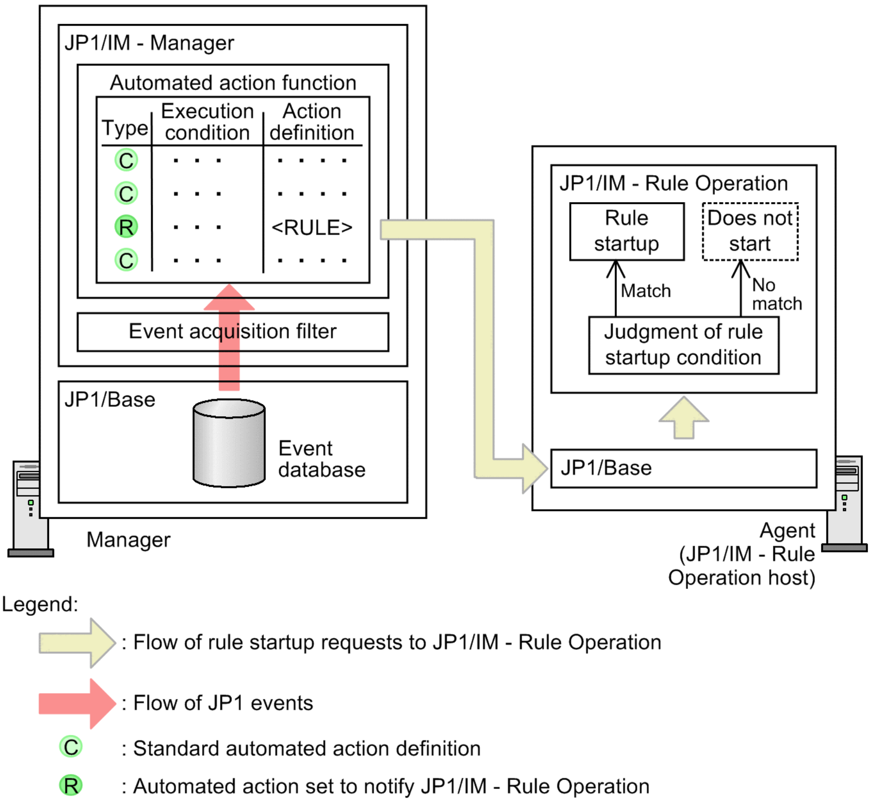
The JP1/IM - Rule Operation linkage function is provided as an extension of the automated action function. For the most part, the setup procedures and flow of processing are the same as for automated actions.

This chapter describes only the characteristics of the JP1/IM - Rule Operation linkage function that differ from automated actions. For details on those that are shared with standard automated actions, see *Chapter 5. Command Execution by Automated Action*.

8.3.1 Sending rule startup requests to JP1/IM - Rule Operation

When JP1/IM - Rule Operation linkage is enabled, rule startup requests are sent to JP1/IM - Rule Operation automatically via automated actions.

Figure 8–5: Overview of JP1/IM - Rule Operation linkage


JP1/IM - Manager
Automated action function
Type
Execution condition
Action definition
C
C
R
C
<RULE>
Event acquisition filter
JP1/Base
Event database
Manager
JP1/IM - Rule Operation
Rule startup
Does not start
Match
No match
Judgment of rule startup condition
JP1/Base
Agent (JP1/IM - Rule Operation host)
Legend:
: Flow of rule startup requests to JP1/IM - Rule Operation
: Flow of JP1 events
C
: Standard automated action definition
R
: Automated action set to notify JP1/IM - Rule Operation

When JP1/IM - Rule Operation linkage is enabled, display items related to JP1/IM - Rule Operation appear in the Action Parameter Detailed Definitions window of JP1/IM - View. This allows you to set the conditions for notifying JP1/IM - Rule Operation.

Once a notification condition has been set, whenever a JP1 event triggers a rule startup request, JP1/IM - Manager automatically sends the request to JP1/IM - Rule Operation.

In JP1/IM - Rule Operation, if the received rule startup request is found to match a rule startup condition, the rule is judged valid and executed.

(1) Enabling and disabling JP1/IM - Rule Operation linkage

To enable or disable JP1/IM - Rule Operation linkage, use the `jcoimdef` command. For details, see *jcoimdef* in *Chapter 1. Commands* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

When you connect from JP1/IM - View to a JP1/IM - Manager with JP1/IM - Rule Operation linkage enabled, display items related to JP1/IM - Rule Operation linkage appear in the following windows:

Additional setup items appear in:

- Action Parameter Definitions window
- Action Parameter Detailed Definitions window

Additional display items appear in:

- Action Log window
- Action Log Details window
- List of Action Results window
- **Search Events** page
- Settings for View Filter window
- Severe Event Definitions window
- Detailed Settings for Event Receiver Filter window

For details about these windows, see *Chapter 2. Event Console Window* in the manual *JP1/Integrated Management - Manager GUI Reference*.

(2) Setting notification conditions for sending rule startup requests to JP1/IM - Rule Operation

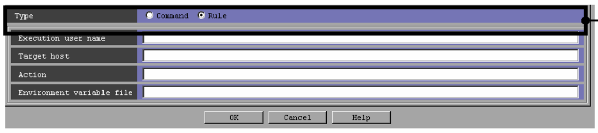
As with standard automated actions, you can set conditions for sending rule startup requests to JP1/IM - Rule Operation in the Action Parameter Detailed Definitions window or in the automated action definition file (`actdef.conf`).

When setting a notification condition to send a rule startup request, include only the JP1 events specified as the rule startup conditions. This ensures that no more than the minimum necessary automated actions will be executed.

Perform the same settings as for a standard automated action, except for the parts shown in the figure below.

Figure 8–6: Condition for sending a startup request to JP1/IM - Rule Operation

Action Parameter Detailed Definitions window



Select Rule as the Type setting in the Action Definition area

Automated action definition file (actdef.conf)

```
DESC_VERSION=3

cmn
      sta false
end-cmn

act Action 1
      prm 0
      eid 123

      cnd
         E.SEVERITY IN Error
      end-cnd

      cmd C:tempsample.exe
end-act

act Action 2
      prm 0
      eid 777

      cnd
         E.SEVERITY IN Critical
      end-cnd

      cmd C:\temp\sample2.exe
end-act

act Action 3
      prm 0
      eid 555

      cnd
         E.SEVERITY IN Emergency Alert Critical Error Warning
      end-cnd

      rul
end-act
```

rul: Set to send a startup request to JP1/IM - Rule Operation#

Legend:

🟧 : Event monitoring condition

🟨 : Action definition

#: The definition sends a startup request to JP1/IM - Rule Operation under the following conditions:
- Event ID: 555
- Event level of JP1 event: Warning, Error, Critical, Alert, or Emergency

The following items, although used when setting an automated action, must be set in a particular way when setting a condition for sending a startup request to JP1/IM - Rule Operation:

- Execution user: Specify a JP1 user mapped to an OS user on the target JP1/IM - Rule Operation host. Set this user by the `jcoimdef` command.
- Target host: Specify the target JP1/IM - Rule Operation host. Set this host by the `jcoimdef` command. Unlike automated actions, you cannot specify a host group.
- Action: Fixed as `<RULE>`. When JP1/IM - Rule Operation receives a startup request, it executes an internal command using as arguments the JP1/IM - Manager host name, the serial number of the JP1 event that triggered the request, and the arrived time.
- Environment variable file: You cannot specify an environment variable file.

For details about the Action Parameter Detailed Definitions window, see *2.33.1 Action Parameter Detailed Definitions window* in the manual *JP1/Integrated Management - Manager GUI Reference*. For details about the definition file, see *Automated action definition file (actdef.conf)* in *Chapter 2. Definition Files* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

(3) Flow of notification processing

As is usual with automated actions, notification processing for JP1/IM - Rule Operation is performed according to the system hierarchy (IM configuration) definition. The status transitions of the communication processing are the same as for a standard automated action.

8.3.2 Checking the status and result of notification to JP1/IM - Rule Operation

You can check the status and result of notification to JP1/IM - Rule Operation using the following windows and command:

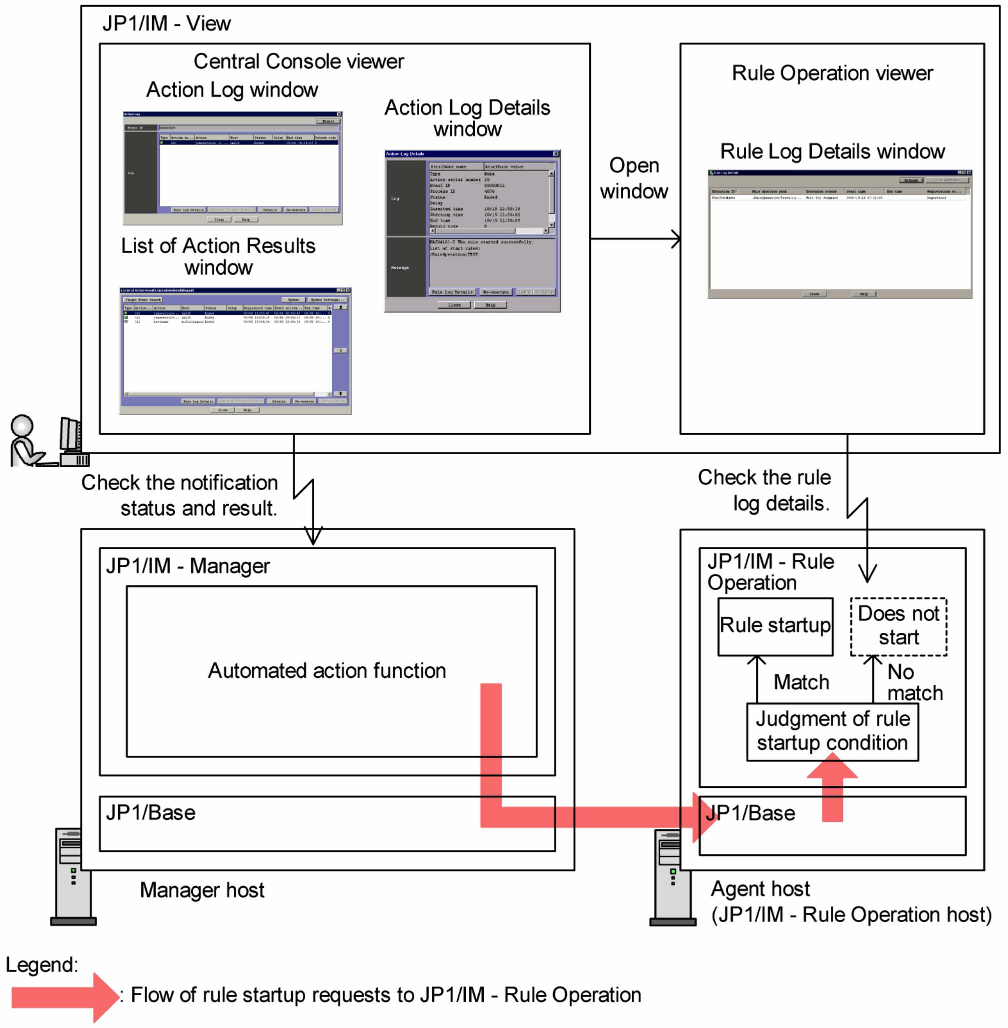
- Action Log window
- Action Log Details window
- List of Action Results window
- `jcashowa` command

For details about how to interpret the notification status and result, see *Chapter 2. Event Console Window* in the manual *JP1/Integrated Management - Manager GUI Reference* and *Chapter 1. Commands* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

When the following conditions are satisfied, you can open the Rule Log Details window, which serves as the GUI for JP1/IM - Rule Operation, from any of the three windows listed above. You can then view the execution status of the rule:

- The **Type** of the automated action is R (**Rule**).
- The **Return code** of the automated action is `0`.
  You cannot open the Rule Log Details window when the return code is non-zero as rule startup will not have occurred.

Figure 8–7: Checking the notification status and result and checking the rule log details


JP1/IM - View
Central Console viewer
Action Log window
Action Log Details window
List of Action Results window
Open window
Rule Operation viewer
Rule Log Details window
Check the notification status and result.
Check the rule log details.
JP1/IM - Manager
Automated action function
JP1/Base
Manager host
JP1/IM - Rule Operation
Rule startup
Does not start
Match
No match
Judgment of rule startup condition
JP1/Base
Agent host
(JP1/IM - Rule Operation host)
Legend:
: Flow of rule startup requests to JP1/IM - Rule Operation

When you open the JP1/IM - Rule Operation window from JP1/IM - View, you are logged in according to the authentication information in JP1/IM - View. Note that JP1/IM - View authentication information is invalidated when:

- The authentication server that you are logged in to is restarted.
- The information is reloaded by the `jbs_spmd_reload` command on the authentication server that you are logged in to.
- The primary authentication server that you are logged in to is switched to the secondary authentication server.

When the authentication information in JP1/IM - View is invalid, the operations you can perform depend on the product versions, as follows:

- When JP1/IM - Manager and JP1/IM - View are both version 08-10 or later, you are automatically re-authenticated and authentication information is re-acquired in JP1/IM - View.
- When either JP1/IM - Manager or JP1/IM - View is version 08-01 or earlier, authentication fails on the JP1/IM - Rule Operation side.

8.3.3 Monitor startup of JP1/IM - Rule Operation

JP1/IM - Rule Operation issues a JP1 event whenever a rule starts, ends, or ends abnormally. In JP1/IM, you can launch the Rule Operation viewer from these types of JP1 events displayed in JP1/IM - View by choosing the `Monitor` command or **Monitor** button.

8.4 Linking with VMware vCenter Operations Manager

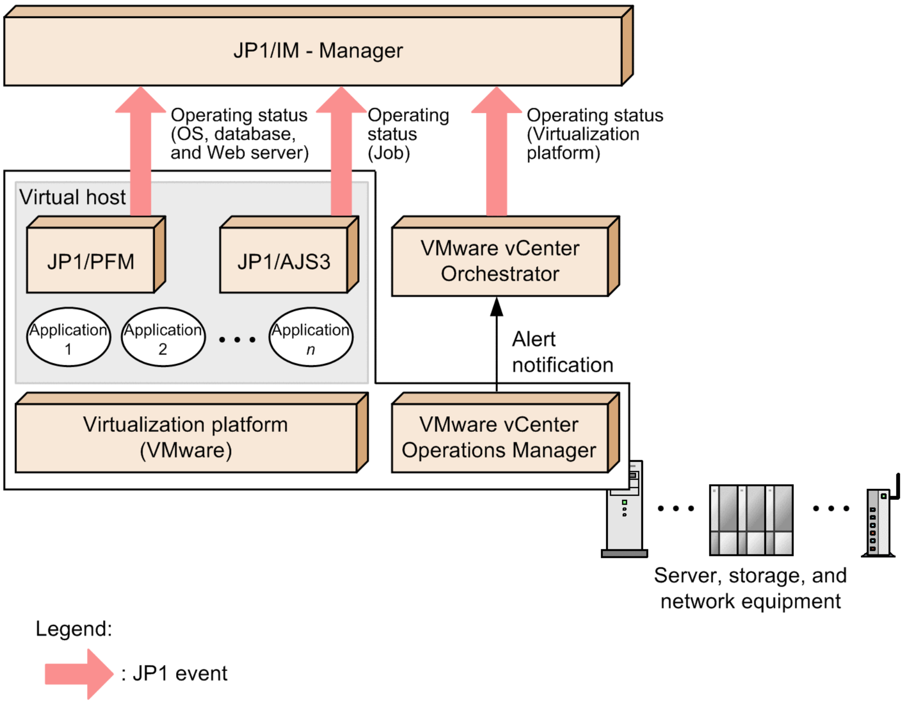
Through linkage with VMware vCenter Operations Manager, the Central Console can centrally manage not only the operation status of a business system but also the operation status of the virtualization platform managed by VMware vCenter Operations Manager.

To centrally manage the operation status of a virtualization platform by the Central Console, the alerts issued by VMware vCenter Operations Manager must be sent to VMware vCenter Orchestrator and converted into JP1 events by VMware vCenter Orchestrator. The `jevsend` command of JP1/Base is used for the conversion of the alerts into JP1 events by VMware vCenter Orchestrator.

For details about the `jevsend` command, see the chapter for commands in the *JP1/Base User's Guide*.

For details about how to execute a command when VMware vCenter Orchestrator receives an alert, see the documentation for VMware vCenter Orchestrator.

Figure 8–8: Overview of the linkage between JP1/IM - Manager and VMware vCenter Operations Manager

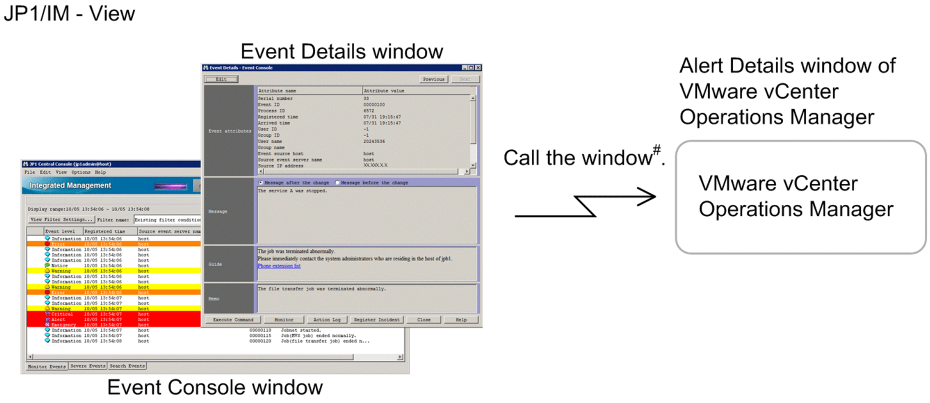

JP1/IM - Manager
Operating status (OS, database, and Web server)
Operating status (Job)
Operating status (Virtualization platform)
Virtual host
JP1/PFM
JP1/AJS3
Application 1
Application 2
Application n
VMware vCenter Orchestrator
Alert notification
Virtualization platform (VMware)
VMware vCenter Operations Manager
Server, storage, and network equipment
Legend:
: JP1 event

You can check the operation status of the virtualization platform by calling the alert details window of VMware vCenter Operations Manager from the Event Details window for a JP1 event managed in the Central Console.

Calling the alert details window of VMware vCenter Operations Manager from the Event Details window for a JP1 event requires setting the information to call that window as an extended attribute of the JP1 event when issuing the JP1 event.

For the information needed to call the alert details window of VMware vCenter Operations Manager, see the documentation for VMware vCenter Operations Manager.

Figure 8–9: Calling VMware vCenter Operations Manager from JP1/IM - View


JP1/IM - View
Event Details window
Event Console window
Call the window#.
Alert Details window of VMware vCenter Operations Manager
VMware vCenter Operations Manager

Event Details - Event Console

Attribute name	Attribute value
Serial number	33
Event ID	00000100
Process ID	6572
Registered time	07/31 19:15:47
Arrived time	07/31 19:15:47
User ID	-1
Group ID	-1
User name	20243536
Group name	
Event source host	host
Source event server name	host
Source IP address	XX.XXX.X.X

Message: ● Message after the change ○ Message before the change

The service A was stopped.

Guide: The job was terminated abnormally.
Please immediately contact the system administrators who are residing in the host of jpb1.
Phone extension list

Memo: The file transfer job was terminated abnormally.

JP1 Central Console (jp1admin@host)

Display range:10/05 13:54:06 - 10/05 13:54:08

Event level	Registered time	Source event server name
Information	10/05 13:54:06	host
Error	10/05 13:54:06	host
Information	10/05 13:54:06	host
Information	10/05 13:54:06	host
Information	10/05 13:54:06	host
Notice	10/05 13:54:06	host
Warning	10/05 13:54:06	host
Information	10/05 13:54:06	host
Information	10/05 13:54:06	host
Warning	10/05 13:54:06	host
Error	10/05 13:54:06	host
Information	10/05 13:54:07	host
Information	10/05 13:54:07	host
Warning	10/05 13:54:07	host
Critical	10/05 13:54:07	host
Alert	10/05 13:54:07	host
Emergency	10/05 13:54:07	host
Information	10/05 13:54:07	host
Information	10/05 13:54:07	host
Information	10/05 13:54:08	host

00000110 Jobnet started.
00000115 Job(MVS job) ended normally.
00000120 Job(file transfer job) ended n...

#: When the window is called, the login window of VMware vCenter Operations Manager appears.

8.5 Linking with OpenStack

The Central Console's log file trapping function enables you to monitor failures in the OpenStack base, virtual machines on OpenStack, and physical servers. JP1/PFM is required for performance monitoring.

For details about the log file trapping function, see the description about converting application program log files in the chapter on setting up the event converters in the *JP1/Base User's Guide*.

8.6 Linking with another system that uses the REST API of JP1/AO

The REST API of JP1/AO enables you to change monitoring settings and add users from another system and user-specific windows. REST API is an abbreviation of Representational State Transfer API. This is a web API that uses a form of HTTP/HTTPS communication that has been become increasingly popular in recent years.

JP1/AO also supports creation of user-specific services, enabling use of the REST API according to the operation.

For details about JP1/AO, see the JP1/AO documentation.

8.7 Linking with JP1/AJS

You can use the following functions to link with JP1/AJS:

- Launching linked products by monitor startup

  You can select a JP1 event in the Event Console window to launch the window for the relevant application. For example, if you launch monitor startup by selecting a job execution event in JP1/AJS, the execution status management window for that job is called directly instead of via an upper-level jobnet window. For details about this function, see *3.19.1 Launching a linked product by monitor startup*.
- Tool Launcher

  From the Tool Launcher window in JP1/IM - View, you can launch windows of various applications, including JP1/AJS. For details about this function, see *3.19.2 Tool Launcher*.
- Event guide function

  By clicking the URL of the JP1/AJS - Web Console that is displayed in the event guide information on Central Console, this function enables you to display the JP1/AJS - Web Console monitor window that corresponds to a JP1/AJS job or jobnet. When displaying the JP1/AJS - Web Console monitor window, you can also display it directly using the single sign-on.
- Automated action function (email transmission)

  This function enables the JP1/AJS - Web Console monitor window to be displayed directly from a sent email by specifying in the email text the URL of the JP1/AJS - Web Console monitor window that corresponds to the JP1/AJS job or jobnet.

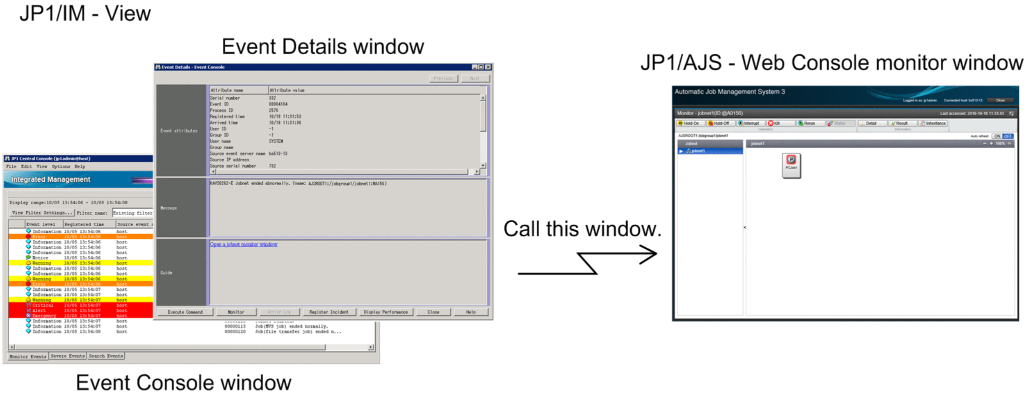
This section explains how to use JP1/AJS to link with the event guide function and the automated action function.

8.7.1 Displaying a monitor window from event guide information (event guide function)

By clicking the URL of the JP1/AJS - Web Console that is displayed in the event guide information, the user can now display the JP1/AJS - Web Console monitor window that corresponds to a JP1/AJS job or jobnet in Central Console (single sign-on).

To display the JP1/AJS - Web Console monitor window, users also can use single sign-on to directly display the window. This subsection assumes that single sign-on is enabled to display the JP1/AJS - Web Console monitor window from the event guide information.

Figure 8–10: Displaying a monitor window from JP1/IM - View



Attribute name	Attribute value
Serial number	332
Event ID	00004104
Process ID	2576
Registered time	10/19 11:31:53
Arrived time	10/19 11:31:36
User ID	-1
Group ID	-1
User name	SYSTEM
Group name	
Source event server name	bs513-13
Source IP address	
Source serial number	732

KAVS0262-E Jobnet ended abnormally. (name: AJSROOT1:/jobgroup1/jobnet1:@A156)

Open a jobnet monitor window

(1) Prerequisites for displaying a monitor window from event guide information

The following are the prerequisites for using single sign-on to display a JP1/AJS - Web Console monitor window from event guide information:

- The version of JP1/IM - Manager, JP1/IM - View, and JP1/AJS - Web Console must be 11-10 or later.
- The prerequisites for JP1/AJS - Web Console must be satisfied.
- The same authentication server must be used for JP1/IM - Manager and the target JP1/AJS - Web Console.
- The JP1 user logged in to JP1/IM - Manager must have the permissions required to display event guide information.
- The JP1 user logged in to JP1/IM - Manager must have the permissions required to display the target window.

(2) Setting for displaying a monitor window from event guide information

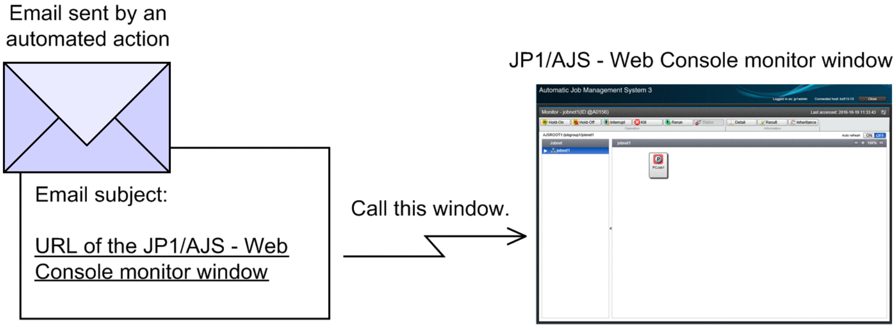
To display a JP1/AJS - Web Console monitor window from a URL in the event guide information, you must specify the URL for linking JP1/AJS - Web Console in the event guide message file.

For details about the setting, see the JP1/AJS documentation.

8.7.2 Displaying a monitor window from an email sent by an automated action (automated action function)

By using the event inheritance information for automated actions to specify in email text the URL of the JP1/AJS - Web Console monitor window that corresponds to the JP1/AJS job or jobnet, the monitor window can now be displayed from a sent email.

Figure 8–11: Displaying the monitor window from an email sent by an automated action


Email sent by an automated action
Email subject:
URL of the JP1/AJS - Web Console monitor window
Call this window.
JP1/AJS - Web Console monitor window

(1) Prerequisites for displaying a monitor window from an email sent by an automated action

The following are the prerequisites for displaying a monitor window from an email sent by an automated action:

- The version of JP1/IM - Manager and JP1/AJS - Web Console must be 11-10 or later.
- The prerequisites for JP1/AJS - Web Console must be satisfied.

(2) Setting for displaying a monitor window from an email sent by an automated action

To display the monitor window from an email sent by an automated action, you have to specify in the email's text the URL of the JP1/AJS - Web Console monitor window.

For details about these settings, see the JP1/AJS documentation.

8.8 Linking with JP1/PFM

You can use the following functions to link with JP1/PFM:

- Launching linked products by monitor startup

  You can select a JP1 event in the Event Console window and launch the window for the relevant application. In JP1/PFM, you can display in the JP1/PFM - Web Console window the reports associated with the alarm events issued by JP1/PFM. For details about this function, see *3.19.1 Launching a linked product by monitor startup*.
- Tool Launcher

  From the Tool Launcher window in JP1/IM - View, you can launch windows of various applications, including JP1/PFM. For details about this function, see *3.19.2 Tool Launcher*.
- Event-source host performance report display function

  This function (referred to as *single sign-on*) enables you to directly display the JP1/PFM - Web Console report window that indicates the performance of a selected event-source host at the time of an event.

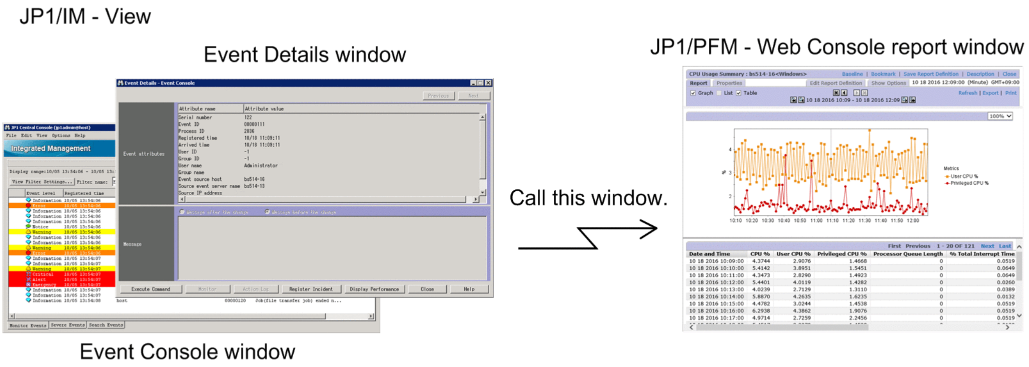
Before JP1/PFM - Web Console reports can be displayed, the performance data to be displayed in reports must be collected and stored. For details about the performance data settings for displaying reports, see the JP1/PFM documentation.

This section explains how to use JP1/PFM to link with the event-source host performance report display function.

8.8.1 Displaying the performance reports of event-source hosts

The user can now display the JP1/PFM - Web Console report window that indicates the performance of a selected event-source host at the time of an event directly in Central Console (single sign-on).

Figure 8–12: Displaying a report window from JP1/IM - View



Attribute name	Attribute value
Serial number	122
Event ID	00000111
Process ID	2836
Registered time	10/18 11:09:11
Arrived time	10/18 11:09:11
User ID	-1
Group ID	-1
User name	Administrator
Group name	
Event source host	bs514-16
Source event server name	bs514-13
Source IP address	

CPU Usage Summary : bs514-16<Windows>

10 18 2016 12:09:00 (Minute) GMT+09:00

☑ Graph □ List ☑ Table

10 18 2016 10:09 - 10 18 2016 12:09

Date and Time	CPU %	User CPU %	Privileged CPU %	Processor Queue Length	% Total Interrupt Time
10 18 2016 10:09:00	4.3744	2.9076	1.4668	0	0.0519
10 18 2016 10:10:00	5.4142	3.8951	1.5451	0	0.0649
10 18 2016 10:11:00	4.3473	2.8290	1.4923	0	0.0649
10 18 2016 10:12:00	5.4401	4.0119	1.4282	0	0.0260
10 18 2016 10:13:00	4.0239	2.7129	1.3110	0	0.0389
10 18 2016 10:14:00	5.8870	4.2635	1.6235	0	0.0132
10 18 2016 10:15:00	4.4782	3.0244	1.4538	0	0.0519
10 18 2016 10:16:00	6.2938	4.3862	1.9076	0	0.0519
10 18 2016 10:17:00	4.9714	2.7259	2.2456	0	0.0519

(1) Prerequisites for displaying the performance reports of event-source hosts

The following are the prerequisites for using the function for displaying the performance reports of event-source hosts:

- The version of JP1/IM - Manager, JP1/IM - View, and JP1/PFM - Web Console must be 11-10 or later.
- The same authentication server must be used for JP1/IM - Manager and the target JP1/PFM - Web Console.
- The authentication mode of the target JP1/PFM must be a JP1 authentication mode that is managed centrally by JP1/Base.
- The user must be able to log in to the target JP1/PFM - Web Console from the JP1/IM - View host.

- The JP1 user logged in to JP1/IM - Manager must have the permissions required to display the target window.

Note that the function for displaying performance reports of event-source hosts is not supported in web-based sessions of JP1/IM - View.

> **Important**
>
> If the system times among the following hosts and servers are not correct and the system time is changed, valid performance reports might not be displayed:
>
> - JP1/IM manager hosts and monitored hosts
> - JP1/PFM monitoring managers, monitoring agents, monitored hosts, and monitoring console server
>
> Synchronize the time throughout the entire system by NTP, and then make sure that the system time is not changed.

(2) JP1 events that can be used to display the performance reports of event-source hosts

You can display the performance reports for event-source hosts from all JP1 events except dummy events.

(3) Hosts subject to display of performance reports

A host subject to display of performance reports must have an event attribute shown in the following table in a selected event. The target event attributes vary according to the settings of the event-source host mapping function.

Table 8–5: Event attributes corresponding to event-source host names

Settings of the event-source host mapping function#	Event attribute
Enabled	Event-source host name (`E.JP1_SOURCEHOST`)
Disabled	Event-issuing server name (`B.SOURCESERVER`)

#: The following notes apply:

- If you have changed the enable/disable setting of the event-source-host mapping function, restart JP1/IM - View and then log in again.
- If you will be enabling the event-source-host mapping function, define mapping in such a manner that the name of the host to be monitored is set as the event-source-host name (`E.JP1_SOURCEHOST`).
- If you will be performing remote monitoring, enable event-source-host mapping.

(4) Timing of the performance reports that are displayed

JP1/PFM displays performance reports for the time specified in the **Registered time** (`B.TIME`) event attribute in the selected event.

The time displayed in performance reports is for the time zone of JP1/PFM - Web Console.

(5) Single sign-on from JP1/IM - View to JP1/PFM - Web Console

When JP1/PFM is linked to display the performance reports of event-source hosts, a JP1 user who is logged in to JP1/IM - Manager from JP1/IM - View is logged in to JP1/PFM - Web Console automatically. If the login processing is successful, the JP1/PFM - Web Console login window is not displayed.

(6) Settings for displaying the performance reports of event-source hosts

To use the event-source host performance report display function, you must define the URLs of the target JP1/PFM - Web Consoles in the performance report display definition file.

For details about the settings, see the JP1/PFM documentation.

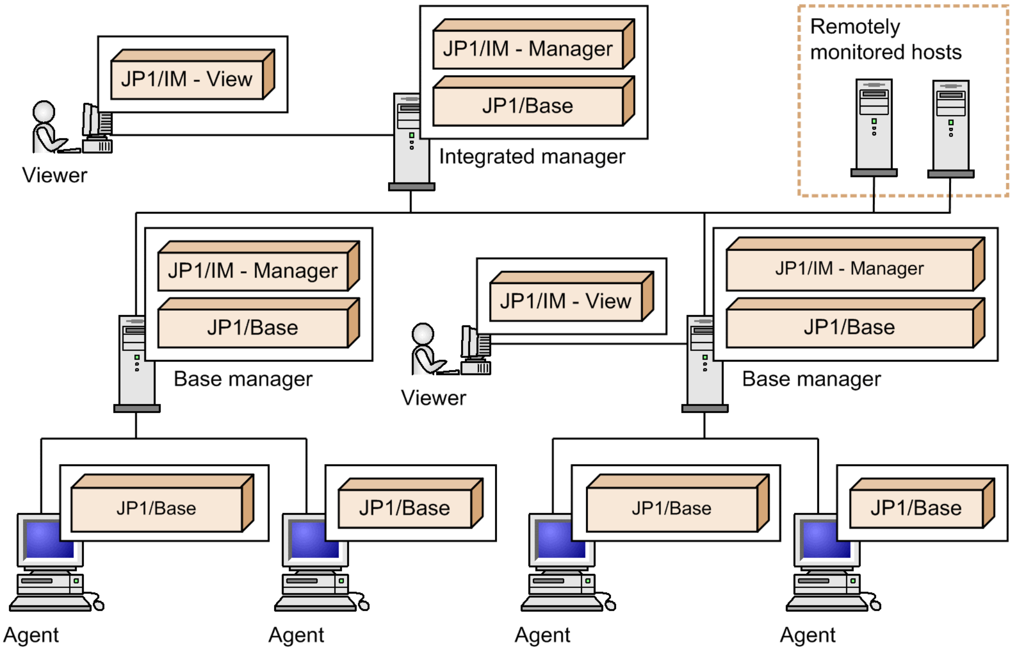
9 JP1/IM Configuration

This chapter describes the configuration and functionality of JP1/IM, and the role played by JP1/Base in the JP1/IM system environment.

9.1 JP1/IM configuration example

This section describes how to configure JP1/IM to perform system operations management.

Figure 9–1: Example of JP1/IM configuration



9.2 Product structure

This section describes the JP1/IM product structure.

9.2.1 JP1/IM product structure

JP1/IM consists of the following products:

- JP1/IM - View
- JP1/IM - Manager
- JP1/Base#

  #: JP1/Base is a prerequisite product for the system that is to be monitored by JP1/IM.

JP1/IM - View

JP1/IM - View is for connecting to JP1/IM - Manager to view or operate on the management information of JP1/IM - Manager.

Some of the functions provided by JP1/IM - Manager for efficient system monitoring can only be set from JP1/IM - View. This includes setting filtering conditions and generating monitoring trees.

JP1/IM - Manager

JP1/IM - Manager provides the components for monitoring the system operation, including the Central Console, Central Scope, and IM Configuration Management.

The following restrictions apply:

- As a prerequisite program, you need the JP1/Base written in the *Release Notes* on the same host.

Web-based JP1/IM - View

This is a light version of JP1/IM - View, provided as a function of the JP1/IM - Manager's Central Console.

The following restrictions apply when you use the Web-based JP1/IM - View in a Web browser:

- You cannot use the Central Scope or IM Configuration Management.
- Some windows, including the Execute Command window and Tool Launcher window, are unavailable. There are also restrictions that disable some operations, such as monitor startup and saving event lists (CSV snapshots). For details, see *Chapter 1. Window Transitions and Login Window* in the manual *JP1/Integrated Management - Manager GUI Reference*.
- Some limits are different. See *Appendix D. Limits*.

9.2.2 Connectivity between JP1/IM products

The following table describes the connectivity, or management relationships, between JP1/IM products.

Table 9–1: Connectivity between viewer and manager products

Viewer product	Manager products that can be connected
JP1/IM - View (version 11)	JP1/IM - Manager (versions 11, 10, and 9)
JP1/IM - View (version 10)	JP1/IM - Manager (versions 11)

Viewer product	Manager products that can be connected
	For connectivity to version 10 or earlier manager products, see the previously published version 10 manuals.
JP1/IM - View (version 9)	JP1/IM - Manager (version 11) For connectivity to version 10 or earlier manager products, see the previously published version 10 manuals.

Table 9–2: Connectivity between manager and agent products

Higher-level manager	Manager and agent products that can be connected or managed
JP1/IM - Manager (version 11)	JP1/IM - Manager (versions 11, 10, and 9) JP1/Base (versions 11, 10, 9)
JP1/IM - Manager (version 10)	JP1/IM - Manager (versions 11) JP1/Base (versions 11) For connectivity to version 10 or earlier manager and agent products, see the previously published version 10 manuals.
JP1/IM - Manager (version 9)	JP1/IM - Manager (version 11) JP1/Base (version 11) For connectivity to version 10 or earlier manager and agent products, see the previously published version 10 manuals.

9.3 Prerequisite operating systems and programs

This section describes the prerequisite operating systems and programs for JP1/IM and JP1/Base.

9.3.1 Prerequisite operating systems

The following table lists the prerequisite operating systems for JP1/IM and JP1/Base. For details, see the *Release Notes* for the applicable products.

Table 9–3: Prerequisite operating systems for JP1/IM

OS	JP1/IM - View	JP1/IM - Manager	JP1/Base[#1]
Windows Server 2008 R2	Y[#2]	Y[#2]	Y
Windows 7	Y[#2]	--	Y
Windows Server 2012	Y[#2]	Y[#2]	Y
Windows 8	Y[#2]	--	Y
Windows 8.1	Y[#2]	--	Y
Windows 10	Y[#2]	--	Y
Windows Server 2016	Y[#2]	Y[#2]	Y
AIX	--	Y	Y
Linux	--	Y	Y

Legend:

Y: Supported.

-- Not supported.

Note: Do not perform at the same time any of the following operations related to the overall system:

- Installing and uninstalling products
- Operations related to the operating environment, such IM database setup
- Changing the system configuration and changing settings that affect the entire system
- Collecting data in response to a problem
- Maintenance tasks, such as system maintenance

#1: The range of supported JP1/Base functionality is OS-dependent. For details, see the *JP1/Base User's Guide*.

#2: Windows Server 2016, Windows 10, Windows 8.1, Windows 8, Windows Server 2012, Windows 7, and JP1/IM - View and JP1/IM - Manager on Windows Server 2008 R2 do not support JIS level 3 kanji or JIS level 4 kanji. If these characters are used in a definition file or as a command argument on JP1/IM - View, the characters might become garbled and not work correctly.

9.3.2 Prerequisite programs

The following table lists the prerequisite programs for JP1/IM and JP1/Base.

Table 9–4: Prerequisite programs for JP1/IM and JP1/Base

Product	Prerequisite programs
JP1/IM - View	To display the windows of a linked program in JP1/IM - View, either of the following is required (depending on the type of linked product): • A JP1 program or other application program to be launched from JP1/IM - View • Web browser
JP1/IM - Manager	• JP1/Base • Web server#
JP1/Base	--

Legend:

--: Not required.

#: Required for the Web-based JP1/IM - View. The Java Runtime Environment (JRE) and the plug-ins bundled with JRE are required in the Web browser (used on the viewer side). For details on the versions and types of Web browser, required JRE, and HTTP server, see the *Release Notes* for JP1/IM - Manager.

9.4 Support for various system configurations

This section describes the various system configurations supported by JP1/IM and JP1/Base.

9.4.1 Firewall support

JP1/IM and JP1/Base can operate in a firewall environment if you perform the appropriate settings in the firewall. Network environments behind packet-filtering and NAT (static mode)-based firewalls are supported. When setting the firewall, see the lists of port numbers in the appendixes of the manuals for JP1/IM and JP1/Base. Also note the following points when setting the firewall:

- There are two methods of communication between the manager and agents: communication performed according to the system hierarchy (IM configuration) definition and direct communication where the manager and the target hosts communicate directly (see *7.3 Communication performed in the JP1/IM system environment*). You must set up the firewall in a manner that allows both types of communication.
- JP1/IM and JP1/Base use ports to communicate even when that communication takes place within a local host. If you use JP1/IM and JP1/Base on a host set up as a firewall, the firewall must permit local traffic through all ports used by JP1/IM and JP1/Base.

If Windows hosts are to be monitored, JP1/IM and JP1/Base are not appropriate for monitoring that must pass through a firewall. We recommend that you set up a network configuration in which the communication between JP1/IM - Manager and monitored hosts is not required to pass through a firewall. Note, however, that DCOM will not work in an environment in which NAT static conversion is executed. Accordingly, if NAT static conversion is executed on a firewall located between JP1/IM - Manager and hosts subject to monitoring, remote monitoring will not be possible.

If you need to perform remote monitoring in an environment subject to NAT static conversion, add an additional base manager so that NAT static conversion is not executed between JP1/IM - Manager and hosts to be monitored, but is executed instead between the integrated manager and the added base manager.

9.4.2 Support for multiple LANs

You can deploy JP1/IM and JP1/Base in network configurations with specific requirements such as the following, by changing the communication settings of JP1/IM and JP1/Base (in a network that allows unrestricted communication between machines, these changes will not be necessary).

Specific requirements:

- Specific communication network

  The JP1/IM - Manager and JP1/Base hosts are connected to multiple LANs, but you require them to communicate over a specific LAN only (using IP addresses other than those associated with the host names).
- Separate network

  The JP1/IM - Manager and JP1/Base hosts are connected to multiple LANs, but you do not want them to communicate across LANs (they cannot communicate using the IP address associated with the destination host name).

For details, see *Appendix F. Support for Changing Communication Settings*.

9.4.3 Operation in a cluster system

JP1/IM can be used in a cluster system.

When JP1/IM is used in a cluster system, a secondary node can take over system operation management if a failure occurs on the primary node.

For details, see *Chapter 6. Operation and Environment Configuration in a Cluster System (for Windows)* or *Chapter 7. Operation and Environment Configuration in a Cluster System (for UNIX)* in the *JP1/Integrated Management - Manager Configuration Guide*.

9.4.4 Logical host operation in a non-cluster environment

A JP1/IM system based on logical hosts is typically a cluster system where JP1/IM is linked with cluster software. However, if you have set up logical hosts running JP1/IM, and have allocated the necessary IP addresses and disk space, JP1/IM can be used in a logical host environment that does not provide failover redundancy or involve linkage with cluster software.

For details, see *6.9 Logical host operation and environment configuration in a non-cluster system (for Windows)* in the *JP1/Integrated Management - Manager Configuration Guide*.

9.4.5 Operation in FQDN format

JP1/IM supports operations in FQDN format.

If multiple machines exist with the same name in a system made up of multiple domains, the names of the monitored hosts are managed in FQDN format.

For details, see *12.3.11 System configuration for managing monitored hosts with host names in FQDN format*.

10 Overview of Design

This chapter gives an overview of the flow of JP1/IM deployment and the design tasks involved.

System operation management takes many forms depending on the work tasks taking place in a given system, and each system also has an operational culture built up over time.

Consider the design tasks so that deploying JP1/IM in an existing system improves the efficiency of operational tasks.

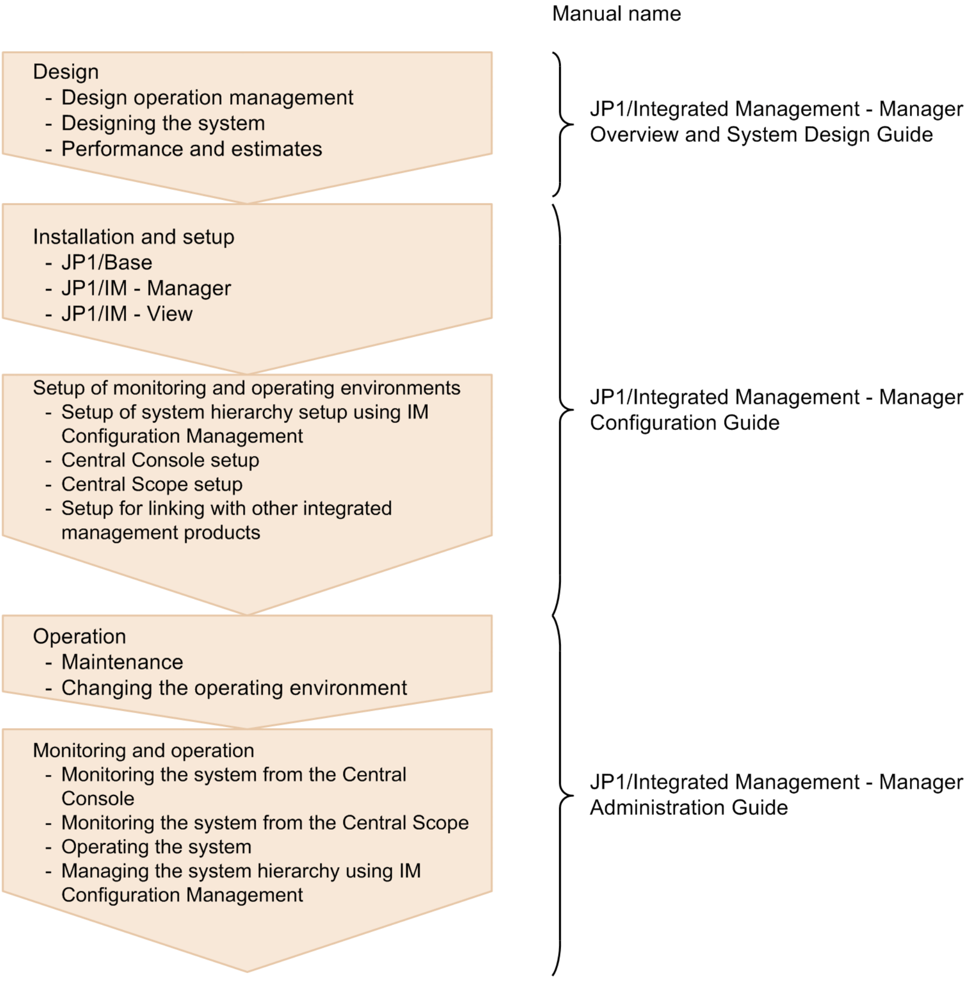
10.1 Flow of JP1/IM deployment

When deploying JP1/IM, follow the tasks set forth in the figure below.

The matters that must be considered and procedures that must be performed in each stage of deployment are described in the corresponding part of the manual.

Schedule individual stages of deployment with an appropriate margin of time.

Figure 10–1: Flow of JP1/IM deployment


Manual name
Design
- Design operation management
- Designing the system
- Performance and estimates
Installation and setup
- JP1/Base
- JP1/IM - Manager
- JP1/IM - View
Setup of monitoring and operating environments
- Setup of system hierarchy setup using IM Configuration Management
- Central Console setup
- Central Scope setup
- Setup for linking with other integrated management products
Operation
- Maintenance
- Changing the operating environment
Monitoring and operation
- Monitoring the system from the Central Console
- Monitoring the system from the Central Scope
- Operating the system
- Managing the system hierarchy using IM Configuration Management
JP1/Integrated Management - Manager Overview and System Design Guide
JP1/Integrated Management - Manager Configuration Guide
JP1/Integrated Management - Manager Administration Guide

10.2 Design considerations

The following table lists the design items to consider when deploying JP1/IM, and the part of the manual where each item is described.

For details, see the corresponding reference for each item.

Table 10–1: Design items

Items to consider at the design stage		Reference
Design related to the JP1/IM integrated monitoring database	Filtering methods	*11.1.3 Considerations for filtering JP1 events*
	JP1 events to be monitored	*11.1.4 Considerations for issuing correlation events*
	JP1 events to be modified	*11.1.8 Considerations for changing JP1 event levels*
	Display messages for JP1 events	*11.1.9 Considerations for changing display messages for JP1 events*
	Storage of event information	*11.1.12 Considerations for saving event information in the integrated monitoring database (output of event report)*
Design related to operation management in JP1/IM	JP1 events to be monitored	*11.1 Considerations for system monitoring using JP1 events*
	Monitoring objects to be monitored	*11.2 Considerations for system monitoring from the Central Scope*
	Action taken by JP1/IM at detection of an error	*11.3 Considerations for error investigation in JP1/IM*
	Automated actions	*11.4 Considerations for automated actions*
Design related to management of the system hierarchy (IM configuration)	How to manage the system hierarchy	*11.5 Considerations for managing the system hierarchy*
	Remote monitoring configuration	*11.5 Considerations for managing the system hierarchy*
	Business group	*11.5.4 Considerations for business groups*
Design related to the JP1/IM system	Operating environment	*12.1 Operating environment considerations*
	Migrating (upgrading) from a previous version of JP1/IM	*12.2 Upgrading from a previous version of JP1/IM*
	System configuration	*12.3 Designing the system configuration*
	Network configuration	*12.4 Network considerations*
	System configuration definition	*12.5 Considerations for the system hierarchy*
	User authentication	*12.6 Considerations for user authentication*
	Designing the environment for JP1/IM and JP1/Base	*12.7 Considerations for the JP1/IM and JP1/Base environments*
	Linking with other integrated management products	*12.8 Considerations for linking with other integrated management products*
	Maintenance	*12.9 JP1/IM maintenance considerations* *12.10 Considerations for JP1/IM system-wide maintenance*
	Encrypted communication	*12.11 Considerations for encrypted communication*

Items to consider at the design stage		Reference
Design related to JP1/IM performance	Performance and estimates	*Chapter 13. Performance and Estimates*

10.3 Overview of design for JP1/IM deployment

This section gives a general idea of the design tasks required when deploying JP1/IM.

When you design for an actual implementation of JP1/IM, you must consider the system configuration and work tasks of the system where JP1/IM is to be deployed. On this basis, plan the deployment in a way that complements the operation of the existing system and improves its efficiency.

10.3.1 Overview of design

There are two aspects to designing JP1/IM deployment: System operation management based on JP1/IM, and the JP1/IM system requirements to achieve those objectives.

- Operation management design (designing JP1/IM-based operation management)
  - Monitoring: What will the system monitor?
  - Error detection and reporting: How will you categorize events occurring in the system and report them for rapid operator response?
  - Investigation and resolution: How will you investigate and resolve problems?

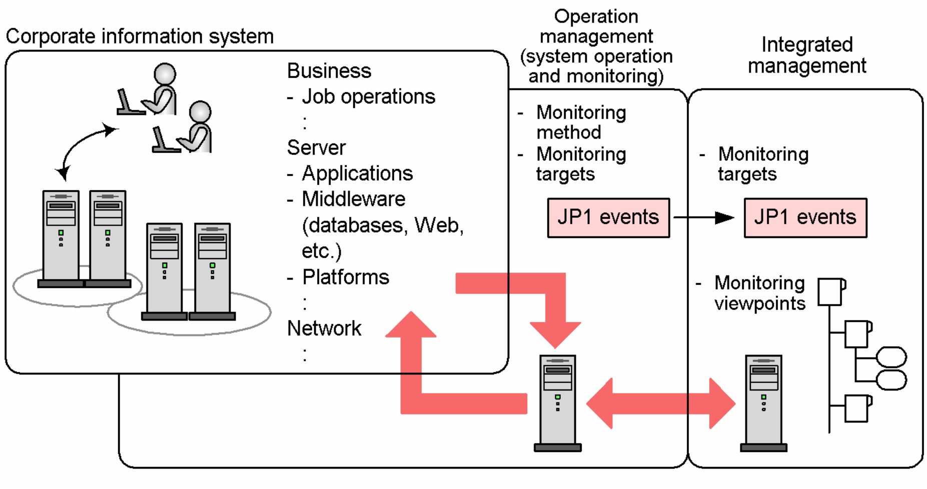
  Consider how to perform these tasks within the system operating cycle using JP1/IM functions.
- System design (designing the JP1/IM system)

  Reliability is imperative when using JP1/IM to manage the operation of a mission-critical system. Consider the JP1/IM system configuration and setup required to ensure that system operation management can be achieved.

10.3.2 Designing monitoring

When designing the system monitoring, consider the elements that must be monitored to ensure reliable operation, the methods to be used, and how monitoring will be managed.

Figure 10–2: Operation management by JP1



(1) Monitoring methods

Consider what elements in the system require monitoring, and in what way, to ensure that the system operates reliably.

System monitoring method:

In considering how the system is to be monitored, you must first analyze the elements that make up the system. Because a system can contain a broad range of elements, you can simplify the process by breaking down the system into a number of layers, such as those shown below, which can then be considered individually.

- Business: The types of jobs executed in the system
- Servers: The software and hardware components
- Network: The network configuration and the types of devices in the network

Next, consider the methods needed to monitor the various elements in the system. You could use a product designed for system management, for example. You could monitor routine business tasks based on information supplied by a job management server, or use tools designed to monitor applications running on a server, for example.

The products in the JP1 series support system operation from a variety of angles, delivering a total support package from system operation to monitoring.

Monitoring by JP1/IM:

JP1/IM manages the system using *JP1 events*.

Consider collecting the events occurring in the system as JP1 events by linking JP1/IM with the other programs that manage the various elements in the system.

You can collect JP1 events across the system by linking with the products in the JP1 series.

Other events, such as messages in log files, SNMP traps, and entries in the Windows event log can be managed by conversion into JP1 events by the JP1/Base event converters.

(2) Monitoring targets

Consider what aspects or items you would need to monitor to ensure that the system is operating in a stable manner.

Monitoring targets:

Assess what sorts of items can be monitored by each monitoring method you considered earlier. For example, a performance management tool can monitor the utilization and load on the resources it monitors.

Consider whether the items each product monitors are set appropriately for the local system. For example, check whether the threshold values defining the level at which resource usage triggers a JP1 event are at a suitable level.

JP1 events:

When you have settled on what items need to be monitored, consider how these items are recorded as values in JP1 events.

For products that issue JP1 events, ascertain how the item name and value are formatted in the JP1 event.

For log files, SNMP traps, or other events that are converted to JP1 events by a JP1/Base event converter, examine how the content of the original event corresponds to the information in the converted JP1 event.

(3) Monitoring viewpoints (when using the Central Scope)

If you wish to use the Central Scope, consider the viewpoints from which you need to monitor the system operation.

The Central Scope enables objective-oriented system monitoring matched to your monitoring viewpoints, and offers visual representation in a tree view in the Monitoring Tree window or map view in the Visual Monitoring window.

Monitoring tree:

The following monitoring trees can be generated using the auto-generation function:

- Work-oriented tree

- Server-oriented tree

You can then customize the tree to suit your needs by adding or deleting elements.

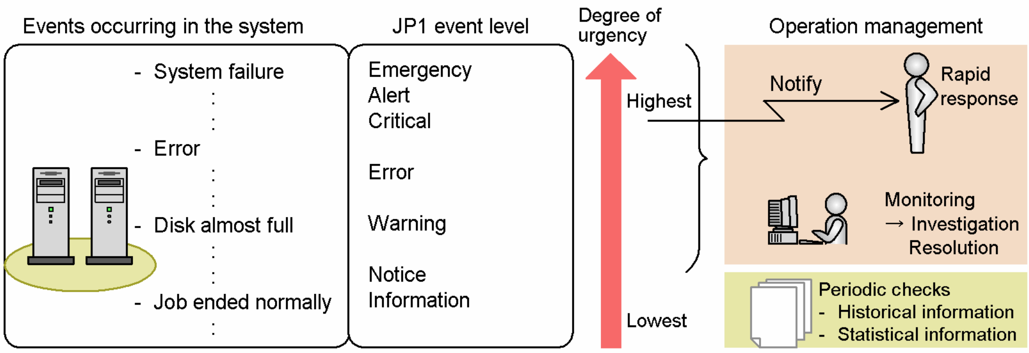
Visual monitoring:

You can arrange the key points that you want to watch closely in a map view using the Visual Monitoring window. Prepare the organizational charts or maps that you want to use as map images.

10.3.3 Designing error detection and reporting

After considering the monitoring methods and targets, consider what action to take when a problem is detected.

Figure 10–3: Considerations for correspondence between event levels and action taken



(1) JP1 events and event levels

JP1/IM uses *JP1 events* to monitor events occurring in the system. Each JP1 event is assigned an event level that indicates its severity.

Consider how to detect and deal with problems in the system according to their event level.

Categorizing JP1 events by event level:

Categorize JP1 events based on their event level (attribute name: `E.SEVERITY`).

JP1 events define an event level associated with a specific event that occurs in the system. Each product that issues JP1 events sets an appropriate event level for the types of events it manages.

When a SNMP trap or entry in the Windows event log is converted to a JP1 event, its severity is associated with a JP1 event level. If you use the integrated monitoring database and change the event level of a JP1 event to one defined by the user, the user-defined event level is associated with a JP1 event level. To monitor these JP1 events, categorize them based on the severity of the source event. When a message in a log file is converted to a JP1 event, the event level of the resulting JP1 event is determined by the converter settings. Set the converters to assign an appropriate event level.

Checking categorized JP1 events:

Check whether the JP1 events are in the appropriate category for their event level.

The event levels assigned by products in the JP1 series are generally suitable for normal operation. However, check whether reclassifying some events under another event level would suit your system operation better. For example, you might want to exclude some events that are normally classed as severe events.

(2) Response based on urgency

For the categorized JP1 events, consider response procedures based on the urgency of the event.

The following describes an example of response procedures for events with three levels of urgency (*Urgent*, *Severe*, and *Normal*).

Events that require immediate attention:

Consider whether any of the events managed by JP1/IM require an urgent response. A system failure, for example, requires an immediate response because of the far-reaching consequences to work tasks.

Consider reporting such an error to the system administrator.

To avoid placing an undue burden on the system administrator, make sure that only JP1 events requiring a rapid response are reported. Also consider changing the range of events reported to the system administrator according to their content.

In JP1/IM, you can send an emergency notice by executing a command from an automated action. Consider how to identify events that need to be reported to the system administrator, and the command to use for notification (for example a mail sending command), and then define an appropriate automated action.

Severe events that require monitoring:

Consider whether events whose event level indicates a problem should be handled as severe events that require monitoring.

Such events can be forwarded to a JP1/IM manager host where they can be centrally managed.

Use the event level or other attribute to define which JP1 events are to be handled as severe events in JP1/IM. On the Severe Events page of the Event Console window, you can view a list of the events defined as severe events and manage their response status.

Normal events that must be checked periodically:

Events issued in the normal course of operation, such as events indicating that a job has ended normally, can be used in the following ways depending on your system operating requirements:

- Keep for use as an operating history.
  Example: JP1 events related to job execution can be saved as a job execution log.
- Use to compile statistical information.
  Example: The start and end times reported in JP1 events related to job execution can be used to compile statistical information on job execution times.

Utilize urgent and severe events, by displaying them in JP1/IM - View or outputting them as a CSV snapshot, when you review the system setup, for example.

You can also utilize events that are not monitored by JP1/IM by using the following commands to output the database contents on the hosts in the system in CSV format.

- The JP1/Base `jevexport` command
  Outputs the contents of the event databases in CSV format.
- The JP1/IM - Manager `jcoevtreport` command
  Outputs the contents of the integrated monitoring database in CSV format.

(3) Monitoring from the Central Scope

You can customize the Central Scope to display events with specific event levels.

Because a monitoring tree shows the layout of the entire system in tree form, you can easily see how the objects being monitored relate to one other. However, depending on the structure of the monitoring tree, a single failure event might cause a large number of monitoring objects to change to a color that indicates an error.

Under the default settings, changes in the status of monitoring objects are triggered by the event levels of JP1 events. However, you can customize the way in which status changes are triggered to suit your system operation.

You can also exclude monitoring objects from monitoring in the Central Scope.

11 Operation Management Design

This chapter describes considerations when monitoring the system operation using JP1/IM.

11.1 Considerations for system monitoring using JP1 events

JP1/IM uses *JP1 events* to monitor events occurring in the system.

You must therefore consider the JP1/IM settings so that the events you want to monitor can be managed using JP1 events.

11.1.1 Considerations for event management using JP1 events

Consider how to set up JP1/IM to manage system events using JP1 events.

(1) Linkage with programs that issue JP1 events

A JP1/IM system can use JP1 events issued by products in the JP1 series or by any other program capable of issuing JP1 events.

Some programs require special settings to issue JP1 events. For details, see the documentation for the product concerned.

(2) Using JP1 event-issuing commands

If you have a program that does not issue JP1 events, consider using the JP1 event-issuing commands (`jevsend` and `jevsendd`) to do so. These two commands differ in whether JP1 event registration is verified. For details, see below.

About JP1 event-issuing commands:

- Registering a JP1 event using a JP1 event-issuing command
  See the description of the `jevsend` command and `jevsendd` command in the *JP1/Base User's Guide*.

(3) Converting non-JP1 events

If you want to monitor an event that is output in any of the following forms, you can use an event converter to convert it into a JP1 event that can be managed by JP1/IM:

- Message in a log file
- SNMP trap
- Windows event log entry

Consider the event converter setup required in JP1/Base to use these non-JP1 events

About event conversion:

- Converting log file messages into JP1 events

  See the description of converting log files output by an application program in the chapter on setting the event converters in the *JP1/Base User's Guide*.

- Converting SNMP traps into JP1 events

  See the description of SNMP trap conversion in the chapter on setting the event converters in the *JP1/Base User's Guide*

- Converting Windows event log entries into JP1 events.

  See the description of Windows event log conversion in the chapter on setting the event converters in the *JP1/Base User's Guide*.

11.1.2 Considerations for forwarding JP1 events to managers

Consider how to set up JP1/IM to forward the JP1 events required for system management to a manager.

JP1 events are managed by the JP1/Base event service and are forwarded according to the target JP1 events and destination hosts defined in the event forwarding settings.

Under the default settings, JP1 events whose event level is `Emergency`, `Alert`, `Critical`, `Error`, or `Warning` are forwarded through the hierarchy of managers and agents set in the system configuration definition.

You will need to customize the default settings in the following cases:

- To manage informational or normal JP1 events using JP1/IM

  Add forwarding settings to manage JP1 events of `Notice` or `Information` level in JP1/IM. For example, if you want to manage a JP1 event (`Information` level) that reports normal termination of a jobnet, so that the execution status of the jobs can be checked from JP1/IM, you must set up JP1/IM to forward that event. When customizing the forwarding settings in this way, specify explicit conditions to minimize the number of JP1 events being forwarded to JP1/IM managers.
- To manage JP1/SES events in JP1/IM

  Add forwarding settings to manage JP1/SES events in JP1/IM. For example, if you want to manage a JP1/SES event issued by JP1/Open Job Entry (a product for linking with a mainframe computer), you must set up JP1/IM to forward that event. When customizing the forwarding settings in this way, specify explicit conditions to minimize the number of JP1 events being forwarded to JP1/IM managers.

About JP1 event forwarding:

- Setting JP1 event forwarding

  See the chapter on setting the event service environment in the *JP1/Base User's Guide*.
- Setting the system configuration definition

  See *Configuration definition file (jbs_route.conf)* in *Chapter 2. Definition Files* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

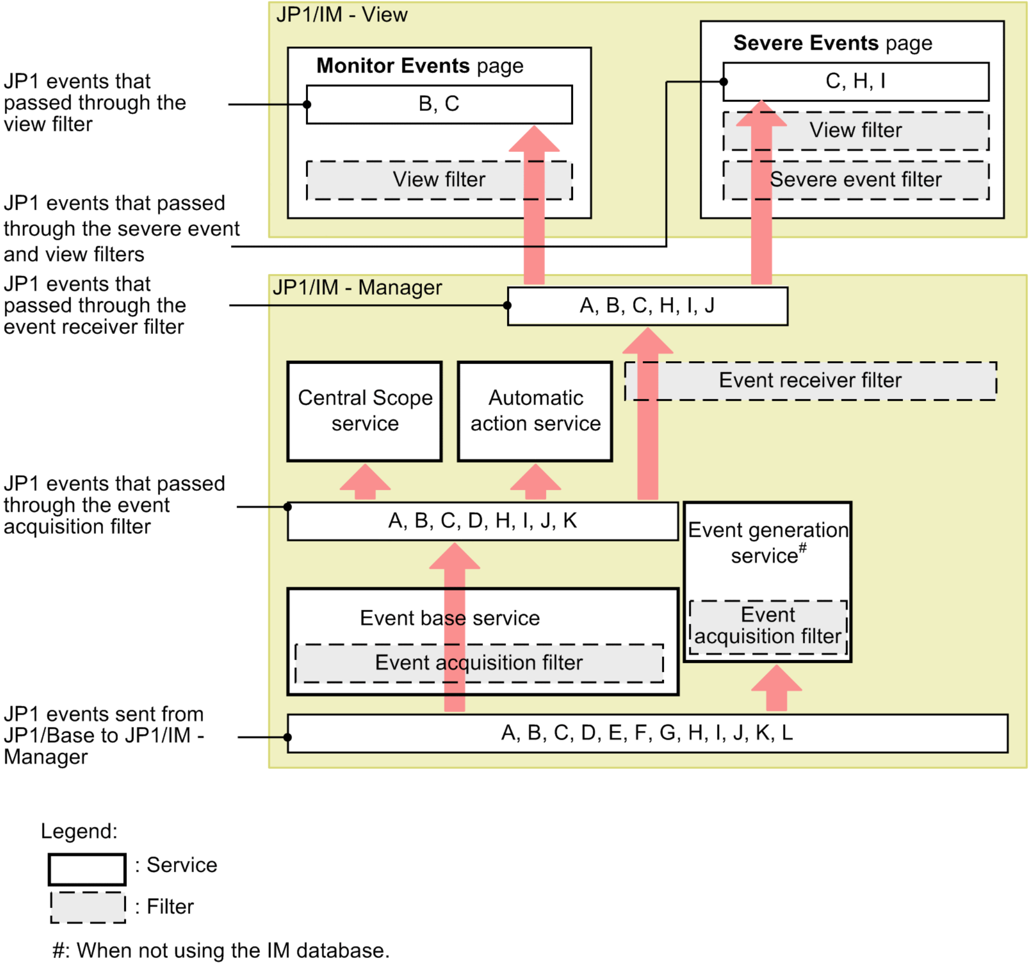
> **Important**
>
> Filter the JP1 events issued by agents so that only severe events that need to be managed by a manager will be forwarded. If all JP1 events from agents are sent to managers, there could be delays in event forwarding or in event registration at the manager host.
>
> When restrictions are set on viewing and operating business groups, do not forward JP1 events between different business groups.
>
> For details, see *3.1.4 Restrictions on viewing and operating business groups*.

11.1.3 Considerations for filtering JP1 events

Consider the JP1 event filtering settings so that appropriate JP1 events can be managed by JP1/IM during system monitoring.

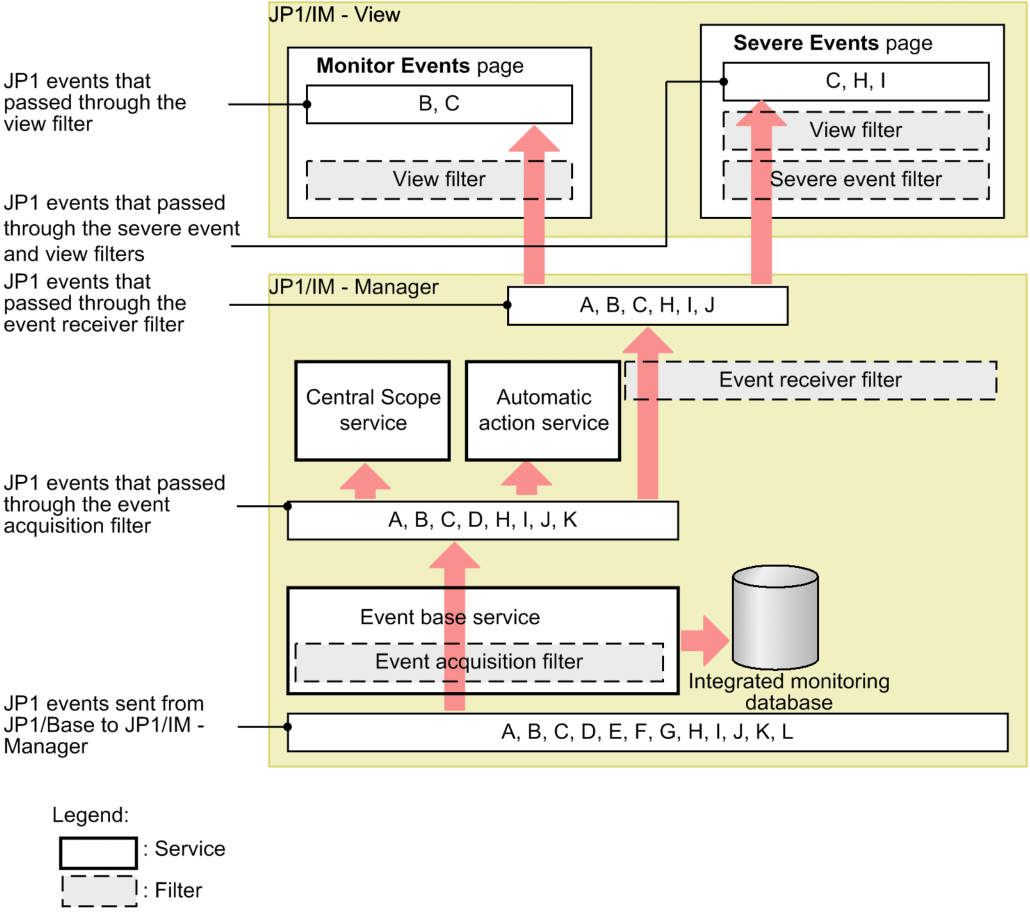
The flow of JP1 events on a JP1/IM manager depends on whether the integrated monitoring database is used. The following figures show this difference with the focus on how filters affect the flow.

Figure 11–1: Effect of filters (when not using the integrated monitoring database)


JP1/IM - View
Monitor Events page
B, C
View filter
Severe Events page
C, H, I
View filter
Severe event filter
JP1 events that passed through the view filter
JP1 events that passed through the severe event and view filters
JP1 events that passed through the event receiver filter
JP1/IM - Manager
A, B, C, H, I, J
Event receiver filter
Central Scope service
Automatic action service
JP1 events that passed through the event acquisition filter
A, B, C, D, H, I, J, K
Event generation service#
Event acquisition filter
Event base service
Event acquisition filter
JP1 events sent from JP1/Base to JP1/IM - Manager
A, B, C, D, E, F, G, H, I, J, K, L
Legend:
: Service
: Filter

#: When not using the IM database.

Figure 11–2: Effect of filters (when using the integrated monitoring database)


JP1/IM - View
Monitor Events page
B, C
View filter
Severe Events page
C, H, I
View filter
Severe event filter
JP1 events that passed through the view filter
JP1 events that passed through the severe event and view filters
JP1 events that passed through the event receiver filter
JP1/IM - Manager
A, B, C, H, I, J
Event receiver filter
Central Scope service
Automatic action service
JP1 events that passed through the event acquisition filter
A, B, C, D, H, I, J, K
Event base service
Event acquisition filter
Integrated monitoring database
JP1 events sent from JP1/Base to JP1/IM - Manager
A, B, C, D, E, F, G, H, I, J, K, L
Legend:
: Service
: Filter

The event base service and event generation service filter JP1 events according to the conditions set in the event acquisition filter. When you use the integrated monitoring database, the filtered JP1 events are stored in the integrated monitoring database. You can display the filtered JP1 events in JP1/IM - View by applying an event receiver filter.

Each filter is described below, starting from when the JP1 event is first issued.

(1) Event acquisition filter

An event acquisition filter sets conditions for the JP1 events to be acquired from JP1/Base (event service) by JP1/IM - Manager.

By default, JP1/IM - Manager acquires all JP1 events for which an event level has been set.

If you use the severity changing feature to change the event level of a JP1 event when using the integrated monitoring database, JP1/IM - Manager acquires JP1 events based on their original event levels.

The following describes how to customize the filter settings and how to set multiple event acquisition filters.

(a) Customizing an event acquisition filter

You will need to customize the event acquisition filter settings in the following cases:

- To exclude JP1 events of `Notice` and `Information` level from display on the Monitor Events page of the Event Console window

  If the managers encounter a large number of informational or normal JP1 events, set the minimum event level of the JP1 events to be acquired to `Warning` in the event acquisition filter. Numerous job execution events might be generated, for example, if JP1/AJS - Manager runs on the same host as JP1/IM - Manager. To set a minimum event level, in the Event Acquisition Settings window create a separate condition group for that event level.

- To monitor JP1/SES events in JP1/IM

  JP1/SES events are not acquired by default because no event level is set. To manage such events in JP1/IM, you must set the event acquisition filter to acquire JP1/SES events. To do so, create a separate condition group with the **Acquire the JP1/SES events** check box selected in the Event Acquisition Settings window.

(b) Setting multiple event acquisition filters

Consider whether you need to set a number of different event acquisition filters. For example, you might wish to use different acquisition conditions for JP1 events inside and outside business hours.

(c) Setting common exclusion-conditions for maintenance purposes

Consider whether you need to add common exclusion-conditions to an event acquisition filter used in maintenance mode. For example, during scheduled maintenance of JP1/IM or JP1/Base, you might wish to prevent JP1 events issued by certain hosts from being collected or exclude those events from automated-action execution.

You can previously define common exclusion-conditions to prevent JP1 events from being collected or exclude them from automated-action execution when the events are from hosts undergoing maintenance. During maintenance work, you can just enable the common exclusion-conditions, rather than editing the standard filter conditions, to prevent JP1 events issued by the hosts undergoing maintenance from being collected or exclude those events from automated-action execution.

For details about maintenance by using common exclusion-conditions in event acquisition filter settings, see *12.10 Considerations for JP1/IM system-wide maintenance*.

(d) Notes

- Event acquisition filters also affect the event generation service. The service is inactive by default. When it is started, however, the filter definitions in effect for the event base service are also applied to the event generation service.

(2) Event receiver filter

An event receiver filter is used when the system administrator wants to restrict the JP1 events that can be monitored by JP1 users. An event receiver filter can be set for a specific JP1 user, and administrator permission (`JP1_Console_Admin`) is required to change the settings.

By default, there are no restrictions and all JP1 users can monitor all JP1 events.

You will need to customize this setting in the following cases:

- To restrict the monitoring range of individual JP1 users

  If you want to prevent a certain JP1 user from viewing certain confidential events, set the events that the JP1 user is allowed to view in an event receiver filter.

- To monitor a specific range

  Using event receiver filters, you can limit the range of resources to be monitored if, for example, you want the JP1 user to monitor specific JP1 events only, or if you want multiple JP1 users to monitor different parts of a large-scale system.

(3) Severe events filter

Use a severe events filter to specify which JP1 events are important in system monitoring. The JP1 events you define in this filter are regarded as *severe events* and appear on the Severe Events page of the Event Console window. In this window you can also manage the response status of each severe event.

Under the default settings, JP1 events whose event level is `Emergency`, `Alert`, `Critical`, or `Error` are defined as severe events.

You will need to customize the default settings in the following cases:

- To exclude specific events from being handled as severe events
  If a JP1 event has a severe event level, but does not need to be treated as a severe event in terms of the system operation, specify the event ID and select **Does not match** in the severe events filter conditions.

(4) View filter

Use a view filter to specify conditions restricting the JP1 events displayed on the **Monitor Events** and **Severe Events** pages of the Event Console window.

By default, no display conditions are set.

This filter is typically used when you need to temporarily display only certain types of JP1 events during monitoring.

(5) Defining filter conditions

If you are defining multiple condition groups as filter conditions, make sure that the condition groups do not conflict with one another before you start running the system.

Example:

Suppose the following two condition groups are defined:

- Condition group A: Specifies that JP1 events of `Warning` level or higher pass through the filter.
- Condition group B: Specifies that JP1 events from hosts other than host A pass through the filter.

Here, if a `Warning` (or higher level) JP1 event arrives from host A, it will meet the condition in condition group A. Thus, a JP1 event that you actually want to exclude will pass through the filter, regardless of the condition defined in condition group B.

When defining conditions, remember that condition groups are related by an OR condition. In the example above, if you define condition group B as an exclusion-condition group that excludes JP1 events arriving from host A, this condition group will take priority over condition group A. In this case, if a `Warning` (or higher level) JP1 event arrives from host A, it will not pass through the filter.

About setting filters:

- Event acquisition filter
  Setting a filter in the Event Acquisition Settings window:
  See *2.12 Event Acquisition Settings window* in the manual *JP1/Integrated Management - Manager GUI Reference*.
  Setting a filter in the Event Acquisition Settings (for compatibility) window:
  See *2.13 Event Acquisition Settings (for compatibility) window* in the manual *JP1/Integrated Management - Manager GUI Reference*.
  Adding or setting a filter in the Event Acquisition Conditions List window:

See *2.14 Event Acquisition Conditions List window* in the manual *JP1/Integrated Management - Manager GUI Reference*.

Changing the filter location using the `jcochafmode` command:

See *jcochafmode (UNIX only)* in *Chapter 1. Commands* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

Switching event acquisition filters using the `jcochfilter` command:

See *jcochfilter* in *Chapter 1. Commands* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

- Event receiver filter

  Adding or setting a filter in the Settings for Event Receiver Filter window:

  See *2.30 Settings for Event Receiver Filter window* in the manual *JP1/Integrated Management - Manager GUI Reference*.

- Severe events filter

  Setting a filter in the Severe Event Definitions window:

  See *2.10 Severe Event Definitions window* in the manual *JP1/Integrated Management - Manager GUI Reference*.

- View filter

  Setting a filter in the Settings for View Filter window:

  See *2.28 Settings for View Filter window* in the manual *JP1/Integrated Management - Manager GUI Reference*.

  Adding or setting a filter in the View List of Filters window:

  See *2.29 View List of Filters window* in the manual *JP1/Integrated Management - Manager GUI Reference*.

11.1.4 Considerations for issuing correlation events

The JP1 events managed by JP1/IM - Manager can burgeon to huge volumes according to the size of the system. The idea behind JP1 events is that they manage each and every event occurring in the system; they therefore cover a wide range of event types.

By using the various filters provided by JP1/IM - Manager, you can restrict the types of JP1 events displayed in the event console. However, when an error occurs, the system might issue a large number of JP1 events reporting the problem and filling up the event console. It would take the system administrator a great deal of time and trouble to analyze and investigate these JP1 events, to identify the cause and remedy every problem.

In JP1/IM - Manager, you can associate a number of predictable JP1 events in advance, or optionally change the JP1 event attribute values, and thereby issue a new event (correlation event). A correlation event can be issued when a conditions is satisfied, or when a conditions fails to be satisfied. By utilizing correlation event generation, you can lessen your workload and reduce the time you spend troubleshooting problems.

Note that the processing by which correlation events are issued differs depending on whether you are using the integrated monitoring database, specifically in terms of the range of events that the correlation processing inherits. For details, see *3.3 Issue of correlation events*.

Some points you need to consider when using correlation event generation are discussed below under the following headings:

- Correlation event generation definition
- Operating environment required for correlation event generation
- Notes on correlation event generation

(1) Correlation event generation definition

A correlation event generation definition consists of correlation source events (event conditions), a timeout period, event correlation type, and the correlation event to be issued.

Give proper consideration to the following points when setting a correlation event generation definition:

- Filtering condition for the correlation target range
  Are the JP1 events that match the event conditions issued from specific hosts only?
- Correlation source events (event conditions)
  - Which JP1 events will be correlation source events?
  - Will you need one correlation source event or more than one?
- Timeout period
- Event correlation type (`sequence`, `combination`, or `threshold`)
- Duplicate attribute value condition
  Will you need to manage correlation events by grouping hosts or users?
- Maximum correlation number
- Correlation event to be issued

Six examples are presented below to illustrate the points above. Refer to these examples when you consider how to set a correlation event generation definition:

- Adding an attribute to the JP1 event attribute values
- Changing a JP1 event message to a more manageable message
- Executing an automated action when hosts A, B, and C have all started
- Issuing correlation events for a JP1 event issued from specific hosts
- Managing JP1 events indicating an authentication error by source server
- Monitoring for a situation where an event does not occur within a specified time period

Each of these six examples states the condition that needs to be satisfied, the reason, and the contents that you need to enter in the correlation event generation definition file.

For details about the correlation event generation definition file, see *Correlation event generation definition file* in *Chapter 2. Definition Files* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

(a) Adding an attribute to the JP1 event attribute values

This example shows how to add an attribute value to the fixed attributes of a JP1 event, issued by another JP1 product or other program, to issue a correlation event.

Condition to be satisfied:

Report JP1 event (00004107), which indicates abnormal termination of a JP1/AJS job, as an event of `Emergency` level.

Set the correlation event for this example as follows:

- Event ID: A01
- Event level: `Emergency`

- Message: Same message as the correlation source event (00004107).

Reason:

The event levels in this system are defined as in the following table, with `Error` level currently set for JP1 event (00004107) indicating abnormal termination of a JP1/AJS job.

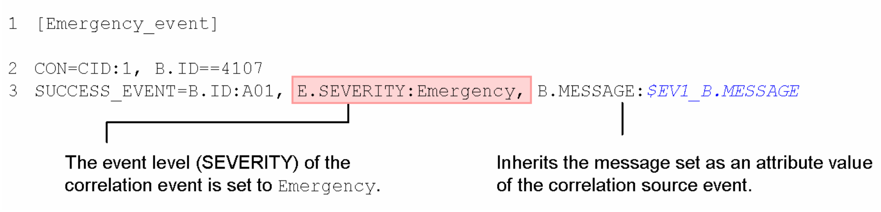
Table 11–1: Event level definitions in the system

Event level	System requirements
`Emergency`	Problem requiring immediate response
`Error`	Problem requiring response within one working day

Contents of the correlation event generation definition file:

The following figure shows the contents of the correlation event generation definition file.

Figure 11–3: Contents of the correlation event generation definition file



```
[Emergency_event]

CON=CID:1, B.ID==4107
SUCCESS_EVENT=B.ID:A01, E.SEVERITY:Emergency, B.MESSAGE:$EV1_B.MESSAGE
```

The event level (SEVERITY) of the correlation event is set to `Emergency`.

Inherits the message set as an attribute value of the correlation source event.

Note: In this example, a line number is inserted at the beginning of each line to indicate the individual lines you need to write in the definition file.

To use the correlation event generation definition shown above, copy the following coding:

```
[Emergency_event]
CON=CID:1,B.ID==4107
SUCCESS_EVENT=B.ID:A01,E.SEVERITY:Emergency,B.MESSAGE:$EV1_B.MESSAGE
```

(b) Changing a JP1 event message to a more manageable message

This example shows how to change the message of a JP1 event, to issue a correlation event containing the new message.

Condition to be satisfied:

Change the message of a JP1 event to a message appropriate to the system requirements, keeping part of the original message in the new message.

Set the correlation event for this example as follows:

- Event ID: A02
- Event level: Same level as the correlation source event (00004107)
- Message: Partly the same as the correlation source event, as shown in the table below.

Table 11–2: Message contents

Event type	Message contents
Correlation source event	`KAVS0265-E Job ended abnormally. (name:` *job-name*`:` *execution-ID*`, status:` *status*`, code:` *code*`, host:` *host-name*`, JOBID:` *job-number*`)`
Correlation event	`Job:job-name ended abnormally with RC=code:Contact job supervisor (ext:xxxx)`

Legend:

(underline): Parts whose value is inherited from the correlation source event.

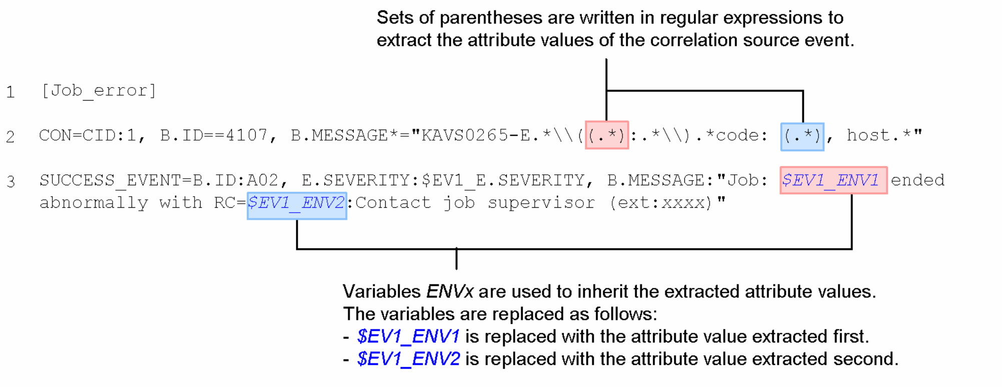
Reason:

When the information needing to be managed comes at the end of a long JP1 event message, you have to scroll to see everything, which increases your workload.

Contents of the correlation event generation definition file:

The following figure shows the contents of the correlation event generation definition file.

Figure 11–4: Contents of the correlation event generation definition file



Sets of parentheses are written in regular expressions to extract the attribute values of the correlation source event.

```
1  [Job_error]
2  CON=CID:1, B.ID==4107, B.MESSAGE*="KAVS0265-E.*\\((.*):.*\\).*code: (.*), host.*"
3  SUCCESS_EVENT=B.ID:A02, E.SEVERITY:$EV1_E.SEVERITY, B.MESSAGE:"Job: $EV1_ENV1 ended
   abnormally with RC=$EV1_ENV2:Contact job supervisor (ext:xxxx)"
```

Variables *ENVx* are used to inherit the extracted attribute values.
The variables are replaced as follows:
- *$EV1_ENV1* is replaced with the attribute value extracted first.
- *$EV1_ENV2* is replaced with the attribute value extracted second.

Note: In this example, a line number is inserted at the beginning of each line to indicate the individual lines you need to write in the definition file. Line 3 spans two lines here, but write it as one line in the definition file.

To use the correlation event generation definition shown above, copy the following coding:

```
[Job_error]
CON=CID:1,B.ID==4107,B.MESSAGE*="KAVS0265-E.*\\((.*):.*\\).*code: (.*), host.*"
SUCCESS_EVENT=B.ID:A02,E.SEVERITY:$EV1_E.SEVERITY,B.MESSAGE:"Job:$EV1_ENV1 ended
abnormally with RC=$EV1_ENV2:Contact job supervisor (ext:xxxx)"
```

(c) Executing an automated action when hosts A, B, and C have all started

This example shows how to associate multiple JP1 events to issue a correlation event. The procedure for defining an automated action is not covered here. For details about defining automated actions, see *5.3 Defining an automated action*.

Condition to be satisfied:

Execute an automated action (for system maintenance purposes) when hosts A, B, and C have all started normally.

Assume that the following JP1 event is issued when host A, B, or C starts normally.

- Event ID: 100
- Event level: `Information`
- Message: *host* `started.`

  The variable value (*host*) in the message is replaced with the host name (`A`, `B`, or `C`).
- Extended attribute (`E.HOST`): Replaced with the name of the host that has started (`A`, `B`, or `C`).

Set the correlation event for this example as follows:

- Event ID: A03
- Event level: `Information`
- Message: `All hosts started normally. Host names: A B C`

A timeout period of 10 minutes is set for a JP1 event indicating normal startup to be issued from each of the three hosts.

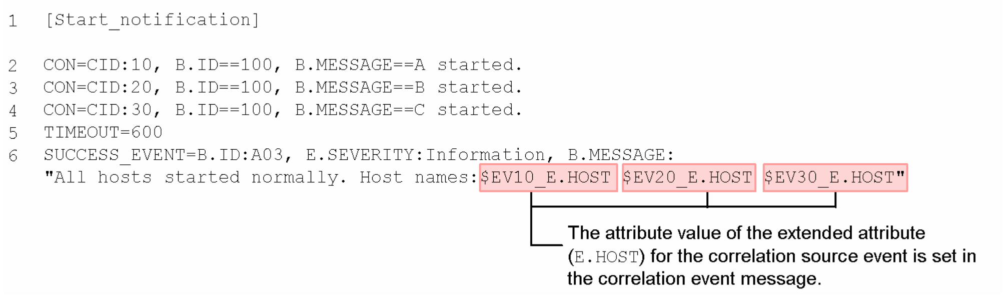
Reason:

The definitions would be complex if you tried to set an automated action for the three JP1 events reporting host startup. Setting an automated action for one correlation event is easier.

Contents of the correlation event generation definition file:

The following figure shows the contents of the correlation event generation definition file.

Figure 11–5: Contents of the correlation event generation definition file



```
1   [Start_notification]

2   CON=CID:10, B.ID==100, B.MESSAGE==A started.
3   CON=CID:20, B.ID==100, B.MESSAGE==B started.
4   CON=CID:30, B.ID==100, B.MESSAGE==C started.
5   TIMEOUT=600
6   SUCCESS_EVENT=B.ID:A03, E.SEVERITY:Information, B.MESSAGE:
    "All hosts started normally. Host names:$EV10_E.HOST $EV20_E.HOST $EV30_E.HOST"
```

The attribute value of the extended attribute (E.HOST) for the correlation source event is set in the correlation event message.

Note: In this example, a line number is inserted at the beginning of each line to indicate the individual lines you need to write in the definition file. Line 6 spans two lines here, but write it as one line in the definition file.

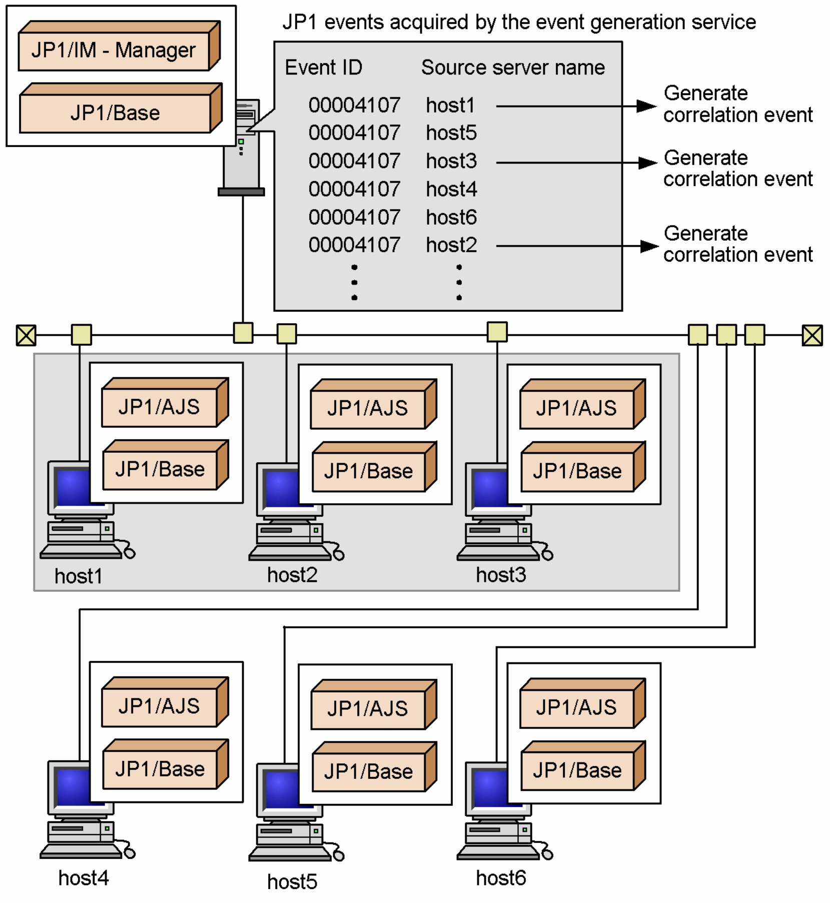
To use the correlation event generation definition shown above, copy the following coding:

```
[Start_notification]
CON=CID:10,B.ID==100,B.MESSAGE==A started.
CON=CID:20,B.ID==100,B.MESSAGE==B started.
CON=CID:30,B.ID==100,B.MESSAGE==C started.
TIMEOUT=600
SUCCESS_EVENT=B.ID:A03,E.SEVERITY:Information,B.MESSAGE:"All hosts started normally. Host
names:$EV10_E.HOST $EV20_E.HOST $EV30_E.HOST"
```

(d) Issuing correlation events for a JP1 event issued from specific hosts

This example shows how to issue correlation events when a JP1 event is issued from specific hosts in the system configuration shown below.

Figure 11–6: Issuing correlation events targeting specific hosts



Condition to be satisfied:

Apply the following requirement (same as in example (a) above) to host1, host2, and host3 only:

Report JP1 event (00004107), which indicates abnormal termination of a JP1/AJS job, as an event of `Emergency` level.

Set the correlation event for this example as follows:

- Event ID: A01
- Event level: `Emergency`
- Message: Same message as the correlation source event (00004107).

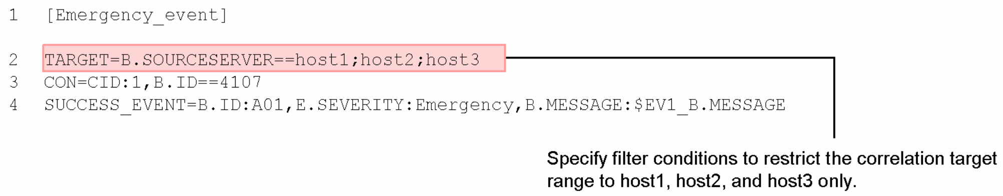
Reason:

Several hosts executing JP1/AJS jobs are being monitored, but you want to change the event level of a JP1 event issued only from specific hosts that are executing mission-critical jobs.

Contents of the correlation event generation definition file:

The following figure shows the contents of the correlation event generation definition file.

Figure 11–7: Contents of the correlation event generation definition file



```
[Emergency_event]

TARGET=B.SOURCESERVER==host1;host2;host3
CON=CID:1,B.ID==4107
SUCCESS_EVENT=B.ID:A01,E.SEVERITY:Emergency,B.MESSAGE:$EV1_B.MESSAGE
```

Specify filter conditions to restrict the correlation target range to host1, host2, and host3 only.

Note: In this example, a line number is inserted at the beginning of each line to indicate the individual lines you need to write in the definition file.

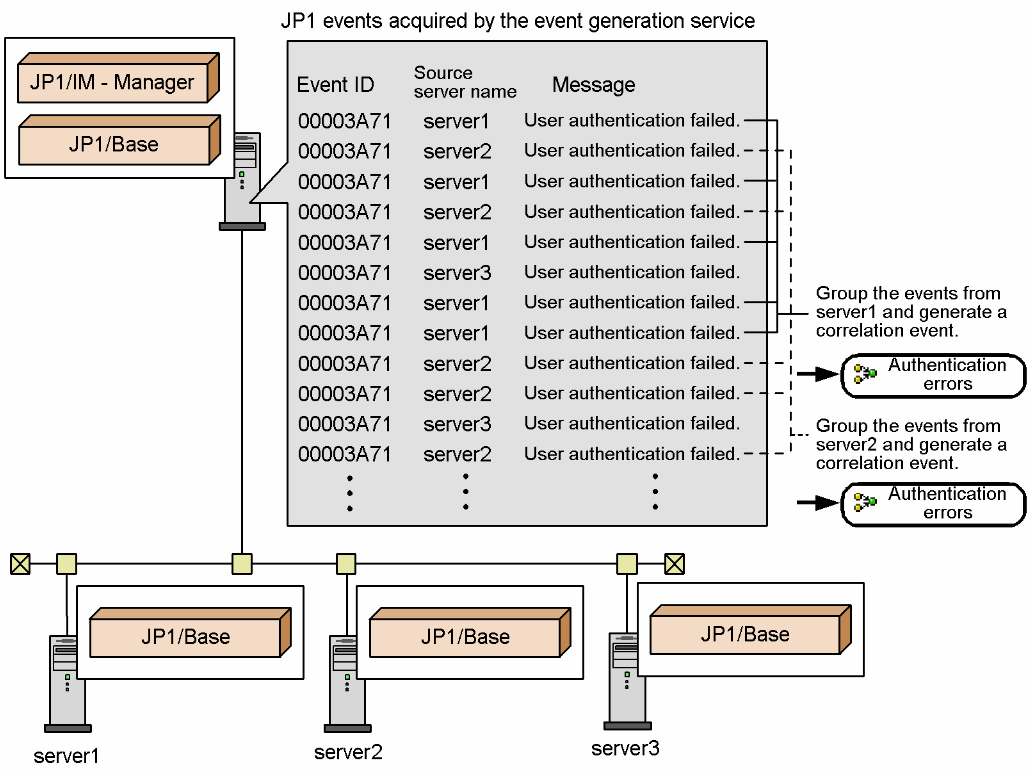
To use the correlation event generation definition shown above, copy the following coding:

```
[Emergency_event]
TARGET=B.SOURCESERVER==host1;host2;host3
CON=CID:1,B.ID==4107
SUCCESS_EVENT=B.ID:A01,E.SEVERITY:Emergency,B.MESSAGE:$EV1_B.MESSAGE
```

(e) Managing JP1 events indicating an authentication error by source server

This example shows how to issue a correlation event for each server from which a JP1 event (00003A71) indicating an authentication error was issued multiple times, as shown in the figure below.

Figure 11–8: Issuing correlation events by grouping JP1 events by source server



JP1 events acquired by the event generation service

Event ID	Source server name	Message
00003A71	server1	User authentication failed.
00003A71	server2	User authentication failed.
00003A71	server1	User authentication failed.
00003A71	server2	User authentication failed.
00003A71	server1	User authentication failed.
00003A71	server3	User authentication failed.
00003A71	server1	User authentication failed.
00003A71	server1	User authentication failed.
00003A71	server2	User authentication failed.
00003A71	server2	User authentication failed.
00003A71	server3	User authentication failed.
00003A71	server2	User authentication failed.
:	:	:

JP1/IM - Manager
JP1/Base
Group the events from server1 and generate a correlation event.
Authentication errors
Group the events from server2 and generate a correlation event.
Authentication errors
JP1/Base
JP1/Base
JP1/Base
server1
server2
server3

00003A71 is the ID of a JP1 event issued by the Windows event log trapping function of JP1/Base. The procedure for setting this function is not covered here. For details, see the description of converting the Windows event log in the chapter on setting the event converters in the *JP1/Base User's Guide*.

Condition to be satisfied:

Issue a correlation event whenever a JP1 event (00003A71) indicating an authentication error is issued five times from the same server.

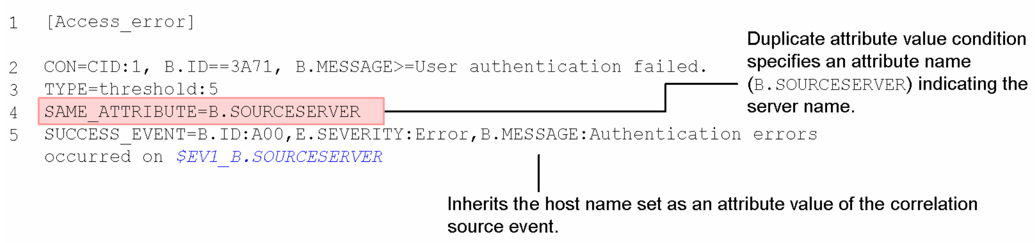
Reason:

User authentication is used to restrict connection to specific servers, and a correlation event is issued by associating JP1 events that indicate an authentication error. Authentication is required for a number of hosts, and you want to manage this correlation event for each individual host.

Contents of the correlation event generation definition file:

The following figure shows the contents of the correlation event generation definition file.

Figure 11–9: Contents of the correlation event generation definition file



```
[Access_error]

CON=CID:1, B.ID==3A71, B.MESSAGE>=User authentication failed.
TYPE=threshold:5
SAME_ATTRIBUTE=B.SOURCESERVER
SUCCESS_EVENT=B.ID:A00,E.SEVERITY:Error,B.MESSAGE:Authentication errors
occurred on $EV1_B.SOURCESERVER
```

Duplicate attribute value condition specifies an attribute name (B.SOURCESERVER) indicating the server name.

Inherits the host name set as an attribute value of the correlation source event.

Note: In this example, a line number is inserted at the beginning of each line to indicate the individual lines you need to write in the definition file.

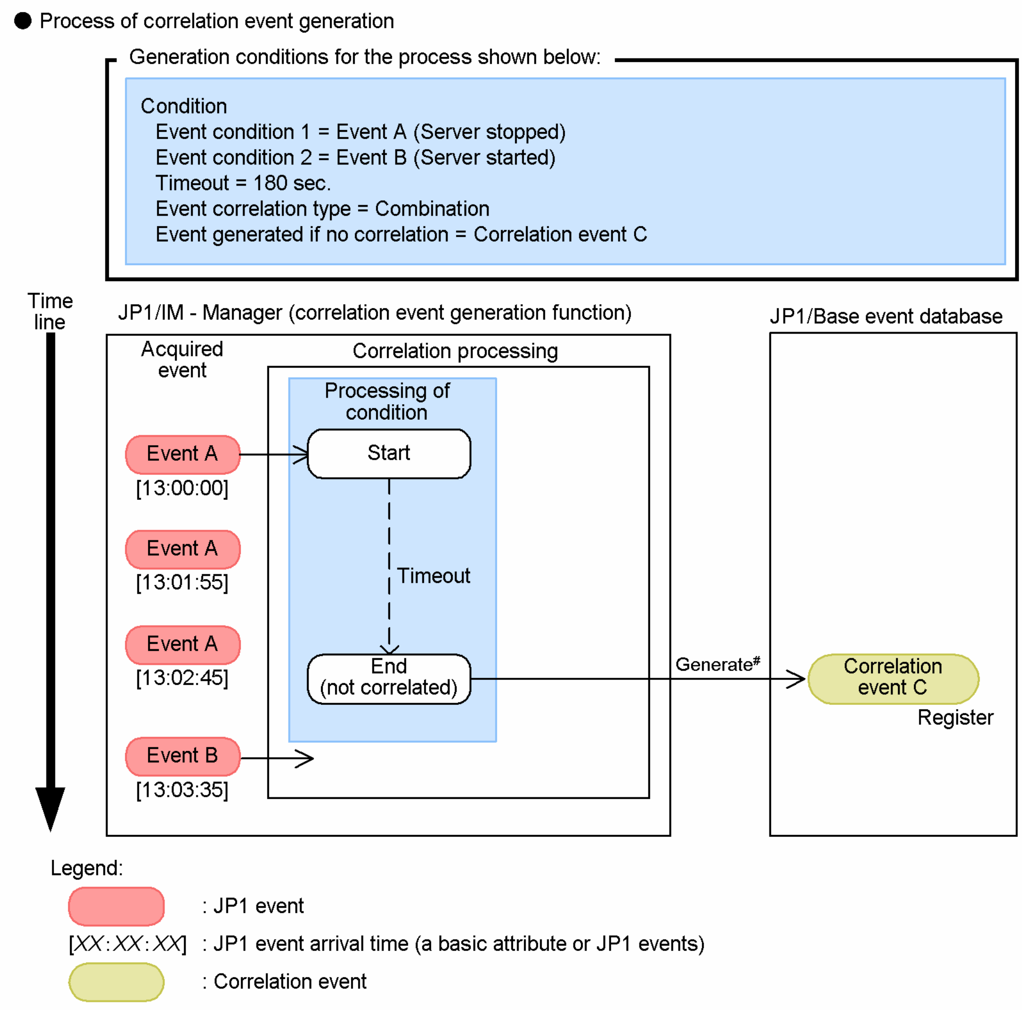
To use the correlation event generation definition shown above, copy the following coding:

```
[Access_error]
CON=CID:1, B.ID==3A71, B.MESSAGE>=User authentication failed.
TYPE=threshold:5
SAME_ATTRIBUTE=B.SOURCESERVER
SUCCESS_EVENT=B.ID:A00,E.SEVERITY:Error,B.MESSAGE:Authentication errors occurred on
$EV1_B.SOURCESERVER.
```

(f) Monitoring for a situation where an event does not occur within a specified time period

This example shows how to issue a correlation event when a particular event has not occurred within a specified time period, as shown by the figure below.

Figure 11–10: Monitoring when an event has not occurred within a specified time period


● Process of correlation event generation
Generation conditions for the process shown below:
Condition
Event condition 1 = Event A (Server stopped)
Event condition 2 = Event B (Server started)
Timeout = 180 sec.
Event correlation type = Combination
Event generated if no correlation = Correlation event C
Time line
JP1/IM - Manager (correlation event generation function)
Acquired event
Correlation processing
Processing of condition
Event A
[13:00:00]
Start
Event A
[13:01:55]
Timeout
Event A
[13:02:45]
End (not correlated)
Generate#
Event B
[13:03:35]
JP1/Base event database
Correlation event C
Register
Legend:
: JP1 event
[XX:XX:XX] : JP1 event arrival time (a basic attribute or JP1 events)
: Correlation event

#: When event generation is defined in the correlation event generation definitions for both correlation success and correlation failure for a particular JP1 event, events are generated in both situations.

Condition to be satisfied:

Suppose that a warning event A is issued, indicating that a server has stopped, followed some time later by an information event B indicating that the server has started. If both A and B are not detected within a specified timeout period, a warning event C is to be issued.

Reason:

You want to monitor for a situation where a particular event has not occurred within a specified period of time, so that you can investigate the cause of the problem.

Contents of the correlation event generation definition file:

The following figure shows the contents of the correlation event generation definition file in this example.

Figure 11–11: Contents of the correlation event generation definition file

```
1  [correlation1]
   TIMEOUT=180
2  CON=CID:1,B.ID==A
3  CON=CID:2,B.ID==B
4  SAME_ATTRIBUTE=B.SOURCESERVER
5  FAIL_EVENT=B.ID:C,E.SEVERITY:Warning,B.MESSAGE:Server$EV1_B.SOURCESERVER has not
   recovered.
   TYPE=sequence
```

Message is issued when correlation fails.

Note: The line number inserted at the beginning of each line indicates the individual lines you need to write in the definition file.

To use the correlation event generation definition shown above, copy the following coding:

```
[correlation1]
TIMEOUT=180
CON=CID:1,B.ID==A
CON=CID:2,B.ID==B
SAME_ATTRIBUTE=B.SOURCESERVER
FAIL_EVENT=B.ID:C,E.SEVERITY:Warning,B.MESSAGE:Server $EV1_B.SOURCESERVER has not recovered.
TYPE=sequence
```

(2) Operating environment required for correlation event generation

The following describes the operating environment required for issuing correlation events.

Memory and disk space requirements for correlation event issue

To issue correlation events, the following process of JP1/IM - Manager must be active:

- When not using the integrated monitoring database:
  Event generation service (`evgen`)
- When using the integrated monitoring database:
  Event base service (`evflow`)

Estimate in advance the extra memory requirements for starting the relevant process.

Correlation event generation history files are added periodically and make demands on disk space. Allocate sufficient resources for the estimated disk space requirements. You can change the number and size of the correlation event generation history files by adjusting a parameter in the correlation event generation environment definition file. For details, see *Correlation event generation environment definition file* in *Chapter 2. Definition Files* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

For details on estimating memory and disk space requirements, see the *Release Notes* for JP1/IM - Manager.

Designing the JP1/IM and JP1/Base filters

Bear in mind the following two points when setting the JP1/IM and JP1/Base filters:

- Filtering of correlation source events

  The JP1 events that you want to use as correlation source events must be distributed to the event generation service. To this end, set the JP1/Base forwarding filter and the JP1/IM event acquisition filter so that the source events will pass through.

  The JP1/IM severe events filter, event receiver filters, and view filter can be optionally set. Set these filters depending on whether you need to monitor correlation source events.

- Filtering of correlation events

  Correlation events must be monitored from JP1/IM - View. As a general rule, set the event acquisition filter and other JP1/IM filters so that correlation events will pass through.

  Filtering can be used when you want to issue correlation events for a purpose other than monitoring, such as to trigger an automated action or to effect a status change in a monitoring node. In this case also, make sure that you set the event acquisition filter so as to allow the correlation events to pass through.

For considerations related to setting the JP1/IM filters, see *11.1.3 Considerations for filtering JP1 events*. For considerations on setting the JP1/Base forwarding filter, see the description of JP1 event forwarding in the chapter on setting the event service in the *JP1/Base User's Guide*.

(3) Notes on correlation event generation

Note the following points regarding correlation event generation:

- You cannot make an issued correlation event subject to any further correlation processing.

  If you register a correlation event as a source event in a correlation event generation definition, the setting will be ignored.

- After editing a correlation event generation definition file, always check its contents by executing the `jcoegscheck` command. This will eliminate invalid or redundant conditions as definition errors.

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

  The event generation service can still operate when a generation definition contains invalid settings, but any invalid parts in the edited file will be ignored.

- If you specify the same attribute as in an event condition in a filtering condition for the correlation target range, or in a duplicate attribute value condition, you might end up with invalid conditions that can never be satisfied. The `jcoegscheck` command does not catch such problems.

  When specifying a filtering condition for the correlation target range or a duplicate attribute value condition, take care that it does not contradict the event conditions.

  Two examples of invalid conditions are discussed below. The first is an example of specifying a filtering condition for the correlation target range.

  Figure 11–12: Invalid conditions: Example 1 (filtering condition for the correlation target range)

```
1   [Wrong_condition1]
2   TARGET=B.SOURCESERVER>=host
3   CON=CID:1,B.ID==999, B.SOURCESERVER==host1;host2;host3
4   CON=CID:2,B.ID==998, B.SOURCESERVER==HOST_A
5   SUCCESS_EVENT=B.ID:A00,E.SEVERITY:Error,B.MESSAGE:$EV1_B.MESSAGE
```

  This example is explained below, following the line numbers.

  Line 2 declares a filtering condition for the correlation target range, and specifies as correlation targets all JP1 events whose source server name contains `host`. As a result, a JP1 event whose source server name is `HOST_A`, specified in the event condition at line 4, will not be correlated.

  Because JP1 events that satisfy the event condition at line 4 are not processed, the correlation event generation condition fails and no correlation event is issued.

  The next example is a duplicate attribute value condition.

  Figure 11–13: Invalid conditions: Example 2 (duplicate attribute value condition)

```
1   [Wrong_condition2]
2   CON=CID:1,B.ID==999, B.MESSAGE*=^ERROR=(.*)
3   CON=CID:2,B.ID==998, B.MESSAGE^="ACCESS ERROR"
4   SAME_ATTRIBUTE=B.MESSAGE
5   SUCCESS_EVENT=B.ID:A00,E.SEVERITY:Error,B.MESSAGE:ErrorCode=$EV1_ENV1
```

  This example is explained below, following the line numbers.

  The event condition at line 2 correlates messages that begin with `ERROR=`, and the event condition at line 3 correlates messages that begin with `ACCESS ERROR`. The duplicate attribute value condition at line 4 groups JP1 events that have identical messages.

  Because the event conditions at line 2 and line 3 target JP1 events that have different messages, the *same message* requirement of the duplicate attribute value condition cannot be satisfied, and correlation events will never be issued.

  However, JP1 events that match the event condition in line 2 or line 3 will be processed, starting a correlation processing which can never succeed. Suppose that JP1 events are issued in the following order:

  1. JP1 event (event ID: 00000999; message: `ERROR=100`) is issued.

This event satisfies the event condition at line 2, so a correlation processing begins. `ERROR=100` is registered as a potential duplicate attribute value, and the number of sets of JP1 events being correlated is incremented by one.

2. JP1 event (event ID: 00000998; message: `ACCESS ERROR`) is issued.

   This event satisfies the event condition at line 3, but its message is not the same as `ERROR=100`, so a new correlation processing begins. `ACCESS ERROR` is registered as a potential duplicate attribute value, and the number of sets of JP1 events being correlated is incremented by one.

- When the correlation event generation function issues correlation and correlation failure events, the total number of events in the whole system increases. The increase of events might cause overall system load to increase.

  Consider the increase of events due to the correlation event function and the total number of events in the whole system, and verify whether the increase of events causes a problem in the overall system load.

11.1.5 Considerations for suppressing the monitoring of repeated events and a large number of events

When the suppression of repeated-event monitoring is enabled, you can consolidate the JP1 events that have occurred during a specified period (end monitoring period) and meet a specified condition, and suppress execution of automated actions. You can thus avoid overlooking other important events. You can also combine the suppression of repeated-event monitoring with the event forwarding suppression by JP1/Base so as to handle the occurrence of a large number of events.

When the suppression of repeated-event monitoring is enabled, you cannot use the consolidated display of repeated events. Consider whether to use the suppression of repeated-event monitoring.

Consider the following points for the suppression of repeated-event monitoring:

- Purpose of using the suppression of repeated-event monitoring
- Repeated event condition

(1) Considering the purpose of using the suppression of repeated-event monitoring

The suppression of repeated-event monitoring is used for one of the following purposes:

1. Suppressing display of the events, in the event list, that do not need to be monitored and execution of the automated actions triggered by those events
2. Suppressing display of the events, in the event list, that have occurred in large numbers and execution of the automated actions triggered by those events

The suppression of repeated-event monitoring applies only to the events JP1/IM - Manager has acquired from the event service. This suppression function cannot prevent the increase of manager load caused when agents forward a large number of events to the manager. Therefore, when you use the suppression of repeated-event monitoring for purpose 2 described above, consider also the suppression of forwarding of a large number of events by JP1/Base.

For the suppression of forwarding of a large number of events by JP1/Base, see *11.1.7 Considerations for suppressing the forwarding of a large number of events*.

(2) Considering the repeated event condition

Consider the repeated event condition according to the purpose of using the suppression of repeated-event monitoring. The following describes two examples of situations requiring setting of the repeated event condition:

Repeated event condition example 1: Suppressing display of events in the event list that do not need to be monitored and execution of the automated actions triggered by those events

To suppress display of the events in the event list that do not need to be monitored during daily monitoring operation and execution of the automated actions triggered by those events, set a repeated event condition without a threshold.

Table 11–3: Example of repeated event condition for suppressing display of the events in the event list that do not specially need to be monitored and execution of the automated actions triggered by those events

Page in the Repeated Event Condition Settings window	Setting item	Setting
--	**Repeated event condition name**	`Repeated event condition example 1`
	Comment	`Suppress display of the events, in the event list, that do not need to be monitored and execution of the automated actions triggered by those events.`
Basic Settings page	**Event conditions**	• Attribute name: `Source host` Attribute value: `host1` Condition: `Match` • Attribute name: `Severity level` Attribute value: `Warning` Condition: `Match` • Attribute name: `Object type` Attribute value: `LOGFILE` Condition: `Match`
	Suppression items	**Suppress display of the repeated events list** Select the check box to enable. **Suppress actions for the following events** Select the check box to enable. (Select **Repeated events other than repeated start events**.)
Options page	**Conditions for same attribute values**	No setting
	Threshold	Clear the **Enable** check box.
	End monitoring period	`3,600` **seconds**
	Suppression start event	Clear the **Issue** check box.
	Suppression end event	Clear the **Issue** check box.
	Checks for suppression to continue	Select the **Enable** check box. (Select **Number of events** for **Timing of checks to decide whether suppression will continue**, and specify 100 [events] as the interval of checking.)

Page in the Repeated Event Condition Settings window	Setting item	Setting
	Processing for when suppression continues	Select **Terminate suppression**. (Clear the **Issue an event to notify that suppression will be terminated** check box.)

Legend:

--: No corresponding page

Explanation of repeated event condition example 1

Repeated event condition example 1 is a repeated event condition to suppress display of the log file traps, in the event list, whose *source host* is `host1` and *severity* is `Warning`, and suppress the automated actions triggered by them. Automated actions are executed only when triggered by the repeated start event, but are not executed because of other repeated events.

During the period after JP1/IM - Manager receives the first repeated start event until monitoring suppression ends, monitoring suppression for the repeated events that meet this repeated event condition is terminated every time 100 events is received. The repeated event received immediately after monitoring suppression is terminated is treated as a repeated start event. Therefore, a preset automated action is executed every time monitoring suppression is terminated.

Monitoring suppression ends when one hour has passed since the last repeated event meeting this repeated event condition was received.

For the monitoring suppression without using a threshold, see the following reference:

About monitoring suppression without a threshold

- Suppressing the display of the events that meet the repeated event condition in the event list
  See *3.4 Suppressing display of repeated events*.
- Repeated event condition without a threshold
  See *3.4.3 Repeated event conditions*.
- Suppressing the execution of automated actions triggered by the events that meet the repeated event condition
  See *3.5.8 Suppressing the execution of automated actions triggered by a large number of events*.

Repeated event condition example 2: Preparing for occurrence of a large number of events

If events occur in large numbers for any reason, their monitoring needs to be suppressed even though the events need to be monitored during daily monitoring operation. If you have ever experienced the occurrence of a large number of events during monitoring operation, set a repeated event condition with a threshold to prepare for a similar occurrence of a large number of events.

Table 11–4: Example of repeated event condition to prepare for occurrence of a large number of events

Page in the Repeated Event Condition Settings window	Setting item	Setting
--	**Repeated event condition name**	`Repeated event condition example 2`
	Comment	`Prepare for occurrence of a large number of events.`
Basic Settings page	**Event conditions**	• Attribute name: `Source host` Attribute value: `hostA` Condition: `Match` • Attribute name: `Severity level`

Page in the Repeated Event Condition Settings window	Setting item	Setting
		Attribute value: `Error` Condition: `Match` • Attribute name: `Object type` Attribute value: `LOGFILE` Condition: `Match`
	Suppression items	**Suppress display of the repeated events list** Select the check box to enable. **Suppress actions for the following events** Select the check box to enable. (Select **All repeated events**.)
Options page	**Conditions for same attribute values**	No setting
	Threshold	Select the **Enable** check box. (`100` **events**/`30` **seconds**)
	End monitoring period	`43,200` **seconds**
	Suppression start event	Select the **Issue** check box.
	Suppression end event	Select the **Issue** check box.
	Checks for suppression to continue	Select the **Enable** check box. (Select **Number Time** for **Timing of checks to decide whether suppression will continue**, and specify 3,600 (seconds) as the interval of checking.)
	Processing for when suppression continues	Select **Issue an event to notify that suppression will continue**.

Legend:

--: No corresponding page

Explanation of repeated event condition example 2

Repeated event condition example 2 is a repeated event condition to suppress display of the log file traps, in the event list, whose *source host* is `hostA` and *severity* is `Error`, and suppress the automated actions triggered by them. Execution of the automated action triggered by every event subject to monitoring suppression is suppressed. At the start and end of monitoring suppression, a JP1 event is issued for notification.

The events that meet the repeated event condition are assumed to be monitoring targets in normal monitoring operation. Therefore, their monitoring is suppressed only when more than 100 events occur within 30 seconds.

During the period after JP1/IM - Manager receives the first repeated start event until monitoring suppression ends, it issues the *event to notify that suppression will continue* every hour to notify that events continue to occur in large numbers.

Monitoring suppression ends when 12 hours has passed since a large number of events occurred (repeated events more than the threshold value per unit of time).

For the monitoring suppression with a threshold set, see the following reference:

About monitoring suppression with a threshold

- Suppressing the monitoring of a large number of events

  See *3.5 Suppressing monitoring of a large number of events*.

- Repeated event condition without a threshold

  See *3.5.3 Repeated event condition for the suppression of monitoring of a large number of events*.

- Suppressing the execution of automated actions triggered by a large number of events
  See *3.5.8 Suppressing the execution of automated actions triggered by a large number of events*.

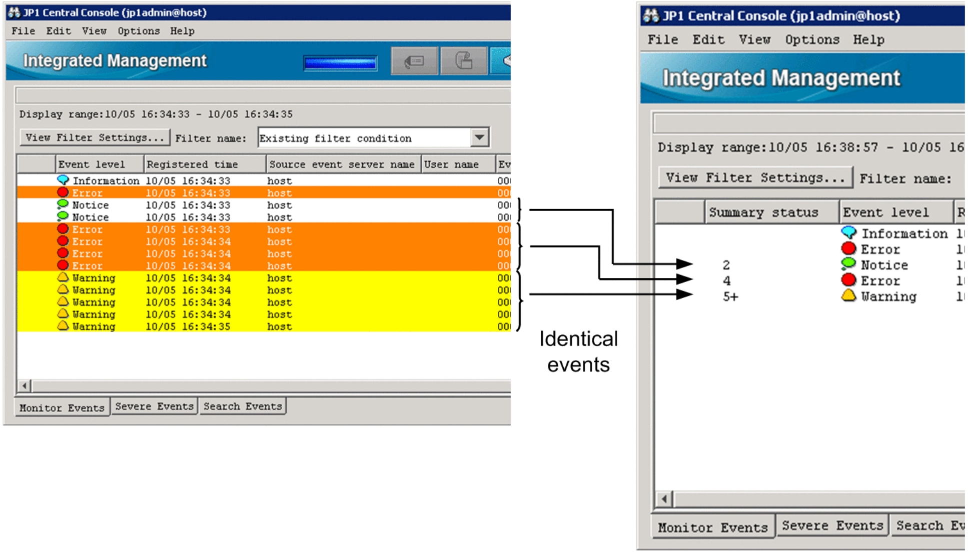
11.1.6 Considerations for consolidated display of repeated events

The consolidated display of repeated events enables you to consolidate successive, identical JP1 events, among the JP1 events JP1/IM - View receives in large numbers in a short period of time, and display them in the Event Console window. Thereby, you can potentially prevent important events from being overlooked. You cannot use both the consolidated display of repeated events and the suppression of repeated-event monitoring at the same time.

Consider whether to use the function for consolidated display of repeated events.

For details about the consolidated display of repeated events, see *3.4.10 Suppressing repeated-event display by the consolidated display of repeated events*.

Figure 11–14: Example of consolidating repeated events



(1) Without consolidated display of repeated events

JP1 Central Console (jp1admin@host)

Display range:10/05 16:34:33 - 10/05 16:34:35

Filter name: Existing filter condition

	Event level	Registered time	Source event server name	User name	Ev
	Information	10/05 16:34:33	host		00
	Error	10/05 16:34:33	host		00
	Notice	10/05 16:34:33	host		00
	Notice	10/05 16:34:33	host		00
	Error	10/05 16:34:33	host		00
	Error	10/05 16:34:34	host		00
	Error	10/05 16:34:34	host		00
	Error	10/05 16:34:34	host		00
	Warning	10/05 16:34:34	host		00
	Warning	10/05 16:34:34	host		00
	Warning	10/05 16:34:34	host		00
	Warning	10/05 16:34:34	host		00
	Warning	10/05 16:34:35	host		00

(2) With consolidated display of repeated events

JP1 Central Console (jp1admin@host)

Display range:10/05 16:38:57 - 10/05 16

Filter name:

	Summary status	Event level	R
		Information	1
		Error	1
	2	Notice	1
	4	Error	1
	5+	Warning	1

When this function is used, event consolidation ends when any one of the following conditions is satisfied:

- The contents of the received JP1 event do not match the consolidation start event.
- The difference between the arrival times of the consolidation start event and received JP1 event exceeds the set timeout value.
- The number of repeated events exceeds the maximum repeat count.
- The user clicks the **OK** button in the Preferences window.
- The event being consolidated was not defined as a severe event, but becomes so due to a change in the severe event definition.
- The event being consolidated was defined as a severe event, but is no longer so due to a change in the severe event definition.

You can set a timeout period in the conditions for ending event consolidation. Consider an appropriate timeout period for the type of application.

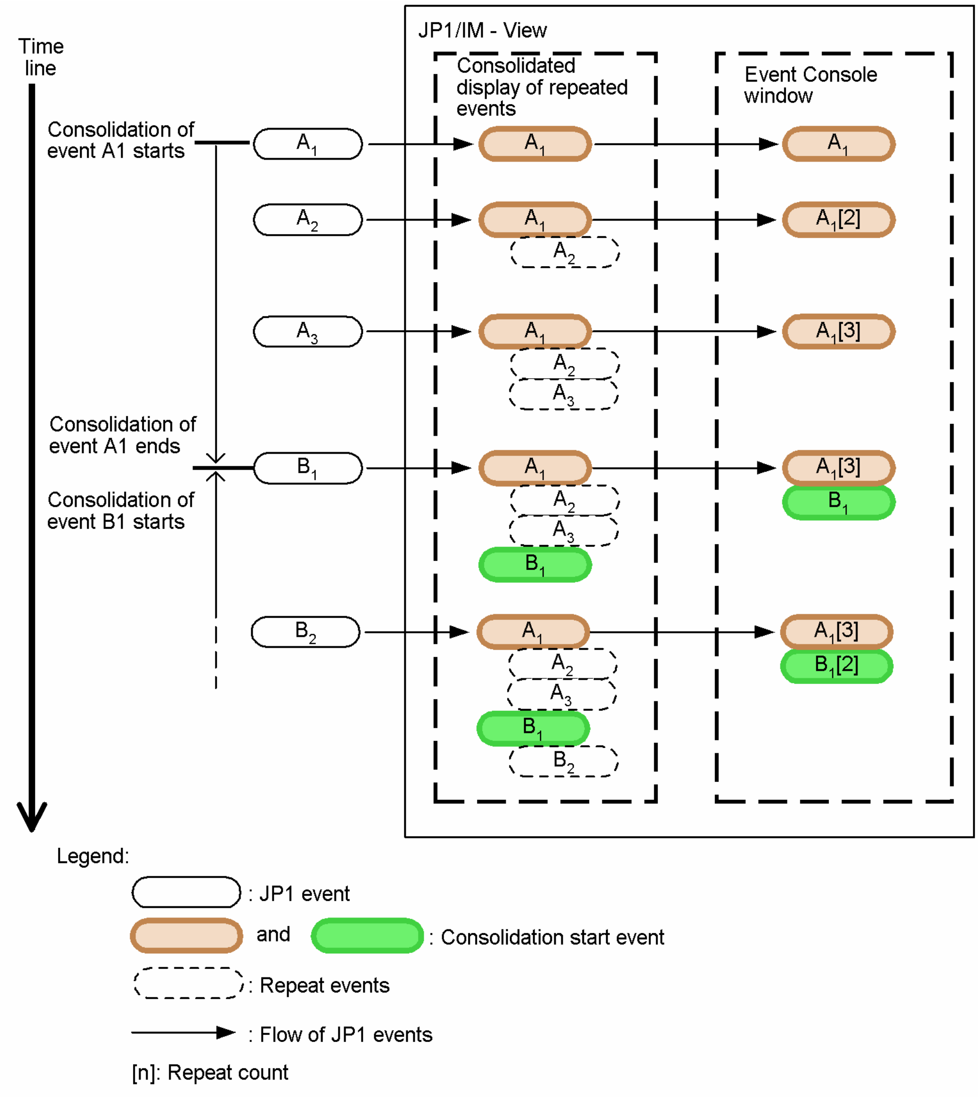
Comparison of event contents

On receipt of a new JP1 event, JP1/IM - View compares its contents with the consolidation start event. If the contents match, the new JP1 event is judged to be a repeated event and the event is consolidated. If the contents do not match, event consolidation ends. The new JP1 event becomes a new consolidation start event, and a new consolidation cycle begins.

For details about the comparison of event contents, see *3.4.10(3) Event comparison attributes*.

The following figure shows an example of what happens when a received JP1 event does not match the contents of the consolidation start event.

Figure 11–15: Ending event consolidation on receipt of a non-matching JP1 event



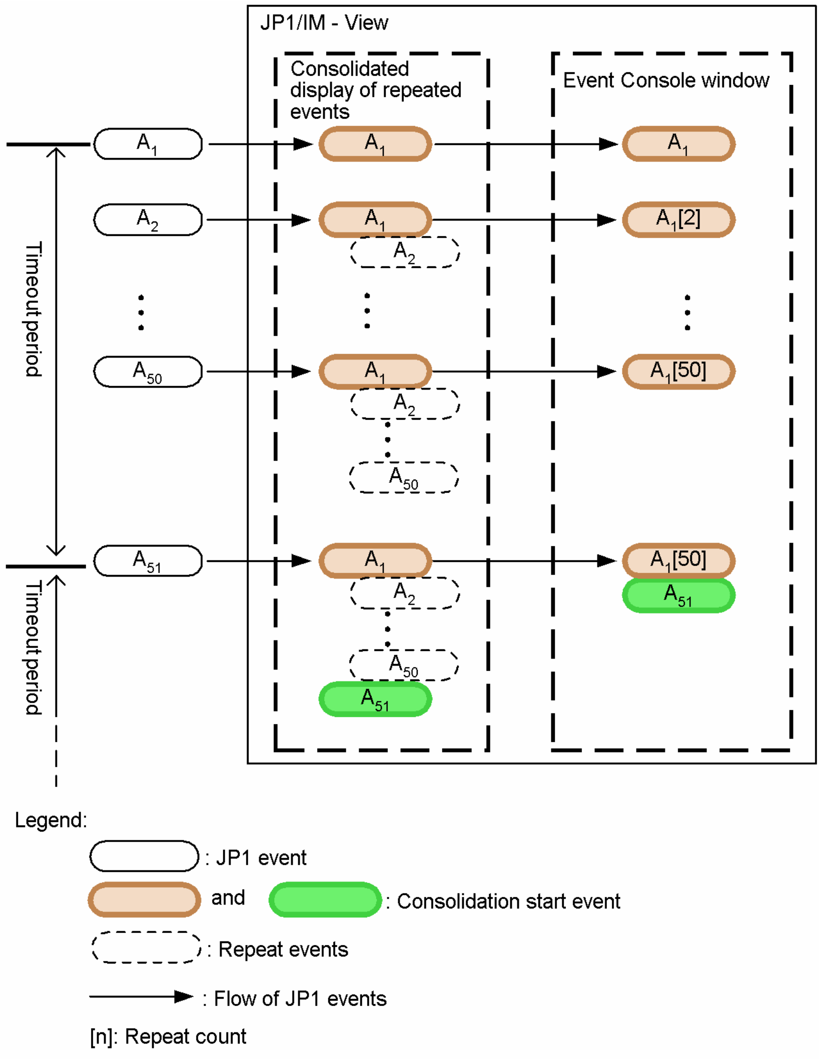
Time line
JP1/IM - View
Consolidated display of repeated events
Event Console window
Consolidation of event A1 starts
Consolidation of event A1 ends
Consolidation of event B1 starts
A1
A2
A3
B1
B2
A1[2]
A1[3]
B1[2]
Legend:
: JP1 event
and
: Consolidation start event
: Repeat events
: Flow of JP1 events
[n]: Repeat count

Timeout period

A timeout period must be specified for consolidating repeated events. You can specify a value in the range from 1 to 3,600 seconds.

The following figure shows an example of what happens when the difference between the arrival times of the consolidation start event and received JP1 event falls outside the timeout period.

Figure 11–16: Ending event consolidation by timeout

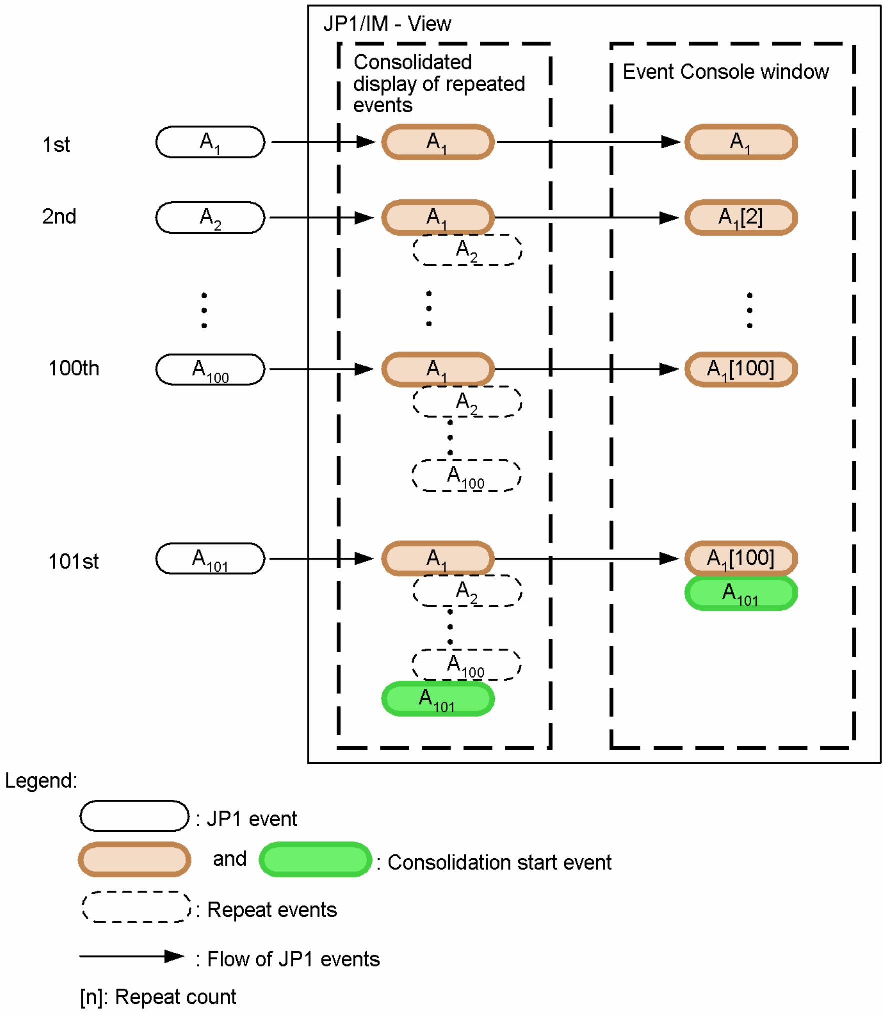


When the difference between the arrival times of the consolidation start event and received JP1 event exceeds the timeout period, event consolidation ends. If an identical event is subsequently received, it becomes a new consolidation start event in a new cycle.

Maximum repeat count

The maximum number of repeated events that can be consolidated in one cycle is 100. You cannot change this limit.

Figure 11–17: Ending event consolidation by exceeding the maximum repeat count



Event consolidation ends when the maximum repeat count is exceeded during a consolidation cycle. If an identical event is subsequently received, it becomes a new consolidation start event in a new cycle.

Setting consolidated display of repeated events

- Setting in the Preferences window

  See *2.24 Preferences window* in the manual *JP1/Integrated Management - Manager GUI Reference*.

11.1.7 Considerations for suppressing the forwarding of a large number of events

If a large number of events occur on an agent, and the system monitoring by the manager is thereby hindered, consider whether to suppress event forwarding from the agent.

Consider the following points for suppressing the forwarding of a large number of events:

- Suppressing the forwarding of a large number of events
- Preventing the forwarding of a large number of events

(1) Considerations for suppressing the forwarding of a large number of events

When a large number of events have occurred on an agent, first consider whether to use the suppression of repeated-event monitoring and whether to suppress the event forwarding from the agent. If you want to reduce the load on the event server of the manager, suppress the event forwarding from the agent. The event forwarding suppression command (`jevagtfw` command) enables you to suppress the event forwarding from the agent by an operation from the manager.

If a log file trap issuing JP1 events has caused the occurrence of a large number of events, consider whether to stop the log file trap. You can stop log file traps individually by using the ID number or log file trap name of each log file trap.

Examine how JP1 events are occurring to determine which of suppressing event forwarding and stopping log file traps is to be used as a measure against the occurrence of a large number of events. For example, when an occurrence of a large number of events is detected, suppress event forwarding as a temporary measure. After that, if you find that a log file trap has caused the occurrence of a large number of events, you can stop the log file trap and release event forwarding from suppression.

> **Note**
>
> Storage of JP1 events in the event server
>
> When event forwarding from an agent is suppressed, only forwarding of events to the manager is suppressed, and JP1 events are stored in the event server of the agent. On the other hand, when a log file trap is stopped, event conversion to JP1 events is also stopped, and, accordingly, JP1 events are not stored in the event server of the agent.

(2) Considerations for preventing the forwarding of a large number of events

To prevent a large number of events from being forwarded, consider the automatic suppression of event forwarding by using a threshold for determining the occurrence of a large number of events.

To automatically suppress event forwarding, you need to consider the event forwarding suppression condition. The event forwarding suppression condition includes the setting of the number of occurring events per unit time.

For details about the event forwarding suppression condition, see descriptions of the forwarding setting file in the *JP1/Integrated Management - Manager Administration Guide*.

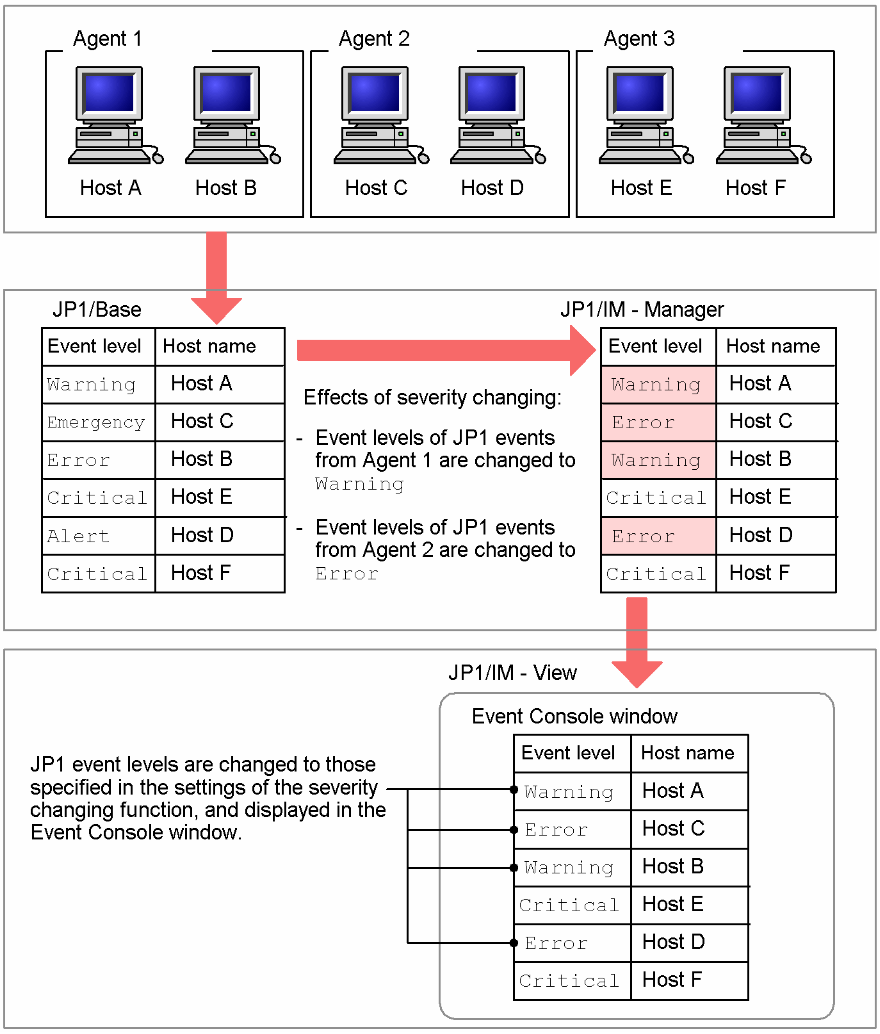
11.1.8 Considerations for changing JP1 event levels

Consider changing the event levels associated with JP1 events so that the events can be appropriately categorized during system monitoring.

A JP1 event issued by a particular host or product and forwarded to the integrated manager might have an event level that does not reflect its importance in terms of system operation.

By using the severity changing function, you can change the event levels of JP1 events to realize event management that takes how you use the system into account. You can also assign a blanket event level to events from a particular agent.

Figure 11–18: Flow of changing event levels of JP1 events



JP1/Base

Event level	Host name
Warning	Host A
Emergency	Host C
Error	Host B
Critical	Host E
Alert	Host D
Critical	Host F

Effects of severity changing:

- Event levels of JP1 events from Agent 1 are changed to Warning
- Event levels of JP1 events from Agent 2 are changed to Error

JP1/IM - Manager

Event level	Host name
Warning	Host A
Error	Host C
Warning	Host B
Critical	Host E
Error	Host D
Critical	Host F

JP1 event levels are changed to those specified in the settings of the severity changing function, and displayed in the Event Console window.

Event Console window

Event level	Host name
Warning	Host A
Error	Host C
Warning	Host B
Critical	Host E
Error	Host D
Critical	Host F

(1) Event types that support event level changing

You can change the event level of JP1 events and events in JP1/SES format, except when the severity level is a character string of 256 or more bytes. If JP1/IM is unable to change a severity level as directed, the message `KAVB4611-E` is output to the integrated trace log file.

(2) Effect on JP1/IM functions

The severity changing function has an effect on various JP1/IM functions. The following table lists the definitions affected by changes to event levels, and indicates which of the event levels you can specify in each function.

Table 11–5: Effect on JP1/IM functions

No.	Definition	Event level prior to change	Event level after change
1	Event acquisition filter	Y	N
2	View filter	Y	Y
3	Event receiver filter	N	Y
4	Severe event definition	N	Y

No.	Definition	Event level prior to change	Event level after change
5	Event search conditions	Y	Y
6	Correlation event generation definition	N	Y
7	Automated action definition	N	Y
8	Definition for extended event attributes	N	Y
9	Event guide information	N	Y
10	Definition for opening monitor windows	N	Y
11	Mapping definition of the event source host	Y	N
12	Repeated event condition	Y	N
13	Display message change definition	N	Y

Legend:

Y: Can be specified.

N: Cannot be specified.

(3) Effect on linked products

The severity changing function has an effect on the products linked with JP1/IM.

The following describes the effects of the severity changing function in the Central Scope and JP1/IM - Rule Operation.

(a) Effects in Central Scope

The Central Scope monitors JP1 events based on their new event levels.

In some cases, changing an event level might cause a status change condition already established for a monitoring node not to match the monitoring condition. To avoid a situation in which the status of a monitoring node does not change as intended, you need to review status change conditions set for the following system-monitoring objects:

- Agent Monitoring (PFM) system-monitoring objects
  - Resource error event (PFM)
  - Resource warning event (PFM)
- HiRDB Monitoring system-monitoring objects
  - HiRDB emergency event
  - HiRDB alert event
  - HiRDB critical event
  - HiRDB error event
  - HiRDB warning event
- Physical Host Monitoring (System Manager) system-monitoring objects
  - Physical host emergency event
  - Physical host alert event
  - Physical host critical event
  - Physical host error event

- Physical host warning event

For details about system-monitoring objects, see *Chapter 4. Lists of System-Monitoring Objects (for Central Scope)* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

(b) Effects in JP1/IM - Rule Operation

In a rule startup condition of JP1/IM - Rule Operation, specify the original event level of the JP1 event.

11.1.9 Considerations for changing display messages for JP1 events

For easier system monitoring and event management, consider changing the format of display messages for JP1 events.

The display message change function enables you to change the display message text for JP1 events to a desired format so that you can display only the important parts of the message text during monitoring to make them more readable.

Carefully evaluate the following items of the display message change definition:

- Determine which JP1 events' display messages need to be changed
- Determine the parts of the original messages you want to be displayed after the change
- Determine the format of the messages after the change

For details about the display message change definition file, see *Display message change definition file (jcochmsg.conf)* (*Chapter 2. Definition Files*) in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

(1) Considerations for the display message change definition

The following table shows an example of a message for a JP1 event.

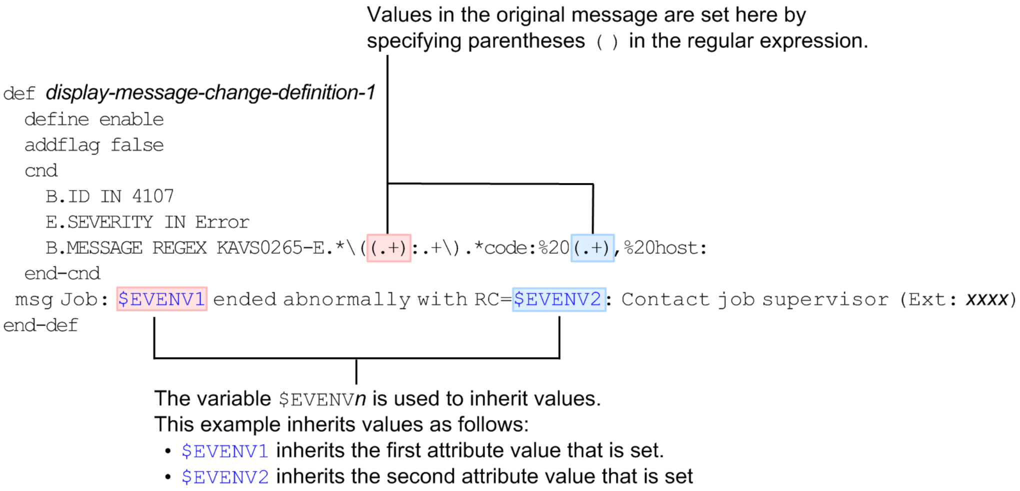
Table 11–6: Example of a message for a JP1 event

Message type	Message contents
Message before change	KAVS0265-E Job ended abnormally. (name: *job-name*: *execution-ID*, status: *status*, code: *code*, host: *host-name*, JOBID: *job-number*)
Message after change	Job: *job-name* ended abnormally with RC=*code*: Contact job supervisor (ext:*xxxx*)

Legend:
Underline (__): Information that is inherited from the message before change.

The following figure shows an example of the definition in the display message change definition file.

Figure 11–19: Example of a definition in the display message change definition file



Values in the original message are set here by specifying parentheses ( ) in the regular expression.

```
def display-message-change-definition-1
  define enable
  addflag false
  cnd
    B.ID IN 4107
    E.SEVERITY IN Error
    B.MESSAGE REGEX KAVS0265-E.*\((.+):.+\).*code:%20(.+),%20host:
  end-cnd
 msg Job: $EVENV1 ended abnormally with RC=$EVENV2: Contact job supervisor (Ext: xxxx)
end-def
```

The variable $EVENV*n* is used to inherit values.
This example inherits values as follows:

- $EVENV1 inherits the first attribute value that is set.
- $EVENV2 inherits the second attribute value that is set

To use the display message change definition shown here, copy the following code:

```
def display-message-change-definition-1
define enable
addflag false
cnd
B.ID IN 4107
E.SEVERITY IN Error
B.MESSAGE REGEX KAVS0265-E.*\((.+):.+\).*code:%20(.+),%20host:
end-cnd
msg Job: $EVENV1 ended abnormally with RC=$EVENV2: Contact job supervisor (Ext: xxxx)
end-def
```

(2) Events for which display messages can be changed

You can change display messages for JP1 events and events in the JP1/SES format. Note that display messages cannot be changed for events whose display messages have already been changed or for JP1 events whose display messages have been converted by JP1/IM - MO (the event ID in both cases is 00006400).

(3) Functions that can use messages whose display messages have been changed

The following functions can use messages whose display messages have been changed:

- Automated action (inheritance to actions)
- View filter
- Event search (search object is the integrated monitoring database)
- Command execution
- Event output

11.1.10 Considerations for setting event guide information

The event guide function supports investigating the causes of problems and solving problems by defining and accumulating know-how as messages. This will typically include such items as investigation methods, solutions, and past cases.

The system administrator manages the system through a process of error detection based on JP1 event monitoring, investigation, and remedial action. By recording your experience and results as event guide information after you have resolved a problem, users can respond quickly if the same type of JP1 event occurs again.

Event guide information is displayed as detailed information about a JP1 event in the Event Details window of the Central Console.

One item of event guide information can be displayed for one JP1 event. But the larger the system, the greater the number of JP1 events issued from linked JP1 products and user applications. Consider the following points when setting event guide information.

(1) Restricting applicable JP1 events

JP1 events cover a wide range and their number increases according to the size of the system. It would not be easy to set event guide information for every event. Also, the number of items that can be defined in an event guide information file is limited to 1,000.

For these reasons, you must restrict the JP1 events for which event guide information is set. Decide how to do this from the following perspectives, for example.

(a) Restricting applicable JP1 events by event level

The JP1 event levels are `Emergency`, `Alert`, `Critical`, `Error`, `Warning`, `Notice`, `Information`, and `Debug`. Depending on the types of JP1 events issued by the managed hosts in your system, register event guide information for the more important JP1 events (`Error` level or higher, for example).

When you use the integrated monitoring database, the user-defined event level applies for JP1 events.

Under the default settings, JP1 events of `Emergency`, `Alert`, `Critical`, `Error`, or `Warning` level are forwarded to a manager from JP1/Base on an agent.

(b) Restricting applicable JP1 events by frequency and urgency

Find out what sort of JP1 events are being issued from the managed hosts by performing an event search or by executing the JP1/Base `jevexport` command, and examine the subtotals in the output results. If it appears that some JP1 events of concern are being issued more often than others, you can target those JP1 events according to which host they originate from, or how urgently they need to be identified and dealt with.

If any JP1 events requiring urgent action are being issued at a high frequency, the system administrator and operators will need to discuss and determine troubleshooting procedures. Set event guide information for these sorts of JP1 events.

For details about the `jevexport` command, see the chapter on commands in the *JP1/Base User's Guide*.

> **Important**
>
> A maximum of 1,000 items of event guide information can be set. Make sure that you prioritize JP1 events to keep them within this limit.

If it is difficult to restrict the applicable JP1 events to no more than 1,000, consider the following strategy:

- Group similar events or related events, and write a list of links (used as an index page) in the event-guide message for the group.

This approach requires the user to search for advice relating to a particular event from the list of links. You should therefore establish clear editing rules and explore other ways of making the list easy to search.

(2) Setting appropriate event guide information

Because you can set event guide information as you choose, you can set appropriate information for your operational requirements, as in the following examples:

- Event guide information for initial response
  State how to respond to a problem detected by a JP1 event, and guide the system administrator on what action to take when the problem occurs. Set this as event guide information.
- Event guide information for error investigation and troubleshooting
  State what JP1/IM functions to use when investigating a problem detected by a JP1 event, and write down the action procedure for the problem. Set this as event guide information.

You can also prepare event guide information according to the nature of the JP1 event. For example, for JP1 events of `Error` level or higher that require urgent action, you might describe the initial response procedure, while for JP1 events of `Warning` level indicating a preventable future problem, you might describe how to investigate and preempt the problem.

(a) Event guide information for initial response (example)

In this example, event guide information is needed for an event indicating that a JP1/AJS job running on a managed host has ended abnormally.

The JP1 event indicating abnormal termination of a JP1/AJS job has an event ID (`B.ID`) of 00004107 and an event level (`E.SEVERITY`) of `Error` level. Set event guide information for this JP1 event as follows.

Example of contents written in the event guide information file (`jco_guide.txt`):

(extract of the condition definition)

```
[EV_GUIDE_001]
EV_COMP=B.ID:00004107:00000000
EV_COMP=E.SEVERITY:Error
EV_GUIDE=The job ended abnormally.\n Contact the system administrator in
charge of host $E.C0 urgently.\n\n List of system administrator contact
details \n Host-A:TEL(03-xxxx-xxxx) Mail(xxxxx@xxx.co.jp) \n Host-B:TEL(03-xxxx-
xxxx) Mail(xxxxx@xxx.co.jp) \n Host-C:TEL(03-xxxx-xxxx) Mail(xxxxx@xxx.co.jp)
[END]
```

(b) Event guide information for error investigation and troubleshooting (example)

In this example, event guide information is needed for an event indicating that the number of commands queued in JP1/Base running on an agent has reached a set threshold.

The JP1 event indicating that the command queue count threshold has been exceeded has an event ID (B.ID) of 00003FA5 and an event level (E.SEVERITY) of Warning level. Set event guide information for this JP1 event as follows.

Example of contents written in the event guide information file (jco_guide.txt):

(extract of the condition definition)

```
[EV_GUIDE_002]
EV_COMP=B.IDBASE:00003FA5
EV_COMP=E.SEVERITY:Warning
EV_FILE=user-specified-folder(path)\jco_guidemes_002.txt
[END]
```

Example of contents written in an event-guide message file (jco_guidemes_002.txt)

The number of queued commands has exceeded the threshold (10).

Determine the JP1/Base host from the message text.

Check whether there is insufficient memory or a backlog of automated actions on the host.

Open the List of Action Results window, or execute the jcashowa and jcocmdshow commands, to check the statuses of the automated actions.

If any urgent automated actions are waiting to be executed, cancel them as a temporary measure.

To cancel an automated action, use the jcacancel or jcocmddel command.

These two commands display a confirmation message requiring you to type y or n. When executing either command from the Execute Command window, specify the -f option to bypass the confirmation message.

If this event occurs frequently, use the jcocmddef command to modify the command execution environment.

(3) Setting event guide information using variables (placeholder strings)

A variable (placeholder string) can be used to represent a JP1 event attribute in an event-guide message. For example, if you set the host name of the server where the problem originated (B.SOURCESERVER) as a variable, the actual host name will be displayed in the event guide information by means of the variable, and the message text will match the actual situation. This reduces the time required to identify the host where the problem occurred.

The following table describes the variables you can use in an event-guide message.

Table 11–7: Variables that can be used in event-guide messages

Event attribute		Variable	Format of substituted value
Basic attribute	Serial number	B.SEQNO	Integer character string
	Event ID	Either of the following: 1. B.ID 2. B.IDBASE	String in the format: 1. *basic-code*:*extended-code* 2. *basic-code*
	Source process ID	B.PROCESSID	Integer character string
	Registered time	B.TIME	
	Arrived time	B.ARRIVEDTIME	
	Source user ID	B.USERID	
	Source group ID	B.GROUPID	
	Source user name	B.USERNAME	Character string

Event attribute		Variable	Format of substituted value
	Source group name	B.GROUPNAME	
	Source event server name	B.SOURCESERVER	
	Destination event server name	B.DESTSERVER	
	Source serial number	B.SOURCESEQNO	Integer character string
	Message	B.MESSAGE	Character string
Extended attribute	Event level	E.SEVERITY	
	User name	E.USER_NAME	
	Product name	E.PRODUCT_NAME	
	Object type	E.OBJECT_TYPE	
	Object name	E.OBJECT_NAME	
	Root object type	E.ROOT_OBJECT_TYPE	
	Root object name	E.ROOT_OBJECT_NAME	
	Object ID	E.OBJECT_ID	
	Occurrence	E.OCCURRENCE	
	Start time	E.START_TIME	
	End time	E.END_TIME	
	Result code	E.RESULT_CODE	
	Event source host name	E.JP1_SOURCEHOST	
	Other extended attribute	E.*xxxxxx*#	

#: Any JP1 product-specific extended attribute can be used. For example, a JP1/AJS job execution host is E.C0. For details about program-specific extended attributes, see the documentation for the particular product that issues JP1 events.

By using these variables, you can write event-guide messages that can be generally applied. For example, if you use the variable for a JP1/AJS job execution host (E.C0), you can write event-guide messages like the following.

Example of an event-guide message using a variable (extract of the EV_GUIDE segment):

```
EV_GUIDE=The job ended abnormally.\n Check whether an error occurred on host
$E.C0.\n In a previous case, the job failed due to insufficient memory on
host A.\n Check the available memory using the vmstat command.
```

If the guide information is in HTML format, the event-guide message is output in HTML format. If the JP1 event attribute value to be converted from the variable is URL-encoded or Base64-encoded, the Web pages of the linked products can be displayed without being garbled. For details about the conversion, see *Event guide information file (jco_guide.txt)* in *Chapter 2. Definition Files* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

For details about JP1 event attributes, see *3.1 Attributes of JP1 events* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

The character strings that can be substituted in a JP1 event attribute (variable) depend on the product. When using variables in event-guide messages, see also the description of JP1 events in the product documentation.

(4) Setting event guide information for each display user

You can set an event guide message for each display user (`EV_USER`). For a JP1 event, you can set an event guide message for system administrators or an event guide message for a certain business group.

For one event guide message, a maximum of 100 JP1 users can be specified as the display users. The following shows an example of a setting in the event guide information file (`jco_guide.txt`).

Example of a setting in the event guide information file (`jco_guide.txt`)

(Excerpt from the condition definitions)

```
[EV_GUIDE_002]
EV_USER=jp1user1 jp1user2 jp1user3
EV_COMP=B.IDBASE:00003FA5
EV_COMP=E.SEVERITY:Warning
EV_FILE=any-folder(path)\jco_guidemes_002.txt
[END]
```

11.1.11 Considerations for saving monitoring information (CSV snapshot)

JP1/IM - View provides functionality for saving the JP1 event information displayed in the Event Console window in CSV format.

Using this function, you can keep a history (CSV snapshots) of problems occurring from day to day, and of actions taken by the operator.# This information can be used, for example, in preparing monitoring reports for the system administrator.

#: If you need to keep records of who dealt with a problem, and when the action was taken, consider issuing a JP1 event when the response status of a JP1 event is changed. For details, see *12.7.5 Issuing a JP1 event when a response status changes*.

11.1.12 Considerations for saving event information in the integrated monitoring database (output of event report)

JP1/IM provides functionality for saving the JP1 event information stored in the integrated monitoring database (output of event report).

Using this feature, you can keep a record of problems associated with JP1 events stored in the integrated monitoring database. You can also keep historical JP1 event information by outputting an event report when the integrated monitoring database reaches capacity.

By specifying an option when using the event report output functionality, you can choose the following output modes:

- Maintenance information output
  Outputs all the JP1 events recorded in the integrated monitoring database.
- Backup information output
  Outputs the JP1 events that are at risk of deletion.

For details about outputting event reports, see *3.15.2 Saving event information in the integrated monitoring database (CSV report)*.

11.2 Considerations for system monitoring from the Central Scope

The Central Scope allows you to monitor the system from the viewpoints required by the system administrator.

This section describes points to consider as regards the system monitoring environment required for using the Central Scope and the auto-generation function.

Before you consider system monitoring from the Central Scope, read the following reference and make sure that you understand how the Central Scope works.

About the Central Scope:

- Central Scope functionality
  See *Chapter 4. Objective-Oriented System Monitoring Using the Central Scope*.

11.2.1 Considerations for monitoring trees

Using a monitoring tree, you can monitor the system by grouping resources according to the viewpoints required by the system administrator and displaying them in a tree format.

A monitoring tree can be easily generated using the auto-generation and editing functions.

To generate a monitoring tree, select a purpose-built template in the Auto-generation - Select Configuration window. JP1/IM provides the following monitoring tree models:

- Work-oriented tree
- Server-oriented tree

For details, see the following references.

About monitoring trees:

- Monitoring tree functionality
  See *4.2 Monitoring tree*.
- Auto-generation of a monitoring tree
  See *4.3 Automatically generating a monitoring tree*.

Note

By setting JP1 resource groups for specific nodes, you can set up the following controls:

- Restrict the range of resources (monitoring nodes) that individual JP1 users can view and monitor
  For example, you can permit a user who has `jp1admin` permission to monitor the entire system, but allow users with `jp1ope` permission to monitor only part of the system.
- Precisely control operations on displayed monitoring nodes to meet your objectives
  For example, you can permit response operations (status changes) on specific monitoring nodes, but allow viewing only on particular nodes.

For details about setting JP1 resource groups for monitoring nodes, see *4.4.3 Setting the monitoring range of a monitoring tree*.

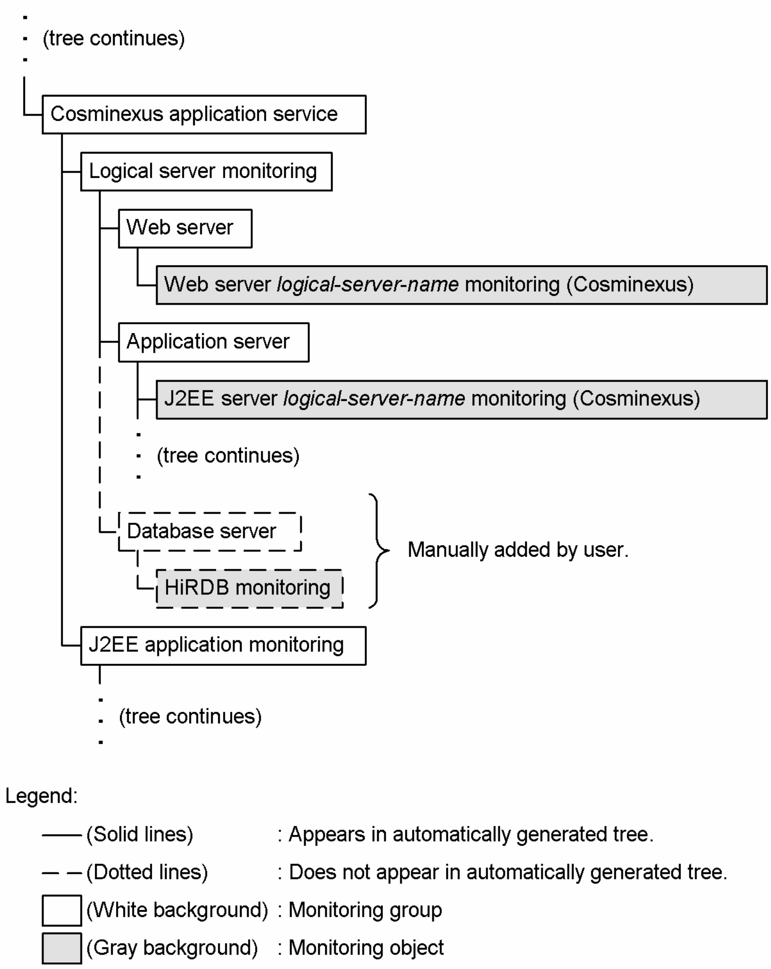
For a JP1 user who is to be registered with JP1/Base (authentication server), the account settings in JP1/Base (JP1 resource group setting) must match the setting in the Central Scope. For details, see the chapter on setting up user management in the *JP1/Base User's Guide*.

(1) Notes

- If you automatically generate a work-oriented or server-oriented monitoring tree for monitoring a Cosminexus system environment, the resulting tree will be unable to acquire information from databases that run under Cosminexus such as HiRDB. To monitor a database as a logical server in a Cosminexus environment, you must manually add the database information to the monitoring tree.

  The following figure shows how you can add database information to a monitoring tree, using HiRDB as an example.

  Figure 11–20: Example of adding database information to a monitoring tree


(tree continues)
Cosminexus application service
Logical server monitoring
Web server
Web server *logical-server-name* monitoring (Cosminexus)
Application server
J2EE server *logical-server-name* monitoring (Cosminexus)
(tree continues)
Database server
HiRDB monitoring
Manually added by user.
J2EE application monitoring
(tree continues)
Legend:
(Solid lines) : Appears in automatically generated tree.
(Dotted lines) : Does not appear in automatically generated tree.
(White background) : Monitoring group
(Gray background) : Monitoring object

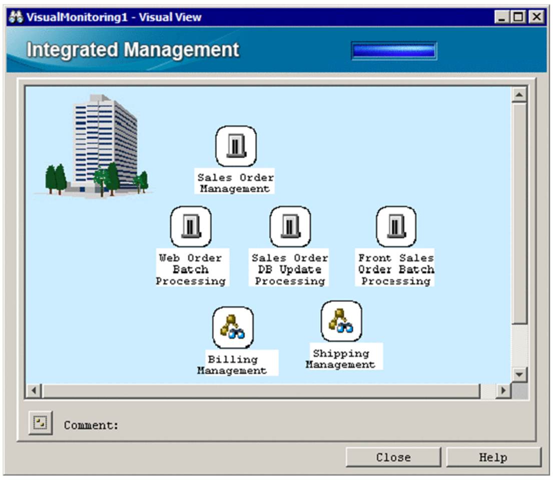
  With HiRDB 07-02 or later, you can use the system-monitoring object provided by the Central Scope to add the database information to the tree. For all other databases, create a general monitoring object and define the monitoring conditions as required.

11.2.2 Considerations for visual monitoring

Using the Visual Monitoring window, you arrange the objects and groups that you want to watch closely in a map view. This allows you to easily monitor even a large system from key perspectives.

By customizing the background image and Visual Icon in the Visual Monitoring window with images of your choice, you can create a window that is tailored to your particular needs. The following figure shows an example of a customized Visual Monitoring window.

Figure 11–21: Example of Visual Monitoring window customized with background image and Visual Icon


VisualMonitoring1 - Visual View
Integrated Management
Sales Order Management
Web Order Batch Processing
Sales Order DB Update Processing
Front Sales Order Batch Processing
Billing Management
Shipping Management
Comment:
Close
Help

For details, see the following reference:

About visual monitoring:

- Visual monitoring functionality
  See *4.5 Visual monitoring*.

(1) Icons and background images used for visual monitoring

Consider what icons and background images are to be used for visual monitoring according to the viewpoint from which you monitor daily tasks.

For example, consider the background images to be used from the following viewpoints:

- Geography of the system monitored with the Visual Monitoring window
  Example: In units of region, business base, or floor of the same building
- Tasks in the system monitored with the Visual Monitoring window
  Example: Customer management, commodity management, sales management, inventory management, order management, and others

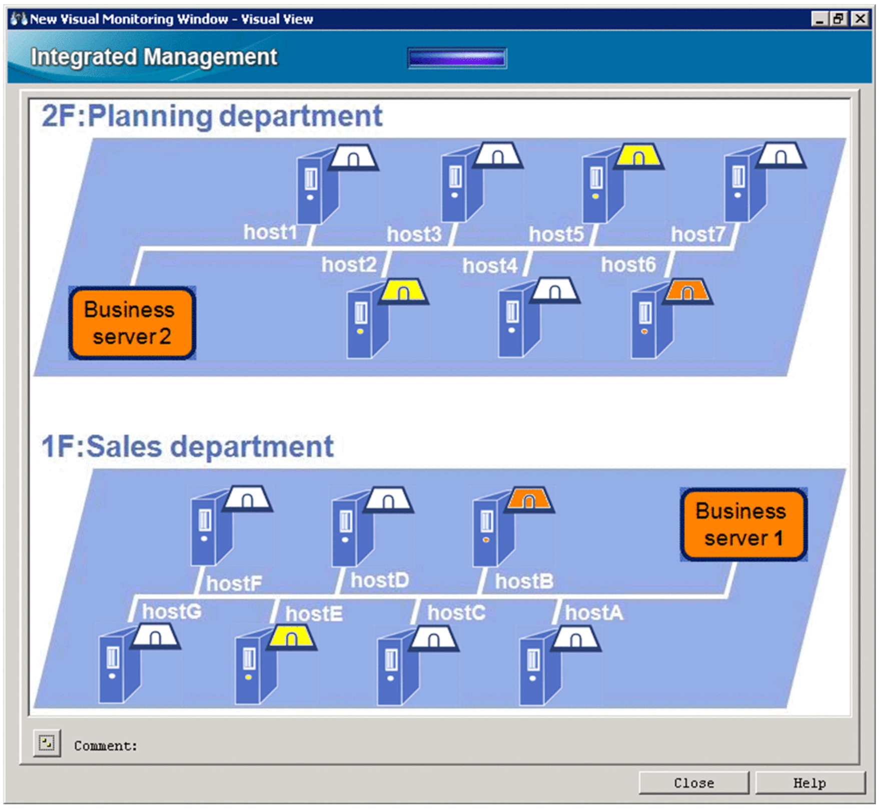
(2) Suppressing the display of monitoring node name and margins of monitoring node icon

Consider whether to suppress the display of monitoring node name and margins of monitoring node icon to adjust to the colors of the Visual Icon and background images to be used.

For example, when you use the Visual Icon and background image described below, you can have a high degree of freedom when creating monitoring windows by suppressing the display of monitoring node name and margins of monitoring node icon.

- Visual Icon that assimilates into the background image
- Background image in which a monitoring node name embedded

Figure 11–22: Example of window that uses a background image in which monitoring node names are embedded



About suppressing the display of monitoring node name and margins of monitoring node icon

- For the display of monitoring node name and margins of monitoring node icon:
  See *4.6.1 Suppressing display of monitoring node name and the margins of monitoring node icon*.

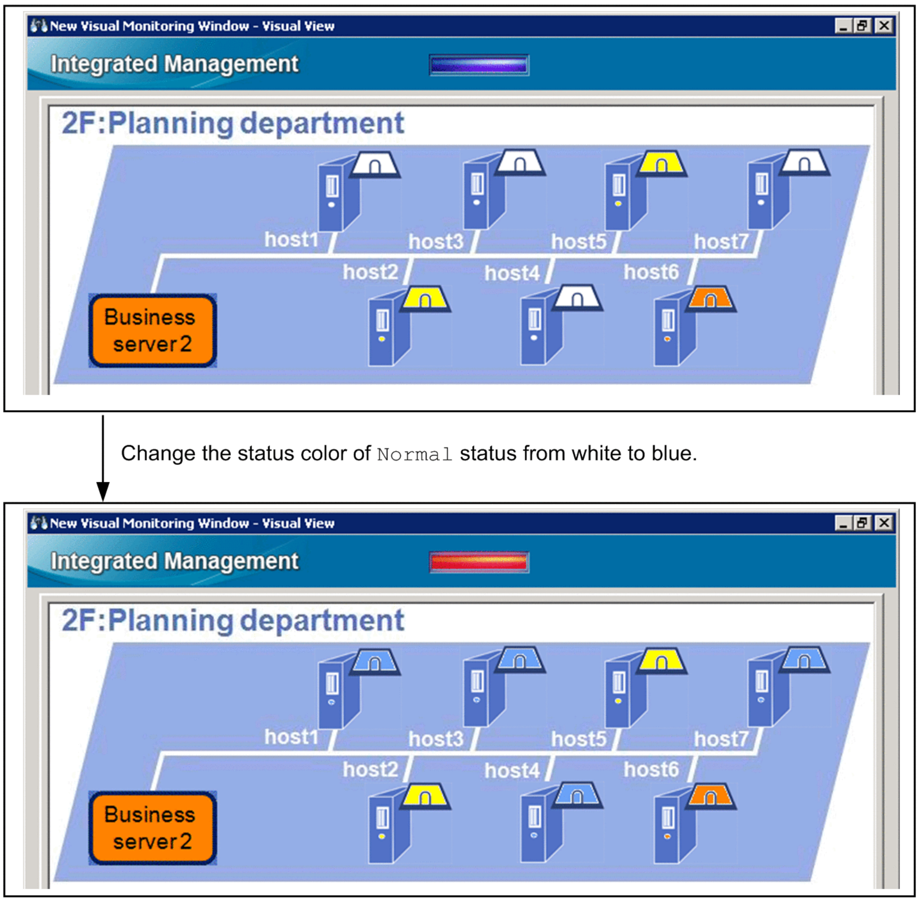
(3) Setting the status colors for monitoring node name and monitoring node

Consider the status colors for monitoring node name and monitoring node in contrast with the colors of the Visual Icon and background image to be used. In particular, avoid setting a status color that is the same as the color of the background image.

For example, change the settings of status colors in the following cases:

- Changing the `Normal` status color (white) to a different color
- Setting a transmission factor for status colors to always show background images
- Changing the `Warning` status color (yellow) to use yellow-themed background images

Figure 11–23: Example of window in which the Normal status color is changed from white to blue



Change the status color of `Normal` status from white to blue.

About setting the status colors for monitoring node name and monitoring node

- For the settings of status colors for monitoring node name and monitoring node
  See *4.6.2 Setting status colors for monitoring node name and monitoring node*.

11.2.3 Considerations for setting guide information

Using the guide function, you can display troubleshooting procedures, examples of how various errors have been handled in the past, and other such operating know-how. This guide information can be used as reference material when a problem occurs, lessening the workload of the system administrator at the initial response stage.

The content and display conditions for guide information must be considered and set by the user. Because the data on which guide information is based (operating know-how and so on) is accumulated and changes while the system is being run, make sure that you review it periodically, and amend or augment the information as required.

For details, see the following reference:

About guide information:

- Guide function
  See *4.8 Guide function*.

Note

Differences between the two guide functions

Guide functions are provided by both the Central Scope and Central Console. They can be used for different purposes, or you might prefer to use them in combination. They differ as follows.

- Guide function of the Central Scope
  Guide information can be set for individual monitoring nodes. A monitoring node is a job or server being monitored in the system. Use the Central Scope's guide function when you are monitoring the system based on a monitoring tree consisting of monitoring nodes.
  Use the guide function to write advice about problems in accounting jobs, for example, or about Web server errors.
- Event guide function of the Central Console
  Event guide information can be set for individual JP1 events. A JP1 event is an event that occurs in the system, and is also a potential cause when a problem occurs.
  Use the Central Console's event guide function to write advice about investigating or handling a specific JP1 event itself. For details, see *3.10 Event guide function* and *11.1.10 Considerations for setting event guide information*.

11.2.4 Considerations for suppressing moving of monitoring node icons

Suppressing moving of monitoring node icons enables you to prevent their layout from being disordered by mouse operations during monitoring in the detail view area (in map view) of the Monitoring Tree window and in the Visual Monitoring window.

If you create windows in which icon positions have special meanings, we recommend that you suppress moving of monitoring node icons.

For details, see the following reference:

About suppressing moving of monitoring node icons

- For details about suppressing moving of monitoring node icons
  See *4.6.3 Suppressing moving of monitoring node icon*.

11.2.5 Considerations for defining a status change condition for a monitoring group

By defining a status change condition for a monitoring group, you can monitor the system more precisely from a monitoring tree.

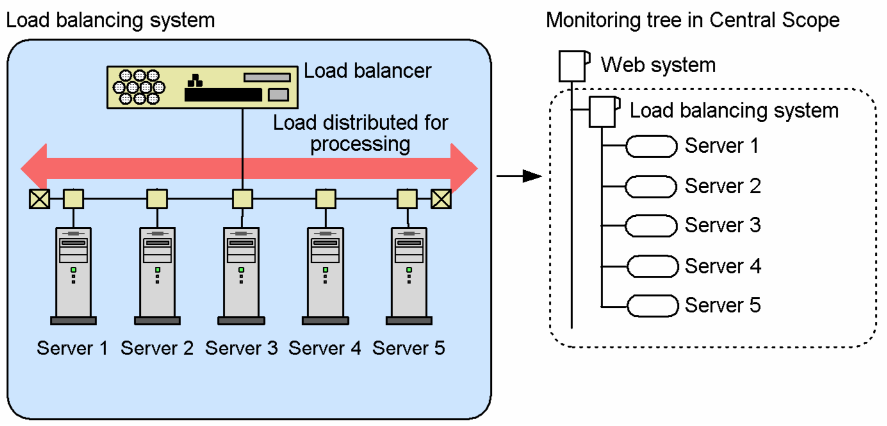
For example, in a system such as described below, where processing loads are distributed using a load balancer, an error on a lower-level node does not necessarily result in a problem in the higher-level monitoring group. In this type of system with special conditions, you can manage the system status more accurately by defining a status change condition for the monitoring group.

Note that the following restrictions apply when you define a status change condition for a monitoring group.

(1) Examples of defining a status change condition for a monitoring group

In the following example, the load-balancing system shown below is being monitored in a monitoring tree. *Load-balancing system* in this context means a system that uses a load balancer to distribute processing loads.

Figure 11–24: Example of monitoring from a tree view



The terms used in the explanation below have the following meaning:

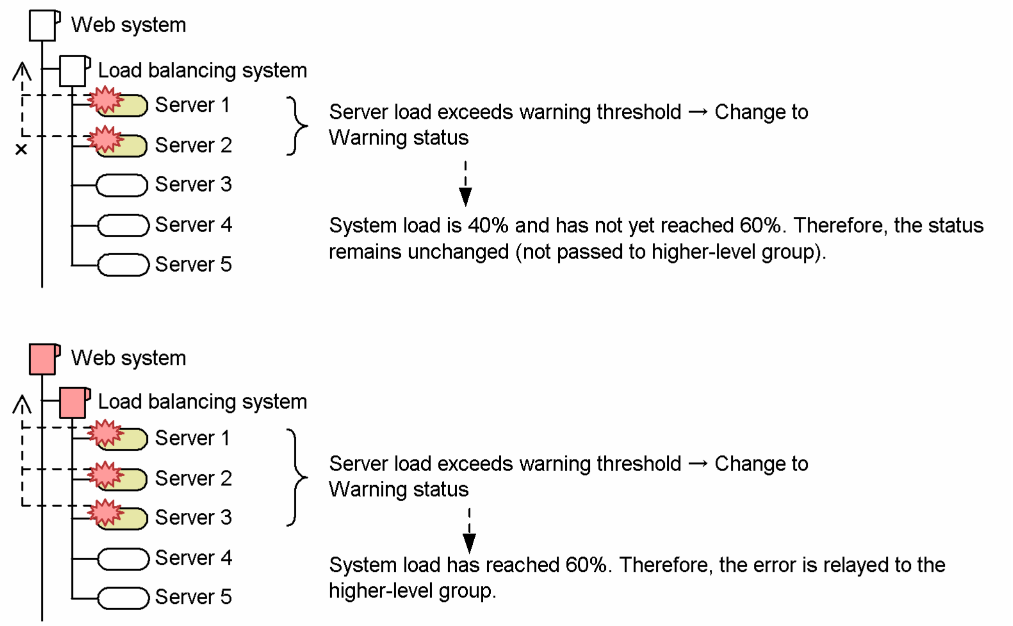
- Web system: Monitoring group (Web system)
- Load-balancing system: Monitoring group (load-balancing system)
- Server *X*: Monitoring object (server *X*)

The following conditions apply:

A Web system problem is assumed when the processing loads of 60% or more (three or more) of the five servers that make up the Web system have reached a **Warning** threshold.

Consider the following approach to relaying the node status when this system is monitored from a tree view.

Figure 11–25: Example of monitoring from a tree view (relaying the node status)


Web system
Load balancing system
×
Server 1
Server 2
Server 3
Server 4
Server 5
Server load exceeds warning threshold → Change to Warning status
System load is 40% and has not yet reached 60%. Therefore, the status remains unchanged (not passed to higher-level group).
Web system
Load balancing system
Server 1
Server 2
Server 3
Server 4
Server 5
Server load exceeds warning threshold → Change to Warning status
System load has reached 60%. Therefore, the error is relayed to the higher-level group.

The status change condition in this example is defined as follows:

Table 11–8: Example of defining a status change condition for a monitoring group

Node name	Status change condition for monitoring group		
	Status	Child node status#	Comparison condition
Load-balancing system	Error	Warning	Percentage: 60% or more or Count: 3 or more

#: The status setting here includes statuses of higher priority. For example, an Error setting includes Emergency, Alert, and Critical statuses.

With these settings, as long as less than 60% of the servers (three of the five servers) are in Warning status or worse, the status of the load-balancing system and Web system remains unchanged from Initial status. Hence, it is not possible to search for status change events from the higher-level load-balancing system or Web system.

If you want to manage status changes in the lower-level monitoring nodes, or to search for status change events in lower-level monitoring nodes from a higher-level monitoring group, we recommend that you define the condition as shown in the following table, for example.

Table 11–9: Example of defining a status change condition for a monitoring group (recommended)

Node name	Status change condition for monitoring group		
	Status	Child node status#	Comparison condition
Load-balancing system	Error	Warning	Percentage: 60% or more or Count: 3 or more
	Warning or Normal	Warning	Percentage: 20% or more or Count: 1 or more

#: The status setting here includes statuses of higher priority. For example, an Error setting includes Emergency, Alert, and Critical statuses.

(2) Limitations on defining a status change condition for a monitoring group

Bear in mind the following limitations when you define a status change condition for a monitoring group:

- The status of a child node color-coded as being in Error status will not necessarily be passed to the higher-level monitoring group.
  The higher-level monitoring group might remain in Initial status, even if a child node is in Error status. Because the child node status is not passed to the top-level monitoring group, the alarm lamp does not flash.
- When you search for status change events, some that affect lower-level nodes might be missing from the results.
  If there is a monitoring group in Initial status between the monitoring group from which you are searching and the monitoring object that has Error color-coding, status change events below the group in Initial status will not be retrieved.
  In this case, perform a monitoring node search to find nodes that have Error color-coding, and then perform a search for status change events.

If these two limitations are likely to be issues, define the condition so that any one child node in Error status will change the higher-level monitoring group to Warning status, for example.

- You must review the status change condition if child nodes are added or deleted and their number changes.

  You must review the definition if the number of child nodes increases or decreases. For example, if a status change condition is set for a monitoring group of five child nodes, the count (3 or more) and the percentage (60% or more) mean the same. However, they mean different things when the number of child nodes increases, as follows:

  - Count: 3 or more. If another five child nodes are added, making a total of 10, the count will be unchanged. (The status of the group changes when three nodes are in the specified status.)
  - Percentage: 60% or more. If another five child nodes are added, making a total of 10, the percentage will be 60% of 10; that is, six. (The status of the group changes when six nodes are in the specified status.)

  The Central Scope does not automatically redefine status change conditions. You should therefore periodically review the condition definitions.

- When the completed-action linkage function is enabled, the status of the monitoring group changes to `Initial` when you finish taking action on all the lower-level monitoring objects (when you change all status change events to **Processed** status). That is, the monitoring group will not be searched when you perform a status-change event search.

  If this limitation is likely to be an issue, define the condition so that a status change in any one child node cause a status change in the monitoring group. For example, specify that when a child node shifts to `Normal` status, the monitoring group changes to `Normal` status.

11.3 Considerations for error investigation in JP1/IM

When a problem is detected during system monitoring in JP1/IM, you can verify and identify the source of the error from JP1/IM - View.

Investigation strategies will depend on the applications and programs that make up the system. Consider investigation and troubleshooting methods suitable for the types of applications and programs you are using.

This section describes considerations regarding the system operations you can perform from JP1/IM.

11.3.1 Monitor startup

You can select a JP1 event displayed in JP1/IM - View and launch the GUI of the application associated with that event.

To open an application that issued a JP1 event in this way, the application must support the monitor startup function.

For details, see the following reference.

About the monitor startup:

- Monitor startup
  See *3.19.1 Launching a linked product by monitor startup*.

11.3.2 Tool Launcher

In the Tool Launcher window, you can register and start programs of your choice.

For details, see the following reference.

About the Tool Launcher:

- Tool Launcher
  See *3.19.2 Tool Launcher*.

11.3.3 Considerations for executing commands from JP1/IM - View

Using JP1/IM, you can execute commands from JP1/IM - View to the monitored hosts based on the configuration defined in JP1/Base Configuration Management. Or, you can execute commands on the client hosts (viewer hosts) by using the client application execution function.

You can register the regularly used commands to command buttons, and execute the commands by clicking the command buttons. This can avoid typos because you do not have to enter the commands from the command line.

For details about how to register command buttons, see *7.1.2 Executing a command by using the Command button* in the *JP1/Integrated Management - Manager Administration Guide*.

In addition, if you use the event information inheritance function, event information is automatically specified for the contents of the command.

For details about the event information inheritance function, see *3.19.5 Inheriting event information when a command is executed*.

For details about command execution, see the following references:

About command execution from JP1/IM - View:

- Execution of commands on managed hosts from JP1/IM - View
  See *3.19.3 Executing commands on managed hosts from JP1/IM - View*.
- Execution of commands on client hosts
  See *3.19.4 Executing commands on client hosts*.
- Overview of the command execution environment
  See *7.4.4 Managing command execution*.
- Overview of the system configuration definition and its effects
  See *7.4.3 Managing the system hierarchy*.

11.4 Considerations for automated actions

Consider both the conditions for executing an automated action, and the resulting action itself (contents of the executed command).

The command execution environment and user authentication functionality are also involved in executing automated actions. Consider these as well.

- Before suppressing an automated action, consider carefully whether the action is one that can be safely discarded. Examples are given below.

  Examples of actions that need to be executed once only during a set period (actions that can be suppressed):

  - An action that flashes a signal light
  - A user-notification action that sends an email
  - An action that needs to be suppressed during troubleshooting

  Examples of actions that should not be suppressed:

  - An action that performs recovery without user intervention
  - An action that changes depending on the event that triggered it

- When setting delay monitoring of an automated action, consider how long the action should take to complete from the time the JP1 event that triggers the action is received. Also consider the following:

  - Number of levels from JP1/IM - Manager to the target host

    The processing for sending an action from JP1/IM - Manager to the target host entails transfer processing to send the action request from the higher-level manager host to the lower-level manager hosts, and finally to have the target host receive the action. The greater the depth of the configuration management hierarchy, the greater the transfer processing involved and the longer the action will take to complete.

  - Network traffic from JP1/IM - Manager to the target host

    If JP1/IM - Manager is on a different server from the target host, the load on the network connecting the two hosts affects how long the action takes to complete. It will take longer when the network is busy than when traffic is light.

  - Load on the JP1/IM - Manager server

    The load on the server on which JP1/IM - Manager is running affects how long the action takes to complete. The greater the load, the longer it will take for the action to be sent from JP1/IM - Manager to JP1/Base on the same manager host, and the longer the action will take to complete.

  - Load on the target host

    The load on the target host affects how long the action takes to complete. The greater the load, the longer the action will take to complete.

  - Action execution time

    When an action takes longer than the delay monitoring time to execute, it will be reported as a delayed action. Make sure that you estimate action execution time accurately and set an appropriate delay monitoring time.

  In JP1/IM, you can set a maximum delay monitoring time of 24 hours. If you need to monitor an action that takes longer than 24 hours to execute, link with JP1/AJS as explained below to monitor the action.

  Example of monitoring the execution of an automated action by linking with JP1/AJS:

  Prepare a batch file or similar as the action to be executed by JP1/IM. The batch file or similar triggers execution of a JP1/AJS job, and then ends.

  To check whether a command (executed as a JP1/AJS job) that takes a day or longer to execute is running properly, use JP1/AJS.

- The commands in automated actions execute one by one, in the sequence that the actions are received at the target host. Delays might occur when one of these commands takes a long time to execute. In this case, you can reduce the chance of a delay by using the `jcocmddef` command to increase the number of commands executed concurrently by the JP1/Base on the target host.

  However, when commands are executed concurrently, those that take less time to process end more quickly. If you want commands to be processed in sequence, do not change the default (execute commands one by one).

  A maximum of 48 commands can be executed concurrently by the JP1/Base on the target host. When automated actions are executed by multiple instances of JP1/IM - Manager, bear the following in mind:

  - The total number of commands being executed concurrently by the instances of JP1/IM - Manager must not exceed 48.
  - Sufficient resources to execute the commands must be available on the target host of the automated action.
- An event that notifies the user of the status of an automated action references information saved in the action information file when invoked. If you are setting this type of action, set an adequate file size for the action information file. You can set the size of the action information file in the automated action environment definition file (`action.conf.update`). An action status notification event is issued at the following times:

  - When a command execution request ends normally and queuing of the action is confirmed
  - When the execution of an action ends (the action status changes to `Ended`, `Cancel`, or `Kill`)

    If the action status is `Ended`, the result code of the command set for the action is displayed. If the action status is `Cancel` or `Kill`, the result code is `-1`.
  - When the action status becomes an abnormal status (the action status changes to `Fail` or `Error`)
  - When the command execution request to command execution control for the action triggered by an action status notification event ends normally and queuing of the action is confirmed
  - The status of the action triggered by an action status notification event becomes an abnormal status
- If you use event information inheritance, event information is automatically specified in the contents of the command. For details about the event information inheritance function, see *3.19.5 Inheriting event information when a command is executed*.

For details about automated actions, see the following references:

About automated actions:

- Overview of automated actions

  See *Chapter 5. Command Execution by Automated Action*.
- Overview of the command execution environment

  See *7.4.4 Managing command execution*.
- Setting automated actions (via the GUI)

  See *2.32 Action Parameter Definitions window* in the manual *JP1/Integrated Management - Manager GUI Reference*.
- Setting automated actions (in a definition file)

  See *Automated action definition file (actdef.conf)* in *Chapter 2. Definition Files* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.
- Setting the automated action environment

  See *Automated action environment definition file (action.conf.update)* in *Chapter 2. Definition Files* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.
- Setting the environment for monitoring the execution of automated actions

See *Automatic action notification definition file (actnotice.conf)* in *Chapter 2. Definition Files* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

- Setting the command execution environment for automated actions on the target host

  See the description of the `jcocmddef` command in the *JP1/Base User's Guide*.

- Configuration definition

  See *Configuration definition file (jbs_route.conf)* in *Chapter 2. Definition Files* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

11.4.1 Notes regarding the considerations for automated actions

- When a command execution log (ISAM) file is wrapped, the results of automated actions can no longer be acquired or displayed.

  Example:

  When you open the Action Log Details window, the message KAVB5150-W appears in the **Message** area.

  If this message is displayed, take action as described in *10.5.1(14) Actions to take when KAVB5150-W is displayed in the detailed information (message) for the action result* in the *JP1/Integrated Management - Manager Administration Guide*.

- Delays might occur when a large number of events that trigger actions are generated in a short space of time, leading to a considerable backlog of actions queued on the target hosts.

  In this situation, consider changing the number of commands that can be executed concurrently. Use the `jcocmddef` command to change this setting. However, when commands are executed concurrently, those that take less time to process end more quickly. If you want commands to be processed in sequence, do not change the default (execute commands one by one).

- If any of the following events occurs during the execution processing of an automated action, the action ceases to proceed through the usual status transition (this applies only to actions whose status is `Wait`, `Send`, `Queue`, `Running`, `Wait (Canceling)`, `Send (Canceling)`, `Queue (Canceling)`, or `Running (Canceling)`):

  - The manager host, action relay host, or action target host is shut down or otherwise stopped.
  - Network error
  - JP1/Base failure

  In this situation, check the status of the automated actions as follows.

  Using the JP1/Base `jcocmdshow` command (supported in version 07-51):

  You can check the action status using this command if the automated action was being processed by JP1/Base (command execution management) on the target host.#

  #: If the processing request has not yet been received or if processing has ended, you cannot use this command to check the action status.

  If an automated action ceases to progress and the `jcocmdshow` command cannot be used to check its status, evaluate whether it needs to be re-executed, and do so if necessary from the Execute Command window.

- If you cannot check the execution status or result of an automated action, there might be inconsistencies in the automated action logs (command execution log file, action information file, and action hosts file).

  In this situation, take action as described in *10.5.1(10) Actions to take when Unknown is displayed as the automated action execution status* in the *JP1/Integrated Management - Manager Administration Guide*.

- Using the `jcocmddef` command, you can disable registration of detailed execution results (message information) to the command execution log file, thereby increasing the processing speed of the underlying JP1/Base components (registration is enabled by default). Disabling registration, by increasing the JP1/Base processing speed, also increases the speed at which automated actions are executed.

However, when you disable registration of detailed information, the **Message** area of the Action Log Details window will show message KAVB2401-I for every action.

Change the setting (disable registration) only if this is not an issue and you definitely need to increase the automated action execution speed.

- Using the `jcocmddef` command, you can restrict the amount of execution log data forwarded to the manager host. This helps control the size of the command execution log file and reduces congestion on the network between the hosts. Note that the default setting for restricting log data transfer differs according to the JP1/Base version, as follows:
  - If you performed a new installation of JP1/Base version 8, the amount of result data logged for an action executed on that host is restricted to a maximum of 1,000 lines.
  - If you are running version 7 or earlier of JP1/Base, or if you upgraded from version 7 to version 8, there is no restriction on the amount of result data logged for an action executed on that host.

  When log data transfer is restricted, only the specified amount of execution results will be forwarded. This might mean that the displayed data is truncated. (The fact that the results have been truncated is mentioned at the end of the displayed information.)

  Change the setting (restrict log data transfer) only after you have considered whether you will need full data in the execution results.
- Do not use a command that directly shuts down the OS in an automated action. Use JP1/Power Monitor to shut down an agent.

11.5 Considerations for managing the system hierarchy

Consider how to manage the system hierarchy to set or change the system configuration managed by JP1/IM (IM configuration). The system hierarchy includes the hierarchy that manages the system configuration of physical hosts and the virtualization system hierarchy that manages the system configuration of virtual hosts. You can also manage the system hierarchy by setting business groups or by placing remotely monitored hosts below the integrated manager or the base managers.

11.5.1 Managing the system hierarchy

Consider how to manage the system hierarchy (IM configuration) to manage the system configuration of physical hosts. You can use either of the following methods to manage the system hierarchy:

Using IM Configuration Management

By using IM Configuration Management, you can centrally manage the system hierarchy from IM Configuration Management - View.

To use IM Configuration Management, you must activate the IM Configuration Management database. Make sure that you take into account the IM database space requirements during the system design stage.

When using IM Configuration Management to manage the system hierarchy, consider the operation in which the configuration management function provided by JP1/Base is not used together with IM Configuration Management. If you have edited configuration definition files that are used by the configuration management function provided by JP1/Base or executed commands associated with the configuration management function, make sure that you re-acquire the IM configuration by IM Configuration Management.

Without using IM Configuration Management

If you do not intend to centrally manage the system hierarchy from a manager, you can use the configuration management function provided by JP1/Base.

With this function, you define the host relationships in the configuration definition file (`jbs_route.conf`) on the manager, and use the associated commands (`jbsrt_distrib`, `jbsrt_sync`, `jbsrt_del`, and `jbsrt_get`) to apply and check the settings.

There is no need to activate the IM Configuration Management database if you do not intend to use IM Configuration Management. Therefore, you do not need to estimate the IM database space requirements during the system design stage.

For details about these functions, see the following references:

Using IM Configuration Management

- Managing the system hierarchy using IM Configuration Management
  See *Chapter 6. System Hierarchy Management Using IM Configuration Management*.

Without using IM Configuration Management

- Managing the system hierarchy using the configuration definition function provided by JP1/Base
  See *7.4.3 Managing the system hierarchy* and *7.4.5 Collecting and distributing definition information*.

When you change the management mode after beginning management of the system hierarchy, if you use IM Configuration Management and the `jbsrt_distrib` command provided by JP1/Base at the same time, the following information might become inconsistent. This might disorder the system operation.

- Information displayed in the IM configuration management viewer
- Information actually applied to the system

- Configuration definition information retained by hosts

Therefore, we do not recommend you to change the management mode after beginning managing the system hierarchy. Carefully consider which mode of hierarchy management you want to employ before you start using the system.

11.5.2 Managing the remote monitoring configuration

Consider how to collect logs from the remotely monitored hosts by managing the remote monitoring configuration. For remote monitoring, the remote monitoring configuration must be set up. For details about considering the system configuration, see *12.5 Considerations for the system hierarchy*.

(1) Collectable log information and connection methods for remote monitoring

Consider the log types to be collected from the remotely monitored hosts and the connection methods for remote connection in a remote monitoring configuration, referring to *6.6.2 Collectable log information and connection methods for remote monitoring* and *6.6.3 Log information that can be monitored*.

To remotely monitor hosts by using NetBIOS (NetBIOS over TCP/IP), WMI, or SSH, the settings for remote connection must be configured on the hosts on which JP1/IM - Manager is installed and on the monitored hosts. For details about how to configure remote connections, see *1.17 Specifying settings for monitoring logs on remotely monitored hosts (for Windows)* (for Windows) or *2.16 Specifying settings for monitoring logs on remotely monitored hosts (for UNIX)* (for UNIX) in the *JP1/Integrated Management - Manager Configuration Guide*.

(2) Log information collection interval

Consider the interval for collecting log information from the remotely monitored hosts beforehand. For details about the collection interval for log information, see *6.6.4 Monitoring interval for log information*.

11.5.3 Managing the virtualization system configuration

Consider how to manage a virtualization system configuration with the virtual hosts running on multiple virtualization system management hosts and VMM hosts.

(1) Considerations related to prerequisites

Check the types of virtualization software and virtualization environment management software and the prerequisite OSs to determine whether a virtualization system configuration can be managed.

Types of virtualization software and virtualization environment management software

To build virtual hosts, virtualization software and virtualization environment management software are required. Determine whether IM Configuration Management can manage the virtualization system configuration of your products. The following products are supported:

- Virtualization environment management software that can be used for the virtualization system management hosts:
  vCenter, JP1/SC/CM, SCVMM, and HCSM
- Virtualization software that can be used for VMM hosts:
  KVM, Hyper-V, Hitachi Compute Blade logical partitioning feature, and VMware ESX

The following table describes the available combinations of virtualization environment management software and virtualization software.

Table 11–10: Combinations of virtualization environment management software and virtualization software

Virtualization environment management software	Virtualization software
vCenter	VMware ESX
JP1/SC/CM	Hitachi Compute Blade logical partitioning feature
SCVMM#	Hyper-V
HCSM	Hitachi Compute Blade logical partitioning feature
--	KVM

Legend:

--: Unnecessary

#

When vCenter is managed by SCVMM, virtualization configuration information of vCenter and VMware ESX can be managed.

Prerequisite operating systems

The prerequisite operating system for JP1/SC/CM, vCenter, and SCVMM is Windows and it is supported by the versions of virtualization environment management software specified in the JP1/IM - Manager *Release Notes*.

Virtualization configuration information of virtualization software and virtualization environment management software that are running on UNIX cannot be collected.

(2) Methods of collecting virtualization configuration information

Virtualization configuration information is collected when the virtualization system configuration is changed, or when information is regularly managed. There are two methods of collecting virtualization configuration information as shown below. Consider which method is better for your environment.

Executing commands to collect virtualization configuration information

You can execute commands to collect virtualization configuration information from the virtualization software and virtualization environment management software. The commands differ depending on the types of the virtualization software and virtualization environment management software.

The following table describes the virtualization software and virtualization environment management software, and the commands you can use with specific software products.

Table 11–11: Virtualization software, virtualization environment management software, and corresponding commands

Type of virtualization software and virtualization environment management software from which information collected	Command name	Collection range
vCenter	`jcfcolvmvc`	• Virtualization system management host running vCenter • Virtual host running VMware ESX
JP1/SC/CM	`jcfcolvmvirtage`	Virtual host running Hitachi Compute Blade logical partitioning feature
SCVMM#1	`jcfcolvmscvmm`	• Virtualization system management host running SCVMM • Virtual host running Hyper-V

Type of virtualization software and virtualization environment management software from which information collected	Command name	Collection range
		- Virtual host running vCenter and VMware ESX if vCenter is managed by SCVMM
HCSM	`jcfcolvmhcsm`	Virtual host running Hitachi Compute Blade logical partitioning feature, and the host name#2 that can be acquired from HCSM
KVM	`jcfcolvmkvm`	Virtual host running KVM
VMware ESX	`jcfcolvmesx`	Virtual host running VMware ESX

#1: This software is available only for Windows.

#2: When collecting virtualization configuration information from hosts that are not virtual hosts running Hitachi Compute Blade logical partitioning feature, the only information you can collect is host names and host types. In addition, `Unknown` is always collected as the host type of the hosts from which the information is collected.

Using the IM configuration management viewer to collect virtualization configuration information

With the IM configuration management viewer, you can collect virtualization configuration information by specifying a virtualization system management host and hosts on which KVM is running. The type of the software running on the specified virtualization system management host determines the types of the virtualization software and virtualization environment management software from which information can be collected.

The following table describes the combinations of the software running on the host that collects virtualization configuration information and the virtualization software and virtualization environment management software from which the information is collected.

Table 11–12: Relationship of virtualization system management host, virtualization software, and virtualization environment management software

Software installed on the host collecting virtualization configuration information	Software from which information collected	Collection range
vCenter	VMware ESX	- Virtualization system management host running vCenter - Virtual host running VMware ESX
JP1/SC/CM	Hitachi Compute Blade logical partitioning feature	Virtual host running Hitachi Compute Blade logical partitioning feature
SCVMM#1	- Hyper-V - vCenter#2 - VMware ESX#2	- Virtualization system management host running SCVMM - Virtual host running Hyper-V - Virtual host running vCenter and VMwareESX when vCenter is managed by SCVMM
HCSM	Hitachi Compute Blade logical partitioning feature	Virtual host running Hitachi Compute Blade logical partitioning feature, and host name#3 that can be obtained from HCSM
KVM	KVM	Virtual host running KVM

#1: This software is available only for Windows.

#2: If vCenter is managed by SCVMM, information from both vCenter and VMwareESX is collected.

#3: When collecting virtualization configuration information from hosts that are not virtual hosts running Hitachi Compute Blade logical partitioning feature, the only information you can collect is host names and host types. In addition, `Unknown` is always collected as the host type of the hosts from which the information is collected.

(3) Methods of monitoring virtualization configuration information in the monitoring tree of the Central Scope

Consider whether to monitor the virtualization system configuration that contains the virtual hosts running on the virtualization system management hosts and VMM hosts in the monitoring tree of the Central Scope.

The method of monitoring virtualization configuration information in the monitoring tree of the Central Scope differs depending on the collection method described in *11.5.3(2) Methods of collecting virtualization configuration information*.

Executing commands to collect virtualization configuration information

Execute a command to import virtualization configuration information to the Central Scope, and apply the information to the monitoring tree.

Using the IM configuration management viewer to collect virtualization configuration information

After you collect virtualization configuration information from the IM configuration management viewer, actions such as the addition of VMM hosts and changes to virtualization configuration are applied to the virtualization configuration information. In the IM configuration management viewer, you can apply this virtualization configuration information to the monitoring tree of the Central Scope.

11.5.4 Considerations for business groups

If you decide to enable business groups, you need to consider how to manage them. Think of the range of monitored hosts to be assigned to business groups and the necessary restrictions on viewing and handling those business groups.

(1) Considerations related to business groups and monitoring groups

Consider the following items beforehand, based on the perspective from which multiple monitored hosts will be managed:

- Range of monitored hosts to be assigned to business groups

  Multiple hosts can be grouped into business groups. Note that one host can belong to only one business group.

- Range of monitored hosts to be assigned to monitoring groups in a business group

  Hosts in a business group can be further grouped from the viewpoint of monitoring the business group. Monitoring groups can be made in multiple tiers.

For details about business groups and monitoring groups, see *6.4 Managing business groups*.

(2) Restrictions on viewing and operating business groups

To use business groups, restrictions must be set on viewing and operating business groups.

To monitor the multiple monitored hosts by grouping them into business groups, JP1 resource groups and JP1 permission levels must be set for JP1 users.

For details about the operations allowed for individual combinations of JP1 resource groups and JP1 permission levels, see *3.1.4(2) Assigning a JP1 resource group and permission level to a JP1 user*.

For details about how to set restrictions on viewing and operating business groups, see *4.20 Setting reference and operation restrictions on business groups* in the *JP1/Integrated Management - Manager Configuration Guide*.

(3) Applying the system hierarchy when restrictions are enabled on viewing and operating business groups

If, while the differential distribution functionality facility is disabled in the settings for distribution of JP1/Base configuration definition information, you enable the restrictions on viewing and operating business groups and execute **Apply Agent Configuration** from the **Operation** menu in the Edit Agent Configuration window, the configuration definition of the newly defined agent configuration is distributed to all hosts. However, the existing agent configuration is not deleted.

Therefore, to delete some hosts from the system hierarchy, before applying the system hierarchy, you must change the settings for Event Forwarding in the profiles of the hosts to be deleted so that events will not be forwarded.

If you do not change the settings, JP1 events generated on agents continue being forwarded to higher level hosts because the configuration information held by the agents remains even after the system hierarchy is applied.

For details about changing the settings for event forwarding information, see *3.4 Setting business groups* in the *JP1/Integrated Management - Manager Configuration Guide*.

(4) Considerations related to monitoring in the Monitoring Tree window

After you apply the setting information of a business group to the Central Scope, the hierarchical configuration of the business group and the restrictions on viewing and operating the business group are inherited in the Monitoring Tree window (Central Scope). After that, users can view and operate on only the JP1 events generated within the business groups they are in charge of. For details about how to apply the setting information of business groups to the Central Scope, see *3.4 Setting business groups* in the *JP1/Integrated Management - Manager Configuration Guide*.

(5) Considerations related to monitoring in the Event Console window

When restrictions are enabled on viewing and operating business groups, a user can view and operate in the Event Console window on only the JP1 events generated within the business group that user is in charge of. For details, see *3.1.4 Restrictions on viewing and operating business groups*.

12 JP1/IM System Design

This chapter describes the system configuration and settings required in a JP1/IM system to achieve integrated system management.

12.1 Operating environment considerations

This section describes points to consider when planning the operating environment for JP1/IM.

12.1.1 Prerequisite operating systems and patches

Check the operating system and OS version required on each server in the JP1/IM system.

Depending on the OS and its version, you might need to apply service packs and patches. Refer to the *Release Notes* accompanying each JP1/IM product, and apply the required service packs and patches.

About prerequisite operating systems and patches:

- Prerequisite OSs
  See *9.3.1 Prerequisite operating systems*.
- Details on prerequisite OSs and patches
  See the *Release Notes*.

12.1.2 Estimating memory and disk space requirements

Estimate the amount of memory and disk space required to execute JP1/IM and JP1/Base on each host in the JP1/IM system.

In a cluster system running a number of logical hosts and physical hosts, estimate the total requirements for each individual host.

About estimating memory and disk space requirements:

- JP1/IM estimates (with equations)
  See the JP1/IM - View *Release Notes*.
  See the JP1/IM - Manager *Release Notes*.
- JP1/IM estimates (with general guidelines for a performance evaluation model)
  See *Chapter 13. Performance and Estimates*.
- JP1/Base estimates
  See the JP1/Base *Release Notes*.

12.1.3 Estimating IM database capacity requirements

When using the integrated monitoring database and the IM Configuration Management database, estimate the amount of capacity required for the databases on the managers where JP1/IM - Manager is running. The following table lists the database sizes available for selection when you set up the system.

Table 12–1: Database size models

Size model	Capacity			Example of system scale
	Total	Details		
Small scale (S)	11 GB	Integrated monitoring database	9 GB	Total items of event information: 1,000,000 (approx.)[#2] This number is based on the following assumptions: • Average event size: 1 KB[#3] • Number of events generated per day: 33,000 • Storage period for event information: 30 days
		IM Configuration Management database	1 GB	Maximum number of managed hosts: 1,024 hosts[#4] Total number of business groups and monitoring groups: 100
		System database area[#1]	1 GB	--
Medium scale (M)	36 GB	Integrated monitoring database	33 GB	Total items of event information: 4,000,000 (approx.)[#2] This number is based on the following assumptions: • Average event size: 1 KB[#3] • Number of events generated per day: 130,000 • Storage period for event information: 30 days
		IM Configuration Management database	1 GB	Maximum number of managed hosts: 1,024 hosts[#4] Total number of business groups and monitoring groups: 100
		System database area[#1]	2 GB	--
Large scale (L)	114 GB	Integrated monitoring database	96 GB	Total items of event information: 12,000,000 (approx.)[#2] This number is based on the following assumptions: • Average event size: 1 KB[#3] • Number of events generated per day: 400,000 • Storage period for event information: 30 days
		IM Configuration Management database	10 GB	Maximum number of managed hosts: 10,000 hosts[#5] Total number of business groups and monitoring groups: 100
		System database area[#1]	8 GB	--

Legend:

--: Not applicable.

#1

The size of the system database area is estimated from the amount of user data to be managed.

#2

Total items of event information might exceed the maximum allowed value depending on the timing of erasing events.

#3

Total items of event information decreases if the event size is larger than 1 kilobyte.

#4

The maximum number of hosts that can be monitored by one IM Configuration Management is 10,000. The number of hosts that can be managed is limited by the system configuration and network traffic. For details about the limit values, see *Appendix D. Limits*.

When the number of hosts (including managers) monitored by IM Configuration Management exceeds 1,024, the size model of the IM database must be the large scale (L).

#5

Considering the configuration of agents, the maximum number of hosts of JP1/IM - Manager and instances of JP1/Base that can be placed directly below JP1/IM - Manager is 2,500. The number of hosts that can be managed is limited by the system configuration and network traffic. For details about the limit values, see *Appendix D. Limits*.

In a cluster system, ensure that sufficient disk space is available on the shared disk and local disk, as specified in the table below.

Table 12–2: Additional disk space requirements in a cluster system

Size model	Total space required	Space required on shared disk			Space required on local disk
		System database area	Integrated monitoring database area	IM Configuration Management database area	System database area
Small scale (S)	11 GB	0.95 GB	9 GB	1 GB	0.05 GB
Medium scale (M)	36 GB	1.9 GB	33 GB	1 GB	0.1 GB
Large scale (L)	114 GB	7.4 GB	96 GB	10 GB	0.6 GB

We recommend that you set a database size that provides sufficient leeway should the number of generated events suddenly increase during system operation.

When the integrated management database reaches its maximum capacity, JP1 events are deleted from the earlier events. The maximum number of JP1 events that can be deleted at one time is 20,000 regardless of the database size (this value might be smaller than 20,000 depending on the size of the stored JP1 events).

12.1.4 Adjusting kernel parameters (in UNIX)

When using JP1/IM - Manager in a UNIX environment, adjust the OS kernel parameters to allocate the resources required for running JP1/IM - Manager.

Kernel parameters are settings for optimizing the resources used by the UNIX system. They include the maximum number of open files in the UNIX environment and the maximum size of shared memory segments. For details about kernel parameters, see the documentation for your OS.

Estimating kernel parameters (in UNIX):

- JP1/IM - Manager estimates
  See the JP1/IM - Manager *Release Notes*.
- JP1/Base estimates
  See the JP1/Base *Release Notes*.

12.1.5 Language environment considerations

Consider the language environments of the various hosts in the JP1/IM system.

Although we recommend that you use one language throughout the system, JP1/IM is capable of operating in a multi-language environment. In JP1/IM version 11-00 or later, the JP1/Base language environment configuration method is used to set the encoding.

A system monitoring JP1/SES events, however, requires you to use only the character encoding used for JP1/SES events as a unified language environment in the system.

Also, you need to use only a single language environment in one server.

Setting the language environment:

- About the JP1/IM language environment

  See *12.1.6 Operation in a multi-language environment*.

  See *1.3.2 Settings required immediately after installation (for Windows)* in the *JP1/Integrated Management - Manager Configuration Guide*

  See *2.3.3 Settings required immediately after installation (for UNIX)* in the *JP1/Integrated Management - Manager Configuration Guide*
- Setting the JP1/Base language environment

  See the description of language type setting in the *JP1/Base User's Guide*.

12.1.6 Operation in a multi-language environment

You can deploy JP1/IM in a system set up with multiple languages#1. For example, JP1/IM - View is able to simultaneously display JP1 events that are registered in JP1/Base under different language codes#2. In JP1/IM version 11-00 or later, the JP1/Base language environment configuration method is used to set the encoding.

#1: If a system that monitors JP1/SES events has a multi-language environment, character conversion errors might occur in the system.

Therefore, in a system that handles JP1/SES events, use only the character codes used by JP1/SES events as a single language environment.

#2: Some extended characters, special characters, and control codes might not display correctly or be recognized as different characters in JP1/IM - View, regardless of whether JP1/IM is being run in a multi-language environment. For details, see *1.3 Notes on operations in windows* in the manual *JP1/Integrated Management - Manager GUI Reference*.

However, there are several conditions that apply when running JP1/IM in a multi-language environment. These conditions might influence your system configuration or manner of operation.

(1) System conditions

The following conditions apply to the JP1/IM system itself (the entire JP1/IM system composed of managers and agents).

- In Windows environment, the following language environment is configured for JP1/Base and JP1/IM according to the locale (system locale) when JP1/Base is installed. In a UNIX environment, the language environment is configured in JP1/Base.

Table 12–3: Language environment for JP1/Base and JP1/IM that is configured for each locale

Locale	Language environment
Japanese	Japanese

Locale	Language environment
Chinese	Chinese
Other than Japanese or Chinese	English

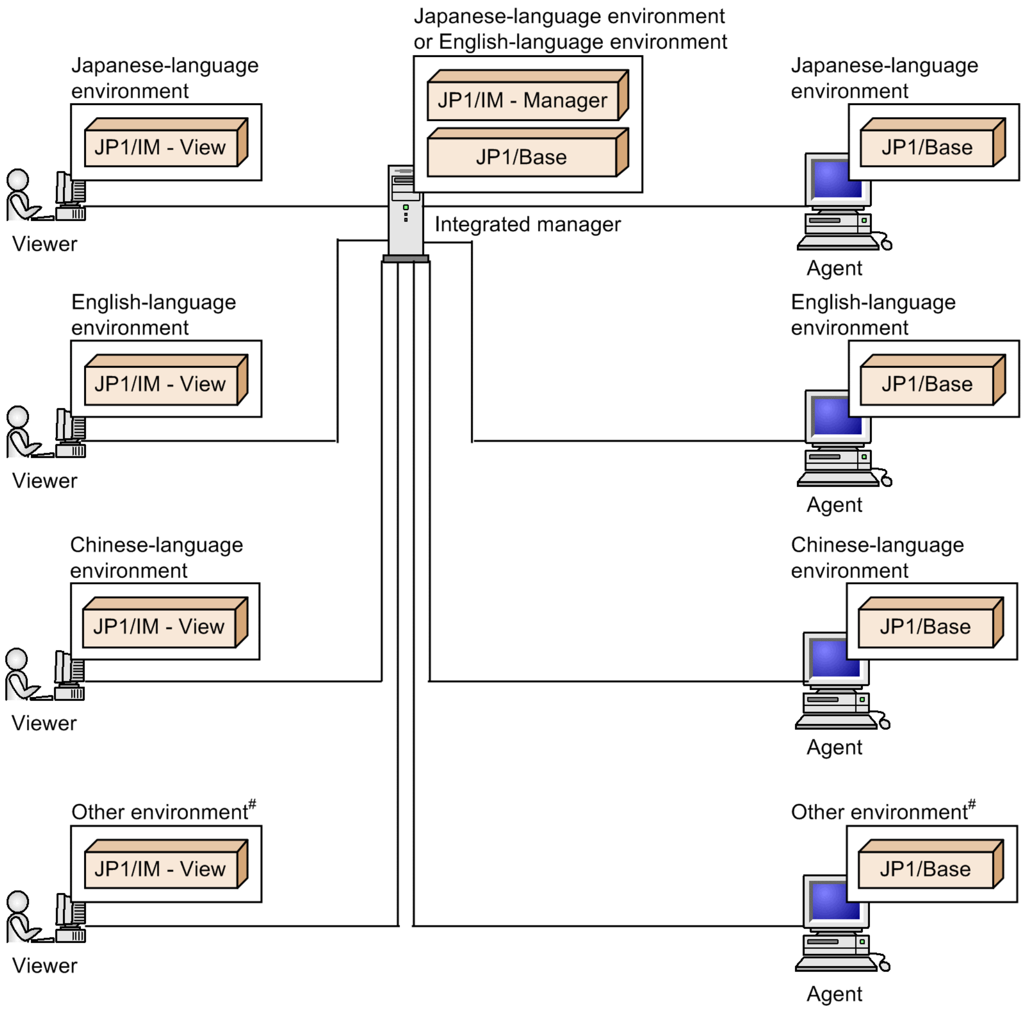
- Note the following when the system contains an agent host that is using the UTF-8 locale environment:
    - Version 8 or later of JP1/Base must be running in the UTF-8 locale environment. Also, any machines to which that agent forwards events must also be running version 8 or later of JP1/Base.
    - The manager must be running version 8 or later of JP1/IM - Manager and JP1/Base.
    - A system with hosts running version 7 of JP1/IM or JP1/Base will be unable to properly deal with JP1 events issued from the UTF-8 locale environment (the hosts will be unable to display the JP1 events or execute automated actions correctly).

      In this case, make sure that the JP1/Base in the UTF-8 environment is version 8 or later, and set up JP1/Base to run in compatibility mode. For details about the setup, see the description of language type setting in the *JP1/Base User's Guide*.
- Two-byte characters in automated actions will appear garbled.# If you specify machine-dependent characters, the automated action might not work correctly.

  #: Level 1 and level 2 Japanese character codes will display normally.
- A system monitoring JP1/SES events requires you to use only the character codes used for JP1/SES events as a unified language environment in the system.
- The following conditions apply to a system in a multi-language environment:
    - In a Japanese-language environment or an English-language environment, use one manager to perform integrated monitoring of the targets (agents) in the supported language environment.
    - Use a viewer (JP1/IM - View) that supports the language of the monitoring targets to perform monitoring tasks.
    - In the viewer, group the monitored hosts by language and monitor only those hosts that use the language that is supported by the viewer.

  The following figure shows an example of a system configuration in which multiple language environments are intermixed.

Figure 12–1: Example of a system configuration in which multiple language environments are intermixed


Japanese-language environment or English-language environment
JP1/IM - Manager
JP1/Base
Integrated manager
Japanese-language environment
JP1/IM - View
Viewer
English-language environment
JP1/IM - View
Viewer
Chinese-language environment
JP1/IM - View
Viewer
Other environment#
JP1/IM - View
Viewer
Japanese-language environment
JP1/Base
Agent
English-language environment
JP1/Base
Agent
Chinese-language environment
JP1/Base
Agent
Other environment#
JP1/Base
Agent

Note: For the limitations when a multi-language environment is used, see Tables 12-5 and 12-6.
#: German, French, Spanish, Korean, and Russian

- The following table describes the supported range of environments in which multiple languages are intermixed.

Table 12–4: Supported range of environments in which multiple languages are intermixed

Item	Supported range
Version	The manager and viewer versions must be 11-00 or later. The version of the agents (JP1/Base) must be 09-00 or later.
Garbled strings	JP1 events are displayed normally within the range of languages that can be recognized by JP1/IM - View. If the language pack for each language has not been applied, characters might appear garbled.
Operating language	The operating languages supported for JP1/IM - Manager in a multi-language environment are Japanese and English. The recommended operating language for JP1/IM - Manager is English. If you have changed the JP1/IM - Manager's operating language to Japanese, apply the Japanese language pack to the JP1/IM - View host. If JP1/IM - Manager and JP1/IM - View use different operating languages, messages or characters that replace messages are output in the JP1/IM - Manager's operating language. If JP1/IM - Manager's operating language is set to Japanese and the Japanese language pack has not been applied to the JP1/IM - View host, messages might look garbled.
Definition files and configuration files	Use alphanumeric characters (ASCII) for definition file names, configuration file names, and the characters and attribute values used in these files. If non-ASCII characters are specified, the definitions might be garbled depending

Item	Supported range
	on the operating language of JP1/IM - Manager. If you will be creating and distributing files on JP1/IM - Manager, ensure that no file containing double-byte characters is distributed.
Command execution	Only ASCII characters are supported for executing commands. If non-ASCII characters are specified, the execution contents and results might be garbled depending on the operating language of JP1/IM - Manager and JP1/Base (agent).
Event Details window	The Event Details window displays attribute names based on the operating language of JP1/IM - View.
Tool Launcher	Tool Launcher displays items based on the operating language of JP1/IM - View.

Notes:

The following notes apply to a system in a multi-language environment:

- Automated actions

  Note the following when executing an automated action on a target host running an English language environment:

  - Do not specify an action that contains 2-byte characters. If you specify such an action, the action results might be garbled and display incorrectly, or the action might fail to execute altogether.
  - When defining variables in the automated action definition, do not specify event information that contains 2-byte characters. If you specify such information, the action results might be garbled and display incorrectly, or the action might fail to execute altogether.
  - Do not use 2-byte characters in the file name of the environment variable definition file used by the automated action, or in the file itself. If the file or its name contains 2-byte characters, the action results might be garbled and display incorrectly, or the action might fail to execute altogether.
  - Do not specify an automated action that outputs execution results containing 2-byte characters. If you specify such an automated action, the action results might be garbled and display incorrectly.

- Searching for events

  Do not use 2-byte characters in search conditions when conducting an event search on a JP1/Base in an English language environment. If you specify a 2-byte character, the search will not be conducted correctly.

- The following tables show the language environments supported by version 10-50 or earlier and by version 11-00 or later.

Table 12–5: Language environments supported by version 10-50 or earlier and by version 11-00 or later (between manager and agent)

Manager's operating language	Agent's operating language	Manager version	
		10-50 or earlier	11-00 or later
Japanese	Japanese	Y	Y
	English	A	O
	Chinese	N	O
English	Japanese	N	O
	English	Y	Y
	Chinese	N	O
Chinese	Japanese	N	N
	English	A	A

Manager's operating language	Agent's operating language	Manager version	
		10-50 or earlier	11-00 or later
	Chinese	Y	Y

Legend:

Y: Supported.

A: ASCII characters are supported.

O: For JP1 events, the agent's operating language is supported. For other events, ASCII characters are supported.

N: Not supported.

Table 12–6: Language environments supported by version 10-50 or earlier and by version 11-00 or later (between manager and viewer)

Manager's operating language	Viewer's operating language	Manager version	
		10-50 or earlier	11-00 or later
Japanese	Japanese	Y	Y
	English	N	O
	Chinese	N	O
English	Japanese	A	O
	English	Y	Y
	Chinese	A	O
Chinese	Japanese	N	N
	English	N	N
	Chinese	Y	Y

Legend:

Y: Supported.

A: ASCII characters are supported.

O: For JP1 events, the agent's operating language is supported. For other events, ASCII characters are supported.

N: Not supported.

(2) Server conditions

The following conditions apply to individual servers (all physical and logical hosts within a given machine).

- You must use the same language edition (English or Japanese) for the manager's JP1/IM and JP1/Base.
- Provide a viewers and agent for each supported language. Group agents into the same languages that are supported by the viewers.
- The same language code (locale setting such as the `LANG` environment variable) must be set for JP1/Base. For details about how to set the language code for JP1/Base, see *1.3.2 Settings required immediately after installation (for Windows)* or *2.3.3 Settings required immediately after installation (for UNIX)* in the *JP1/Integrated Management - Manager Configuration Guide*.
- You must set the `LANG` environment variable for JP1/Base event servers. For details about how to set the `LANG` environment variable, see the description of setting the language type in the *JP1/Base User's Guide*.

12.1.7 Notes on operation when running anti-virus software

Some files and folders being used by JP1/IM might be locked by exclusive access control as the result of using anti-virus software. If files and folders are locked, the following problems can result:

- JP1/IM is unable to start.
  If the definition files JP1/IM references at startup are locked by exclusive access control, JP1/IM might fail to start.
- Automated actions cannot be executed.
  If the files required to execute automated actions are locked by exclusive access control, the execution of automated actions might fail.
- Event monitoring with the Central Console and Central Scope is disabled.
  If the files required for event monitoring with the Central Console and Central Scope are locked by exclusive access control, event monitoring with the Central Console and Central Scope might fail.
- Correlation events cannot be issued.
  If the files necessary for issuing correlation events are locked by exclusive access control, the issuance of correlation events might fail.
- Incidents cannot be registered.
  If the files required for registering incidents are locked by exclusive access control, the registration of incidents might fail.
- JP1/IM definitions cannot be changed.
  If JP1/IM definition files are locked by exclusive access control, the addition or modification of definitions might fail.
- Log data cannot be written.
  If JP1/IM log files are locked by exclusive access control, data might not be written to log files, making it impossible to troubleshoot problems that occur.
- JP1/IM commands end abnormally.
  If the files JP1/IM commands use are locked by exclusive access control, the commands might end abnormally.

If you run a virus scan while JP1/IM is operating, exclude the files and folders listed below from the scan. If you run a virus scan while JP1/IM is stopped and then start JP1/IM, make sure that scanning of the following files and folders for viruses has finished.

Files and folders of JP1/IM - Manager (for Windows)

- All files and folders in *manager-path*\
- All files and folders in *console-path*\
- All files and folders in *scope-path*\
- All files and folders in *IM-database-installation-directory*\#
- All files and folders in *IM-database-data-storage-directory*\#

#: Exclude these files and folders from the scan when an IM database has been set up.

In a logical host environment, exclude the files and folders in shared folders from the scan.

- All files and folders in *shared-folder*`\jp1imm\`
- All files and folders in *shared-folder*`\jp1cons\`
- All files and folders in *shared-folder*`\jp1scope\`
- All files and folders in *IM-database-data-storage-directory-(for-local-working-area)-on-logical-host*\ #

- All files and folders in *IM-database-data-storage-directory-(for-shared-data-area)-on-logical-host*\ #

#: Exclude these files and folders from the scan when an IM database has been set up.

Files and folders of JP1/IM - Manager (for UNIX)

- All files and folders in `/opt/jp1imm/`
- All files and folders in `/opt/jp1cons/`
- All files and folders in `/opt/jp1scope/`
- All files and folders in `/etc/opt/jp1imm/`
- All files and folders in `/etc/opt/jp1cons/`
- All files and folders in `/etc/opt/jp1scope/`
- All files and folders in `/var/opt/jp1imm/`
- All files and folders in `/var/opt/jp1cons/`
- All files and folders in `/var/opt/jp1scope/`
- All files and folders in *IM-database-installation-directory*/#
- All files and folders in *IM-database-data-storage-directory*/#

#: Exclude these files and folders from the scan when an IM database has been set up.

In a logical host environment, exclude the files and folders in shared directories from the scan.

- All files and folders in *shared-directory*`/jp1imm/`
- All files and folders in *shared-directory*`/jp1cons/`
- All files and folders in *shared-directory*`/jp1scope/`
- All files and folders in *IM-database-data-storage-directory-(for-local-working-area)-on-logical-host*/#
- All files and folders in *IM-database-data-storage-directory-(for-shared-data-area)-on-logical-host*/#

#: Exclude these files and folders from the scan when an IM database has been set up.

Files and folders of JP1/IM - View

- All files and folders in *view-path*\
- All files and folders in *system-drive*: `\ProgramData\Hitachi\jp1\jp1_default\JP1CoView\`

12.2 Upgrading from a previous version of JP1/IM

This section provides some notes on upgrading from a previous version of JP1/IM.

"Upgrading" as used in this manual:

> *Upgrading* as used in this manual refers to an upgrade installation from a previous version (including a corrected version or patch version) to the version current in this edition of the manual.
>
> For the JP1/IM version assumed in this manual, see the bottom of the copyright page at the front of this manual.
>
> The product version is stated in the *Release Notes* accompanying the product. If the product version stated there differs from the product version to which this manual applies, read the *Release Notes* first (including any notes on upgrading).

12.2.1 Upgrading from version 10 JP1/IM - Manager products

(1) Upgrading from Central Console version 10

Back up the settings information before you upgrade JP1/IM - Manager from version 10 to version 11. For the procedure, see the manual for the previous version.

If you use the integrated monitoring database, execute the `jimdbupdate` command after you have upgraded JP1/IM - Manager from version 10 to version 11. Make a backup copy before you execute the `jimdbupdate` command.

When you upgrade, the definition information for the Central Console is migrated from JP1/IM - Manager version 10. However, note the following:

- In a logical host (cluster) environment, you must execute the `jp1cohaverup` command to apply definition information that has been added in the current version.
  See *jp1cohaverup* (in *Chapter 1. Commands*) in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

(2) Upgrading from Central Scope version 10

Back up the settings information and the databases before you upgrade JP1/IM - Manager from version 10 to version 11. For the procedure, see the manual for the previous version.

When you upgrade, the definition information for the Central Scope is migrated from JP1/IM - Manager version 10, regardless of whether the Central Scope is enabled or disabled.

(3) Upgrading from the IM Configuration Management version 10

Before you upgrade JP1/IM - Manager from version 10 to version 11, back up the settings information. For the procedure, see the manual for the previous version.

If you use the integrated monitoring database, execute the `jimdbupdate` command after you have upgraded JP1/IM - Manager from version 10 to version 11. Make a backup copy before you execute the `jimdbupdate` command.

When you upgrade, the definition information for IM Configuration Management is migrated from JP1/IM - Manager version 10, regardless of whether IM Configuration Management is enabled or disabled.

12.2.2 Upgrading from version 9 JP1/IM - Manager products

(1) Upgrading from the Central Console version 9

Back up the settings information before you upgrade from version 9 to version 11 of JP1/IM - Manager. For the procedure, see the manual for the previous version.

If you use the integrated monitoring database, execute the `jimdbupdate` command after you have upgraded JP1/IM - Manager from version 9 to version 10. Make a backup copy before you execute the `jimdbupdate` command.

When you upgrade, the definition information for the Central Console is migrated from JP1/IM - Manager version 9. However, note the following points:

- In a logical host (cluster) environment, you must execute the `jp1cohaverup` command to apply the definition information added in the current version.
  See *jp1cohaverup* in *Chapter 1. Commands* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

(2) Upgrading from the Central Scope version 9

Back up the settings information and the databases before you upgrade JP1/IM - Manager from version 9 to version 11. For the procedure, see the manual for the previous version.

When you upgrade, the definition information for the Central Scope is migrated from JP1/IM - Manager version 9, regardless of whether the Central Scope is enabled or disabled.

(3) Upgrading from the Central Scope version 9

Back up the settings information before you upgrade JP1/IM - Manager from version 9 to version 11. For the procedure, see the manual for the previous version.

If you use the integrated monitoring database, execute the `jimdbupdate` command after you have upgraded JP1/IM - Manager from version 9 to version 10. Make a backup copy before you execute the `jimdbupdate` command.

When you upgrade, the definition information for the IM Configuration Management is migrated from JP1/IM - Manager version 9, regardless of whether the IM Configuration Management is enabled or disabled.

12.2.3 Upgrading from viewer version 10 or 9

If you are upgrading from viewer version 10 or 9 and the central information master viewer has been registered in the start menu, remove the central information master viewer from the start menu.

You can then install JP1/IM - View.

12.2.4 Upgrading from JP1/Base version 10

To use JP1/IM - Manager, you must install JP1/Base version 11 on the same host. For notes about upgrading JP1/Base, see notes on installing and uninstalling JP1/Base in the *JP1/Base User's Guide*.

12.2.5 Upgrading from JP1/Base version 9

To use JP1/IM - Manager, you must install JP1/Base version 11 on the same host. For notes on upgrading JP1/Base, see the description in *Notes on installing and uninstalling JP1/Base* in the *JP1/Base User's Guide*.

12.2.6 Upgrading from JP1/Base version 8

To use JP1/IM - Manager, you must install JP1/Base version 11 on the same host. Note the following points when you upgrade JP1/Base on a manager:

- If there are any command execution log files from version 8, version 7, or version 6, make sure that you execute the `jcocmdconv` command after you upgrade JP1/Base and before you begin running JP1/IM.

  This command migrates command execution logs from the previous version to version 11. (If this is not done, the command execution logs cannot be accessed.)

  If you are using JP1/IM in a cluster environment, execute the `jcocmdconv` command once only on the logical host from either the primary node or secondary node with the shared disk online.

  See the section describing the `jcocmdconv` command in the *JP1/Base User's Guide*.
- The start sequence definition file is not updated when you upgrade. The definitions related to JP1/IM - Manager and the Central Console will need to be changed manually to the definitions of JP1/IM - Manager version 11.

For other cautionary notes that apply when upgrading JP1/Base, see the notes on installation and uninstallation in the *JP1/Base User's Guide*.

12.2.7 Upgrading from JP1/Base version 7

To use JP1/IM - Manager, you must install JP1/Base version 11 on the same host. When you upgrade JP1/Base on a manager, the same cautionary notes apply as when upgrading from JP1/Base version 8. For details, see *12.2.6 Upgrading from JP1/Base version 8*.

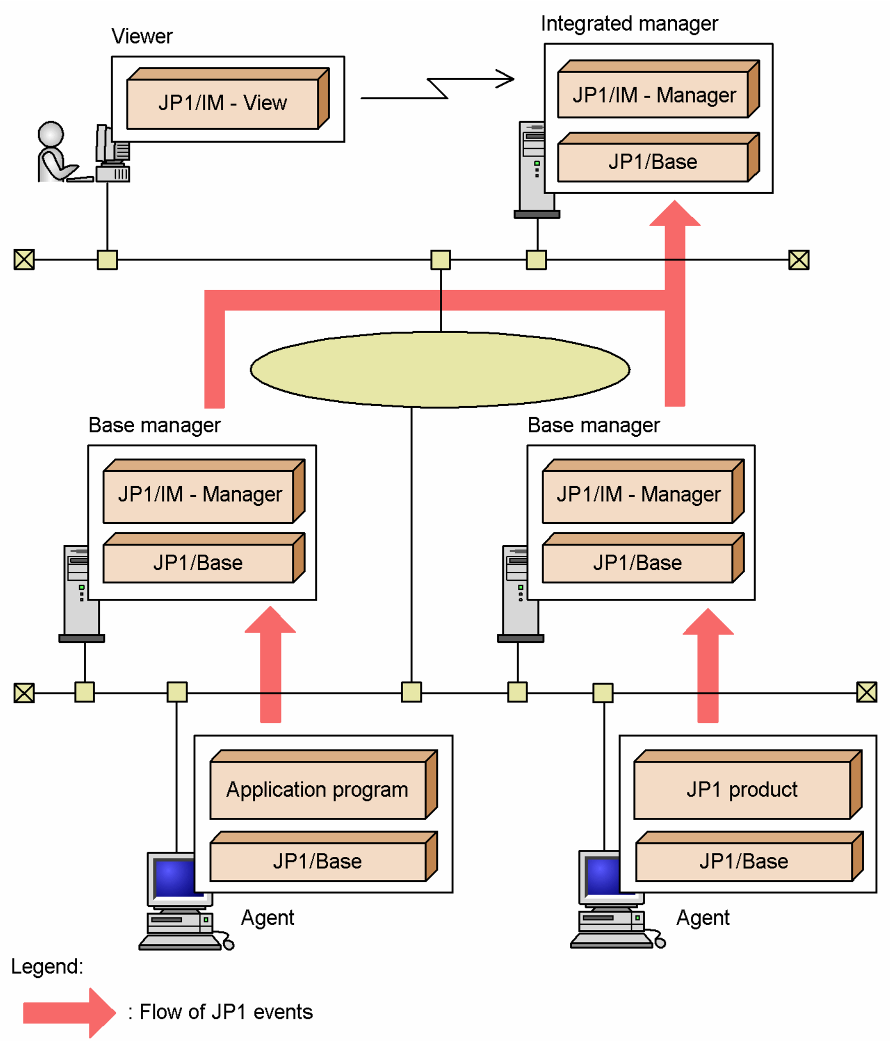
12.3 Designing the system configuration

This section provides some examples of configuring JP1/IM with a variety of programs.

12.3.1 Basic configuration

An example of a basic JP1/IM configuration is shown below.

Figure 12–2: Example of a basic configuration



This example shows a system configuration that manages job execution in a two-tier structure.

The following products are required on each host:

Integrated manager (top-level manager)

- JP1/IM - Manager

  Runs the Central Console, Central Scope, and IM Configuration Management. The Central Scope is required to monitor the system by associating jobs and JP1 events. It is not required to monitor job execution simply by monitoring JP1 events. The IM Configuration Management feature is available when the IM Configuration Management database is activated.

- JP1/Base

Base manager

- JP1/IM - Manager
- JP1/Base

Base manager

- JP1/IM - Manager
- JP1/Base

Agents (job execution hosts)

- JP1/Base
  JP1/Base is required on every agent. JP1/Base performs processing such as sending and receiving JP1 events and executing commands.
- Job execution programs (user application programs, JP1 products, and so on)

Viewers (for monitoring the system)

- JP1/IM - View

In the system shown in this example, JP1 events related to the status of jobs executing on the agents are forwarded to the base manager by JP1/Base. Then, if necessary, each JP1 event is forwarded from the base manager to the integrated manager.

The administrator can manage the whole system by logging into the integrated manager from JP1/IM - View on a viewer.

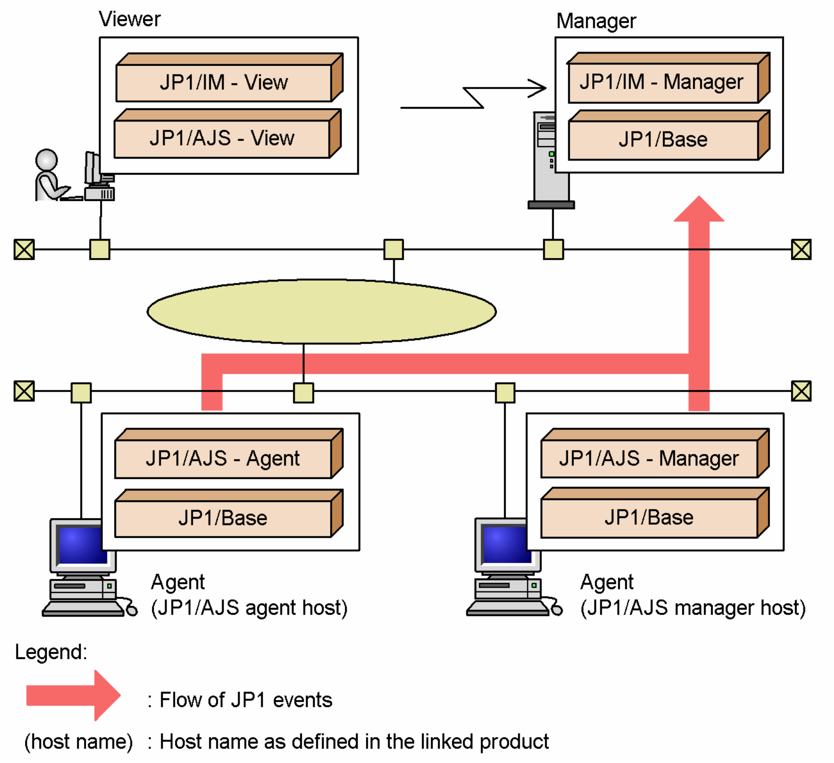
JP1/IM supports multi-level system configurations. JP1/IM - Manager is required on the top-level manager and on each intermediate-level manager. The Central Scope can also be used on the intermediate-level managers.

12.3.2 Configuration with JP1/AJS for monitoring job execution

By linking JP1/IM with JP1/AJS, you can view information about jobs being executed by JP1/AJS from JP1/IM - View. Also, you can open JP1/AJS windows from JP1/IM - View, and then define or operate on jobs.

The figure below shows an example of a system configuration that links JP1/IM with JP1/AJS.

Figure 12–3: Example of linkage with JP1/AJS



The following products are required on each host:

Managers

- JP1/IM - Manager
  Runs the Central Console and Central Scope. The Central Scope is required to monitor the system by associating jobs and JP1 events. It is not required to monitor job execution simply by monitoring JP1 events.
- JP1/Base

Agents (JP1/AJS manager hosts)

- JP1/AJS - Manager
- JP1/Base

Agents (JP1/AJS agent hosts)

- JP1/AJS - Agent
- JP1/Base

Viewer

- JP1/IM - View
- JP1/AJS - View
  JP1/AJS - View is required on the viewer to open and work with JP1/AJS windows from JP1/IM - View.

In this example, JP1 events related to the execution status of JP1/AJS jobs are forwarded to the manager, and the status of each job is monitored from JP1/IM - View.

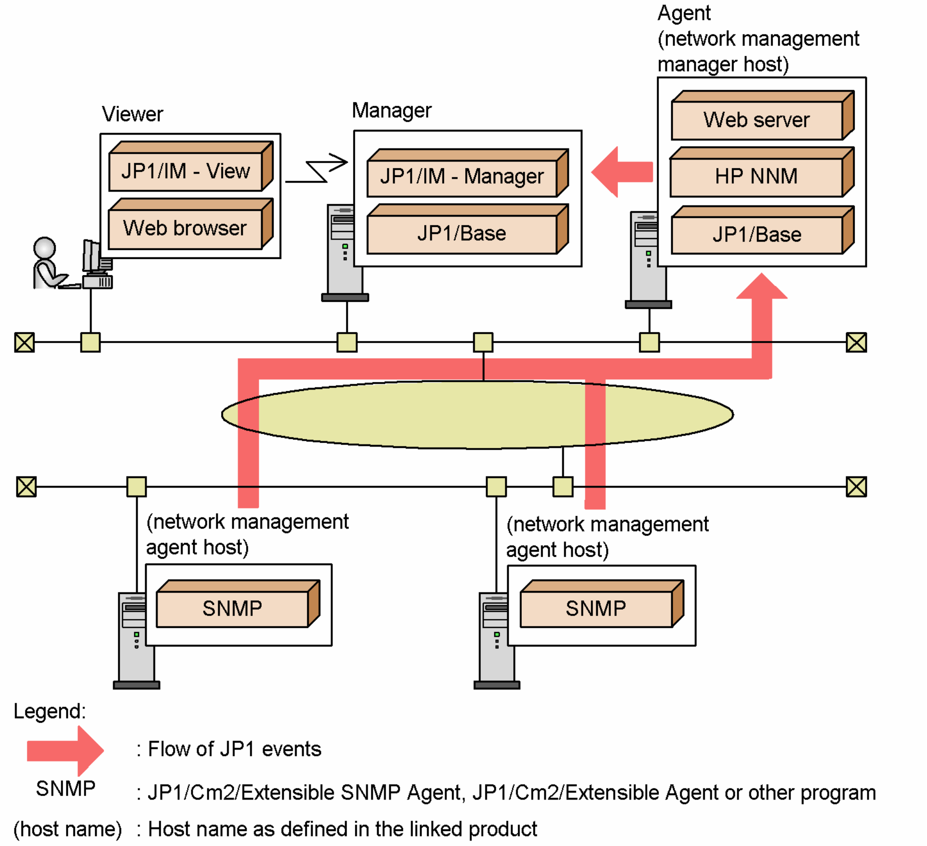
On the viewer, the user accesses JP1/AJS - View from JP1/IM - View. JP1/AJS - View connects to JP1/AJS - Manager for performing operations in JP1/AJS.

12.3.3 Configuration with HP NNM for monitoring a network

By using JP1/IM - Manager linking with HP NNM version 7.5 or earlier, you can monitor the network in the system.

From JP1/IM - View windows, you can launch the windows of HP NNM version 7.5 or earlier. You can also convert the SNMP traps managed by HP NNM version 7.5 or earlier into JP1 events and monitor the events in the Event Console window of JP1/IM - View.

Figure 12–4: Example of linkage with HP NNM version 7.5 or earlier



The following products are required on each host:

Managers

- JP1/IM - Manager
  Runs the Central Console and Central Scope. The Central Scope is required to monitor the system by associating jobs and JP1 events. It is not required to monitor job execution simply by monitoring JP1 events.
- JP1/Base

Agents (network management manager host)

- HP NNM version 7.5 or earlier
- HTTP server
  Required to display the Web page of HP NNM version 7.5 or earlier.
- JP1/Base

(Network management agent hosts)

- JP1/Extensible SNMP Agent (as an example)

Viewer

- JP1/IM - View
- Web browser
  Required to display the Web page of HP NNM version 7.5 or earlier.

Event levels of SNMP traps after conversion to JP1 events

- When a SNMP trap is converted into a JP1 event, the trap severity level is converted into an event level, as listed in the table below.

  Table 12–7: Event level when a SNMP trap is converted into a JP1 event

Severity level of SNMP trap	Display (event level) after conversion into a JP1 event
Normal	`Information`
Warning	`Warning`
Minor	`Error`
Major	`Critical`
Critical	`Alert`

  SNMP trap conversion and precautions are described in the *JP1/Base User's Guide*. See the chapter on setting the event converters for details about converting SNMP traps.

- When the SNMP traps issued by HP NNM version 7.5 or earlier are converted by JP1/Base into JP1 events and monitored, the IP address of the error source host might not be correctly received. This is because, when JP1/Base converts a SNMP trap into a JP1 event, the value set in the *source IP address* attribute of the JP1 event is the IP address of the host on which JP1/Base resides, not the IP address of the host that issued the SNMP trap. To acquire the name of the issuing host, specify the *SNMP trap source* extended attribute. To define the attribute value, specify the `$EV"SNMP_SOURCE"` variable.

Note

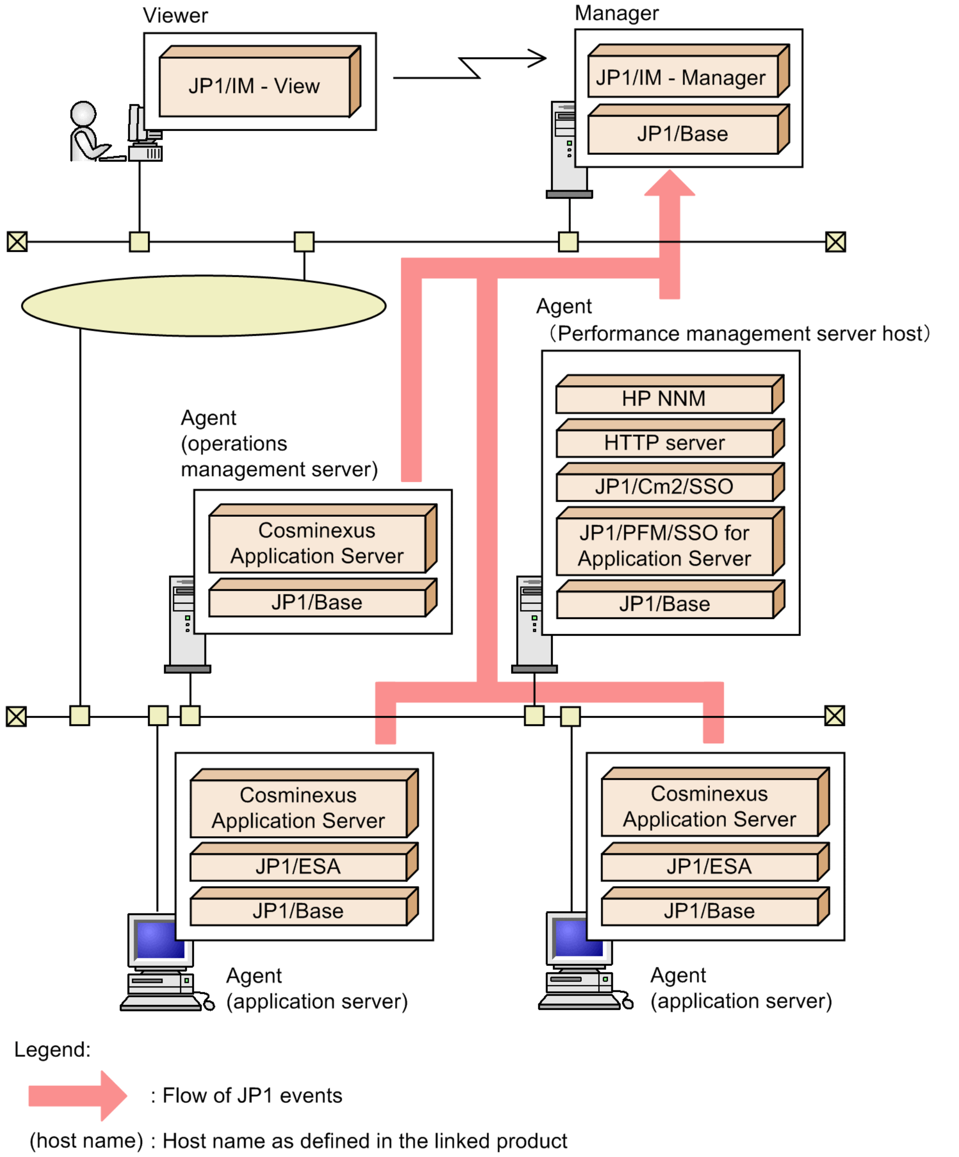
For details about system configurations with HP NNMi, see the manual *Job Management Partner 1/Integrated Management - Event Gateway for Network Node Manager i Description, User's Guide and Reference*.

12.3.4 Configuration for monitoring the status of the Cosminexus system environment and the status of resources being used (Cosminexus + JP1/Cm2/SSO linkage)

When JP1/Cm2/SSO version 8 or earlier monitors the resources used by the Cosminexus system environment, you can use the Central Scope (in JP1/IM) to collect and monitor the Cosminexus system environment information and the resource information related to business operations executed in the system environment. The monitoring objects for Cosminexus + JP1/Cm2/SSO linkage are the user monitoring objects.

The following figure shows an example of the system configuration in this case.

Figure 12–5: Example of linking with Cosminexus + JP1/Cm2/SSO


Viewer
JP1/IM - View
Manager
JP1/IM - Manager
JP1/Base
Agent
(Performance management server host)
HP NNM
HTTP server
JP1/Cm2/SSO
JP1/PFM/SSO for Application Server
JP1/Base
Agent
(operations management server)
Cosminexus Application Server
JP1/Base
Cosminexus Application Server
JP1/ESA
JP1/Base
Agent
(application server)
Cosminexus Application Server
JP1/ESA
JP1/Base
Agent
(application server)
Legend:
: Flow of JP1 events
(host name) : Host name as defined in the linked product

The following products are required for each host:

Manager

- JP1/IM - Manager
  Runs the Central Console and Central Scope. The Central Scope is required to monitor the system by associating jobs and JP1 events. It is not required to monitor job execution simply by monitoring JP1 events.
- JP1/Base

Agent (Cosminexus operations management server host)

- Cosminexus Application Server
  Required to run and manage the applications on the application servers.
  This host requires the Cosminexus Management Server and its prerequisite processes, provided with the application server.
- JP1/Base

Agents (Performance management server host for JP1/Cm2/SSO)

- NNM

  Prerequisite product for JP1/Cm2/SSO. NNM manages the SNMP traps issued by JP1/Cm2/SSO version 8 or earlier. HP NNM version 7.5 or earlier is required.

- HTTP server

  Required to display the NNM's window (Web page).

- JP1/Cm2/SSO

  JP1/Cm2/SSO version 8 or earlier is a prerequisite product for JP1/PFM/SSO for Application Server. It is required to monitor the server resources on the network (the resource status is collected from JP1/ESA).

  JP1/Cm2/SSO is required for managing JP1/ESA running on business servers.

- JP1/PFM/SSO for Application Server

  Required to monitor the Cosminexus Application Server resources on the network (the resource status is collected from JP1/ESA).

- JP1/Base

Agents (application server hosts)

- Cosminexus Application Server

  On an application server host, install Cosminexus Application Server and use the configuration software according to your needs. Operation and management of Cosminexus Application Server is performed by Cosminexus Manager (Cosminexus Management Server) on the operations management server.

- JP1/ESA

  Required to monitor the status of the resources used by the applications managed by Cosminexus running on business servers.

- JP1/Base

Viewer

- JP1/IM - View

Note:

With the above system configuration, if you want to monitor the status of Cosminexus operation and their resources, select the work-oriented tree when automatically generating a monitoring tree. If the server-oriented tree is selected, monitoring objects for monitoring the resource status of the Cosminexus operations are not generated. For details about the relationship between the monitoring tree types and monitoring objects, see *4.3.3 Monitoring tree structures*.

12.3.5 Configuration for monitoring JP1 events from a Web browser

JP1 events can be monitored in JP1/IM using a Web browser. In this case, JP1/IM - View is not required on the viewer.

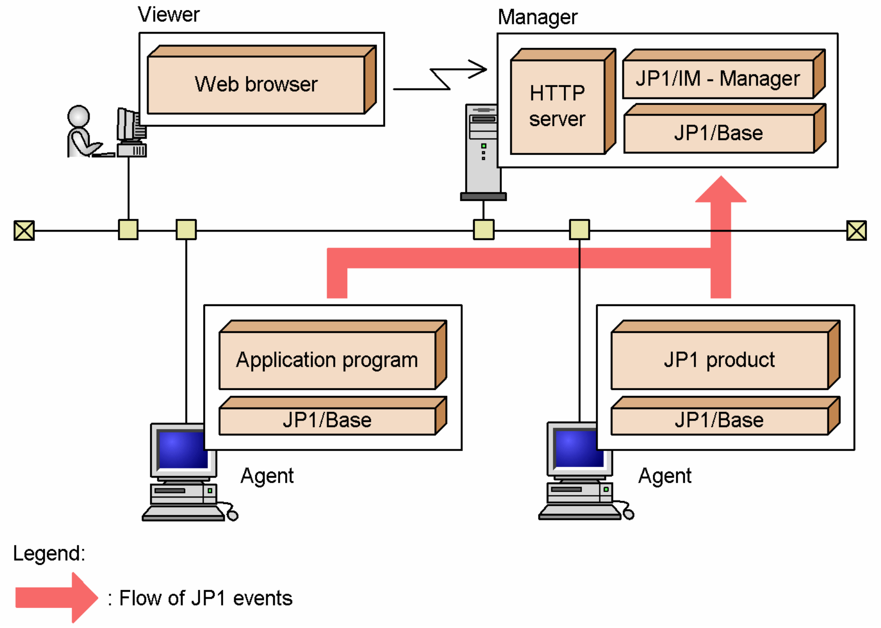
However, the following limitations apply when you use a Web browser:

- You cannot connect to JP1/IM - Manager (Central Scope).
- You cannot access windows such as the Execute Command window and Tool Launcher window. There are also operational limitations: You cannot invoke the monitor startup to launch linked applications, and you cannot save event list information (as CSV snapshots). For details about browser limitations, see *Chapter 1. Window Transitions and Login Window* in the manual *JP1/Integrated Management - Manager GUI Reference*.
- Some limits are different. See *Appendix D. Limits* for details.

- You cannot specify an IPv6 address for the name of the host to which the Web browser connects. Specify an IPv4 address or a host name for which an IPv4 address can be resolved.
- The communication encryption function is not supported.
- A cluster system is not supported.

A system configuration example is shown below.

Figure 12–6: Example of configuration for monitoring JP1 events from a Web browser



The following products are required on each host:

Manager

- JP1/IM - Manager
- JP1/Base
- HTTP server

Agents

- JP1/Base
- JP1-series products, application program, and so on

Viewer

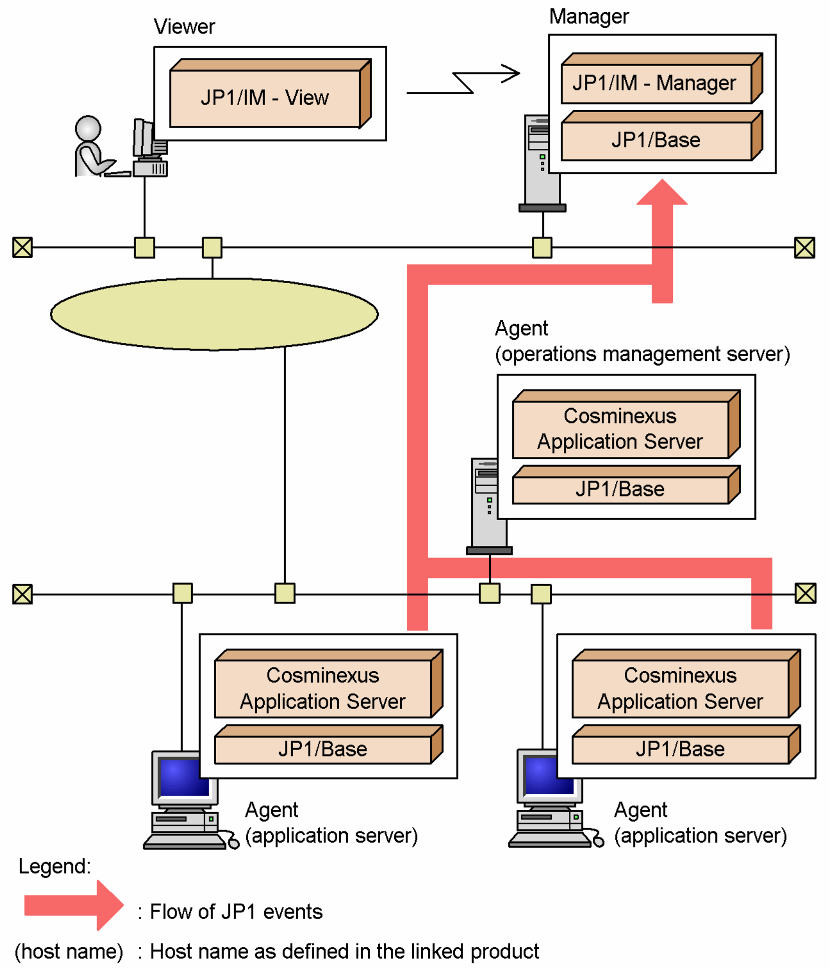
- Web browser
  The Java Runtime Environment (JRE) and bundled plug-ins are required in the Web browser to monitor JP1 events. For details, see the JP1/IM - Manager *Release Notes*.

12.3.6 Configuration for monitoring the status of a Cosminexus system environment

You can monitor the status of a Cosminexus system environment (an execution and management environment for a Web system) by linking JP1/IM with Cosminexus. This streamlines the process of error investigation by allowing you to open the Cosminexus windows from JP1/IM - View, in the same manner as with other linked products.

An example system configuration is shown below.

Figure 12–7: Example of linkage with Cosminexus



The following products are required on each host:

Manager

- JP1/IM - Manager

  Runs the Central Console and Central Scope. The Central Scope is required to monitor the system by associating jobs and JP1 events. It is not required to monitor job execution simply by monitoring JP1 events.

- JP1/Base

Agent (Cosminexus operations management server host)

- Cosminexus Application Server

  Required to run and manage the applications on the application servers.

  This host requires the Cosminexus Management Server and its prerequisite processes, provided with the application server.

- JP1/Base

Agents (application server hosts)

- Cosminexus Application Server

  On an application server host, install Cosminexus Application Server and use the configuration software according to your needs. Operation and management of Cosminexus Application Server is performed by Cosminexus Manager (Cosminexus Management Server) on the operations management server.

- JP1/Base

Viewer

- JP1/IM - View

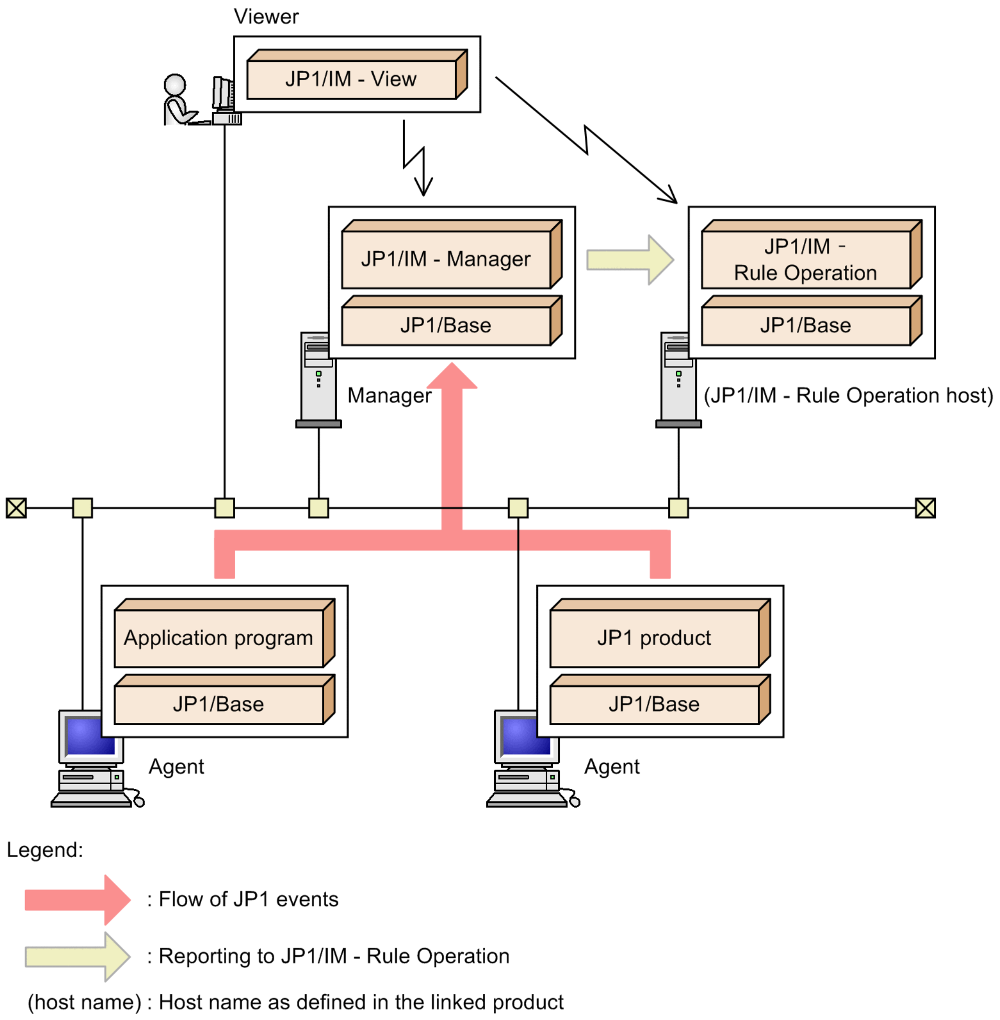
> **Note**
>
> Cosminexus is an application server that allows you to consolidate information from distributed systems accessed via a network (Internet or intranet). Cosminexus can be used to manage environments such as the execution environment of a Web system.
>
> Errors that occur at startup or shutdown or during execution of a logical server managed by Cosminexus (J2EE servers, Web servers, naming services, CTM and so on) are converted into JP1 events and initially registered with JP1/Base on the Cosminexus operations management server host. These events are later forwarded to the JP1/IM - Manager host by the JP1 event forwarding function of JP1/Base. In this manner, JP1/IM can monitor JP1 events that occur on the Cosminexus operations management server host by monitoring the associated JP1 events registered on the JP1/IM - Manager host.

12.3.7 Configuration with JP1/IM - Rule Operation

By linking JP1/IM - Manager with JP1/IM - Rule Operation, you can automatically notify JP1/IM - Rule Operation when a rule startup event (JP1 event) is issued in the system.

An example of a system configuration for this purpose is shown below.

Figure 12–8: Example of configuration with JP1/IM - Rule Operation



The following products are required on each host:

Viewer

- JP1/IM - View

Manager

- JP1/IM - Manager
  The JP1/IM - Rule Operation linkage function must be enabled.
- JP1/Base

(JP1/IM - RL host)

- JP1/IM - Rule Operation
- JP1/Base

Agents

- Application program, JP1-series products, and so on
- JP1/Base

In this example, JP1 events related to the status of application programs and JP1 products executing on the agents are forwarded to the manager and are monitored from JP1/IM - View.

When a rule startup request event is received among the forwarded JP1 events, JP1/IM - Manager on the manager sends the request to JP1/IM - Rule Operation automatically.

JP1/IM - Rule Operation invokes the rule specified in the rule startup request. The user can check whether it was executed by accessing JP1/IM - Rule Operation from JP1/IM - View. The JP1/IM - Rule Operation host and manager can be the same server.

Important

The reporting to JP1/IM - Rule Operation is performed according to the system hierarchy (IM configuration) in the same way as for normal automated actions.

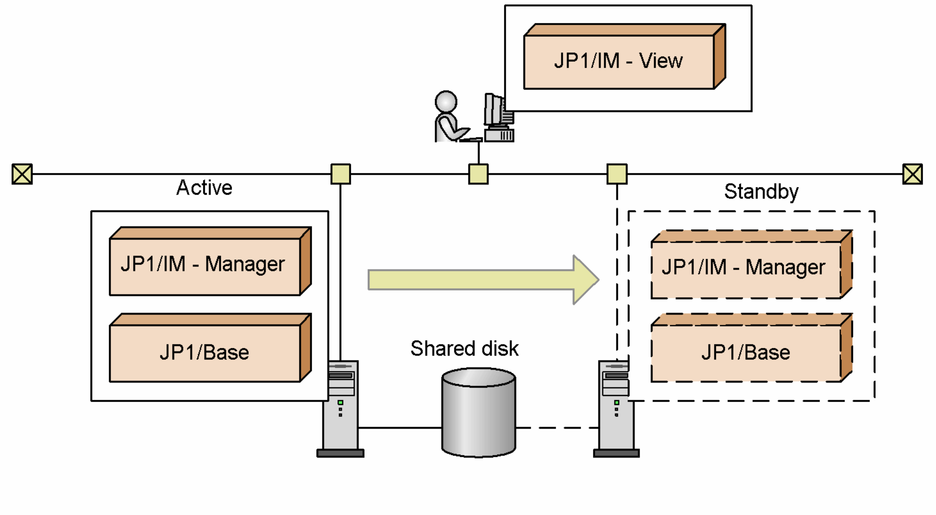
For this reason, if you want to run JP1/IM - Manager and JP1/IM - Rule Operation on different hosts, you must configure the JP1/IM - Rule Operation host at a level below the JP1/IM - Manager host.

12.3.8 Configuration for operation in a cluster system

JP1/IM supports cluster systems. When used in a cluster system, JP1/IM - Manager is failed over to the secondary node when a problem occurs on the primary node, and system monitoring continues without interruption.

An example of a system configuration for using JP1/IM - Manager in a cluster system is shown below.

Figure 12–9: Example of configuration for operation in a cluster system (active-standby configuration)



In this configuration, there is a primary server and a secondary server.

JP1/IM - Manager executes on the primary server. The secondary server stands by in case a failure occurs on the primary server. In normal circumstances, JP1/IM - Manager on this server is in stopped state.

For details, see *Chapter 6. Operation and Environment Configuration in a Cluster System (for Windows)* or *Chapter 7. Operation and Environment Configuration in a Cluster System (for UNIX)* in the *JP1/Integrated Management - Manager Configuration Guide*.

(1) Notes

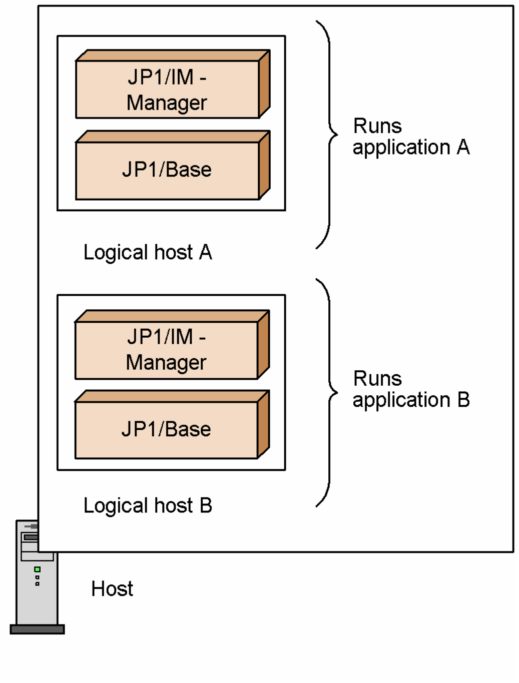
- When using JP1/IM in a cluster system, do not set up JP1/IM - Manager to restart after abnormal termination. If you need to restart JP1/IM - Manager, do so under the control of the cluster software.
- When a process management process is activated on a logical host in a cluster configuration, if the logical host's `conf` folder does not contain an extended startup process definition file, the extended startup process definition file on the physical host is copied.

12.3.9 Configuration for operation on a logical host in a non-cluster environment

JP1/IM - Manager can be run on a logical host in a non-cluster environment. By using a logical host that is not subject to failover, you can run multiple instances of JP1/IM - Manager, each dedicated to a particular application.

You can monitor more than one system from a single machine by running an instance of JP1/IM - Manager on a logical host corresponding to each system. The following figure shows an example of using JP1/IM - Manager to perform integrated monitoring of two systems from a single machine.

Figure 12–10: Performing integrated monitoring of two systems from one machine

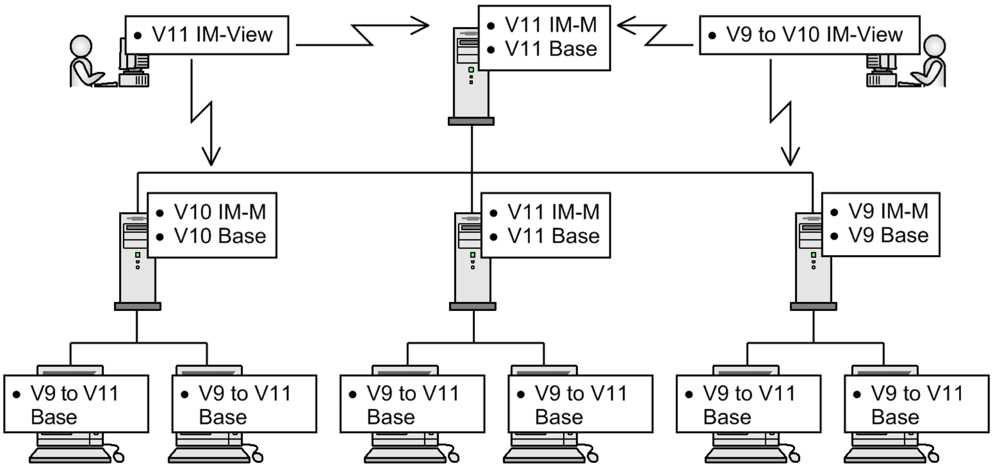


For details, see *6.9 Logical host operation and environment configuration in a non-cluster system (for Windows)* in the *JP1/Integrated Management - Manager Configuration Guide*.

12.3.10 Configuration for differing product versions

An example of a system configuration in which differing versions of JP1 products coexist is shown below.

Figure 12–11: Example of configuration for differing product versions



Legend:

V11 IM-View	: JP1/IM - View version 11
V11 IM-M	: JP1/IM - Manager version 11
V11 Base	: JP1/Base version 11
V10 IM-M	: JP1/IM - Manager version 10
V10 Base	: JP1/Base version 10
V9 Base	: JP1/Base version 9
V9 IM-M	: JP1/IM - Manager version 9
V9 to V10 IM-View	: JP1/IM - View version 9 to version 10
V9 to V11 Base	: JP1/Base version 9 to version 11

Note the following points when monitoring operations in a JP1/IM system with differing product versions:

- Versions 11, 10, and 7 cannot coexist on the same machine.
  For example, you cannot run JP1/Base version 11 and JP1/IM - Manager version 10 on the same machine.
- When products of different versions are linked, only the functions provided by the oldest of the versions can be used.
  For example, if JP1/IM - View version 10 connects to JP1/IM - Manager version 11, the operations you can perform are limited to those supported in JP1/IM - View version 10.
  For details about the restrictions that apply when different product versions coexist, see *Appendix H. Connectivity with Previous Versions*.

12.3.11 System configuration for managing monitored hosts with host names in FQDN format

In JP1/IM - Manager, monitored hosts are managed by their host names.

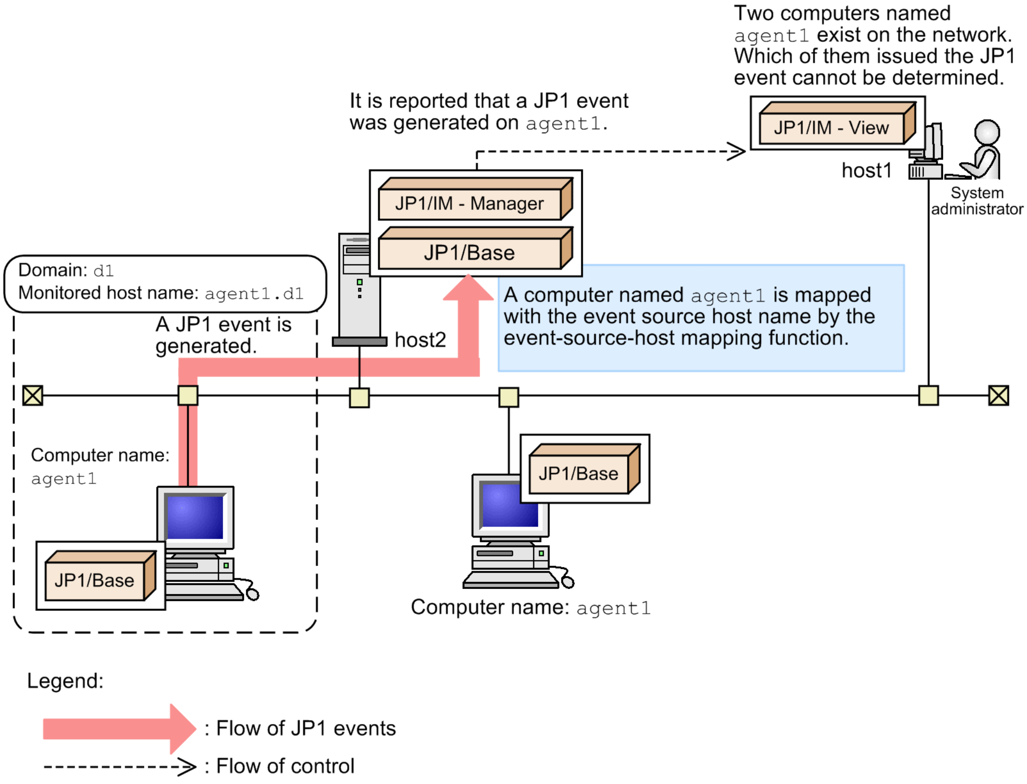
Using JP1/IM - Manager, you can manage monitored hosts with host names in FQDN format or with the host names that are displayed when the `hostname` command is executed (short names).

To manage monitored hosts with names in FQDN format, change the JP1/Base event server name to FQDN format. To manage monitored hosts with names in short name format (the host names displayed when the `hostname` command is executed), change the JP1/Base event server name to short name format.

The following describes how a monitored host with a host name in FQDN format is managed.

In a system with a domain name, a monitored host name and the event source host name might be different as shown in the following figure.

Figure 12–12: System with a domain name


Two computers named agent1 exist on the network. Which of them issued the JP1 event cannot be determined.
It is reported that a JP1 event was generated on agent1.
JP1/IM - View
host1
System administrator
JP1/IM - Manager
JP1/Base
Domain: d1
Monitored host name: agent1.d1
A JP1 event is generated.
host2
A computer named agent1 is mapped with the event source host name by the event-source-host mapping function.
Computer name: agent1
JP1/Base
JP1/Base
Computer name: agent1
Legend:
: Flow of JP1 events
: Flow of control

A JP1 event issued on `agent1.d1` is forwarded to `host2`, and displayed in JP1/IM - View. In this case, the event-source-host mapping function processes the computer name as the event source host name. JP1/IM - View displays `agent1` as the event source host name. In this figure, two `agent1` hosts exist in the network, so which of them issued the JP1 event cannot be determined.

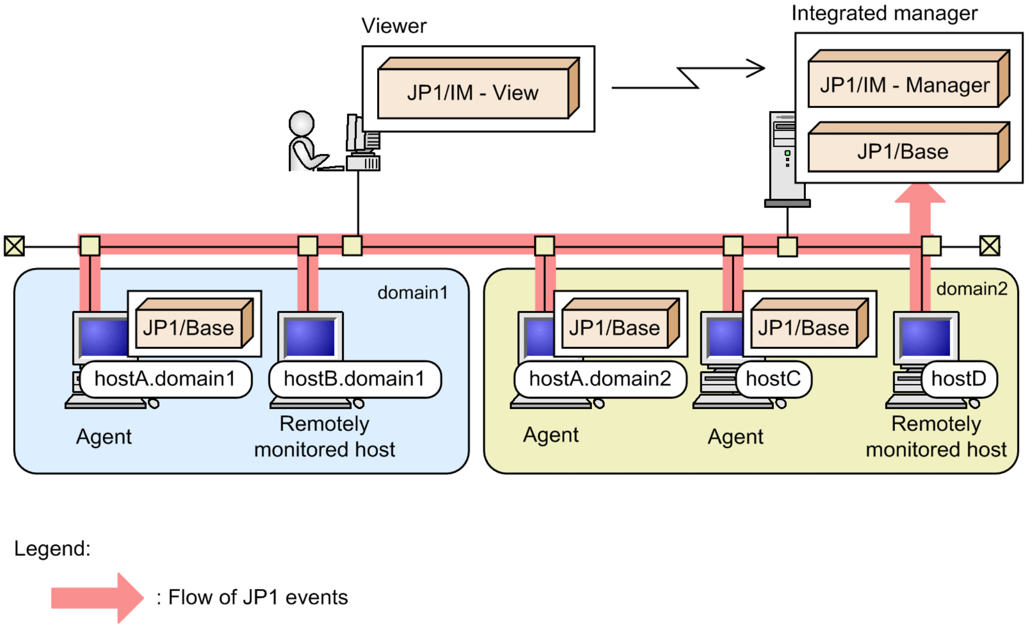
Because of this, even if the host names are mapped by the event-source-host mapping function, monitoring of hosts for each business group or filtering of JP1 events by host names might not properly work.

To avoid this problem, when you manage a host with the host name in FQDN format, configure JP1/Base and JP1/IM - Manager, referring to *12.3.11(2) Registering a host in an agent configuration or a remote monitoring configuration*.

(1) Basic configuration when monitored hosts with names in FQDN format are managed

The following figure shows the basic configuration of JP1/IM - Manager when monitored hosts with names in FQDN format are monitored.

Figure 12–13: Example of the basic configuration of JP1/IM - Manager (monitored hosts are monitored in FQDN format)



Viewer

- JP1/IM - View (no restrictions on the version)

Integrated manager

The following products, which support FQDN format, are required:

- JP1/IM - Manager version 10 or later
- JP1/Base version 10 or later

Agents (monitored hosts)

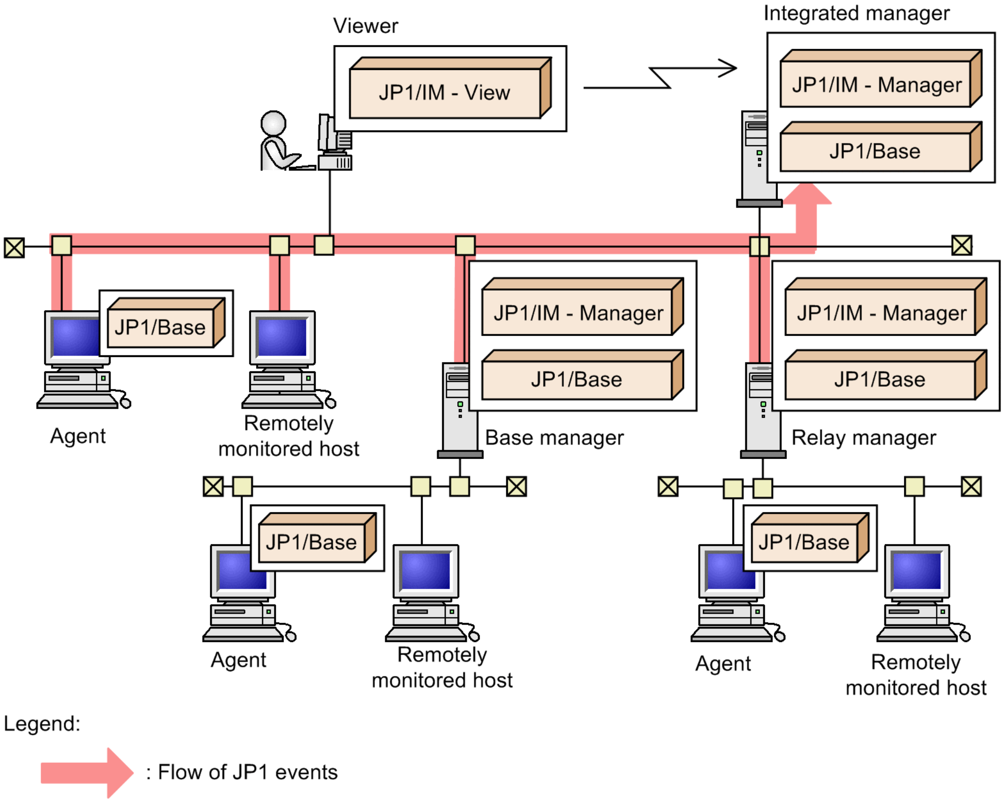
- JP1/Base (no restrictions on the version)
  Note that if a monitored host with a name in FQDN format is registered in agent configuration, the version of JP1/Base on the agent host must be 09-00 or later.

Remotely monitored hosts

- JP1/Base and JP1/IM - Manager are not required.

In the system hierarchy (IM configuration), you can also place the base managers that manage remotely monitored hosts, and relay managers that consolidate events on individual agents (monitored hosts).

Figure 12–14: Example of the JP1/IM - Manager configuration when a base manager and relay manager are used (monitored hosts are monitored in FQDN format)



The integrated manager and base managers

The following products, which support FQDN format, are required:

- JP1/IM - Manager version 10 or later
- JP1/Base version 10 or later

Relay manager

- JP1/IM - Manager (no restrictions on the version)
- JP1/Base (no restrictions on the version)

Agents (monitored hosts)

- JP1/Base (no restrictions on the version)

Remotely monitored hosts

- JP1/Base and JP1/IM - Manager are not required.

(2) Registering a host in an agent configuration or a remote monitoring configuration

(a) Using the same name for the host name to be registered in IM Configuration Management and as the event server name for the registered host (setting for JP1/Base)

Register the event server name of the registered host as the host name in IM Configuration Management. For details about how to set the same name, see *Setting up an event server in a system that uses DNS services* in the *JP1/Base User's Guide*.

If you change the event server name when the system is monitored by JP1/Base, the event source host name is changed. Therefore, check and, if necessary, revise the conditions of automated actions and the conditions for filtering JP1 events. For details about the items to be checked or revised, see *12.3.11(2)(c) Items to be reviewed when the event server name is changed*.

(b) Changing JP1 event attributes (Setting for JP1/IM - Manager)

When managing a host with a name in FQDN format, the attribute for the event source host name for event log traps (JP1 event 3A71) differs depending on the JP1/IM - Manager version as shown in the following table.

Table 12–8: Attributes for the event source host name

Change	Conditions of the event to be mapped		Attribute to be mapped to the event source host name	Description
	Event ID (`B.ID`)	Product name (`E.PPNAME`)		
Before change (JP1/IM - Manager version 09-50 or earlier)	3A71	--	Computer name (`E.A1`)	Event-source-host mapping definition for event 3A71 issued by remote-monitoring event log traps and JP1/Base event log traps
After change (JP1/IM - Manager version 10-00 or later)	3A71	`/HITACHI/JP1/NTEVENT_LOGTRAP`	Source event server name (`B.SOURCESERVER`)	Event-source-host mapping definition for event 3A71 issued by JP1/Base event log traps
		--	Computer name (`E.A1`)	Event-source-host mapping definition for event 3A71 that is issued by a remote-monitoring event log trap and forwarded from a submanager host when JP1/IM - Manager version 09-50 is used

Legend:

--: None

In the case of "Before change" (in the above table), the computer name is mapped to the event source host name. In the case of "After change" (in the above table), the source event server name is mapped to the event source host name.

To change the JP1 event attribute as in "After change" (in the above table), edit the file for setting common definitions (changing JP1 event attributes) as follows:

1. Perform a new installation or overwrite installation of JP1/IM - Manager.
2. Copy the model file (`jp1im_jp1_event_attributes.conf.model`) of the file for setting common definitions (changing JP1 event attributes) to any location.

   For details about the file for setting common definitions (changing JP1 event attributes), see *Common definition settings file (changing the attribute of JP1 events)* in *Chapter 2. Definition Files* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.
3. Edit the `ATTR_EVENT_LOGTRAP_SOURCEHOST` line of the copied file as follows:

   ```
   [JP1_DEFAULT\JP1CONFIG]
   "ATTR_EVENT_LOGTRAP_SOURCEHOST"=dword:00000001
   ```
4. Execute the `jbssetcnf` command.

   For details on the `jbssetcnf` command, see the *JP1/Base User's Guide*.
5. Restart JP1/IM - Manager.

   Make sure that you restart JP1/IM - Manager.

(c) Items to be reviewed when the event server name is changed

If the event server name is changed, the event source host name is also changed. Check and, if necessary, revise the following items related to the event source host name.

Table 12–9: Items that must be reviewed

Product	Function	Item	What to be checked
JP1/IM - Manager	Event list display and detailed event display	Checking the display contents	If an item of the event source host is displayed, the format of the displayed host name is changed. Check whether the displayed format is acceptable.
	JP1 event filtering	Checking the conditions of event receiver filters, view filters, severe event definitions, and common exclusion-conditions (in extended mode)	If the event source host name is specified for filter conditions, check whether filtering can be performed correctly.
	Event guide display	Checking the display conditions	If an item of the event source host is displayed, the format of the displayed host name is changed. Check whether the displayed format is acceptable.
		Checking the event attributes used for event guide messages	If the event source host name is used for an event attribute, check whether the attribute is correct.
	Event search	Checking the search conditions	If the event source host name is specified for filter conditions, check whether filtering can be performed correctly.
	Event report output	Checking the filter conditions	
		Checking the output attributes	If the attribute for the event source host name is output, check whether the output value is acceptable.
	Correlation event generation	Checking the correlation event generation conditions	If the attribute of the event source host name is inherited to a correlation event, check whether the inherited value is acceptable. If an automated action is executed for a correlation event, also check the execution conditions of the automated action.
	Changing severity of JP1 events	Checking the severity changing conditions	If the event source host name is specified for filter conditions, check whether filtering can be performed correctly.
	Event-source-host mapping	Checking the event-source-host mapping definition	
	Command execution and automated action	Checking the execution conditions	If the event source host name is specified for the execution conditions, check whether the action can be correctly executed.
		Checking the inherited information	If the attribute information of the event source host name is specified in the action definitions of commands and actions, check whether the commands and actions can be correctly executed.
	Restrictions on viewing and operating business groups	Checking the restrictions on viewing events	Check whether event 3A71 is displayed only for the users in the business group to which the event is applied.
	Change of the handling for JP1 events, and setting of memo information	You do not have to check this function.	

Product	Function	Item	What to be checked
JP1/Base		Event forwarding setting	When JP1/IM - Manager version 09-50 is used, if a submanager host forwards a 3A71 event to a higher-level manager by using a remote-monitoring event log trap, upgrade JP1/IM - Manager on the submanager host to version 10-00 or later. After that, change the attributes of JP1 events.
Other products	Launching of a linked product by monitor startup, linkage with the Tool Launcher window JP1/IM - Rule Operation, and management of response-waiting events	You do not have to check this function.	

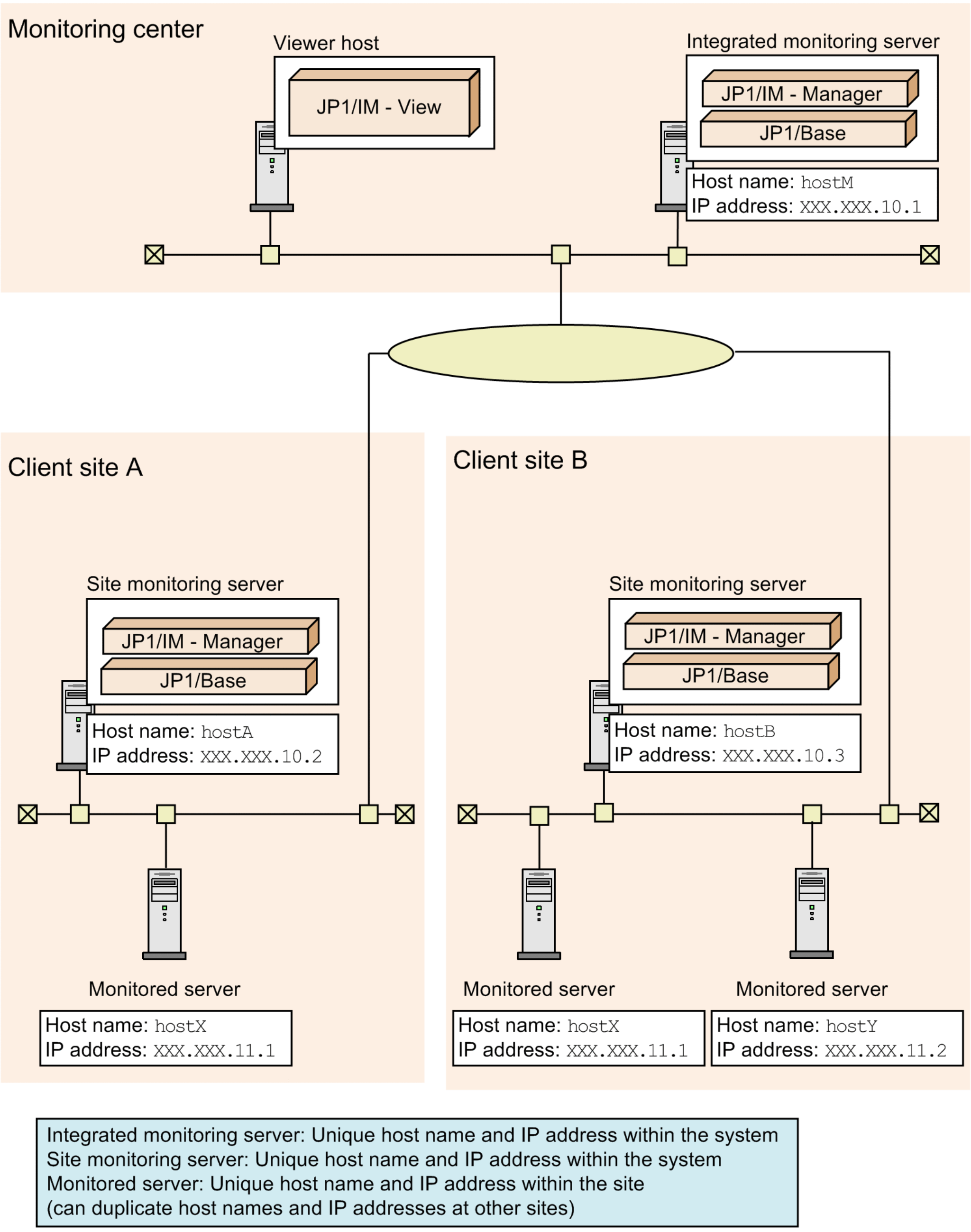
12.3.12 Monitoring multiple sites

By using JP1/IM - Manager running on one integrated monitoring server, you can centrally monitor events that occur on monitored servers at multiple sites.

You can specify a desired host name and IP address for a monitored server running at each site, regardless of the host names and IP addresses of the monitored servers running at other sites. However, the host name and IP address must be unique within the same site.

For the integrated monitoring server and the site monitoring servers, specify host names and IP addresses that are unique within the system.

Figure 12–15: System configuration



The following tables describe the prerequisites and limitations when host names and IP addresses are duplicated at different sites.

(1) Prerequisites

No.	Server	Prerequisite
1	Site monitoring server	A site monitoring server on which JP1/IM - Manager and JP1/Base are installed is required for monitoring the monitored servers at each site.
2	Site monitoring server Monitored server	The target servers are monitored remotely from the site monitoring server. The integrated monitoring server cannot monitor remote servers that are subject to monitoring. If you use an agent configuration (JP1/Base is installed on a monitored server) for monitoring, configure a FQDN-format event server on the monitored server. For details, see the *JP1/Base User's Guide*.

No.	Server	Prerequisite
3	Integrated monitoring server Site monitoring server	Set up an environment in such a manner that the integrated monitoring server and the site monitoring server can communicate with each other.
4	Integrated monitoring server Site monitoring server	The host names and IP addresses of the integrated monitoring server and the site monitoring servers must be fixed and unique within the system configuration. If you change the host name and IP address of a site monitoring server, you must check and, if necessary, revise settings such as filter conditions for JP1/IM - Manager and JP1/Base, and restart services. For details, see *2.2 Tasks necessary when a host name is changed* and *2.3 Tasks necessary when an IP address is changed* in the *JP1/Integrated Management - Manager Administration Guide*.
5	Monitored server	The host names and IP addresses of monitored servers must be unique within the same site.
6	Monitored server	The host name of a monitored server must be fixed. If you change the host name of a monitored server, you must change the host information registered in the IM Configuration Management database. For details see, *3.1.5 Changing the attributes of host information* in the *JP1/Integrated Management - Manager Configuration Guide*.
7	Integrated monitoring server Site monitoring server Monitored server	If you use DHCP to connect to monitored servers, configure the environment so that the site monitoring server can dynamically resolve IP addresses from the monitored servers' host names by using, for example, DNS. Note that there is no need for the integrated monitoring server to resolve monitored servers' host names. If you use DHCP to manage the IP addresses of an integrated monitoring server and site monitoring servers, set the expiration of IP address allocation to infinite so that the IP addresses will never change. For details, see *12.4.1 Host names and IP addresses*.
8	Monitored server	When you change the IP address of a monitored server, first stop the monitoring of that monitored server, change the IP address, and then restart the monitoring. The same applies when an IP address is reallocated by DHCP. You must also ensure that the site monitoring server can resolve the new IP address by using (for example) DNS.

(2) Limitations

No.	Condition	Limitation
1	Employing a system hierarchy (configuring the integrated monitoring server and site monitoring servers in a hierarchy) by using IM Configuration Management	IM Configuration Management of the integrated monitoring server cannot manage monitored servers. Do not set a site monitoring server at a site as a *base manager* for monitoring multiple sites.
2	System configuration (remote monitoring of servers by a site monitoring server)	For remote monitoring, the supported log file size and the maximum number of Windows event logs that can be acquired differ from those values for an agent configuration. For details, see *6.6 Managing remotely monitored hosts*.
3	Manipulating monitored servers	The integrated monitoring server cannot manipulate monitored servers by using, for example, commands, because the integrated monitoring server cannot identify the monitored servers individually.

12.4 Network considerations

Consider the configuration of the network in which JP1/IM will be used.

There are several aspects to consider, from the network settings on each host through to the network as a whole.

JP1/IM communication is controlled by the JP1/Base core functionality. This section discusses JP1/IM, but you should also consider JP1/Base network requirements.

12.4.1 Host names and IP addresses

JP1/IM operates using the host name displayed by the `hostname` command or, in a cluster system, the specified logical host name.

When specifying a host name in a JP1/IM function, set the host name displayed by the `hostname` command or the logical host name.

Set the host names to be used by JP1/IM in the `hosts` file or similar so that they can be converted into IP addresses.

If you are managing host names and IP addresses in the FQDN format by using the DNS, see *12.3.11 System configuration for managing monitored hosts with host names in FQDN format*.

When specifying a logical host name, comply with the following conventions:

Number of specifiable characters when not using the IM database:

- In Windows: 1 to 196 bytes (recommended: 63 bytes or less)
- In UNIX: 1 to 255 bytes (recommended: 63 bytes or less)

Number of specifiable characters when using the IM database:

- 1 to 32 bytes

If you are using any other host names, see *12.4.3 Operation in a configuration connected to multiple networks*.

- When a host has multiple IP addresses, and a local host name is defined for each IP address in the `hosts` file, you can only specify the host name output by the `hostname` command as the **Target host** setting for an automated action.
  An example is shown below.
  Suppose that the following is defined in the `hosts` file:
  ```
  100.0.0.10 hostA
  200.0.0.10 hostB
  ```
  If the host name displayed by the `hostname` command is `hostA`, you can only specify `hostA` as the target host name.
- The definition in the `hosts` file is not referred to for the host names and IP addresses that are defined in `jp1hosts` information or `jp1hosts2` information.
  An example is shown below.
  Suppose that the following is defined in the `jp1hosts` information:
  ```
  hostA 100.0.0.10 200.0.0.10
  ```
  Suppose also that the following is defined in the `hosts` file:
  ```
  100.0.0.10 hostA hostB
  ```

```
200.0.0.10 hostC
```

In this case, the `hosts` file is not referenced for hostA, IP address 100.0.0.10, or IP address 200.0.0.10. For this reason, you cannot specify hostB and hostC, which are not defined in the `jp1hosts` information, as target host names for command execution.

- Associations between the host names and IP addresses that are defined in `jp1hosts` or `jp1hosts2` information must be the same as the corresponding definitions in the system. If you define an IP address different from the corresponding definition in the system, an inconsistency will occur in name resolution, and abnormal system operation will result.

Note the following points:

- Using DHCP

  If the IP addresses used by JP1/IM and JP1/Base are managed using DHCP, set an unlimited duration for the IP address lease so that the IP address does not change.

  JP1/IM and JP1/Base will not work properly if the IP address changes during JP1/IM and JP1/Base operation.

- Using a DNS server

  Set the DNS server so that host names can be converted to IP addresses, and IP addresses can be converted to host names (reverse lookup). Note that when a DNS server (including Active Directory) is used for name resolution, you must purposely set JP1/IM to allow address lookup in both directions.

12.4.2 Server network configuration

Check the following points regarding the server network configuration in which JP1/IM is to be used:

- Media sense (in Windows)

  We recommend that you disable the Windows media sense functionality that detects LAN cable disconnection and inactivates IP addresses. If the media sense functionality is enabled, a temporary network error will cause IP addresses to be lost, disabling JP1 communication.

- Duplicate NIC

  Some OSs provide duplicate NIC functionality (for example, Windows NIC teaming or AIX Ethernet channel) for switching to a standby NIC if the primary NIC fails. A server running JP1 that uses the duplicate NIC functionality must be completely compatible with non-duplicate NIC operations and must not affect JP1 operations.

12.4.3 Operation in a configuration connected to multiple networks

When the JP1/IM hosts are configured in an environment connected to multiple networks, requirements like the following might apply to the JP1/IM system:

- Example: The host name should not be the host name displayed by the `hostname` command or a host name specified as a logical host name.
- Example: JP1 needs to communicate over a designated LAN dedicated for operation management, separate from other products.

If your system has such requirements, use the special setting called *multiple LAN connection* in JP1/IM and JP1/Base. For example, set `jp1hosts` information to associate host names with IP addresses uniquely in JP1.

See the following references when considering setup and operation.

About multiple networks:

- Operation in a multi-network environment

  See *8. Operation and Environment Configuration Depending on the Network Configuration* in the *JP1/Integrated Management - Manager Configuration Guide*.

  Also see the description of JP1/Base communication settings according to network configuration in the *JP1/Base User's Guide*.

Notes:

The definition in the `hosts` file is not referred to for the host names and IP addresses that are defined in `jp1hosts` information or `jp1hosts2` information.

12.4.4 Operation behind a firewall

JP1/IM supports operation in a network configuration through a firewall. JP1/IM supports the firewall packet filtering method and the NAT static conversion method.

See the following references when considering setup and operation.

About operation behind a firewall:

- Use in a firewall environment

  See *8. Operation and Environment Configuration Depending on the Network Configuration* in the *JP1/Integrated Management - Manager Configuration Guide*.

  Also see the description of JP1/Base communication settings according to network configuration in the *JP1/Base User's Guide*.

(1) Notes

- There are two types of communication between the manager and the agents: communications performed according to the system hierarchy (IM configuration), and direct communication between hosts (see *7.3 Communication performed in the JP1/IM system environment*). The firewall settings must support the type of communication being used.
- JP1/IM and JP1/Base use ports even for communication within the local host. If you are using JP1/IM and JP1/Base on the host set up as a firewall, the firewall settings must permit local traffic through all the ports used by JP1/IM and JP1/Base.

12.4.5 WAN connection

JP1/IM - Manager can be used on a WAN only if the line is always connected.

Notes on connecting JP1/IM - Manager and monitored hosts

When you use JP1/IM - Manager in a WAN environment, we recommend that you consider communication speed and traffic and create a multi-level system configuration. The recommended configuration has from tens to hundreds of monitored hosts that are installed in each building or work place and that are connected to a LAN and a base manager located in the work place. Note the following when using JP1/IM - Manager in a WAN environment:

- When JP1/IM - Manager monitors a log on a monitored host, it periodically communicates with the monitored host. Accordingly, we do not recommend that you connect JP1/IM - Manager and monitored hosts on a network that charges according to time or traffic (for example, an INS-P or INS-C WAN).

- Timeouts might be frequent during communication between JP1/IM - Manager and monitored hosts.
- Remote monitoring is disabled if the firewall located between the integrated manager and monitored hosts uses NAT static conversion. Be careful when a firewall is installed between the integrated manager and monitored hosts in a WAN environment. You can avoid this problem by adding an additional base manager on the monitored-host side. By doing so, NAT static conversion moves from the firewall between the integrated manager and monitored hosts to between the integrated manager and the additional base manager.

For firewall settings, see *12.4.4 Operation behind a firewall*.

Notes on connection between JP1/IM - Manager and JP1/IM - View

Notes the following when using JP1/IM - Manager in a WAN environment:

- Because JP1/IM - Manager and JP1/IM - View periodically communicate with each other, we recommend that you do not connect JP1/IM - Manager and monitored hosts on a network that charges according to time or traffic (for example, an INS-P or INS-C WAN).
- Communication timeouts might tend to occur between JP1/IM - View and JP1/IM - Manager. If this is the case, review the timeout periods set for communication between JP1/IM - View and JP1/IM - Manager.

About JP1/IM - View and JP1/IM - Manager timeout periods:

See *Communication environment definition file (console.conf.update)* in *Chapter 2. Definition Files* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

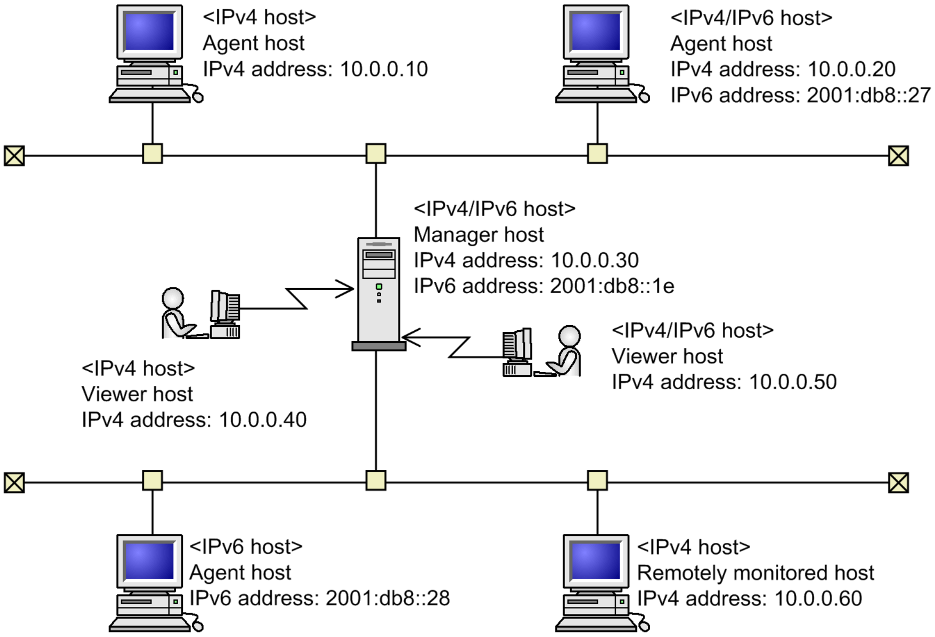
See *Communication environment definition file (view.conf.update)* in *Chapter 2. Definition Files* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

See *Communication environment definition file (tree_view.conf.update)* in *Chapter 2. Definition Files* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

12.4.6 System configuration that supports IPv6 hosts

JP1/IM can manage JP1/Base running on *IPv6* hosts. You can manage IPv6 hosts on which JP1/Base is running in the same way as *IPv4* hosts on which JP1/Base is running. You can collect host information, manage profiles, execute commands, and display JP1 events for IPv6 hosts.

Figure 12–16: System configuration



- IPv6 host
  Indicates a host with an IPv6 address.
- IPv4 host
  Indicates a host with an IPv4 address.
- IPv4/IPv6 host
  Indicates a host that has both the IPv4 and IPv6 addresses.

A network environment in which IPv4 hosts, IPv6 hosts, and IPv4/IPv6 hosts coexist is called an *IPv6 environment*.

As shown in the above figure, the viewer hosts and the manager host communicate with each other using IPv4 addresses. The agent hosts and the manager host communicate with each other using IPv4 or IPv6 addresses.

Examples of IPv4 and IPv6 addresses:

- Example of an IPv4 address
  `11.22.33.44`
- Example of an IPv6 address
  `0011:2233:4455:6677:8899:aabb:ccdd:eeff`

You cannot specify IPv4-mapped addresses and IPv4-compatible addresses. In addition, some functions do not support the abbreviated format of IPv6 addresses. For details about the functions for which the abbreviated format of IPv6 addresses can be specified, see *12.4.6(3) Functions supported in an IPv6 environment*.

- Example of 11.22.33.44 in IPv4-mapped address format:
  `::ffff:11.22.33.44`
- Example of 11.22.33.44 in IPv4-compatible address format:
  `::11.22.33.44`
- Example of 2012:0007:0008:0000:0000:0000:000a:000b in abbreviated IPv6 format:
  `2012:7:8::a:b`

(1) Prerequisites for monitoring system configuration in an IPv6 environment

Prerequisites differ depending on the network environment for the manager host.

For cluster configuration, the system configuration of the primary node and the standby node must be the same.

(a) When the manager host is an IPv4 host

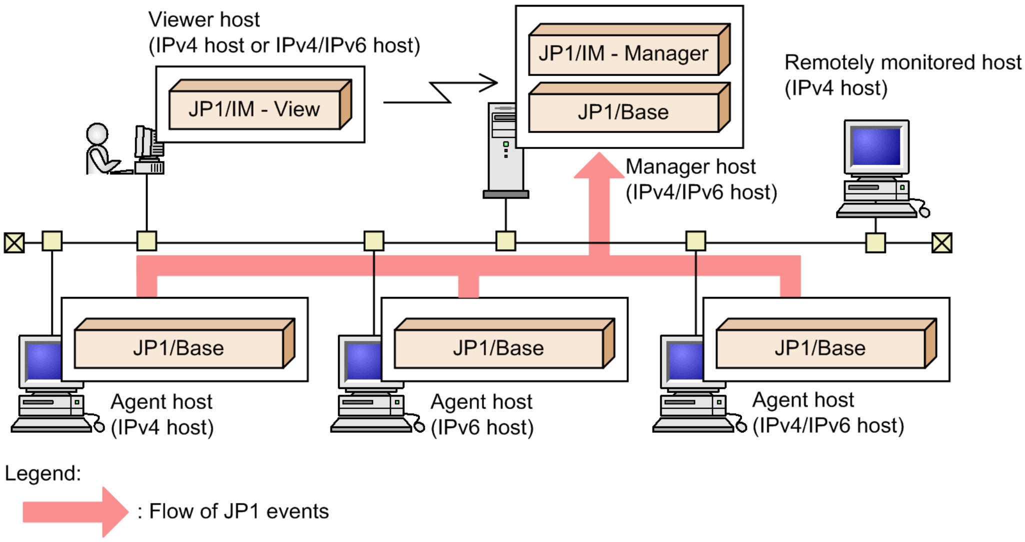
When the manager host is an IPv4 host, the manager cannot manage IPv6 hosts and IPv4/IPv6 hosts.

(b) When the manager host is an IPv6 host

An IPv6 manager host is not supported.

(c) When the manager host is an IPv4/IPv6 host

Figure 12–17: Prerequisites when the manager host is an IPv4/IPv6 host



Manager host

- The host is an IPv4/IPv6 host.
- The version of JP1/IM - Manager is 10-00 or later.
- The version of JP1/Base is 10-00 or later, and `jp1hosts2` information has been defined.
- For the JP1/Base `jp1hosts2` definition, the IPv4 address and IPv6 address of the manager host have been defined.
- The OS is Windows Server 2016, Windows Server 2012, Windows Server 2008 R2 (x64), or Linux.

Viewer host

- The host is an IPv4 host or IPv4/IPv6 host.
- For JP1/IM - View running on an IPv4/IPv6 host, the IPv4 address is used.

Agent hosts

- The hosts are IPv4 hosts, IPv6 hosts, or IPv4/IPv6 hosts.
- The version of JP1/Base is 10-00 or later.
- For JP1/Base running on an IPv6 host or IPv4/IPv6 host, `jp1hosts2` information has been defined.
- For JP1/Base running on an IPv6 host or IPv4/IPv6 host, the OS is Windows Server 2016, Windows Server 2012, Windows Server 2008 R2, or Linux.

Remotely monitored hosts and virtualization system configuration

- The host is an IPv4 host.

When you want JP1/IM - Manager to link with other products, it can link with products on IPv4 hosts. However, it cannot link with products on IPv6 hosts. The one exception is that JP1/IM - Manager can link with BJEX or JP1/AS on IPv6 hosts in order to manage response-waiting events.

(2) Maximum configuration of the JP1/IM - Manager system for managing an IPv6 environment

The number of agent hosts that can be managed by one JP1/IM - Manager does not depend on whether the agent hosts are IPv4 hosts, IPv6 hosts, or IPv4/IPv6 hosts.

For details about the maximum system configuration, see *D.3(1) JP1/IM - Manager limits*.

(3) Functions supported in an IPv6 environment

The following describes the functions supported in an IPv6 environment when the version of JP1/IM - Manager is 10-00 or later.

(a) Login

You cannot specify an IPv6 address for the name of a host used for remote login. Specify an IPv4 address or a host name for which an IPv4 address can be resolved.

(b) Event monitoring

You can display and specify JP1 events whose source IP address (`B.SOURCEIPADDR`) or destination IP address (`B.DESTIPADDR`) is an IPv6 address.

Event filtering

For a condition of the JP1 event to be filtered, you can specify the source IP address (`B.SOURCEIPADDR`) in IPv6 format. You can specify the source IPv6 address for the event acquisition filter (common exclusion-conditions in extended mode). For an event condition, you can specify an IPv6 address by using four-digit hexadecimal numbers (0-9 and a-f) as follows:

Example: `0011:2233:4455:6677:8899:aabb:ccdd:eeff`

You cannot use upper-case characters, and cannot specify an IPv4-mapped address, IPv4-compatible address, or abbreviated format IPv6 address.

Also, in the Common Exclusion-Condition Settings (Extended) window, if you click the **Read From Selected Event** button, the source IP address of the JP1 event selected in the event list is automatically set for the event condition. However, if the version of JP1/IM - View is earlier than 10-00 and the source IP address in the common exclusion-condition is an IPv6 address, the source IP address is not automatically set even if you click the **Read From Selected Event** button in the Common Exclusion-Condition Settings (Extended) window. In that case, manually specify an IPv6 address for the filter condition. When you manually specify an IPv6 address for the filter condition, follow the specification format for an event condition regardless of the version of JP1/IM - View.

Note that the destination IP address (`B.DESTIPADDR`) cannot be specified for a filter condition in the same way as when IPv4 addresses are managed.

Display of event details

In the Event Details window and the Edit Event Details window, you can display the source IP address (`B.SOURCEIPADDR`) in IPv6 address format in the **Event attributes** field. An IPv6 address is specified with four-digit hexadecimal numbers (0-9 and a-f) as follows:

Example: `0011:2233:4455:6677:8899:aabb:ccdd:eeff`

Note that the destination IP address is not displayed in the same way as when IPv4 addresses are managed. If the version of JP1/IM - View is earlier than 10-00, the source IP address and the destination IP address are not displayed in the **Event attributes** field regardless of whether those addresses are IPv4 addresses or IPv6 addresses.

Display of event guide

For a condition for comparing JP1 events, you can specify an IPv6 address for the source IP address (`B.SOURCEIPADDR`) or the destination IP address (`B.DESTIPADDR`). You cannot specify the source IP address and the destination IP address for variables for an event guide message. (This is also true for IPv4 addresses.)

Event search

You can specify an IPv6 address or a host name that can be resolved to an IPv6 address for the search host.

For the search host, you can specify IPv6 addresses in the following formats:

- Four-digit hexadecimal (0-9 and a-f)
  Example: `0011:2233:4455:6677:8899:aabb:ccdd:eeff`
- Four-digit hexadecimal (0-9 and A-F)
  Example: `0011:2233:4455:6677:8899:AABB:CCDD:EEFF`
- Abbreviated IPv6
  Example: `2012:7:8::a:b`

If restrictions are set on viewing and operating business groups, specify the host name (domain name) managed by IM Configuration Management. To specify a manager host for the search host, specify the host name or IPv4 address of the manager host.

Event report output

You can output JP1 events in which an IPv6 address is specified for the source IP address (`B.SOURCEIPADDR`) or the destination IP address (`B.DESTIPADDR`) to a csv file. IPv6 addresses are output to a csv file as sequences of four-digit hexadecimal numbers (0-9 and a-f) as follows:

Example: `0011:2233:4455:6677:8899:aabb:ccdd:eeff`

For the output items and event conditions of a report, you cannot specify the source IP address and the destination IP address. (This is also true for IPv4 addresses.)

Handling status change

When executing the `jcochstat` command to change the handling status, you cannot specify an IPv6 address for the `-h` option.

Issuance of correlation events

The source IP address and the destination IP address for correlation events are the IPv4 address of the manager host.

(c) Command execution and automated action

You can execute commands or automated actions on IPv6 managed hosts. For the target host name, you can specify IPv6 addresses in the following formats:

- Four-digit hexadecimal (0-9 and a-f)
  Example: `0011:2233:4455:6677:8899:aabb:ccdd:eeff`
- Four-digit hexadecimal (0-9 and A-F)
  Example: `0011:2233:4455:6677:8899:AABB:CCDD:EEFF`
- Abbreviated IPv6
  Example: `2012:7:8::a:b`

If you specify a value that cannot be specified in JP1/Base, the execution fails. If restrictions are set on viewing and operating business groups, specify the host name (domain name) managed by IM Configuration Management.

Conditions for executing an automated action

For the conditions for executing an automated action, you can specify the source IP address (`B.SOURCEIPADDR`). You cannot specify the destination IP address (`B.DESTIPADDR`). (This is also true for IPv4 addresses.) Specify the source IP address with four-digit hexadecimal numbers (0-9 and a-f) as follows:

Example: `0011:2233:4455:6677:8899:aabb:ccdd:eeff`

You cannot use upper-case characters, and cannot specify an IPv4-mapped address, IPv4-compatible address, or abbreviated IPv6 address.

Inheritance of event information to command execution and automated action

The attribute information of a JP1 event in which an IPv6 address is specified for the source IP address (`B.SOURCEIPADDR`) can be inherited to command execution contents. The variables `EVIPADDR` (source IP address) and `EVBASE` (basic event information) can be inherited. The IPv6 address is output to the command execution contents as four-digit hexadecimal numbers (0-9 and a-f) as follows:

Example: `0011:2233:4455:6677:8899:aabb:ccdd:eeff`

The attribute information of the destination IP address (`B.DESTIPADDR`) cannot be inherited. (This is also true for IPv4 addresses.)

Acquiring the event source host name

You can acquire the event source host name from the source IP address (`B.SOURCEIPADDR`). This method is also available when the source IP address is an IPv6 address.

For details about how to acquire the event source host name, see *Automated action environment definition file (action.conf.update)* in *Chapter 2. Definition Files* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

Note that the value of the source IP address is not guaranteed after it is forwarded. For details, see the description of basic attributes in the *JP1/Base User's Guide*.

(d) IM Configuration Management

You can manage IPv6 agent hosts. You can collect and manage host information or manage JP1/Base profiles on IPv6 hosts.

You cannot manage remotely monitored IPv6 hosts.

(e) Linked products

Launch of a linked product by monitor startup

You can launch a monitor window of a linked product from a JP1 event in which an IPv6 address is specified for the source IP address (`B.SOURCEIPADDR`) or the destination IP address (`B.DESTIPADDR`). If you monitor a system in which IPv4 hosts and IPv6 hosts coexist, however, check the specification of the linked application. Note that you cannot specify the source IP address and the destination IP address for the subkey definition nor for the call interface definition in the definition file for opening monitor windows. For details about the definition file for opening monitor windows, see *Automated action environment definition file (action.conf.update)* in *Chapter 2. Definition Files* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

Registering incidents

You can register into JP1/Service Support a JP1 event whose source IP address (`B.SOURCEIPADDR`) or destination IP address (`B.DESTIPADDR`) registered in the manager host's event database or integrated monitoring database is an IPv6 address. However, attribute information for the source IP address and destination IP address cannot be set in an incident that is registered into JP1/Service Support.

(f) Web browser

You cannot specify an IPv6 address for the name of the host that the Web browser connects to.

(g) Email notification function

An IPv6 address cannot be specified as the IP address of a mail server that communicates with the email notification function.

(4) Items to be checked when the system configuration is changed

(a) Items to be checked when the manager host is changed from an IPv4 host to an IPv4/IPv6 host

- Check whether the OS on the manager host supports IPv6 addresses.
- Check whether JP1/Base on the manager host supports IPv6 addresses.
- Check and, if necessary, change the connection target host so that the IPv4 address of the connection target host can be acquired on the viewer host when logging into JP1/IM - Manager.

(b) Items to be checked when a monitored host is changed from an IPv4 host to an IPv6 host

- Check whether the OS on the monitored host supports IPv6 addresses.
- Check whether JP1/Base on the monitored host supports IPv6 addresses.
- When filtering events, if the source IP address (`B.SOURCEIPADDR`) is specified in the event acquisition filter (common exclusion-condition in the extended mode), check the settings of the common exclusion-conditions to determine whether IPv6 address filtering is required.
- When searching events, check whether the manager host and the search host with an IPv6 address can communicate using IPv6 protocol.
- When changing the handling status, check and, if necessary, change the connection target host so that the IPv4 address of the connection target host can be acquired on the host on which the `jcochstat` command is executed.
- When the attribute information of the source IP address (`B.SOURCEIPADDR`) is inherited by command execution and automated actions, confirm that there is no problem if an IPv6 address is inherited as attribute information.
- When a source IP address is specified for the execution conditions for automated actions, check the execution conditions to determine whether IPv6 address filtering is required.
- When `local` is specified as the method for acquiring the event source host name, check whether name resolution of a host with an IPv6 address is required.

(c) JP1/Base settings

For details about the items to be checked, see the *JP1/Base User's Guide*.

(5) Changing system configuration

(a) Changing the manager host from an IPv4 host to an IPv4/IPv6 host

- JP1/Base
  Move from `jp1hosts` information to `jp1hosts2` information. For details about the procedure, see the *JP1/Base User's Guide*.
- JP1/IM - Manager
  You do not have to change anything.

(b) Changing a monitored host from an IPv4 host to an IPv6 host

- JP1/Base on the monitored host

  Overwrite install JP1/Base to version 10-00 or later.

  Then, move from `jp1hosts` information to `jp1hosts2` information. For details about the procedure, see the *JP1/Base User's Guide*.

- Manager host

  You need to configure the manager host to use IPv6. For details about the procedure, see *12.4.6(5)(a) Changing the manager host from an IPv4 host to an IPv4/IPv6 host*.

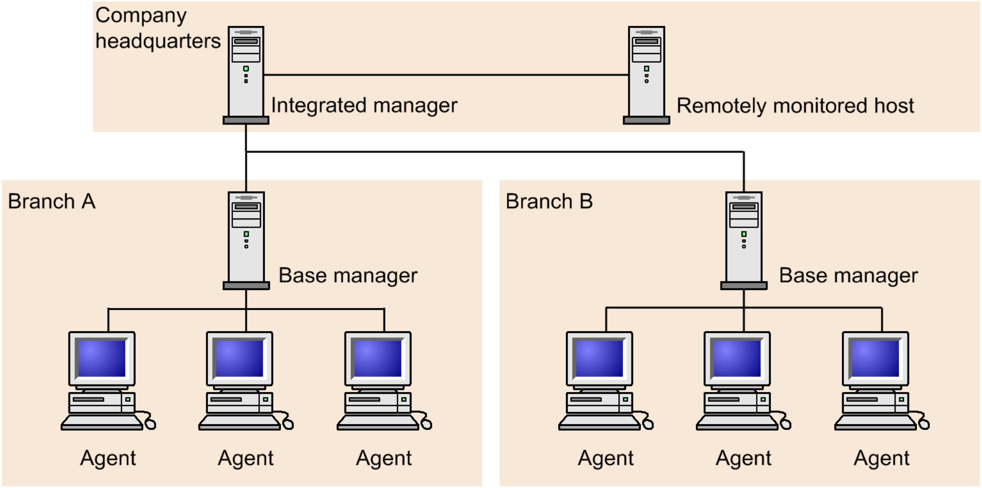
12.5 Considerations for the system hierarchy

Consider the hosts to be managed by JP1/IM and their hierarchical relationships.

In JP1/IM, the configuration management functionality is used to determine the range of the systems to be monitored by JP1/IM. You can also configure a hierarchy with base managers or relay managers arranged below the integrated manager, and agents placed below the base managers or relay managers. You can also place hosts in a remote monitoring configuration, for which remote communication is set, below the integrated manager or the base managers.

For example, as shown in the figure below, you can have a mixed agent and remote monitoring configuration. In this figure, the machines placed in the head office are used as the integrated manager and a remotely managed host, the main machine placed in each branch office is used as the base manager, and other machines placed in individual branch offices are used as agents.

Figure 12–18: Example system hierarchy



Using IM Configuration Management, you can monitor the hosts by business groups or monitoring groups, by defining business groups or by defining monitoring groups in each business group. Determine whether to operate the system by defining business groups, and consider the system hierarchy (IM configuration). For details about business groups, see *6.4 Managing business groups*.

Using the configuration management functions, you can define the configuration of the system to be managed by JP1/IM as *configuration definition* information. This allows you to perform the following tasks:

- Forward JP1 events to higher-level hosts
- Execute commands remotely from JP1/IM - View
- Execute automated actions from JP1/IM
- Collect and distribute definition information

When using IM Configuration Management, you define the system hierarchy through IM Configuration Management - View. If you are not using IM Configuration Management, you define the system hierarchy using the JP1/Base configuration management functionality.

For details about these functions, see the following references:

When using IM Configuration Management:

- Hierarchical configurations that can be set with IM Configuration Management
  See *6.2.1 Hierarchical configurations managed by IM Configuration Management*.

When not using IM Configuration Management:

- Hierarchical configurations that can be set with the JP1/Base configuration management functions
  See *7.4.3 Managing the system hierarchy*.

Assume if you use IM Configuration Management and the `jbsrt_distrib` command provided by JP1/Base at the same time when you change the management mode after beginning managing the system hierarchy. If you do so, inconsistencies might occur between the information actually applied to the system and the configuration definition information retained by hosts, and the system operation might be disordered.

Therefore, we do not recommend that you change the management mode after beginning management of the system hierarchy. Carefully consider which mode of hierarchy management you want to employ before you start using the system.

12.6 Considerations for user authentication

Consider the authentication servers used to manage JP1 users.

To monitor the system operation in JP1/IM, the user logs in to JP1/IM - Manager on the manager from JP1/IM - View. The authentication server authenticates the user at login, and the user's operating permissions are returned to JP1/IM - View. In JP1/IM, this processing flow is called *user authentication*.

In JP1/IM, user authentication setup is required on the managers and on the host on which JP1/Base serves as the authentication server. (For details about setting up user authentication, see the description of setting up the user management functionality in the *JP1/Base User's Guide*.)

12.6.1 User authentication blocks

On a manager, you must specify the authentication server that is accessed by the manager. If multiple managers access the same authentication server, the management range of the authentication server will cover all those managers. This management range is called a *user authentication block*.

You can construct one or more user authentication blocks within a system by specifying settings in JP1/Base. The table below describes the relative advantages and disadvantages of having one or multiple user authentication blocks. Determine how many to construct by referring to this table and *12.6.1(1) Recommended number of user authentication blocks*.

Table 12–10: Number of user authentication blocks and advantages/disadvantages

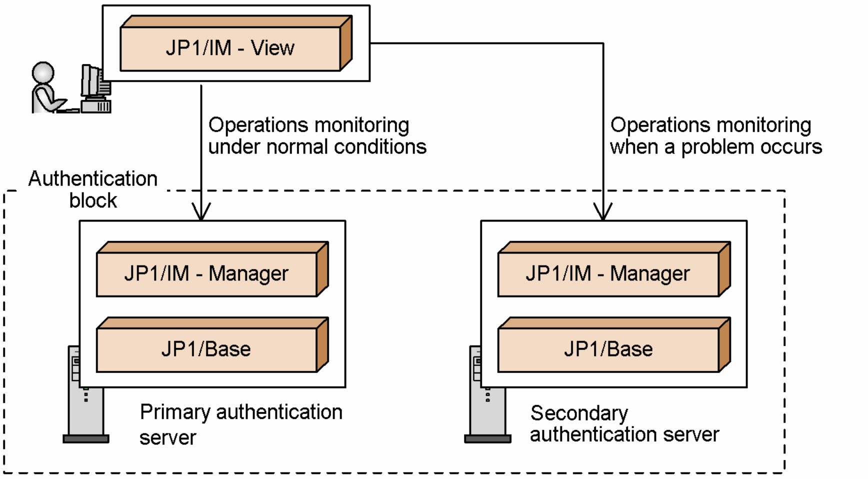
Number of user authentication blocks	Advantages/disadvantages
Only one user authentication block in the system	The system administrator can centrally manage the JP1 users. However, if the authentication server goes down, JP1/IM will be inoperable because the entire system will be affected and its reliability impaired.
Multiple user authentication blocks in the system	The system administrator must manage every block of JP1 users. However, because the authentication servers are independent, the system is more robust.

(1) Recommended number of user authentication blocks

Management of multiple user authentication blocks in a system can be complex. We recommend that you construct one or only a few blocks, and take measures to make the system more robust.

One way of making the system more robust is to install two authentication servers (primary and secondary authentication servers) in one user authentication block.

Figure 12–19: Authentication servers


JP1/IM - View
Operations monitoring under normal conditions
Operations monitoring when a problem occurs
Authentication block
JP1/IM - Manager
JP1/Base
Primary authentication server
JP1/IM - Manager
JP1/Base
Secondary authentication server

By having two authentication servers, the secondary authentication server can be swapped in automatically and you can perform uninterrupted system operation monitoring if a problem occurs on the primary authentication server. You can also enhance the robustness of the system by running the authentication server hosts in a cluster system, or by setting automatic restart if an authentication server terminates abnormally.

About authentication servers:

- JP1 user management and authentication servers

  See *7.4.1 Managing JP1 users*.

  Also see the description of setting up the user management functionality in the *JP1/Base User's Guide*.

- Authentication servers to be used by JP1/IM

  Specification via the JP1/Base Environment Settings window or the `jbssetusrsrv` command

  See the description of setting up the user management functionality in the *JP1/Base User's Guide*.

12.6.2 Access permissions of JP1 users

When registering a JP1 user on an authentication server, you must assign the most appropriate JP1 resource group and JP1 permission level for the JP1 user's scope of operation.

Using the Central Console:

Assign to the JP1 user, JP1 resource group `JP1_Console` and JP1 permission level `JP1_Console_Admin`, `JP1_Console_Operator`, or `JP1_Console_User` (assign the appropriate JP1 permission level according to your operation).

You can restrict viewing or operating on business groups. To do so, assign the JP1 resource group corresponding to the business group and the preferable JP1 permission level to the JP1 user to be registered in the authentication server. For details about how to assign JP1 resource groups and JP1 permission levels to JP1 users, see *3.1.4 Restrictions on viewing and operating business groups*.

Using the Central Scope:

Assign JP1 resource group `JP1_Console` and JP1 permission level `JP1_Console_Admin` to the JP1 user who edits the monitoring tree and applies the tree information to the server. Assign JP1 resource group `JP1_Console` and JP1 permission level `JP1_Console_Admin`, `JP1_Console_Operator` or `JP1_Console_User` to the JP1 user who performs monitoring on the Central Scope (assign the appropriate JP1 permission level according to your operation).

If you want to set a different monitoring range within a monitoring tree for each JP1 user, you must set JP1 resource groups for specific nodes, and then allocate the appropriate JP1 resource group to each of the JP1 users you are registering on the authentication server. For details about setting a resource group for selected nodes, see *4.4.3 Setting the monitoring range of a monitoring tree*.

Using IM Configuration Management:

Assign JP1 resource group `JP1_Console` and JP1 permission level `JP1_CF_Admin`, `JP1_CF_Manager`, or `JP1_CF_User` to the JP1 user (assign the appropriate JP1 permission level according to your operation).

For details about JP1/IM user operation control based on JP1/IM permission levels, see *Appendix E. Operating Permissions*.

(1) Notes

- To implement user operation control based on JP1 permission level in JP1/IM - View, use JP1/Base version 7 or later as the authentication server.
- When two authentication servers are used, they must be running the same version of JP1/Base.
- The JP1 user information registered on each authentication server must be identical. For details about the setting procedure, see the description of setting up the user management functionality in the *JP1/Base User's Guide*.

12.7 Considerations for the JP1/IM and JP1/Base environments

Consider the JP1/IM and JP1/Base environments.

12.7.1 Selecting regular expressions

In JP1/IM and JP1/Base, you can use regular expressions when specifying items such as filter conditions and search conditions. The default values of the available regular expressions depend on the OS and the function in which the regular expression is interpreted.

When using the default values, you need to be aware of how each function and operating system interprets regular expressions differently. If you prefer to use regular expressions transparently, you can change a setting in JP1/IM - Manager or JP1/Base to standardize regular expressions.

Use the default setting for the type of regular expressions only if a large number of filter conditions with regular expressions are already set, for example, and compatibility is your primary concern.

Set the type of regular expressions to be used in JP1/Base and in the `REGEXP` parameter of the automated action environment definition file.

About regular expressions:

- Description of regular expression types

  See *Appendix G. Regular Expressions*.
- Setting the regular expressions to be used

  See *Automated action environment definition file (action.conf.update)* in *Chapter 2. Definition Files* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

  See the description of available regular expressions in the chapter on installation and setup in the *JP1/Base User's Guide*.

12.7.2 Troubleshooting in JP1/IM and JP1/Base

System operation management is affected by any failure that causes JP1/IM or JP1/Base to stop. JP1/IM and JP1/Base therefore provides the following functionality to enhance failure tolerance:

- Automatic restart if a process ends abnormally (process management)
- Issuing of a JP1 event when an error is detected during process start or stop processing (process management)
- Issuing of a JP1 event and execution of a notification command when a hangup is detected in a process (health check function)

Consider enabling these functions. They are disabled by default.

About process error troubleshooting and reporting:

- Process management

  See *7.1 JP1/IM - Manager process management*.
- Setting to enable process restart after an error

  See *Extended startup process definition file (jp1co_service.conf)* in *Chapter 2. Definition Files* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

- Setting to enable issuing of a JP1 event when a process error occurs

  See *IM parameter definition file (jp1co_param_V7.conf)* in *Chapter 2. Definition Files* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

- Health check function

  See *7.2 JP1/IM - Manager health check function*.

- Setting to enable issuing of a JP1 event and execution of a notification command on detection of a process hangup

  See *Health check definition file (jcohc.conf)* in *Chapter 2. Definition Files* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

- JP1/Base troubleshooting and error reporting

  See the description of setup for troubleshooting JP1/Base errors in the *JP1/Base User's Guide*.

To enable prompt retrieval of relevant information in the event of a failure, JP1/IM provides dump output commands and data collection tools. These are normally used to collect data when a problem occurs in JP1/IM. However, they cannot be used with the Web-based JP1/IM - View; instead, you must use the debugging tools provided by Java^{TM} Plug-in to collect error information.

Dump output commands

JP1/IM - View and JP1/IM - Manager each have their own dump output command.

Table 12–11: Dump output commands

Command	Description
`jcothreaddmp`	Dump output command for JP1/IM - View. Outputs the following dump as diagnostic data when a hangup occurs in JP1/IM - View: • Java thread dump
`jcogencore`	Dump output command for JP1/IM - Manager. Outputs the following dump as diagnostic data when a hangup occurs in JP1/IM - Manager processes: • Java thread dump: Outputs failure data for the `evflow`, `evtcon`, `evgen`, and `jcfmain` processes. • Core dump (UNIX only)#: Outputs failure data for the `evtcon`, `evgen`, `jcamain`, `evflow`, and `jcfmain` processes. To check for a process hangup, use the health check function.

#: If the core dump for the four processes excluding `jcfmain` is output, the total size of core dump might be as much as 8,419 megabytes. If the core dump also includes the `jcfmain` process, the total size might be as much as 560 + 230 × *number-of-jcfallogtrap-processes* megabytes. Therefore, check whether disk capacity is sufficient before outputting the dump.

Data collection tools

The data collection tools are provided as a batch files (in Windows) or scripts (in UNIX).

Table 12–12: Data collection tools provided by JP1/IM

OS	Data collection tool	Description
Windows	`jcoview_log.bat`	Tool for collecting in a batch all data required for error investigation in JP1/IM - View
	`jim_log.bat`	Tool for collecting in a batch all data required for error investigation in JP1/IM - Manager#
UNIX	`jim_log.sh`	Tool for collecting in a batch all data required for error investigation in JP1/IM - Manager#

#: To collect data for investigating an error in JP1/Base, you must execute the data collection tool provided by JP1/Base. (The JP1/Base data collected by the tools in the above table relates to JP1/IM operation only.)

For details about the collected data, see *10.3 Data that needs to be collected when a problem occurs* in the *JP1/Integrated Management - Manager Administration Guide*. In Windows, a memory dump or crash dump might be required if a problem occurs. We recommend that you set Windows to output these dump files in case they are needed.

However, note the following points:

- The size of the memory dump depends on the real memory size. The larger the installed physical memory, the larger the memory dump. Allocate sufficient disk space to collect a memory dump. For details, see *STOP errors* in the Windows help.
- Not only JP1 event information but also error data for other application programs is output in a crash dump. Output of a crash dump reduces the amount of available disk space by the volume of output data. Allocate sufficient disk space if you have set Windows to output a crash dump.

Java^{TM} Plug-in debugging tool

If a hangup occurs while you are using the Web-based JP1/IM - View, collect a Java stack trace log using the debugging tool provided by Java^{TM} Plug-in. You must first set up the Java^{TM} Plug-in Control Panel window so that the tool will be accessible when the Web-based JP1/IM - View is running. For details, see *4.19.4 Specifying display settings for the Java Console window* in the *JP1/Integrated Management - Manager Configuration Guide*.

12.7.3 JP1/IM - Manager system environment

You can change the JP1/IM - Manager system environment via the GUI or by using a profile (system profile). The changes are managed by JP1/IM - Manager on the manager.

The following describes settings related to the JP1/IM - Manager system environment that can be changed by the user. Consider changing the settings as required.

(1) Considerations for the JP1/IM - Manager system environment

Consider the event buffer and permission for connection from the `jcochstat` command.

(a) Event buffer

The event buffer is an area of memory used by JP1/IM - Manager (Central Console) to store JP1 events extracted from the event service of JP1/Base.

Set the maximum number of events that can be extracted from the event service and buffered on the manager. You can set the number in the range from 10 to 2,000 (events).

If the event buffer size is too small, some JP1 events might be missing from the **Monitor Events** page and **Severe Events** page of the Event Console window.

On the other hand, if the event buffer size is too large, the Event Console window might take a long time to display when you start JP1/IM - View.

When setting the event buffer size, estimate the memory requirements of the Central Console and make sure that sufficient resources are available on the machine. For the equations you can use to estimate memory requirements, see the JP1/IM - Manager *Release Notes*.

(b) Connection permission from the jcochstat command

Using the `jcochstat` command, you can change the response status of JP1 events in the event database or integrated monitoring database. This allows you to change the response status of JP1 events from other applications, but it might impair JP1/IM operation management.

For this reason, you can set JP1/IM - Manager to prohibit response status changes by the `jcochstat` command to the event database or integrated monitoring database on the manager. We recommend that you prohibit changes by the `jcochstat` command if there is no need for other applications to change the response status of JP1 events.

(c) Setting the range of events to be collected at login

When you log in to JP1/IM - Manager, the events ranging from the event that occurred at a specified point of time to the most recent event are collected from the integrated monitoring database. You can specify whether to set the range the events to be collected at login separately on the **Monitor Events** and **Severe Events** pages. On the **Severe Events** page, you can also specify exclusion of processed severe events in the event collection from the integrated monitoring database.

About customizing the JP1/IM - Manager system environment:

- Customizing the JP1/IM - Manager system environment via the GUI (recommended procedure)

  See *2.11 System Environment Settings window* in the manual *JP1/Integrated Management - Manager GUI Reference*.

- Customizing the JP1/IM - Manager system environment in a definition file

  In normal circumstances, customize the settings in the System Environment Settings window rather than in a definition file.

  See *System profile (.system)* in *Chapter 2. Definition Files* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

(2) Notes

If the system profile contains any errors, such as an attribute value that is out of range, JP1/IM - Manager might not work properly.

12.7.4 JP1 user environment

You can change the JP1/IM user environment (contents displayed in the Event Console window, for example, for an individual JP1 user) via the GUI or by using a profile (user profile). The changes are managed by JP1/IM - Manager.

The following discusses some points and precautions you should consider in regard to the JP1 user environment settings.

(1) Scroll buffer

The *scroll buffer* is an area of memory used by JP1/IM - View to store JP1 events extracted from the event buffer of JP1/IM - Manager.

A scroll buffer is kept for each of the **Monitor Events** page, **Severe Events** page, and **Search Events** page.

The JP1 events that JP1/IM - View displays on each page is determined by the contents of the scroll buffer for that page.

You can change the scroll buffer size (maximum number of JP1 events that can be buffered) in the Preferences window.

If the scroll buffer size is too large, the Event Console window might take a long time to display when you start JP1/IM - View.

When setting the scroll buffer size, estimate the memory requirements of the Central Console viewer and make sure that sufficient resources are available on the machine. For the equations you can use to estimate memory requirements, see the JP1/IM - View *Release Notes*.

About customizing the user environment:

- Customizing the user environment via the GUI
  See *2.24 Preferences window* in the manual *JP1/Integrated Management - Manager GUI Reference*.

(2) Notes

- When a user is deleted from the JP1 user management, the associated user profile is not deleted.
- When a user name is changed in the JP1 user management, the associated user profile is not updated.
- The JP1 user environment definitions are also written in the user profile. However, in the user profile, do not directly change the attributes and attribute values that are not described in *Information that is specified* in *User profile (defaultUser | profile_user-name)* of *Chapter 2. Definition Files* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*. If you change them, JP1/IM - View might not work properly.
- If a user profile contains any errors, such as an attribute value that is out of range, JP1/IM - View might not work properly.

12.7.5 Issuing a JP1 event when a response status changes

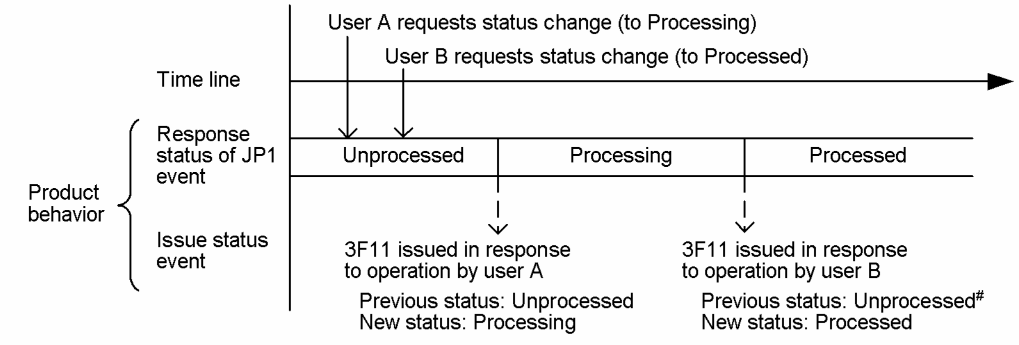
By setting JP1/IM to issue a JP1 event (3F11) when the response status of a JP1 event changes, you can achieve the following control. Hereafter, the JP1 event issued when a response status changes is referred to as a *status event*.

- Keeping a history of response operations
  When a number of operators perform response operations, you can utilize the issued status events to see who changed the response status, when it was changed, and to what status.
  You can also obtain a historic record of operator responses for auditing purposes by outputting the event information (including status events) displayed in the Event Console window as a CSV snapshot.

(1) Notes

- When JP1/IM is set to issue JP1 events for response status changes, one status event (3F11) is issued for one JP1 event that has been resolved. When the operator changes the response status of a number of JP1 events in a single operation, either in the **Severe Events** page of the Event Console window or by the `jcochstat` command, a status event (3F11) will be issued for every one of those JP1 events. Bear this in mind when using status event issue.
- A status event (3F11) is triggered when a JP1 user changes the response status of a JP1 event in JP1/IM, and the status event is then registered in JP1/Base. If another JP1 user changes the response status of the same JP1 event before the preceding status event (3F11) is registered, the pre-response status stored in the new status event (3F11) might not be the actual status.
  For example, if user A changes an *Unprocessed* JP1 event to *Processing*, and user B changes it to *Processed* at roughly the same time (slightly later than user A), the product will behave as follows.

Figure 12–20: Product behavior when a response status is changed by multiple users


User A requests status change (to Processing)
User B requests status change (to Processed)
Time line
Product behavior
Response status of JP1 event
Unprocessed
Processing
Processed
Issue status event
3F11 issued in response to operation by user A
Previous status: Unprocessed
New status: Processing
3F11 issued in response to operation by user B
Previous status: Unprocessed#
New status: Processed

#: Previous status other than Processing.

The actual status transition follows the order in which the change requests are received (in this case, *Unprocessed* -> *Processing* -> *Processed*), but the pre-response status stored in the triggered status events (3F11) is the response status that applied when each user issued the change request (in this case, *Unprocessed*).

12.7.6 Command execution environment

Consider the environment for the command execution functionality.

The command execution environment comes into play when the user executes a command from JP1/IM - View or when a command is executed in an automated action.

The command execution environment also relates to the system configuration management and user authentication functionality.

(1) Considerations for the command execution environment

- Setting the number of commands to be executed concurrently

  The commands that are executed in automated actions are normally set to execute one by one on the host concerned. However, concurrent execution is supported if you want the next command to start executing sooner when it follows a command that takes a long time to complete.

  To enable commands to be executed concurrently on a host, set the *command-concurrent-execution-count* parameter by specifying the `-execnum` option in the `jcocmddef` command.

  Commands are executed in parallel up to the number defined as *command-concurrent-execution-count*. Although the number of commands being executed at any one time depends on how long each command takes to execute and on the command execution environment, it never exceeds the specified count. Delays might occur when a command executed by an automated action takes a long time to execute and commands are set to execute serially (the default setting). In this case, you can reduce delays by setting the command execution control to execute commands in parallel.

  When you specify a value greater than 1 in this option, commands will be executed concurrently, which means that the command executed first will not necessarily end first. For this reason, do not specify this option if you want the automated actions to end in execution order.

For details, see the following reference:

About the command execution environment:

- Overview of the command execution environment

  See *7.4.4 Managing command execution*.

(2) Notes

- If the number of queued commands is exceeded when an automated action is executed, the action returns an error. Wait until the queued actions have executed, and then retry the failed action. To do so, in the Execute Command window, type the contents displayed in the **Action** field of the Action Log Details window.

  Specify the number of queued commands in the `-queuenum` option in the `jcocmddef` command. For details about the `jcocmddef` command, see the chapter on commands in the *JP1/Base User's Guide*.
- If JP1/Base stops while an automated action is being executed, the action will result in an error.

12.7.7 System design for using the Central Scope

Consider the following points in regard to using the Central Scope.

(1) Host information managed by JP1/IM - Manager (Central Scope)

JP1/IM - Manager (Central Scope) compares host names to determine the monitoring tree structure, or to change the status of monitoring objects, when a monitoring tree is generated automatically or when the status of a monitoring object is changed.

When comparing host names, JP1/IM - Manager (Central Scope) uses the JP1/Base `jp1hosts` information or `jp1hosts2` information, the OS `hosts` file, and the DNS or NIS settings. Where there are discrepancies between the host names defined in these settings and those recognized by the products to be represented in an automatically generated tree, or by products that issue JP1 events, information might not be acquired correctly or the status of a monitoring object might not be changed correctly.

Examples:

- The monitoring objects collected by the auto-generation function relating to the same host appear as monitoring objects of different hosts.
- The status of a monitoring object fails to change because the name of the host it is monitoring differs from the name of the host that issued the JP1 event.

To avoid these sorts of problems, JP1/IM - Manager (Central Scope) can manage host information using a database of its own. You can preempt any problems by registering the host names recognized by other programs in the JP1/IM - Manager (Central Scope)-specific host information.

To utilize host information in JP1/IM - Manager, prepare a `jcs_hosts` file, and register the information in the host information database. In the `jcs_hosts` file, write the real host name, alias, and IP address of the hosts to be monitored in the Monitoring Tree window, using the same format as the OS `hosts` file. You can specify a maximum of eight host names for one IP address.

Make sure that you prepare the host information file and register the information in the host information database before you configure the monitoring object environment.

(a) Notes

- If referencing of the host information is unsuccessful, JP1 event processing and monitoring tree auto-generation by JP1/IM - Manager (Central Scope) might take a long time.

  So that the information can be referenced, set the following host names in the host information database of JP1/IM - Manager (Central Scope), the JP1/Base `jp1hosts` information or `jp1hosts2` information, the `hosts` file of the host running JP1/IM - Manager (Central Scope), and the DNS or NIS:

1. Any host name set in the status change condition for a monitoring object as an individual attribute value in an individual condition for which **Host name comparison** is selected.
2. Any host name included in the attribute values of a JP1 event monitored by JP1/IM that might be set as the event attribute specified in an individual condition for which **Host name comparison** is selected (as in 1 above).
3. All host names defined in the JP1/IM configuration management.
4. All host names included in the configuration information of a linked product set up to support auto-generation of monitoring trees.

12.7.8 Communication timeout period

If the network uses low-speed lines or if the viewer is heavily loaded, a timeout during server communication processing might result in a communication error. You can correct such errors by changing the JP1/IM settings.

By default, the timeout period is 2,500 milliseconds. Increase this value if JP1/IM is used in a low-speed network or in an environment that generates considerable event traffic.

About adjusting the communication timeout value:

- Modifying the communication timeout value of JP1/IM - Manager (Central Scope)

  See *Communication environment definition file (console.conf.update)* in *Chapter 2. Definition Files* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

- Modifying the communication timeout value of JP1/IM - View

  See *Communication environment definition file (view.conf.update)* in *Chapter 2. Definition Files* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

  See *Communication environment definition file (tree_view.conf.update)* in *Chapter 2. Definition Files* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

There is no need to adjust the communication timeout value of JP1/IM - Manager (Central Scope).

12.7.9 JP1/IM - View environment

(1) Customizing JP1/IM - View

You can customize aspects of JP1/IM - View operation, such as the number of connection hosts displayed in the Login dialog box and the startup behavior of the Tool Launcher window.

About customizing JP1/IM - View:

- Customizing how JP1/IM - View operates (the Central Console viewer and Central Scope viewer)

  See *IM-View settings file (tuning.conf)* in *Chapter 2. Definition Files* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

  See *1.19.2 Customizing operation of JP1/IM - View (Central Console viewer and Central Scope viewer) (for Windows)* in the *JP1/Integrated Management - Manager Configuration Guide*.

- Customizing how JP1/IM - View operates (IM configuration management viewer)

  See *Operation definition file for IM Configuration Management - View (jcfview.conf)* in *Chapter 2. Definition Files* in the *JP1/Integrated Management - Manager Command and Definition File Reference*.

  See also *1.19.3(2) Customizing operation of IM Configuration Management - View* in the *JP1/Integrated Management - Manager Configuration Guide*.

(2) Setting up linkage with JP1/IM - Rule Operation

To use the JP1/IM - Rule Operation linkage component of JP1/IM - View, you must execute the set command `jcovrmsetup`.

For details about window operations after setup is completed, see the JP1/IM - Rule Operation manuals.

JP1/IM - Rule Operation manuals:

- *Job Management Partner 1/Integrated Management - Rule Operation System Configuration and User's Guide*
- *Job Management Partner 1/Integrated Management - Rule Operation GUI Reference*

12.7.10 Event monitoring from the Web-based JP1/IM - View

JP1/IM - Manager provides a Web-based JP1/IM - View. By using this program, users can log in to a manager from a host that does not have JP1/IM - View, and perform event monitoring. However, the Web-based JP1/IM - View has the following limitations:

- The Web-based JP1/IM - View, however, does not support a cluster system. When you intend to monitor events in a cluster system, use JP1/IM - View.
- Encryption is not available. You should use JP1/IM - View unless your environment is on a secure network, such as a trusted intranet.
- The Execute Command window and Tool Launcher window are not available.

The Web-based JP1/IM - View is subject to some limitations. For example, the Execute Command window and Tool Launcher window are not available.

Before using the Web-based JP1/IM - View, make sure that you are aware of the limitations described in *Chapter 1. Window Transitions and Login Window* in the manual *JP1/Integrated Management - Manager GUI Reference*.

To use the Web-based JP1/IM - View, an HTTP server must be installed and set up on the host on which JP1/IM - Manager is installed, and the Java Runtime Environment (JRE) and bundled plug-ins are required in the Web browser. For details, see the JP1/IM - Manager *Release Notes*.

About event monitoring from the Web-based JP1/IM - View:

- Using the Web-based JP1/IM - View
  See *4.19 Settings for using a Web-based JP1/IM - View* in the *JP1/Integrated Management - Manager Configuration Guide*.

12.7.11 Setting the event acquisition start location

The event acquisition start location is set by the `-b` option of the `jcoimdef` command. The location is determined as shown in the table below, according to the value specified in the `-b` option.

Table 12–13: Relationship between -b option value and acquisition start location

Value specified in -b option	Acquisition start location
-1	The event following the last event processed by JP1/IM - Manager
0	Events registered since JP1/IM - Manager started

Value specified in -b option	Acquisition start location
1 to 144	Events registered within a specified period of time before JP1/IM - Manager started

The effect of each setting is as follows:

(1) Acquisition start location when -1 is specified

If you start JP1/IM - Manager with -1 specified in the `-b` option of the `jcoimdef` command, the event base service sends the event with the oldest serial number (the event at the location where processing stopped) to JP1/IM - Manager.

(2) Acquisition start location when 0 is specified

If you start JP1/IM - Manager with 0 specified in the `-b` option of the `jcoimdef` command, the event base service sends events registered after JP1/IM - Manager startup to JP1/IM - Manager in the order in which they were registered.

If no such events exist, the event base service remains in standby mode until a new event is registered.

(3) Acquisition start location when 1 to 144 is specified

If you start JP1/IM - Manager with any of 1 to 144 specified in the `-b` option of the `jcoimdef` command, the event base service sends events to JP1/IM - Manager that were registered within the length of time specified by the `-b` option before JP1/IM - Manager started.

In this case, the acquisition start location is the time at which JP1/IM - Manager started, less the time specified by the `-b` option of the `jcoimdef` command.

12.8 Considerations for linking with other integrated management products

Consider the environment settings required for linking with the following integrated management product:

- JP1/IM - Rule Operation

12.8.1 System design for linking with JP1/IM - Rule Operation

To link with JP1/IM - Rule Operation, the following setup is required on the JP1/IM side. For details about JP1/IM - Rule Operation, see the *Job Management Partner 1/Integrated Management - Rule Operation System Configuration and User's Guide*.

(1) Settings for JP1/IM - Rule Operation linkage

The following settings are required for linking with JP1/IM - Rule Operation:

Settings for JP1/IM - Rule Operation linkage (`jcoimdef` command)#

- Enable or disable JP1/IM - Rule Operation linkage (`-rule` option)
- Specify the JP1/IM - Rule Operation host (`-rulehost` option)
- Specify the execution user (`-ruleuser` option)

  #: Enabling the linkage function enables the notification condition settings to be exported from JP1/IM - View to JP1/IM - Rule Operation.

Condition for notifying JP1/IM - Rule Operation

Set in either of the following:

- Action Parameter Detailed Definitions window
- Automated action definition file (`actdef.conf`)

Display settings

- Preferences window
- Settings for View Filter window
- Severe Event Definitions window
- Detailed Settings for Event Receiver Filter window

Registration in the Start menu of JP1/IM - View (rule operation viewer)

- `jcovrmsetup` command

(2) Notes

- In the JP1/IM - Rule Operation notification conditions, specify all the JP1 events that could potentially match a rule startup condition. (Rule startup judgments for notifications from JP1/IM - Manager are performed on the JP1/IM - Rule Operation side.)
- Reporting to JP1/IM - Rule Operation is performed according to the system hierarchy (IM configuration) as is usual for automated actions.

  For this reason, if you want to run JP1/IM - Manager and JP1/IM - Rule Operation on different hosts, you must configure the JP1/IM - Rule Operation host at a level below the JP1/IM - Manager host.

- The following problems occur if you enable JP1/IM - Rule Operation linkage and set a notification condition, and then disable the function without first deleting the condition settings:
    - Automated actions cannot be set from JP1/IM - View.
    - Because the notification conditions in JP1/IM - Manager are still in effect, JP1/IM - Manager will send a rule startup request to JP1/IM - Rule Operation whenever a JP1 event matching a notification condition occurs.

  To prevent such problems, before you disable the linkage function, delete the condition settings for notifying JP1/IM - Rule Operation from JP1/IM - View, or open the automated action definition file (`actdef.conf`) and delete the automated action definition parameter for JP1/IM - Rule Operation linkage. For details about the automated action definition file (`actdef.conf`), see *Automated action definition file (actdef.conf)* in *Chapter 2. Definition Files* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.
- JP1/IM - Rule Operation issues a JP1 event whenever a rule starts, finishes, or ends abnormally, for example. If you want to monitor such JP1 events in JP1/IM, change the filter settings so that they can be forwarded and displayed in JP1/IM - View.

12.9 JP1/IM maintenance considerations

Not only when running JP1/IM but for any IT system generally, establishing and implementing a maintenance plan is necessary to guard against problems and to be prepared in case of an emergency.

The following discusses some points you should consider when carrying out maintenance tasks in a system that uses JP1/IM.

12.9.1 Backup requirements

Consider how to back up the JP1/IM and JP1/Base settings information and the databases so that if the system crashes, it can be rebuilt and restarted in the same environment. Take backup at the following times:

- When you set up JP1/IM or otherwise reconfigure the system
- Before you perform an upgrade installation

For details about the settings information to back up in JP1/IM, and on backup and recovery procedures, see *1.1 Managing the configuration information* in the *JP1/Integrated Management - Manager Administration Guide*. For details about database reorganization, backup and recovery, and recreation, see *1.2 Managing the databases* in the *JP1/Integrated Management - Manager Administration Guide*. For details about JP1/Base, see the description of backup and recovery in the chapter on installation and setup in the *JP1/Base User's Guide*.

12.9.2 Database maintenance considerations

Repeated addition and deletion of data in the IM database might increase invalid areas in the database. As a result, you might not be able to register new hosts or properties before the number of hosts or profiles reaches the limit set in IM Configuration Management. Also, delays might occur if you try to add, update, or delete data. To avoid these problems, we recommend that you periodically re-organize the database.

For details about when and how to re-organize the IM database, see *1.2.1 Database reorganization* in the *JP1/Integrated Management - Manager Administration Guide*.

The other databases used by JP1/IM are designed so that there is no increase in invalid areas when the system is run continuously. Therefore, there is no need to check the databases if enough disk space is available.

12.9.3 Checking disk space

To ensure that JP1/IM operates reliably during continuous operation, you must ensure that sufficient disk space is available.

For example, when an error occurs during JP1/IM operation, a dump file might be required for troubleshooting. Because a dump file temporarily occupies a large amount of disk space, estimate the disk space required and ensure that sufficient disk space is available.

12.9.4 Use of failure reports

JP1/IM - View provides functionality for saving the JP1 event information listed in the Event Console window in CSV format. By using this functionality in conjunction with an event search (see *3.6 Searching for events*), you can view a listing of JP1 events that occurred around the same time as an error in the system, and output the list as a CSV snapshot for use in analyzing the error.

Consider saving monitoring information (CSV snapshots) as a task within your system management program. If applicable, also consider saving the event information stored in the integrated monitoring database (output of event report).

Note

Producing JP1/Base failure reports (`jevexport` command)

Various events are recorded in a standard format as JP1 events in the JP1/Base event databases used by JP1/IM. By periodically reviewing the database contents, you can use the JP1 event records as failure reports, to find out which hosts or products are experiencing frequent problems, for example. Use the JP1/Base `jevexport` command to review the event database contents. The `jevexport` command outputs the contents to a CSV file.

Because the event databases have a fixed size (by default, 10 MB per database; total capacity 20 MB), you should output the contents using the `jevexport` command before the database is full. Consider doing so at regular intervals.

12.10 Considerations for JP1/IM system-wide maintenance

Among the hosts monitored by JP1/IM, some might be running processing that cannot be halted even when the server requires maintenance. For example, if a host runs 24 hours a day, 365 days a year, you will need to schedule maintenance work so as to minimize its impact, by migrating job processing to another server or by suspending some processing for a short time, for example.

During maintenance work, you might need to stop and start the server several times, or halt job processing temporarily, potentially issuing a large volume of events that detected these start/stop operations as errors.

To enable continuous operation monitoring by JP1/IM, you must filter out redundant events and keep only those that are required. You should therefore consider the order in which maintenance tasks will be carried out, and perform settings in advance to filter out unwanted JP1 events.

This section describes some points to consider in maintaining the entire system including JP1/IM, and discusses how to implement a maintenance schedule that allows for uninterrupted system monitoring. It also provides an example of carrying out urgent maintenance when a problem occurs on an agent.

12.10.1 Preparatory tasks

The following describes some precautions and points to consider at the planning stage before you implement maintenance.

(1) Maintenance planning for the entire system

- Decide the order in which maintenance will be implemented throughout the system.

  Make sure that you implement maintenance *from higher-level hosts to lower-level hosts* according to the system hierarchy (IM configuration).

  You should also consider the following points when planning the order in which maintenance is implemented:

  - When grouping the agents, make sure that maintenance of one host will not affect job processing on another host.
  - If a system operates around the clock, prepare a server that can take over processing while the system is being maintained.
  - Estimate how long maintenance will take for the JP1/IM servers and agents.

> **Important**
>
> When maintaining the entire system, use the `jcoimdef` command to adjust the event acquisition start location, and switch between event acquisition filters prepared in advance.
>
> The event acquisition start location and event acquisition filter are inter-related. That is, one setting affects the other. In brief, the relationship is as follows:
>
> - Event acquisition start location
>
>   At startup, JP1/IM - Manager acquires events from the JP1/Base event database, according to the start location setting, and stores them in its event buffer.
> - Event acquisition filter
>
>   When the events acquired from JP1/Base are stored in the JP1/IM - Manager event buffer, the event acquisition filter processes them according to the set conditions.

In other words, if the event acquisition filter is switched (hence, different filter conditions apply when JP1/IM - Manager stops and when it restarts), and if the event acquisition start location is set so that events will be acquired from before JP1/IM - Manager restarts, the events stored in the event buffer after JP1/IM - Manager restarts might differ from those when it stopped (that is, the events you can see in JP1/IM - View might be different). To avoid this problem, always schedule maintenance starting with the top-level host and proceeding down the hierarchy.

(2) Maintenance planning for managers (JP1/IM - Manager)

The following points should be considered in regard to performing maintenance on the managers (JP1/IM - Manager):

- Backup requirements
- Database maintenance
- Disk space checks
- Use of failure reports

For details about these aspects, see *12.9 JP1/IM maintenance considerations*. You should also consider the following points from a monitoring perspective:

- Acquire JP1 events generated while the manager (JP1/IM - Manager) is in stopped state.

  To manage JP1 events generated while JP1/IM - Manager is being maintained, you must set up JP1/IM - Manager to acquire JP1 events from before it restarts.

  During maintenance of the whole JP1/IM system, JP1/IM - Manager on the manager will be stopped at some stage. To enable management of all generated events, set up JP1/IM - Manager so that events generated while it is stopped will be acquired.

  Use the `jcoimdef` command to acquire events from before JP1/IM - Manager is restarted.

  The parameter settings are described below, based on an example.

  Events generated while JP1/Base is stopped on the manager cannot be acquired. This is because JP1 events cannot be registered in the event database while JP1/Base is in stopped state. For details, see *12.10.1(3) Maintenance planning for agents (JP1/Base)*.

- Disable monitoring of error events (JP1 events indicating failure occurrence) generated during agent maintenance.

  Maintenance work will involve restarting the server at some point, which could generate a large number of unwanted error events. As this might disrupt ongoing monitoring operations, set up filtering to eliminate unwanted events.

  To filter out unwanted events, you can define an event acquisition filter in which common exclusion-conditions exclude JP1 events issued by hosts that are under maintenance. You can then activate this filter during maintenance. The parameter settings are described below, based on an example.

  If JP1/Base is in stopped state on the agent throughout the maintenance work, there is no need for filtering because events will not be registered in the event database.

- Exclude error events generated during agent maintenance from action execution.

  When an automated action, such as sending an email triggered by a reception of an error event, is configured, the automated action can be executed even due to an error event caused by maintenance work. If you want to collect error events generated during maintenance work but exclude them from automated-action execution, you can consider setting a common exclusion-condition to exclude JP1 events from automated-action execution.

  By setting automated actions as the exclusion target of a common exclusion-condition, you can configure to exclude error events generated by agents undergoing maintenance from automated-action execution. You do not need to change existing automated action definitions for maintenance.

(3) Maintenance planning for agents (JP1/Base)

- Forward JP1 events generated while JP1/Base is stopped on the manager.

  Set JP1/Base on the agents to retry event forwarding, bearing in mind how long JP1/Base will be stopped on the manager. Set JP1/Base to retry at set intervals in case event forwarding fails because an error occurs or because JP1/Base is stopped on the destination host.

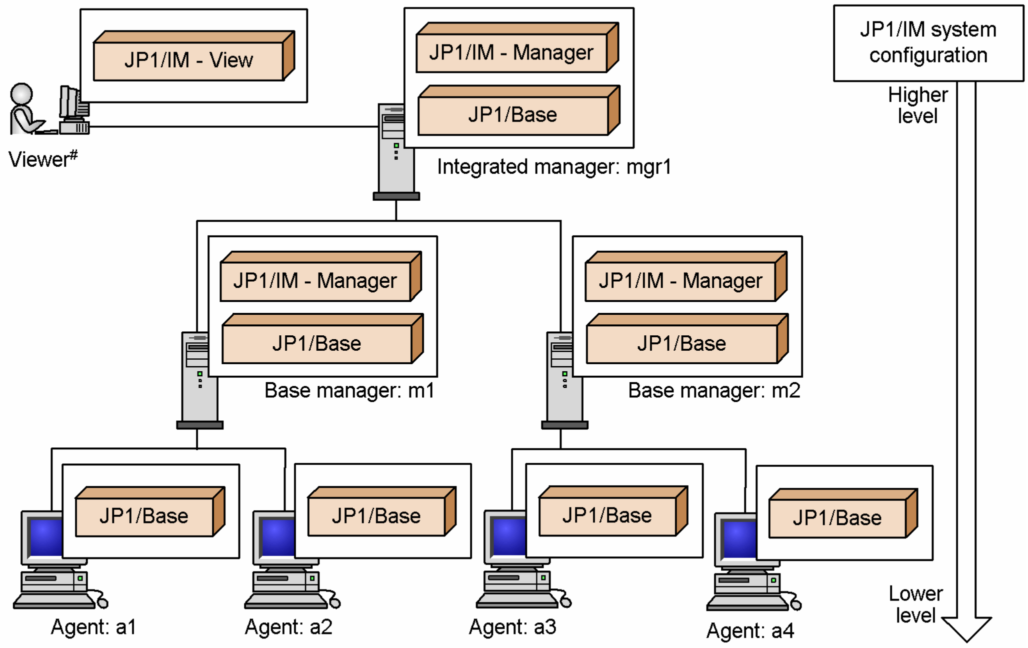
  For details, see the description of setting the event service in the *JP1/Base User's Guide*.

12.10.2 Example of JP1/IM system-wide maintenance

The following describes an example of implementing maintenance throughout the JP1/IM system.

In this example, maintenance is implemented for the system hierarchy (IM configuration) managed by JP1/IM as shown in the following figure (one integrated manager, two base managers, and four agents).

Figure 12–21: Hierarchical structure of a system monitored by JP1/IM



#: As viewers can be subjected to maintenance at any time and in any order, they are omitted from the following description.

This system monitored by JP1/IM is configured as defined by the JP1/Base configuration management. For details about defining a system hierarchy, see *7.4.3 Managing the system hierarchy*.

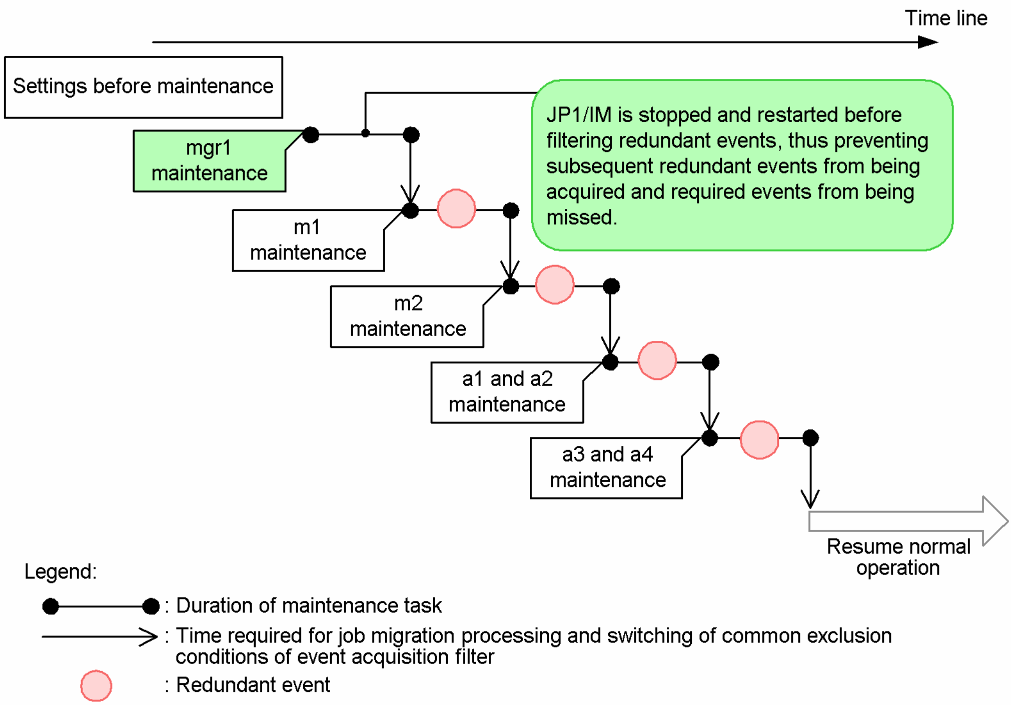
(1) Order of maintenance

Maintenance is carried out in order, from the higher-level hosts to the lower-level hosts, following the definition of the system hierarchy. In this example, the order of maintenance is as follows:

1. Integrated manager (mgr1)
2. Base manager (m1)
3. Base manager (m2)
4. Agents (a1 and a2)

5. Agents (a3 and a4)

Figure 12–22: Order of maintenance


Time line
Settings before maintenance
mgr1 maintenance
m1 maintenance
m2 maintenance
a1 and a2 maintenance
a3 and a4 maintenance
JP1/IM is stopped and restarted before filtering redundant events, thus preventing subsequent redundant events from being acquired and required events from being missed.
Resume normal operation
Legend:
: Duration of maintenance task
: Time required for job migration processing and switching of common exclusion conditions of event acquisition filter
: Redundant event

Maintenance is carried out on the integrated manager (mgr1), base manager (m1 or m2), and agent (a1, a2, a3, or a4), in that order. This prevents redundant events from being acquired and required events from being overlooked.

Important

Always schedule maintenance work on the manager (in this case, mgr1) first of all. Determine the order for the other hosts according to the system hierarchy.

(2) Settings on the integrated manager (JP1/IM - Manager) side

Using the JP1/IM - Manager functionality, set up filtering of redundant events and specify JP1 event acquisition while JP1/IM - Manager is in stopped state.

(a) Setting the event acquisition start location

Use the `jcoimdef` command to set the event acquisition start location. There are two settings for acquiring events from before JP1/IM - Manager restarts:

- `jcoimdef -b` -1

  Acquires JP1 events going back to the status when JP1/IM - Manager was last stopped.

- `jcoimdef -b` *xxx* (*xxx*: length of time; from 1 to 144 (hours))

  Acquires JP1 events going back the specified length of time before JP1/IM - Manager restarts.

There is also a setting for starting event acquisition from the JP1 events issued after JP1/IM - Manager starts, but the setting does not apply in this example because the starting point needs to be specified explicitly.

For details about setting the event acquisition start location, see *12.7.11 Setting the event acquisition start location*. For details about the `jcoimdef` command, see *jcoimdef* in *Chapter 1. Commands* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

(b) Setting common exclusion-conditions in an event acquisition filter

You can define common exclusion-conditions in an event acquisition filter to temporarily prevent some JP1 events from being monitored or exclude them from automated-action execution You can add and edit common exclusion-conditions from the Event Acquisition Conditions List window, leaving the standard filter conditions unchanged.

Maintenance is to be carried out in the order shown in *Figure 12-21 Hierarchical structure of a system monitored by JP1/IM*, starting with the integrated manager (`mgr1`), then the base managers (m1 -> m2), and lastly the agents (a1, a2 -> a3, a4). Four common exclusion-conditions separate from the event acquisition filter normally used, that is one for each setting, will be required for maintenance purposes. These common exclusion-conditions are described in the table below. Here it is assumed that the settings to prevent redundant events generated by a host undergoing maintenance from being collected or exclude such events from automated-action execution will be performed on the integrated manager (`mgr1`) only.

Table 12–14: Common exclusion-condition set in the event acquisition filter

Common exclusion-condition ID	Host undergoing maintenance	Common exclusion-condition
1	Base manager (m1)	Include source host m1
2	Base manager (m2)	Include source host m2
3	Agents (a1 and a2)	Include source hosts a1 and a2
4	Agents (a3 and a4)	Include source hosts a3 and a4

Source host in the event acquisition conditions means a host from which events are issued.

If you want to set up the same type of filtering for the base managers, set common exclusion-conditions in event acquisition filters, referring to the settings given above. Note that common exclusion-conditions must be changed to extended mode if you want the conditions to exclude JP1 events from action execution. And if you use common exclusion-conditions in extended mode, you will be able to specify the application period of a condition group. For details about common exclusion-conditions for the event acquisition filter, see *3.2.7 Common exclusion-conditions*.

For detailed settings for common exclusion-conditions, the setting windows differ depending on whether extended mode is used. See the following descriptions in the manual *JP1/Integrated Management - Manager GUI Reference*:

- Common exclusion-conditions: *2.15 Common Exclusion-Conditions Settings window*
- Common exclusion-conditions (when extended mode is used): *2.16 Common Exclusion-Condition Settings (Extended) window*

(3) Settings in JP1/Base on the base managers and agents

Set the event forwarding retry parameters, bearing in mind how long the destination host will be in stopped state. Set the parameters on the base managers (m1 and m2) and agents (a1, a2, a3, and a4). By default, the retry time limit is 3,600 seconds (that is, JP1/Base retries at set intervals for 60 minutes). Adjust this value if JP1/Base on the destination host will be stopped for longer than 60 minutes.

For details, see the *JP1/Base User's Guide*.

(4) Maintenance procedures

The following describes the maintenance procedure on each host.

(a) Maintenance procedure on the integrated manager

Follow these steps to carry out maintenance on the integrated manager (mgr1):

1. Stop JP1/IM - Manager.

2. Stop JP1/Base.

3. Perform maintenance of JP1/IM - Manager and JP1/Base.

   For details about backup and recovery of JP1/IM - Manager settings information and disk space management, see *Chapter 1. JP1/IM System Maintenance* in the *JP1/Integrated Management - Manager Administration Guide*. For details about JP1/Base maintenance, see the description of maintenance in the *JP1/Base User's Guide*.

4. Start JP1/Base.

5. Start JP1/IM - Manager.

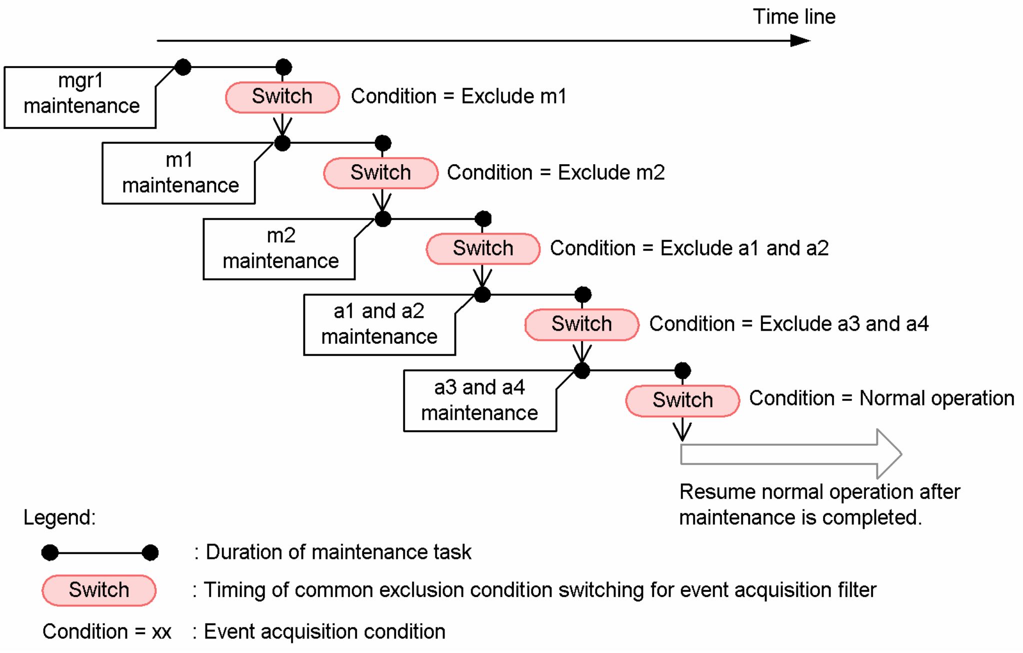
The same procedure applies for maintenance of JP1/IM - Manager on the base managers.

(b) Maintenance procedure on the base managers and agents

To carry out maintenance on the base managers (m1 and m2) and agents (a1, a2, a3, and a4), switch the common exclusion-conditions associated with the event acquisition filter on the integrated manager (mgr1) to eliminate redundant events.

The figure below shows the order of the maintenance tasks and when to switch the common exclusion-conditions defined for the event acquisition filter.

Figure 12–23: Maintenance task order and timing of common exclusion-condition switching


Time line
mgr1 maintenance
Switch
Condition = Exclude m1
m1 maintenance
Switch
Condition = Exclude m2
m2 maintenance
Switch
Condition = Exclude a1 and a2
a1 and a2 maintenance
Switch
Condition = Exclude a3 and a4
a3 and a4 maintenance
Switch
Condition = Normal operation
Resume normal operation after maintenance is completed.
Legend:
: Duration of maintenance task
Switch
: Timing of common exclusion condition switching for event acquisition filter
Condition = xx
: Event acquisition condition

You can switch the common exclusion-conditions of the event acquisition filter using the `jcochfilter` command, the System Environment Settings window, or the Event Acquisition Conditions List window.

Procedure for switching the common exclusion-conditions of the event acquisition filter

See *5.5.3 Switching the event acquisition filter to be applied* in the *JP1/Integrated Management - Manager Administration Guide*.

Details on the `jcochfilter` command

See *jcochfilter* in *Chapter 1. Commands* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

Details on the System Environment Settings window

See *2.11 System Environment Settings window* in the manual *JP1/Integrated Management - Manager GUI Reference*.

Details on the Event Acquisition Conditions List window

See *2.14 Event Acquisition Conditions List window* in the manual *JP1/Integrated Management - Manager GUI Reference*.

The maintenance procedure and files needing to be backed up will depend on the products installed on the base managers and agents. When carrying out maintenance, see the manual *JP1/Base User's Guide* or the documentation for the particular products that issue JP1 events.

Note

When you use the `jcochfilter` command, you can switch the event acquisition filter automatically at a specified time, based on the JP1/AJS scheduling and calendar functionality. This also lets you change the monitoring status of the host automatically.

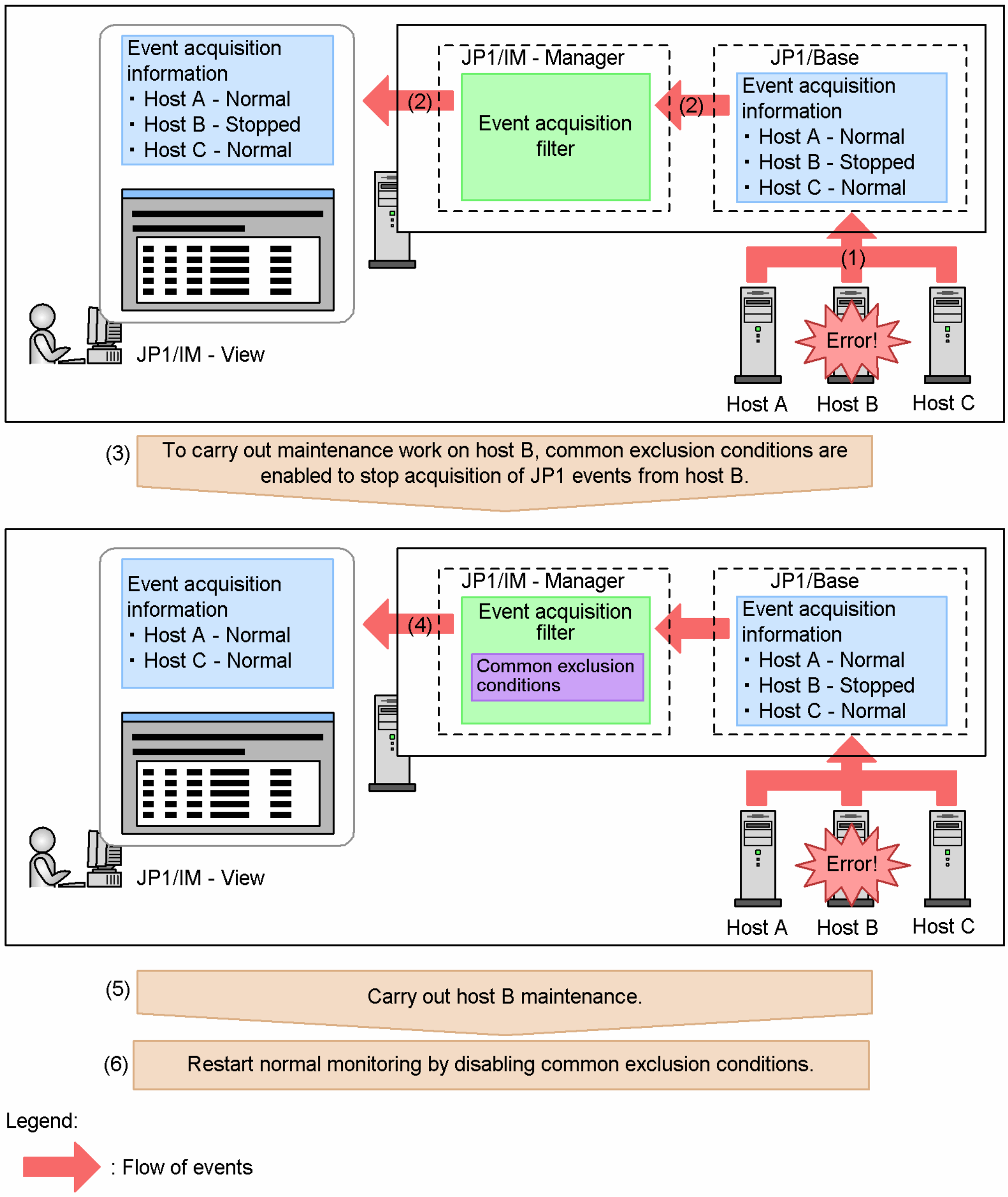
12.10.3 Example of agent maintenance

The following describes an example of implementing maintenance on a specific agent.

When a problem needing urgent attention occurs on an agent, events related to the issue should be monitored, but events occurring after maintenance is underway will not be required. Before maintenance work starts, set common exclusion-conditions in an event acquisition filter that prevents redundant events from being collected, so that JP1/IM - Manager can continue monitoring other hosts. You can also use common exclusion-conditions to exclude collected events from automated-action execution.

The figure below shows an example of implementing maintenance on a specific agent while preventing redundant events from being collected.

Figure 12–24: Example of agent maintenance



The workflow is described below, following the numbers in the figure:

1. An error occurs on agent B being monitored by JP1/IM, and a JP1 event is issued.
2. The JP1 event is relayed through JP1/Base and through the event acquisition filter in JP1/IM - Manager on the manager, and is displayed in JP1/IM - View.
3. To carry out maintenance tasks on host B, enable the predefined common exclusion-conditions for host B maintenance (a set of common exclusion-conditions which exclude JP1 events issued from host B from acquisition by JP1/IM - Manager).

   The common exclusion-conditions can be switched from the JP1/IM - View System Environment Settings window or Event Acquisition Conditions List window, or by using the `jcochfilter` command.
4. Because the common exclusion-conditions for host B maintenance are now in effect, JP1 events issued from host B are not acquired by JP1/IM - Manager (they do not appear in the JP1/IM - View windows).
5. Carry out host B maintenance.

6. After maintenance is completed, disable the common exclusion-conditions from the JP1/IM - View System Environment Settings window or Event Acquisition Conditions List window, or by using the `jcochfilter` command.

For the procedure for enabling or disabling common exclusion-conditions, see *5.5.3 Switching the event acquisition filter to be applied* in the *JP1/Integrated Management - Manager Administration Guide*.

12.11 Considerations for encrypted communication

This section explains the communication encryption function that encrypts communication data using SSL communication. However, the encryption function cannot be used in the Web-based IM-View.

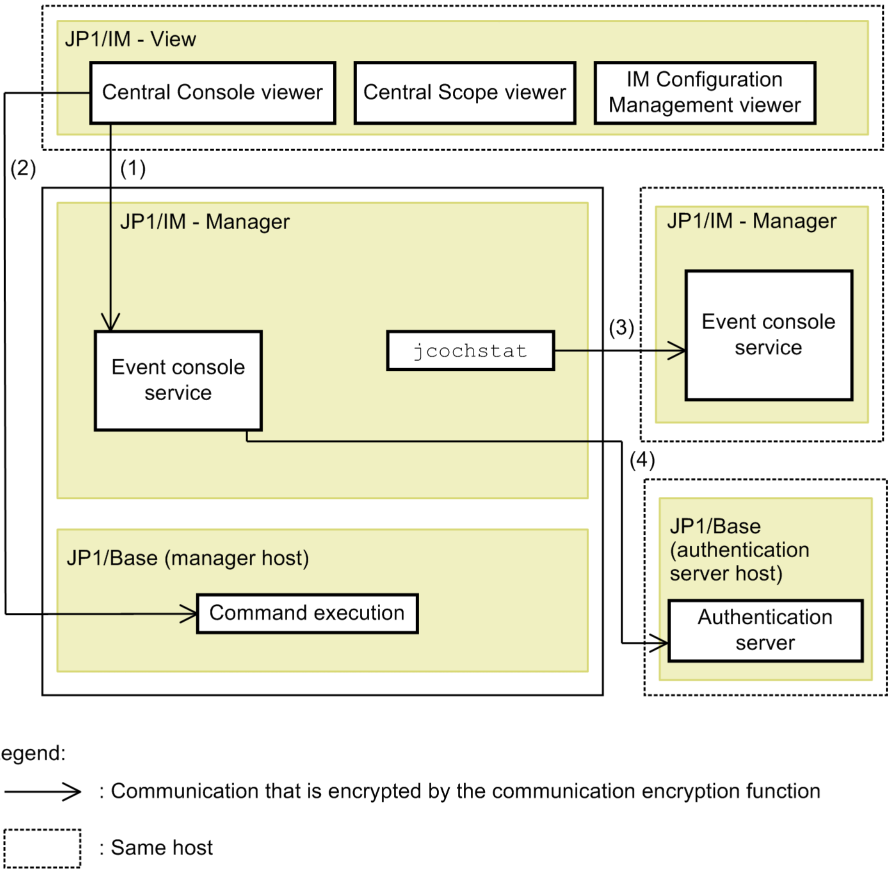
Required OS and operating language

For the required OS and operating language for the communication encryption function, see the *Release Notes*.

12.11.1 Range of communication that can be encrypted by the communication encryption function

The following figures and tables explain the range of communication that can be encrypted by the communication encryption function.

Figure 12–25: Range of Central Console communication that can be encrypted



The parenthesized numbers in the figure correspond to the numbers in the following table.

Table 12–15: Range of Central Console communication that can be encrypted

No.	Location of communication#1		Description
	Connection source	Connection target	
1	Central Console viewer	Event console service#2	Used for connection from JP1/IM - View to JP1/IM - Manager (event console service)

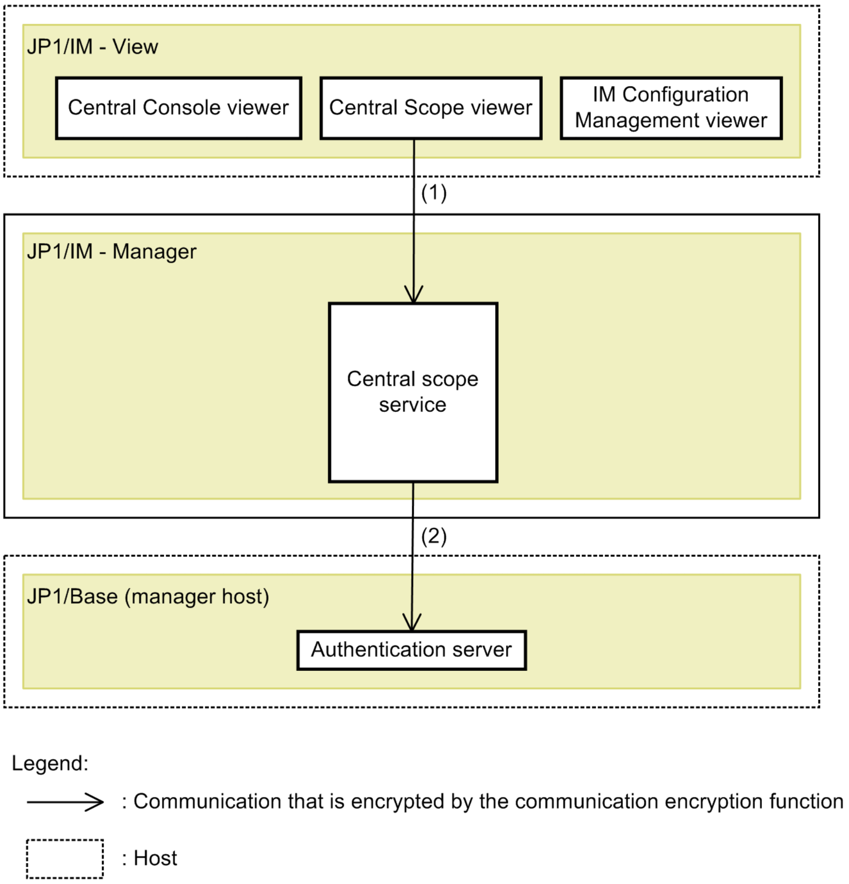
No.	Location of communication#1		Description
	Connection source	Connection target	
2	Central Console viewer	Command execution#2	Used when commands are executed from JP1/IM - View
3	`jcochstat` command#2	Event console service (another host)#2	Used when the `jcochstat` command with another host specified in the `-h` option is executed
4	Event console service#3	Authentication server#3	Used for user authentication

#1: The `jcochfilter` command, the `jcochstat` command (with a logical host name specified in the `-h` option or with the `-h` option omitted), the event base service, and the automatic action service use the communication encryption function in internal processing.

#2: To encrypt the corresponding part of the communication, specify `jp1imcmda` in the `BASESSL` parameter in JP1/Base's SSL communication definition file. For details, see the *JP1/Base User's Guide*.

#3: To encrypt the corresponding part of the communication, specify `jp1bsuser` in the `BASESSL` parameter in JP1/Base's SSL communication definition file. For details, see the *JP1/Base User's Guide*.

Figure 12–26: Range of Central Scope communication that can be encrypted



The parenthesized numbers in the figure correspond to the numbers in the following table.

Table 12–16: Range of Central Scope communication that can be encrypted

No.	Location of communication#1		Description
	Connection source	Connection target	
1	Central Scope viewer	Central Scope service#2	Used for connection from JP1/IM - View to JP1/IM - Manager (Central Scope service)

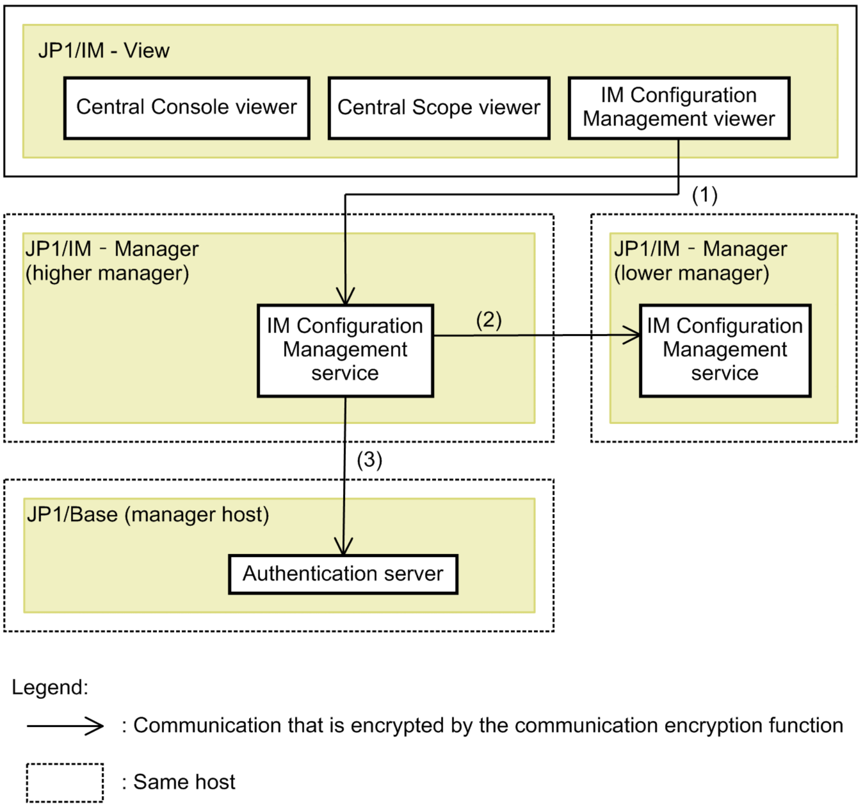
No.	Location of communication#1		Description
	Connection source	Connection target	
2	Central Scope service#3	Authentication server#3	Used for user authentication

#1: The `jcschstat`, `jcsdbexport`, and `jcsdbimport` commands use the communication encryption function in internal processing.

#2: To encrypt the corresponding part of communication, specify `jp1imcmda` in the `BASESSL` parameter in JP1/Base's SSL communication definition file. For details, see the *JP1/Base User's Guide*.

#3: To encrypt the corresponding part of communication, specify `jp1bsuser` in the `BASESSL` parameter in JP1/Base's SSL communication definition file. For details, see the *JP1/Base User's Guide*.

Figure 12–27: Range of IM Configuration Management communication that can be encrypted


JP1/IM - View
Central Console viewer
Central Scope viewer
IM Configuration Management viewer
(1)
JP1/IM - Manager (higher manager)
IM Configuration Management service
(2)
JP1/IM - Manager (lower manager)
IM Configuration Management service
(3)
JP1/Base (manager host)
Authentication server
Legend:
: Communication that is encrypted by the communication encryption function
: Same host

The parenthesized numbers in the figure correspond to the numbers in the following table.

Table 12–17: Range of IM Configuration Management communication that can be encrypted

No.	Location of communication#1		Description
	Connection source	Connection target	
1	IM Configuration Management viewer	IM Configuration Management service#2	Used for connection from JP1/IM - View to JP1/IM - Manager (IM Configuration Management service)
2	IM Configuration Management service	IM Configuration Management service on a lower manager#2	Used when IM connections are synchronized

No.	Location of communication[#1]		Description
	Connection source	Connection target	
3	IM Configuration Management service[#3]	Authentication server[#3]	Used for user authentication

#1: The jcfexport, jcfimport, jcfvirtualchstat, jcfaleltdef, jcfaleltreload, jcfaleltstart, jcfaleltstat, jcfaleltstop, jcfallogdef, jcfallogreload, jcfallogstart, jcfallogstat, and jcfallogstop commands use the communication encryption function in internal processing.

#2: To encrypt the corresponding part of communication, specify jp1imcmda in the BASESSL parameter in JP1/Base's SSL communication definition file. For details, see the *JP1/Base User's Guide*.

#3: To encrypt the corresponding part of communication, specify jp1bsuser in the BASESSL parameter in JP1/Base's SSL communication definition file. For details, see the *JP1/Base User's Guide*.

12.11.2 Certificates needed for using the communication encryption function

Each manager host whose communication must be encrypted requires a private key and a server certificate. The same server certificate cannot be shared among different hosts. However, if a wildcard certificate is used, the same server certificate can be shared among different hosts. For details about wildcard certificates, see *(1) Wildcard certificates*.

There is no problem if the root certificate corresponding to each server certificate is different for each manager host. If the root certificates are the same, you can place only one root certificate on the manager host and the viewer host, thereby making operation easier.

If there is no need to encrypt communication for a manager host, you need not create a client certificate or a server certificate for that manager host. For details about the configuration in which a manager host that encrypts communication is intermixed with a manager host that encrypts communication, see *12.11.6(2) System configuration in which connection is established with multiple manager hosts*.

If you have changed the host name of a manager host after you started using the communication encryption function and the new host name differs from CN and SAN in the server certificate, re-create the server certificate.

For details about how to re-create server certificates, see *8.4.2 Changing configured certificates* in the *JP1/Integrated Management - Manager Configuration Guide*.

(1) Wildcard certificates

The communication encryption function supports wildcard certificates.

A wildcard certificate is one that uses the asterisk (*) as a wildcard in a CN or SAN in a server certificate so that multiple subdomains (hosts) can be supported by a single server certificate.

For a server certificate in which the CN or SAN host name begins with an asterisk, the same server certificate can be shared among multiple hosts with different host names as long as they are all in the same domain. The asterisk can be used only at the beginning of a CN or SAN (host name part) and must be followed immediately by a period (.). An asterisk cannot be used at any location other than the beginning or in a regular expression (such as a* to indicate host names beginning with a). The wildcard cannot be used for host names in a top-level domain or a generic domain. The following table shows the validity of CN and SAN values used in wildcard certificates.

Table 12–18: Values of CN and SAN that can be specified in wildcard certificates

No.	CN or SAN value	Supported by JP1/IM
1	`*.example.com`	Y
2	`**.example.com`	N
3	`t*.example.com`	N
4	`*t.example.com`	N
5	`test.*.com`	N
6	`*.com`	N
7	`*.co.jp`	N
8	`*.168.0.2`	N

Legend:

Y: Supported

N: Not supported

(2) Self-signed certificate

The communication encryption function supports not only certificates signed by a certificate authority but also self-signed certificates. If you will be using self-signed certificates, ensure that you understand the differences in characteristics from when certificates from a public certificate authority are used.

(3) Maintaining certificates

The communication encryption function checks that certificates have not expired. Ensure that your certificates have been properly maintained by renewing them before they expire. For details about the procedure, see *1.6.1 Managing the effective duration of the server certificate* in the *JP1/Integrated Management - Manager Administration Guide*.

For details about the expiration period for certificates, see *12.11.4 Verifying server certificates* and *12.11.5 Verifying root certificates*.

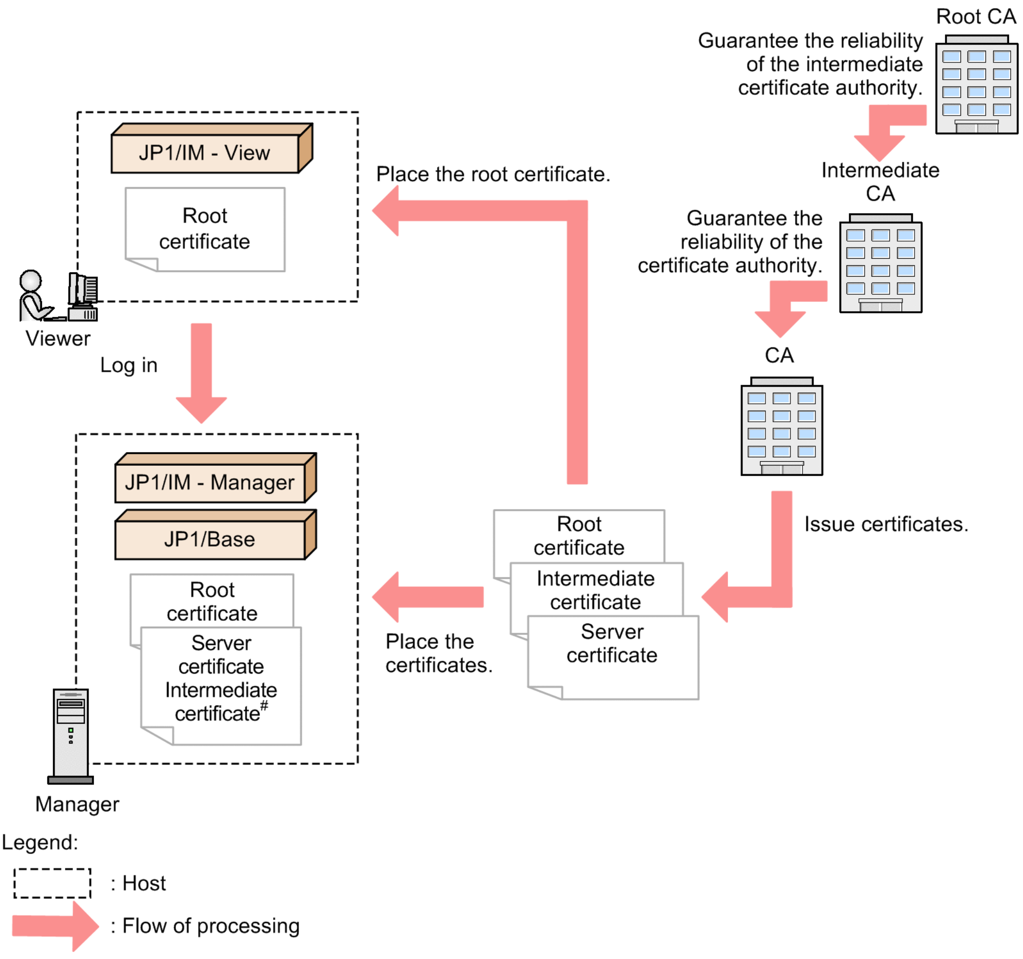
12.11.3 Placing certificates

This subsection explains the placement of certificates that are used by the communication encryption function.

(1) Encryption between a manager host and a viewer host

The following figure shows the certificates required for encrypting communication between a manager host and a viewer host.

Figure 12–28: Certificates required for encrypting communication between a manager and a viewer

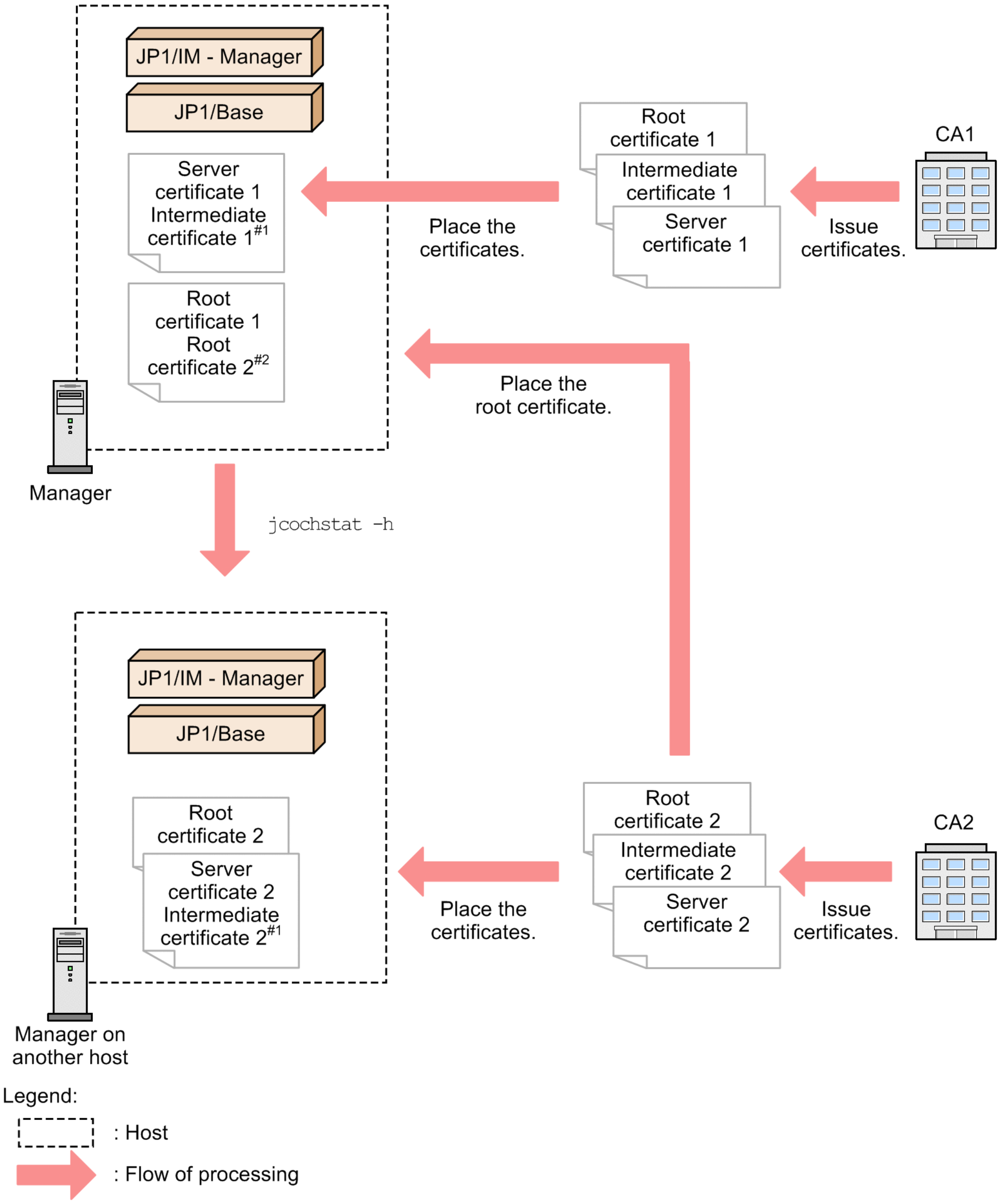


#: If an intermediate certificate is used, it is combined with the server certificate.

- Certificates needed for a manager host
    - Server certificate for the manager host
    - Root certificate that corresponds to the manager host's server certificate
    - If there is an intermediate certificate authority, an intermediate certificate from the intermediate certificate authority that issued the manager host's server certificate
- Certificates needed for a viewer host
    - Root certificate that corresponds to the manager host's server certificate

In addition to *Figure 12-28 Certificates required for encrypting communication between a manager and a viewer*, the following figure shows the certificates required for changing the manager support status on another host by using the `-h` option in the `jcochstat` command.

Figure 12–29: Certificates required for specifying the -h option in the jcochstat command



#1: If an intermediate certificate is used, it is combined with the server certificate.
#2: If multiple root certificates are used, they are combined.

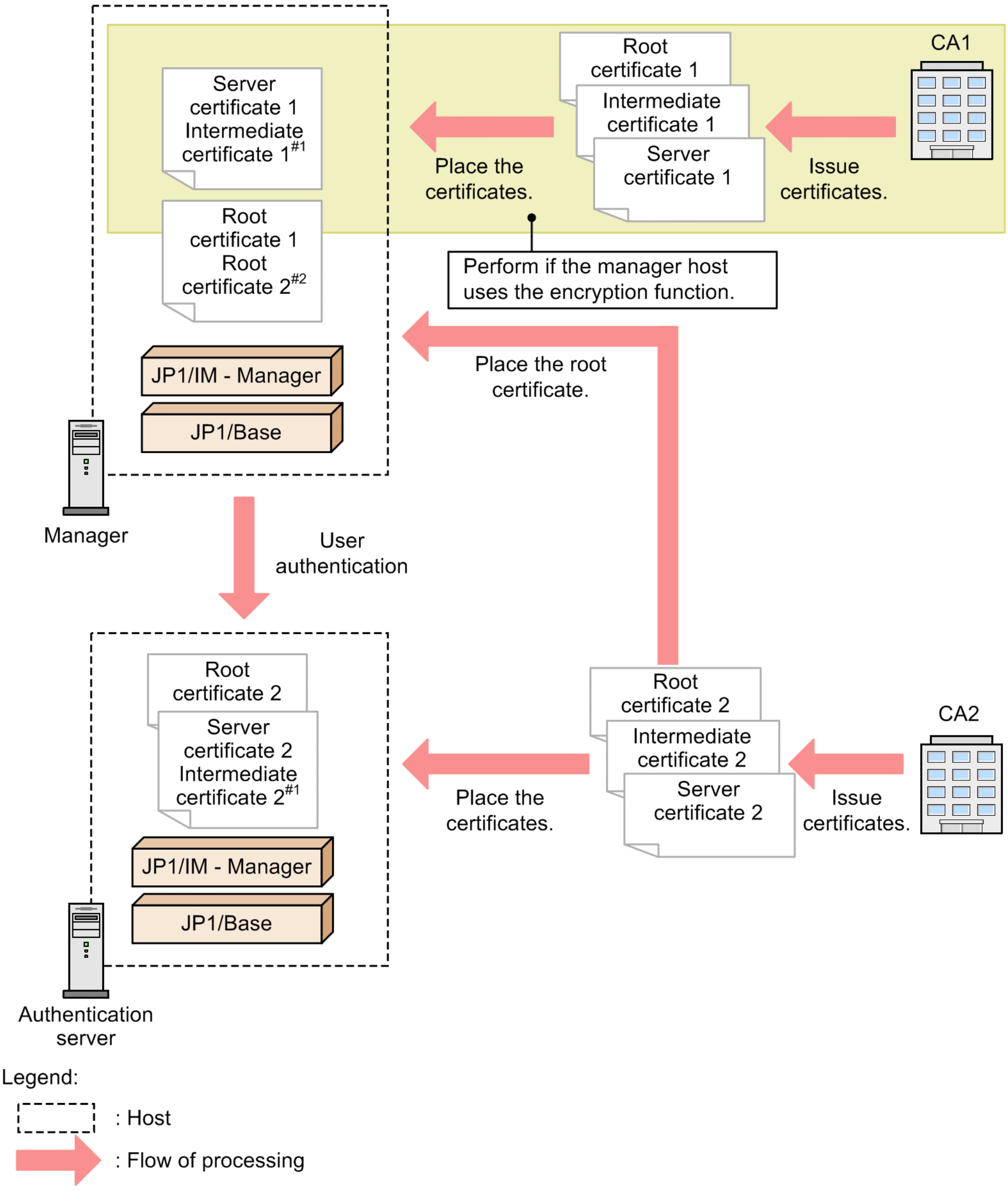
- Certificates needed for a manager host
  - Server certificate for the manager host
  - Root certificate that corresponds to the manager host's server certificate
  - If there is an intermediate certificate authority, an intermediate certificate from the intermediate certificate authority that issued the manager host's server certificate
  - Root certificate that corresponds to another manager host's server certificate
- Certificates needed for another manager host
  - Server certificate for the other manager host
  - Root certificate that corresponds to the other manager host's server certificate

- An intermediate certificate from the intermediate certificate authority that issued the other manager host's server certificate (if there is an intermediate certificate authority)

(2) Encryption between a manager host and an authentication server

The figure below shows the certificates required for encrypting communication between a manager host and an authentication server. For details about encryption of communication with authentication servers (SSL communication), see the *JP1/Base User's Guide*.

Figure 12–30: Certificates required for encrypting communication between a manager and an authentication server



#1: If an intermediate certificate is used, it is combined with the server certificate.
#2: If multiple root certificates are used, they are combined.

- Certificates needed for a manager host
  - Server certificate for the manager host#
  - Root certificate that corresponds to the manager host's server certificate#

    - If there is an intermediate certificate authority, an intermediate certificate from the intermediate certificate authority that issued the manager host's server certificate#
    - Root certificate for the server certificate of JP1/Base (authentication server) that the manager host uses

  #: This certificate is not needed if communication between the manager host and the viewer host is not encrypted. For details about encrypting communication between a manager host and a viewer host, see *12.11.3(1) Encryption between a manager host and a viewer host*.

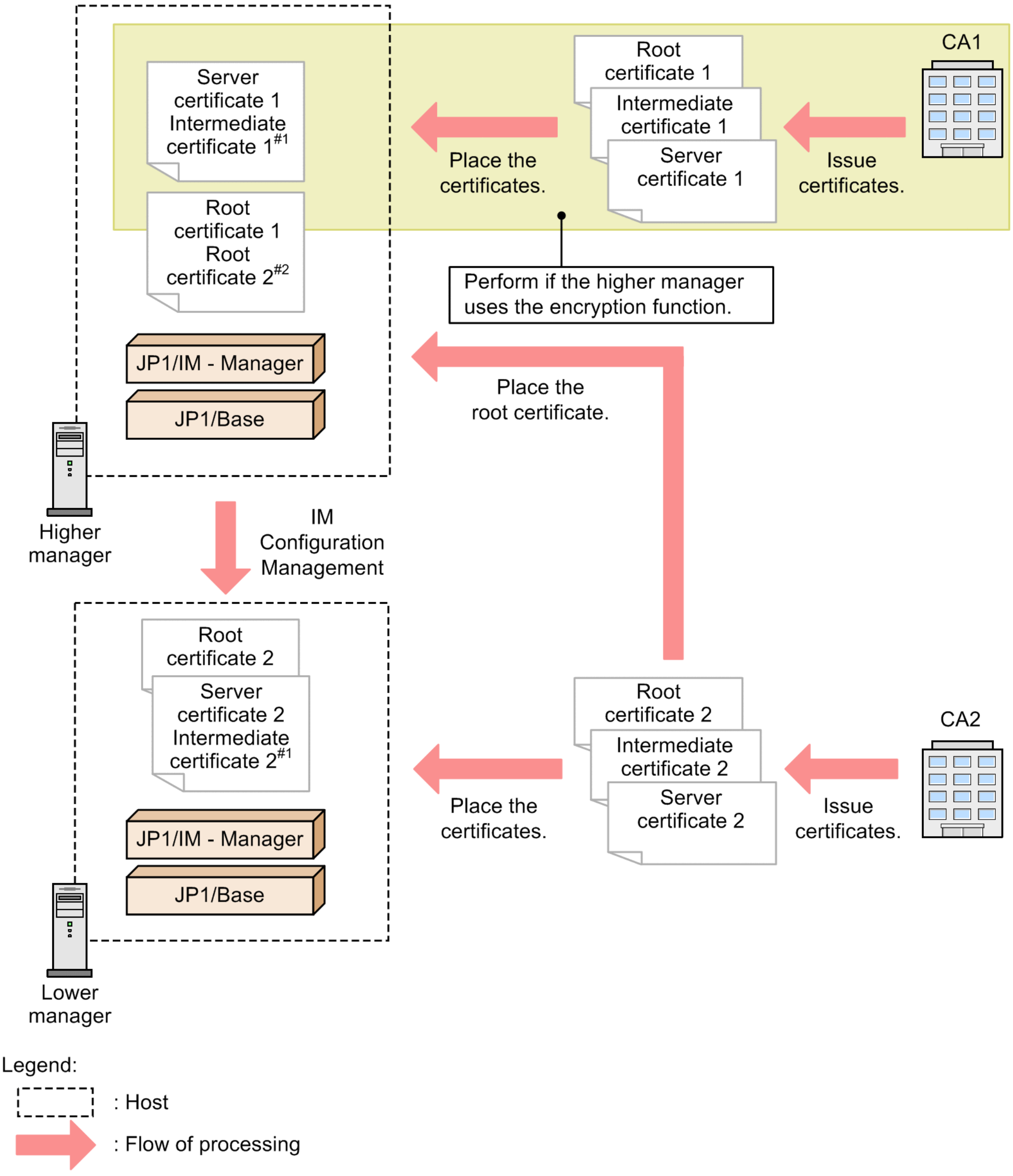
- Certificates needed for an authentication server
    - Server certificate for the authentication server
    - Root certificate for the server certificate of the authentication server
    - If there is an intermediate certificate authority, the intermediate certificate from the intermediate certificate authority that issued the authentication server's server certificate

(3) Using IM Configuration Management on a higher manager

In a hierarchical configuration (IM configuration), if the IM Configuration Management function is used on a higher manager and the communication encryption function is used on a lower manager, place a root certificate for the lower manager host on the higher manager host.

For details about the IM Configuration Management function, see *Chapter 6. System Hierarchy Management Using IM Configuration Management*.

Figure 12–31: Certificates needed when a higher manager uses the IM Configuration Management function


Server certificate 1 Intermediate certificate 1#1
Root certificate 1 Root certificate 2#2
JP1/IM - Manager
JP1/Base
Higher manager
Place the certificates.
Root certificate 1
Intermediate certificate 1
Server certificate 1
Issue certificates.
CA1
Perform if the higher manager uses the encryption function.
Place the root certificate.
IM Configuration Management
Root certificate 2
Server certificate 2 Intermediate certificate 2#1
JP1/IM - Manager
JP1/Base
Lower manager
Place the certificates.
Root certificate 2
Intermediate certificate 2
Server certificate 2
Issue certificates.
CA2
Legend:
: Host
: Flow of processing

#1: If an intermediate certificate is used, it is combined with the server certificate.
#2: If multiple root certificates are used, they are combined.

- Certificates needed for a higher manager host
    - Server certificate for the higher manager host
    - Root certificate that corresponds to the higher manager host's server certificate#
    - If there is an intermediate certificate authority, the intermediate certificate from the intermediate certificate authority that issued the higher manager host's server's server certificate#
    - Root certificate that corresponds to the lower manager host's server certificate

  #: This certificate is not needed if communication between the higher manager host and the viewer host is not encrypted. For details about encrypting communication between a manager host and a viewer host, see *12.11.3(1) Encryption between a manager host and a viewer host*.

- Certificates needed for a lower manager host

- Server certificate for the lower manager host
- Root certificate that corresponds to the lower manager host's server certificate
- If there is an intermediate certificate authority, the intermediate certificate from the intermediate certificate authority that issued the lower manager host's server's server certificate

(4) Details about placing root certificates

The communication encryption function updates and deletes the root certificates placed on clients. Therefore, you need to place the correct root certificates for servers on clients.

Client hosts for encrypted communication include viewer hosts and manager hosts.

If you are placing multiple root certificates on a manager host, combine all root certificates into one file.

If you are placing multiple root certificates on a viewer host, there is no need to combine the root certificates into one file.

A root certificate is updated and deleted mainly at the following times:

- When the root certificate is changed by the certificate authority
- When no more servers correspond to the root certificate because, for example, the hosts using the server certificates that correspond to the root certificate have stopped using the communication encryption function.

The following examples using viewer hosts (clients) and manager hosts (servers) provide details about the placement of root certificates.

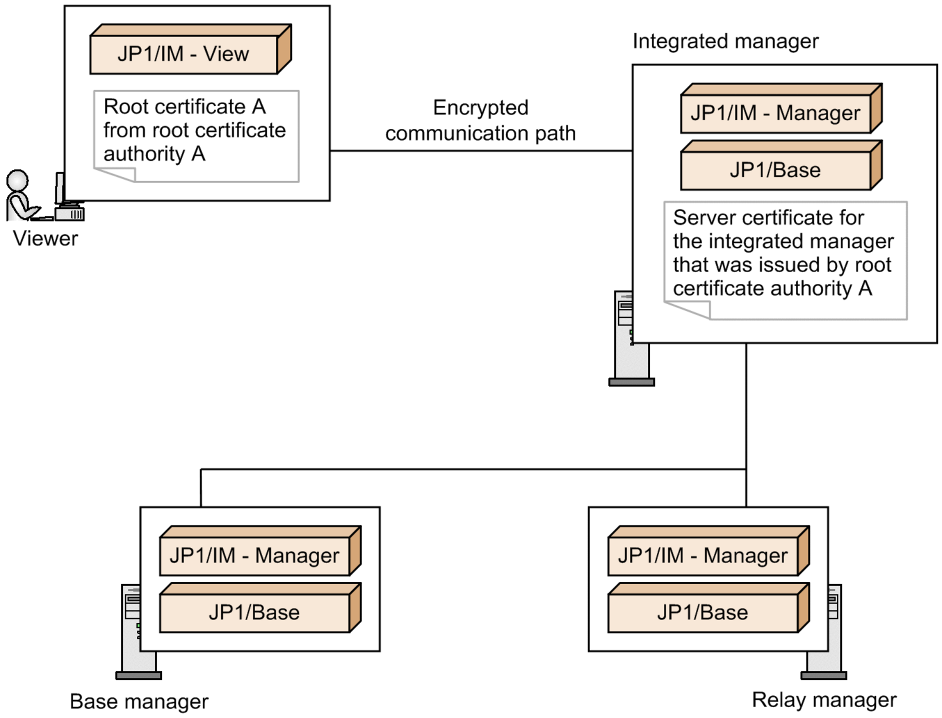
- Connection is established from one viewer host to one manager host.

  This example places one root certificate on the viewer host because there is only one manager host.

  - Communication between the viewer host and the integrated manager host is encrypted.

    The following figure shows a configuration in which the communication encryption function is enabled on the integrated manager, and the base manager and the relay manager are configured as a hierarchy.

Figure 12–32: Placement of the root certificate for the viewer host (example 1)


JP1/IM - View
Root certificate A from root certificate authority A
Viewer
Encrypted communication path
Integrated manager
JP1/IM - Manager
JP1/Base
Server certificate for the integrated manager that was issued by root certificate authority A
JP1/IM - Manager
JP1/Base
Base manager
JP1/IM - Manager
JP1/Base
Relay manager

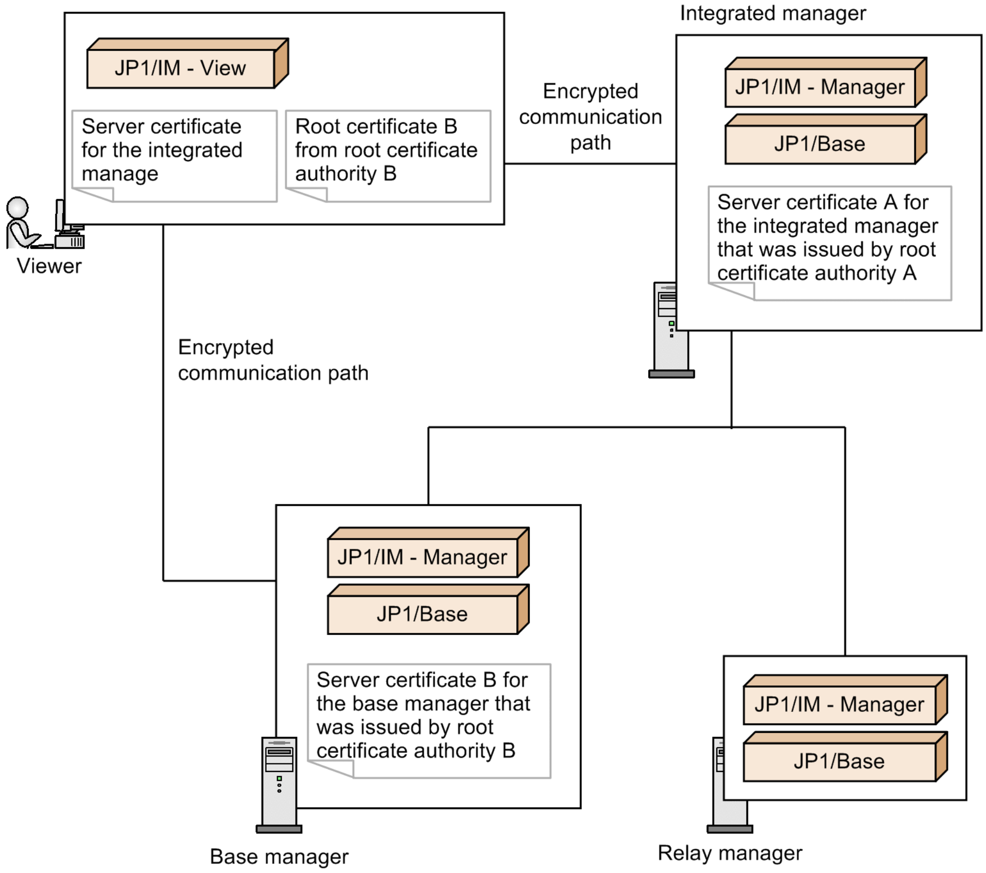
- Connection is established from one viewer host to multiple manager hosts and the root certificate corresponding to the server certificates differs from one manager host to another.

  This example places the root certificate corresponding to each manager host on the viewer host. Therefore, as many root certificates as there are manager hosts must be placed on the viewer host.

  - Communication is encrypted between the viewer host and the integrated manager and between the viewer host and the base manager host.

    The figure below shows a configuration in which the communication encryption function is enabled on the integrated manager and the base manager, the root certificate corresponding to the server certificate for the integrated manager differs from that for the base manager, and multiple manager hosts are monitored by one viewer host. The integrated manager has a hierarchical configuration with the base manager and the relay manager.

Figure 12–33: Placement of the root certificates for the viewer host (example 2)


Integrated manager
JP1/IM - View
Server certificate for the integrated manage
Root certificate B from root certificate authority B
Encrypted communication path
JP1/IM - Manager
JP1/Base
Server certificate A for the integrated manager that was issued by root certificate authority A
Viewer
Encrypted communication path
JP1/IM - Manager
JP1/Base
Server certificate B for the base manager that was issued by root certificate authority B
JP1/IM - Manager
JP1/Base
Base manager
Relay manager

- Connection is established from one viewer host to multiple manager hosts and the root certificate corresponding to the server certificates is the same for all manager hosts.

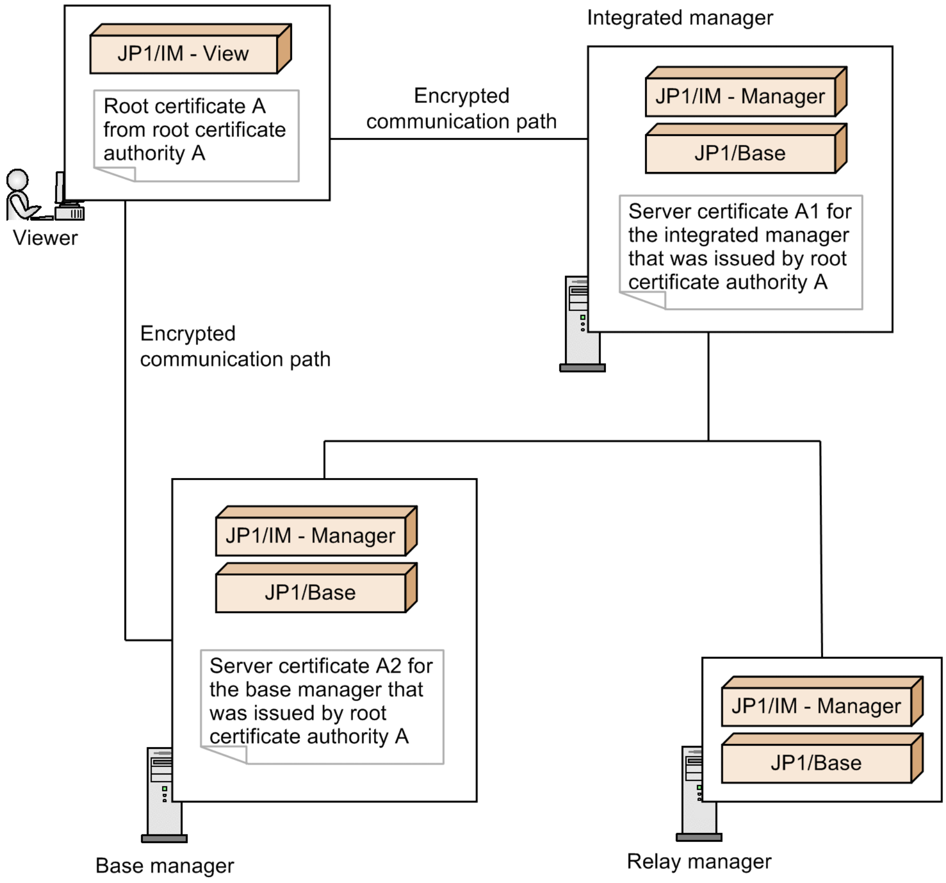
  This example places one root certificate on the viewer host because the root certificates for all manager hosts are the same. If the same root certificate is placed under different file names, a one-to-one correspondence can be maintained between manager host and root certificate. This helps to identify the correct root certificate for each manager host when root certificates are to be deleted. To delete a root certificate that corresponds to multiple manager hosts, you must verify that the root certificate has no corresponding manager hosts.

  - Communication is encrypted between the viewer host and the integrated manager host and between the viewer host and the base manager host.

    The same root certificate is placed on JP1/IM - View for both the integrated manager and the base manager because the root certificates corresponding to server certificates for these managers are the same.

    The figure below shows a configuration in which the communication encryption function is enabled on the integrated manager and the base manager, the root certificates corresponding to the server certificates for the integrated manager and the base manager are the same, and multiple manager hosts are monitored by one viewer host. The integrated manager has a hierarchical configuration with the base manager and the relay manager.

Figure 12–34: Placement of the root certificate for the viewer host (example 3)


Integrated manager
JP1/IM - View
Root certificate A from root certificate authority A
Viewer
Encrypted communication path
JP1/IM - Manager
JP1/Base
Server certificate A1 for the integrated manager that was issued by root certificate authority A
Encrypted communication path
JP1/IM - Manager
JP1/Base
Server certificate A2 for the base manager that was issued by root certificate authority A
JP1/IM - Manager
JP1/Base
Base manager
Relay manager

12.11.4 Verifying server certificates

This subsection explains the verification of server certificates that is performed by clients (connection sources) when encrypted communication begins.

When encrypted communication begins, a client receives a server certificate from the server (connection target). The client then checks the validity of the received server certificate.

The subsections below explain the contents of server certificates that clients verify by using the communication encryption function.

For details about the communication to be verified, see *Table 12-19 Contents of certificates verified for Central Console*, *Table 12-20 Contents of certificates verified for Central Scope*, or *Table 12-21 Contents of certificates verified for IM Configuration Management*.

(1) Verifying signatures

A client receives a server certificate and verifies the signature in the server certificate by using the root certificate that has been placed on the client.

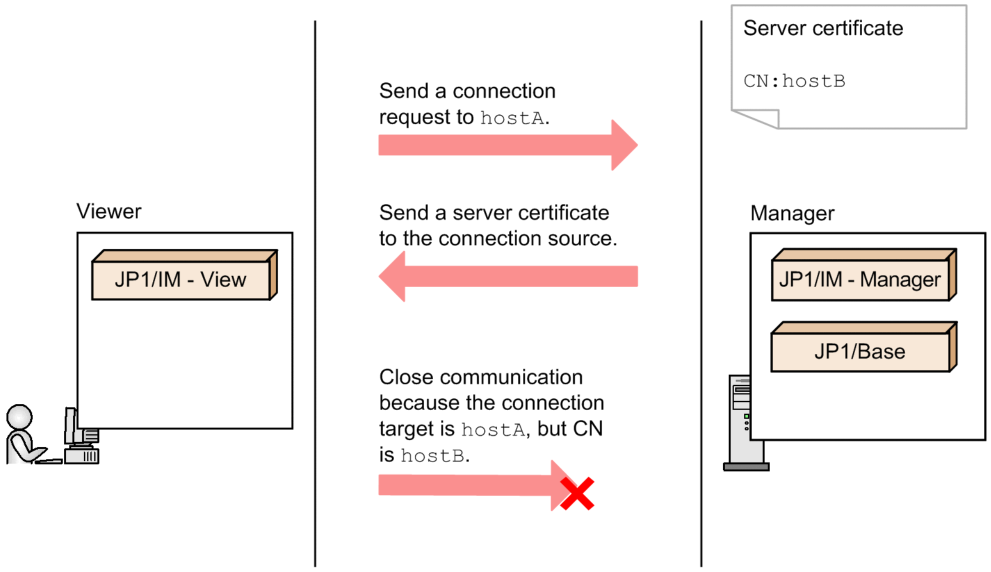
(2) Verifying host names (CN and SAN) in server certificates

The client verifies that the host name (CN and SAN) in the server certificate matches the host name of the client's connection target. This is done by comparing the host name specified for CN or SAN (`dNSName`) in the server certificate with the host name at the connection target that the client recognizes.#

If the host name specified for CN or SAN (`dNSName`) in the server certificate is not a host name for the connection target that the client recognizes, communication is closed.

#: If the server certificate contains SAN (`dNSName`), only SAN (`dNSName`) is compared, in which case CN is not compared.

Figure 12–35: Processing when the host name specified for the connection target differs from CN


Server certificate
CN:hostB
Send a connection request to hostA.
Viewer
JP1/IM - View
Send a server certificate to the connection source.
Manager
JP1/IM - Manager
JP1/Base
Close communication because the connection target is hostA, but CN is hostB.

For details about connection-target host names that are used for verifying host names (CN and SAN) in server certificates, see *12.11.4(3) Host names used for verifying host names (CN and SAN) in server certificates*.

(3) Host names used for verifying host names (CN and SAN) in server certificates

The host names listed below are used to verify host names (CN and SAN) in server certificates. If the communication encryption function is used, IP addresses cannot be used for the following host names:

- Connection-target host name in the JP1/IM - View - Login window
- Manager host name specified in the `-h` option in the `jcochstat` command
- Host name registered as the system hierarchy in IM Configuration Management

For details about communication for which host names (CN and SAN) in server certificates are to be verified by JP1/IM - Manager, see *Table 12-19 Contents of certificates verified for Central Console*, *Table 12-20 Contents of certificates verified for Central Scope*, or *Table 12-21 Contents of certificates verified for IM Configuration Management*.

(4) Expiration date of server certificates

A client checks the expiration date of the server certificate.

Because an expiration date is set for server certificates to maintain security, the client closes communication with the server if the server certificate has expired.

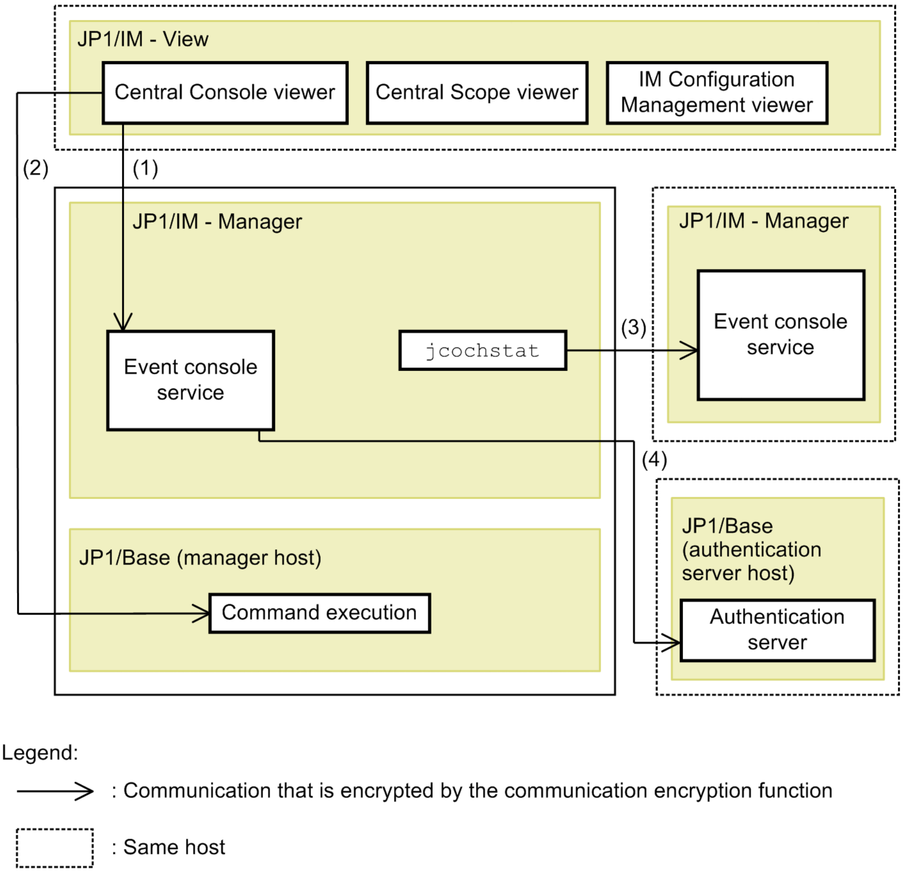
If you want to receive advance notice of server certificate expiration, use a public certificate authority service.

For details about renewing certificates, see *12.11.2(3) Maintaining certificates*.

(5) Contents of certificates that are verified for Central Console

The following figure shows the range of Central Console communication that can be encrypted and the contents of certificates that are verified.

Figure 12–36: Range of Central Console communication that can be encrypted



The parenthesized numbers in the figure correspond to the numbers in the following table.

Table 12–19: Contents of certificates verified for Central Console

No.	Location of communication#1		Verification of server certificate by the connection source			Verification of root certificate by the connection source#2
	Connection source	Connection target	Verification of signature	Host name used for verifying the host name (CN and SAN) in server certificate	Expiration date	Expiration date
1	Central Console viewer	Event console service	Y	Y **Host to connect** in the Login window	Y	Y Verifies the root certificate that is placed in JP1/IM - View
2	Central Console viewer	Command execution	Y		Y	

No.	Location of communication[#1]		Verification of server certificate by the connection source			Verification of root certificate by the connection source[#2]
	Connection source	Connection target	Verification of signature	Host name used for verifying the host name (CN and SAN) in server certificate	Expiration date	Expiration date
3	`jcochstat` command	Event console service (another host)	Y	Y Manager host name specified in the `-h` option	Y	Y Verifies the root certificate that is placed on the manager host
4	Event console service	Authentication server	The communication encryption function of JP1/Base is used for communication. For details about the communication encryption function of JP1/Base, see the *JP1/Base User's Guide*.			

Legend:

Y: Verified

#1

For details, see *12.11.1 Range of communication that can be encrypted by the communication encryption function*.

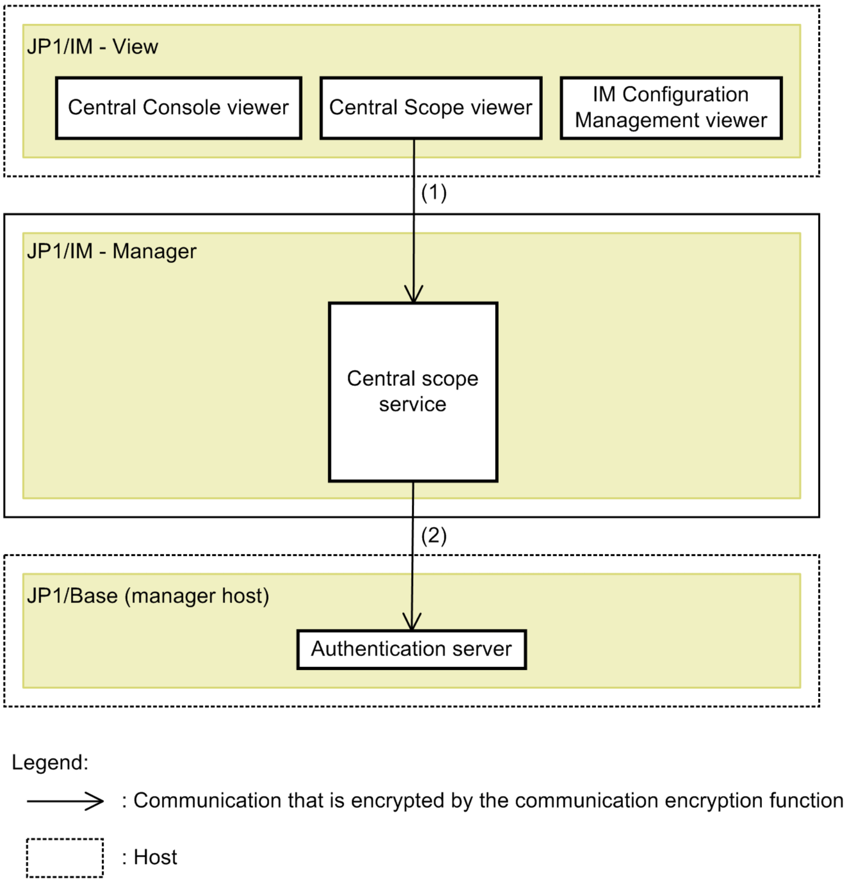
#2

For details about verifying root certificates, see *12.11.5 Verifying root certificates*.

(6) Contents of certificates that are verified for Central Scope

The following figure shows the range of Central Scope communication that can be encrypted and the contents of certificates that are verified.

Figure 12–37: Range of Central Scope communication that can be encrypted



The parenthesized numbers in the figure correspond to the numbers in the following table.

Table 12–20: Contents of certificates verified for Central Scope

No.	Location of communication[#1]		Verification of server certificate by the connection source			Verification of root certificate by the connection source[#2]
	Connection source	Connection target	Verification of signature	Host name used for verifying the host name (CN and SAN) in server certificate	Expiration date	Expiration date
1	Central Scope viewer	Central Scope service	Y	Y **Host to connect** in the Login window	Y	Y Verifies the root certificate that is placed in JP1/IM - View
2	Central Scope service	Authentication server	The communication encryption function of JP1/Base is used for communication. For details about the communication encryption function of JP1/Base, see the *JP1/Base User's Guide*.			

Legend:

Y: Verified

#1

For details, see *12.11.1 Range of communication that can be encrypted by the communication encryption function*.

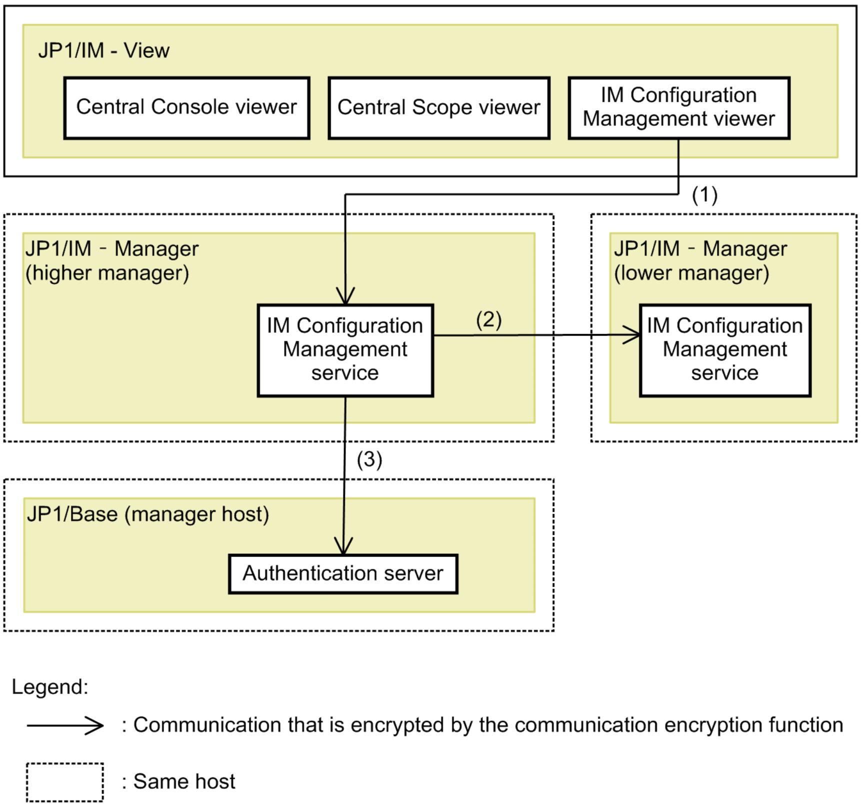
#2

For details about verifying root certificates, see *12.11.5 Verifying root certificates*.

(7) Contents of certificates that are verified for IM Configuration Management

The following figure shows the range of IM Configuration Management communication that can be encrypted and the contents of certificates that are verified.

Figure 12–38: Range of IM Configuration Management communication that can be encrypted


JP1/IM - View
Central Console viewer
Central Scope viewer
IM Configuration Management viewer
(1)
JP1/IM - Manager (higher manager)
IM Configuration Management service
(2)
JP1/IM - Manager (lower manager)
IM Configuration Management service
(3)
JP1/Base (manager host)
Authentication server
Legend:
: Communication that is encrypted by the communication encryption function
: Same host

The parenthesized numbers in the figure correspond to the numbers in the following table.

Table 12–21: Contents of certificates verified for IM Configuration Management

No.	Location of communication[#1]		Verification of server certificate by the connection source			Verification of root certificate by the connection source[#2]
	Source	Connection target	Verification of signature	Host name used for verifying the host name (CN and SAN) in server certificate	Expiration date	Expiration date
1	IM Configuration Management viewer	IM Configuration Management service	Y	Y **Host to connect** in the Login window	Y	Y Verifies the root certificate that is placed in JP1/IM - View
	IM Configuration Management viewer (when Base View is running)		Y	Y **Host** registered in IM Configuration Management	Y	Y Verifies the root certificate that is placed in JP1/IM - View
2	IM Configuration Management service (integrated manager)	IM Configuration Management service (base manager)	Y	Y **Host** registered in IM Configuration Management	Y	Y Verifies the root certificate that is placed on the manager host

No.	Location of communication#1		Verification of server certificate by the connection source			Verification of root certificate by the connection source#2
	Source	Connection target	Verification of signature	Host name used for verifying the host name (CN and SAN) in server certificate	Expiration date	Expiration date
3	IM Configuration Management service	Authentication server	The communication encryption function of JP1/Base is used for communication. For details about the communication encryption function of JP1/Base, see the *JP1/Base User's Guide*.			

Legend:

Y: Verified

#1

For details, see *12.11.1 Range of communication that can be encrypted by the communication encryption function*.

#2

For details about verifying root certificates, see *12.11.5 Verifying root certificates*.

12.11.5 Verifying root certificates

Clients use root certificates to verify signatures in server certificates.

A client checks the expiration date of the imported root certificate to see if the certificate has expired. If the root certificate has expired, the client outputs a warning message to the integrated trace log, but uses the root certificate to verify the signature in the server certificate.

For details about renewing certificates, see *12.11.2(3) Maintaining certificates*.

For details about the certificate contents to be verified, see the following subsections:

- *12.11.4(5) Contents of certificates that are verified for Central Console*
- *12.11.4(6) Contents of certificates that are verified for Central Scope*
- *12.11.4(7) Contents of certificates that are verified for IM Configuration Management*

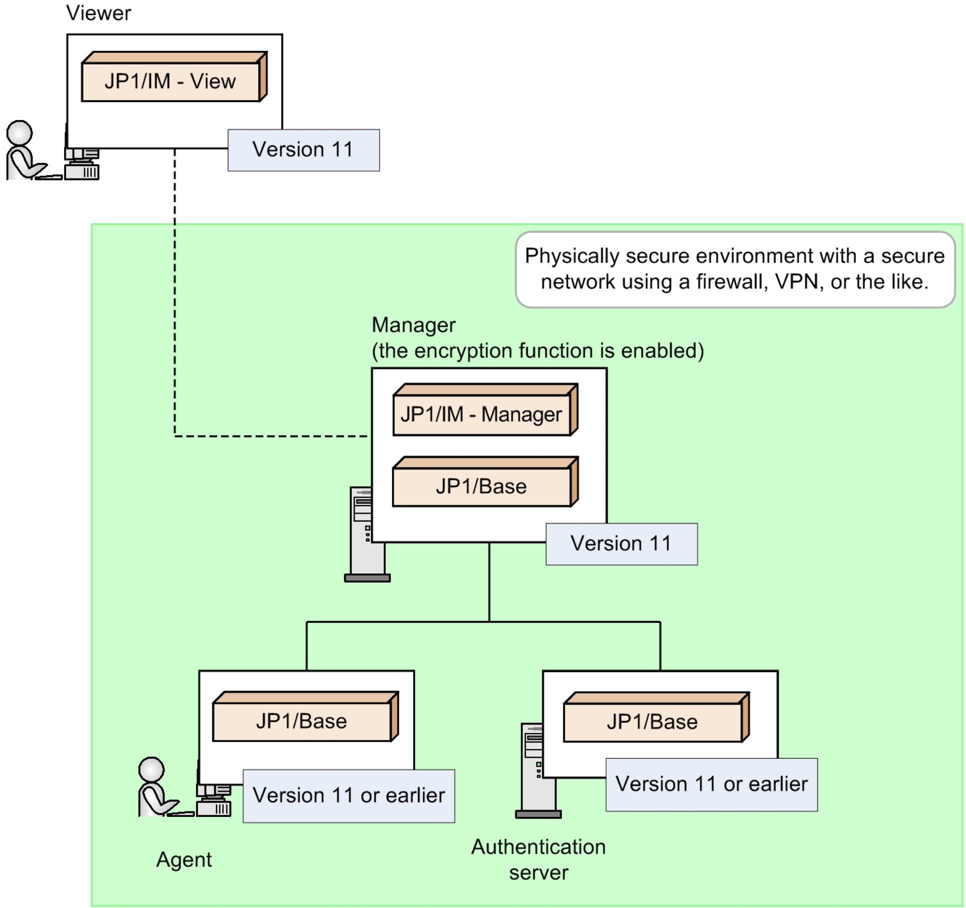
12.11.6 System configuration

The communication encryption function enables you to maintain the confidentiality of communication data on viewer hosts and manager hosts. The following subsections explain the recommended system configurations for using the communication encryption function.

(1) Basic system configuration

This configuration supports an environment in which JP1/Base 11 or earlier is run on an agent and an authentication server and also JP1/Base 10 or earlier is run.

Figure 12–39: Basic configuration



Legend:

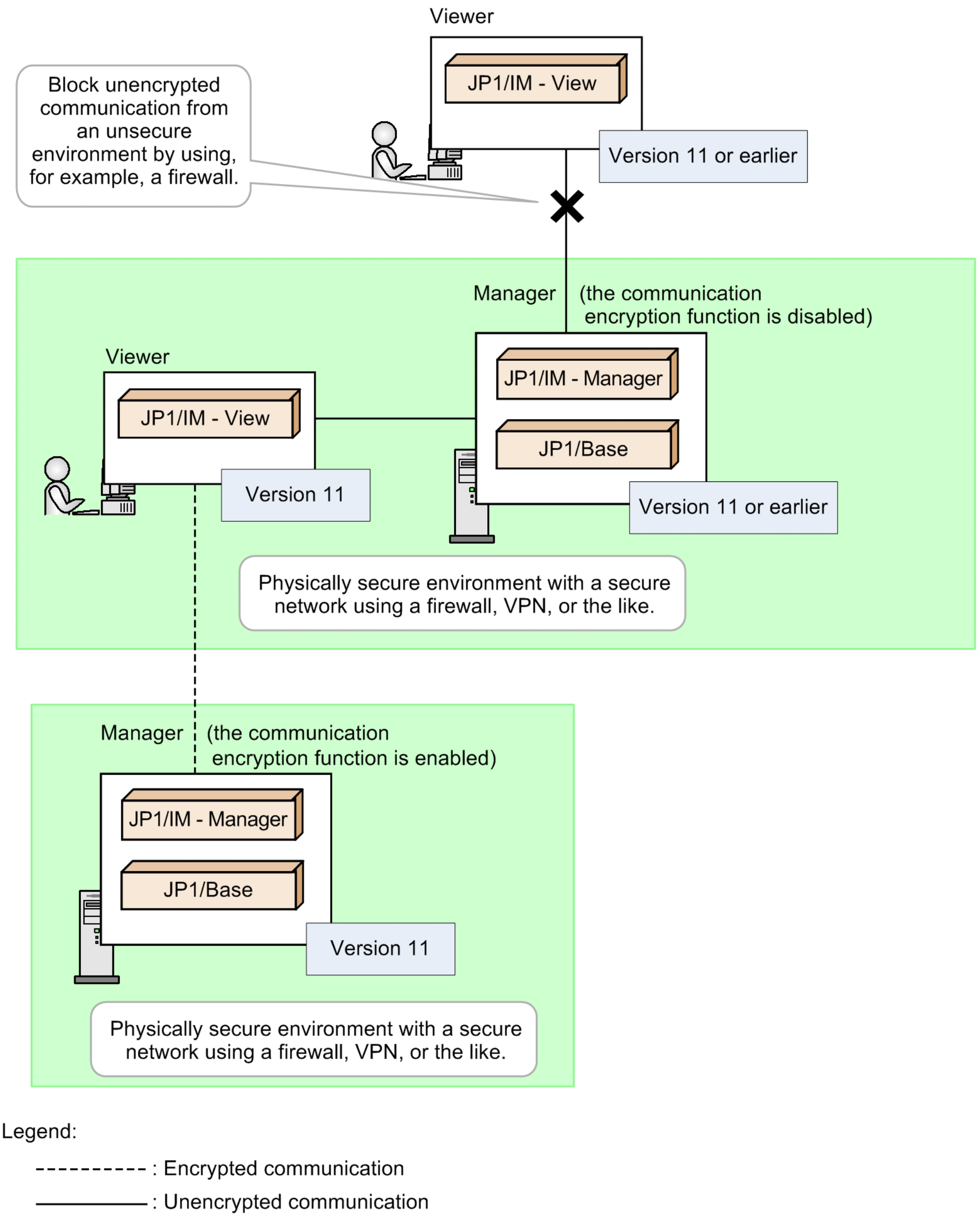
---------- : Encrypted communication

———— : Unencrypted communication

(2) System configuration in which connection is established with multiple manager hosts

The following figure shows a system configuration in which one viewer host starts two viewers, one of which is connected to a manager host on which the communication encryption function is enabled and the other is connected to a manager host on which the communication encryption function is disabled.

Figure 12–40: Configuration in which connection is established with multiple manager


Viewer
JP1/IM - View
Version 11 or earlier
Block unencrypted communication from an unsecure environment by using, for example, a firewall.
Manager
(the communication encryption function is disabled)
Viewer
JP1/IM - View
Version 11
JP1/IM - Manager
JP1/Base
Version 11 or earlier
Physically secure environment with a secure network using a firewall, VPN, or the like.
Manager
(the communication encryption function is enabled)
JP1/IM - Manager
JP1/Base
Version 11
Physically secure environment with a secure network using a firewall, VPN, or the like.
Legend:
----------- : Encrypted communication
———— : Unencrypted communication

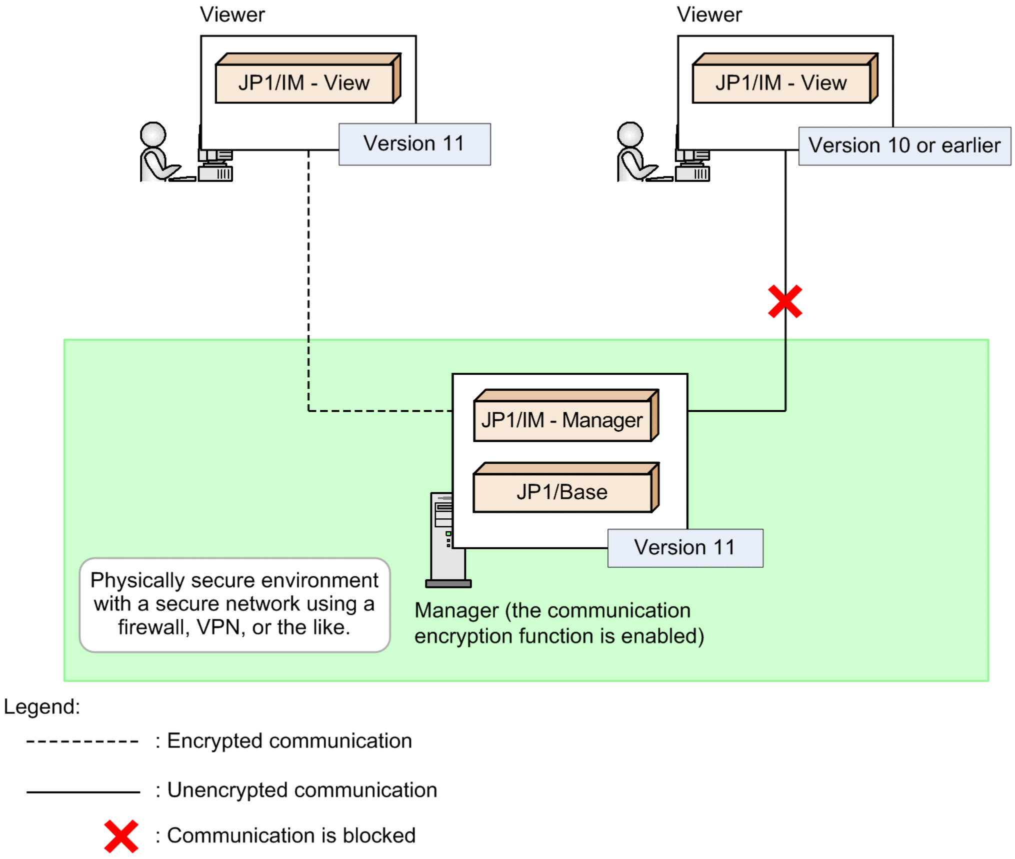
In this system configuration, a host that encrypts communication with JP1/IM - View and a host that does not encrypt communication with JP1/IM - View are configured. For details about the configuration method, see *Non-encryption communication host configuration file (nosslhost.conf)* (in *Chapter 2. Definition Files*) in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

To maintain the confidentiality of communication data between the viewer host and the manager host on which the communication encryption function is disabled, configure a physically secure environment with a secure network by using a firewall, VPN, or the like, so that unencrypted communication from the viewer host in the unsecure environment to the manager host can be blocked.

(3) System configuration in which multiple viewer hosts establish connection

An environment in which JP1/IM - View version 11 is intermixed with JP1/IM - View version 10 or earlier is not supported because a manager host does not allow unencrypted communication with viewer hosts.

Figure 12–41: Configuration in which multiple viewer hosts establish connection



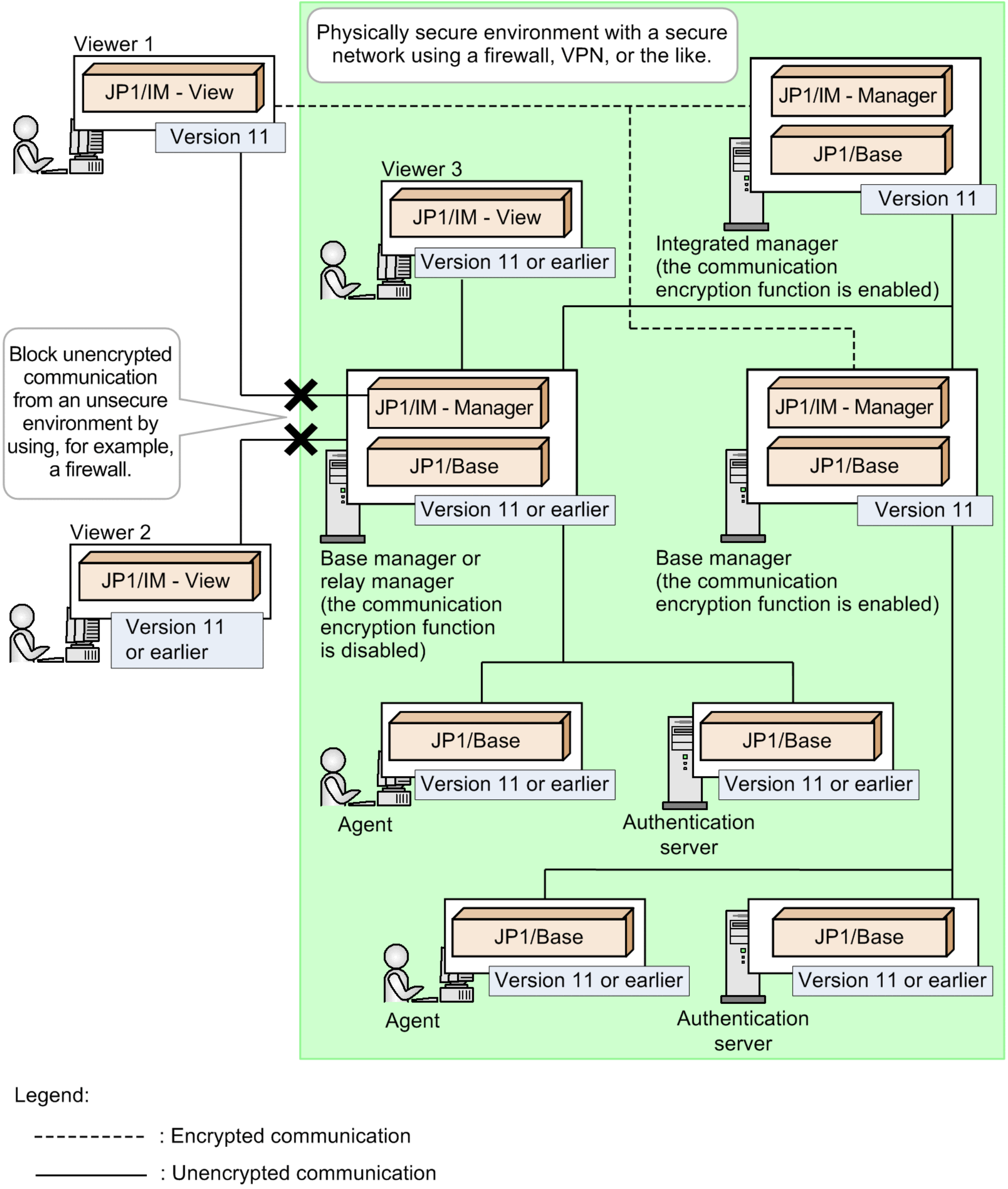
Viewer
JP1/IM - View
Version 11
Viewer
JP1/IM - View
Version 10 or earlier
JP1/IM - Manager
JP1/Base
Version 11
Physically secure environment with a secure network using a firewall, VPN, or the like.
Manager (the communication encryption function is enabled)
Legend:
: Encrypted communication
: Unencrypted communication
: Communication is blocked

(4) Tree configuration of manager hosts and viewer hosts

If the communication encryption function is disabled on a base manager host or a relay manager host, communication with the viewer host is not encrypted.

To maintain the confidentiality of communication data, configure a physically secure environment with a secure network by using a firewall, VPN, or the like. Encrypt all communication from a viewer host in an unsecure environment and block unencrypted communication by using a firewall, for example. Also, place a viewer host that uses unencrypted communication in a secure environment.

Figure 12–42: Tree configuration of managers

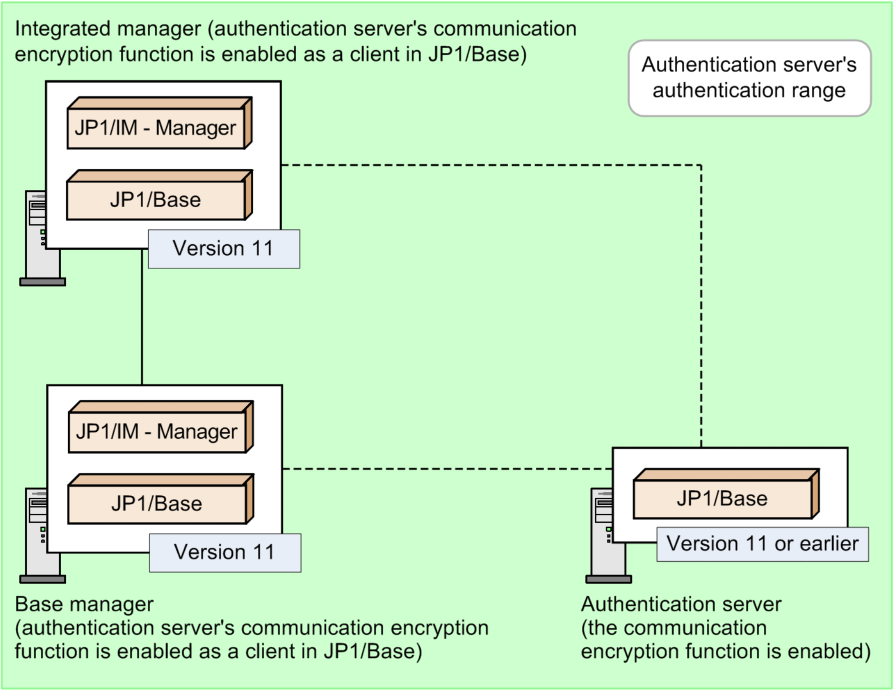

Physically secure environment with a secure network using a firewall, VPN, or the like.
Viewer 1
JP1/IM - View
Version 11
JP1/IM - Manager
JP1/Base
Version 11
Integrated manager (the communication encryption function is enabled)
Viewer 3
JP1/IM - View
Version 11 or earlier
Block unencrypted communication from an unsecure environment by using, for example, a firewall.
JP1/IM - Manager
JP1/Base
Version 11 or earlier
Base manager or relay manager (the communication encryption function is disabled)
JP1/IM - Manager
JP1/Base
Version 11
Base manager (the communication encryption function is enabled)
Viewer 2
JP1/IM - View
Version 11 or earlier
JP1/Base
Version 11 or earlier
Agent
JP1/Base
Version 11 or earlier
Authentication server
JP1/Base
Version 11 or earlier
Agent
JP1/Base
Version 11 or earlier
Authentication server
Legend:
: Encrypted communication
: Unencrypted communication

(5) Configuration of manager hosts and an authentication server

If you will be encrypting communication between manager hosts and an authentication server, consider the authentication server's authentication range.

- When all manager hosts are version 11
  If the authentication server's communication encryption function is enabled, enable the communication encryption function (authentication server's function as a client) in all JP1/Bases (manager hosts).

Figure 12–43: When all manager hosts are version 11


Integrated manager (authentication server's communication encryption function is enabled as a client in JP1/Base)
Authentication server's authentication range
JP1/IM - Manager
JP1/Base
Version 11
JP1/IM - Manager
JP1/Base
Version 11
JP1/Base
Version 11 or earlier
Base manager (authentication server's communication encryption function is enabled as a client in JP1/Base)
Authentication server (the communication encryption function is enabled)

Legend:

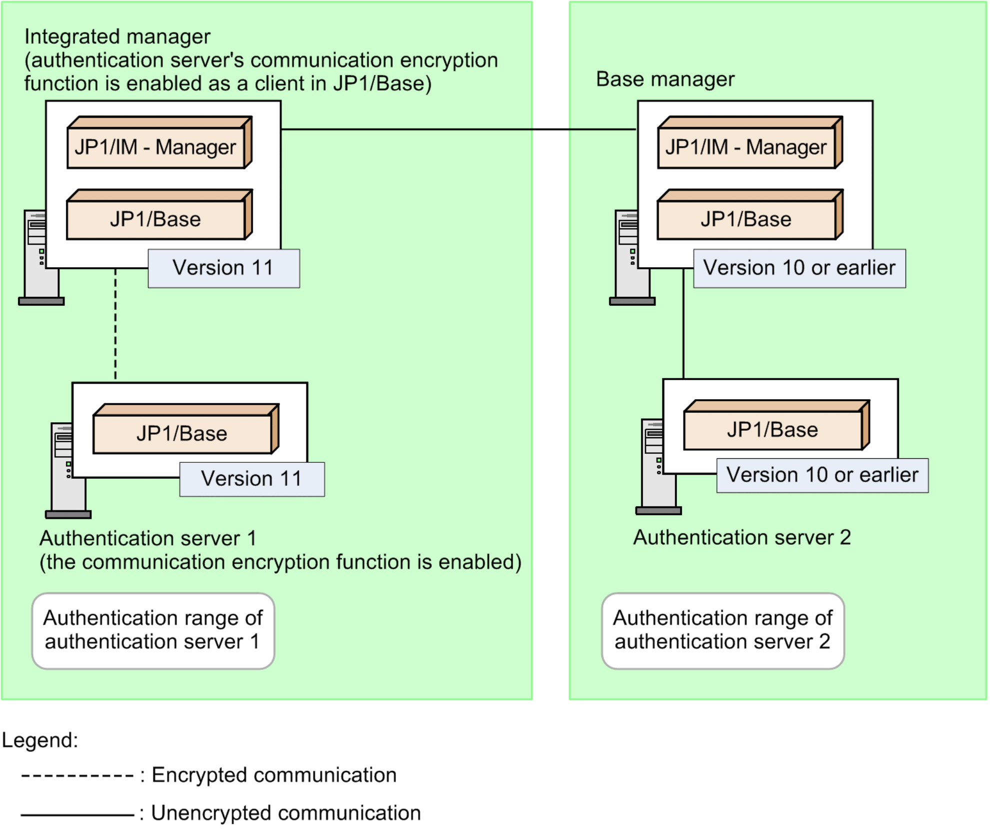
---------- : Encrypted communication

———— : Unencrypted communication

- When manager hosts with version 11 are intermixed with manager hosts with version 10 or earlier

  If the authentication server's communication encryption function is enabled, separate authentication ranges must be provided by configuring a server for which the authentication server's communication encryption function is disabled.

Figure 12–44: When manager hosts with version 11 are intermixed with manager hosts with version 10 or earlier


Integrated manager
(authentication server's communication encryption function is enabled as a client in JP1/Base)
JP1/IM - Manager
JP1/Base
Version 11
JP1/Base
Version 11
Authentication server 1
(the communication encryption function is enabled)
Authentication range of authentication server 1
Base manager
JP1/IM - Manager
JP1/Base
Version 10 or earlier
JP1/Base
Version 10 or earlier
Authentication server 2
Authentication range of authentication server 2
Legend:
----------- : Encrypted communication
———— : Unencrypted communication

12.11.7 Communication encryption function setting (enable/disable) and connectivity among product versions

This subsection explains the communication encryption function setting (enable/disable), connectivity among product versions (10-50 or earlier and 11-00 and later), and connectivity with linked products.

(1) Connectivity between JP1/IM - View and JP1/IM - Manager and when the jcochstat command with the -h option specified is executed

JP1/IM - View version 11-00 or later checks the non-encryption communication host configuration file to determine whether unencrypted communication is to be established with the connection-target JP1/IM - Manager.

For details about the non-encryption communication host configuration file, see *Non-encryption communication host configuration file (nosslhost.conf)* (in *Chapter 2. Definition Files*) in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

Table 12–22: Connectivity between JP1/IM - View and JP1/IM - Manager

JP1/IM - Manager		JP1/IM - View		
Version	Communication encryption function	Version 10-50 or earlier	Version 11-00 or later	
			Unencrypted#1	Encrypted#2
10-50 or earlier	Always disabled	U	U	N

JP1/IM - Manager		JP1/IM - View		
Version	Communication encryption function	Version 10-50 or earlier	Version 11-00 or later	
			Unencrypted[#1]	Encrypted[#2]
11-00 or later	Disabled	U	U	N
	Enabled (`jp1imcmda`)[#3]	N	N	Y

Legend:

Y: Encrypted communication is used.

U: Unencrypted communication is used.

N: Communication is blocked.

#1

The manager host name in the non-encryption communication host configuration file must be the connection-target JP1/IM - Manager or the asterisk (`*`).

#2

In the non-encryption communication host configuration file, the manager host names must not include the connection-target JP1/IM - Manager and must not be an asterisk (`*`).

#3

This applies when `jp1imcmda` is specified in the `BASESSL` parameter in the SSL communication definition file in JP1/Base.

The following example shows connectivity when the `jcochstat` command is executed from JP1/IM - Manager (`hostA`) to JP1/IM - Manager (`hostB`) on another manager host.

Table 12–23: Connectivity when the jcochstat command with the -h option specified is executed

JP1/IM - Manager (hostA)		JP1/IM - Manager (hostB)		
Version	Communication encryption function	Version 10-50 or earlier	Version 11-00 or later	
		Communication encryption function		
		Always disabled	Disabled	Enabled (jp1imcmda)[#1]
10-50 or earlier	Always disabled	U	U	N
11-00 or later	Disabled	U	U	N
	Enabled (`jp1imcmda`)[#1]	N	N	Y[#2]

Legend:

Y: Encrypted communication is used and the `jcochstat` command executes successfully.

U: Unencrypted communication is used and the `jcochstat` command executes successfully.

N: Communication is blocked and execution of the `jcochstat` command fails.

#1

This applies when `jp1imcmda` is specified in the `BASESSL` parameter in the SSL communication definition file in JP1/Base.

#2

The following prerequisites must be satisfied:

- The root certificate from the root certification authority corresponding to the server certificate of the JP1/IM - Manager that is specified in the `-h` option must be placed on the manager host on which the `jcochstat` command is executed. If this root certificate is not available, the `jcochstat` command fails because encrypted communication cannot be established.
- The manager host name specified in the `-h` option must be the host name specified for the CN or SAN in the server certificate of that manager host. If the correct manager host name is not specified, the `jcochstat` command fails because encrypted communication cannot be established. For details about verification of host names (CN and SAN) in server certificates, see *12.11.4(2) Verifying host names (CN and SAN) in server certificates*.

If you enable the communication encryption function on the manager host on which the jcochstat command is executed and on the manager host that is specified in the -h option of the jcochstat command, you can use the jcochstat command to change the response status of JP1/IM - Manager (other hosts). Note that this functionality for using the jcochstat command to change the response status of JP1/IM - Manager (other hosts) is for compatibility with version 6.

(2) Connectivity between JP1/IM - View and JP1/Base (manager host)

Table 12–24: Connectivity between JP1/IM - View and JP1/Base (manager host)

JP1/Base (manager host)		JP1/IM - View		
Version	Communication encryption function	Version 10-50 or earlier	Version 11-00 or later	
			Unencrypted#1	Encrypted#2
10-50 or earlier	Always disabled	U	U	N
11-00 or later	Disabled	U	U	N
	Enabled (jp1imcmda)#3	N	N	Y
	Enabled (jp1bsuser)#4	U	U	N
	Enabled (jp1imcmda, jp1bsuser)#5	N	N	Y

Legend:

Y: Encrypted communication is used.

U: Unencrypted communication is used.

N: Communication is blocked.

#1

The manager host name in the non-encryption communication host configuration file must be the connection-target JP1/IM - Manager or an asterisk (*).

#2

In the non-encryption communication host configuration file, the manager host names must not include the connection-target JP1/IM - Manager and must not be an asterisk (*).

#3

This applies when only jp1imcmda is defined in the BASESSL parameter in the SSL communication definition file in JP1/Base.

#4

This applies when only jp1bsuser is defined in the BASESSL parameter in the SSL communication definition file in JP1/Base.

#5

This applies when jp1imcmda and jp1bsuser are defined in the BASESSL parameter in the SSL communication definition file in JP1/Base.

(3) Connectivity between JP1/Base (authentication server) and JP1/IM - Manager

The following explains encrypted communication between JP1/Base (authentication server) and JP1/IM - Manager that is supported.

- Event console service (authentication API of JP1/Base) and JP1/Base authentication server

For details, see *12.11.1 Range of communication that can be encrypted by the communication encryption function*.

Table 12–25: Connectivity between JP1/IM - Manager and JP1/Base (authentication server)

JP1/Base (authentication server)		JP1/IM - Manager			
Version	Communication encryption function	Version 10-50 or earlier	Version 11-00 or later		
		Communication encryption function			
		Always disabled	Disabled	Enabled (jp1bsuser)#2	Enabled (jp1imcmda and jp1bsuser)#3
10-50 or earlier	Always disabled	U	Not supported#1		
11-00 or later	Disabled	U	U	N	N
	Enabled (jp1bsuser)#2	N	N	Y	Y
	Enabled (jp1imcmda, jp1bsuser)#3	N	N	Y	Y

Legend:

Y: Encrypted communication is used.

U: Unencrypted communication is used.

N: Communication is blocked.

#1

JP1/Base is not supported if a prerequisite product in the same device is version 10-50 or earlier.

#2

This applies when only `jp1bsuser` is defined in the `BASESSL` parameter in the SSL communication definition file in JP1/Base.

#3

This applies when `jp1imcmda` and `jp1bsuser` are defined in the `BASESSL` parameter in the SSL communication definition file in JP1/Base.

(4) Connectivity between JP1/Base (manager host) and JP1/Base (agent host)

The communication encryption function settings have no effect on the connectivity between JP1/Base (manager host) and JP1/Base (agent host).

(5) Connectivity between JP1/IM - Manager and JP1/Base (agent host)

The communication encryption function settings have no effect on the connectivity between JP1/IM - Manager and JP1/Base (agent host).

This means that communication between JP1/IM - Manager and JP1/Base (agent host) is always unencrypted.

(6) Connectivity of IM Configuration Management

The table below explains connectivity of the synchronization function for JP1/IM - Manager's IM Configuration Management information. The synchronization function acquires IM configuration (remote configurations) by establishing connection from the integrated manager to base managers. Depending on the versions of the connection-source JP1/IM - Manager and the connection-target JP1/IM - Manager and whether the communication encryption function is enabled, communication is encrypted, unencrypted, or blocked.

Table 12–26: Connectivity of IM Configuration Management

JP1/IM - Manager (connection source integrated manager)		JP1/IM - Manager (connection-target base manager)		
Version	Communication encryption function	Version 10-50 or earlier	Version 11-00 or later	
		Communication encryption function		
		Always disabled	Disabled	Enabled (jp1imcmda)#
10-50 or earlier	Always disabled	U	U	N
11-00 or later	Disabled	U	U	Y
	Enabled (jp1imcmda)#	U	U	Y

Legend:

Y: Connection can be established for encrypted communication.

U: Connection can be established for unencrypted communication.

N: Connection cannot be established.

#

This applies when jp1imcmda is specified in the BASESSL parameter in the SSL communication definition file in JP1/Base.

(7) Connectivity between JP1/IM - Manager and linked products

When the communication encryption function is enabled, linkage with JP1/Service Support is not supported.

When the communication encryption function is enabled, linkage with JP1/IM - Rule Operation is not supported.

13 Performance and Estimates

This chapter gives an overview of JP1/IM processing performance, and provides a model case that illustrates the memory and disk space requirements for a particular implementation of JP1/IM. Use this information as a reference when reviewing the JP1/IM settings for your system requirements.

Equations for calculating the memory and disk space requirements of JP1/IM can be found in the *Release Notes* for JP1/IM - Manager and JP1/IM - View. Use these references when estimating system requirements.

13.1 JP1/IM processing performance

The performance of the integrated monitoring system depends on the performance of:

- Event display in JP1/IM - View, event reception by JP1/IM - Manager, and automated actions
- The machines on which JP1/IM - Manager and JP1/IM - View are installed
- The network environment

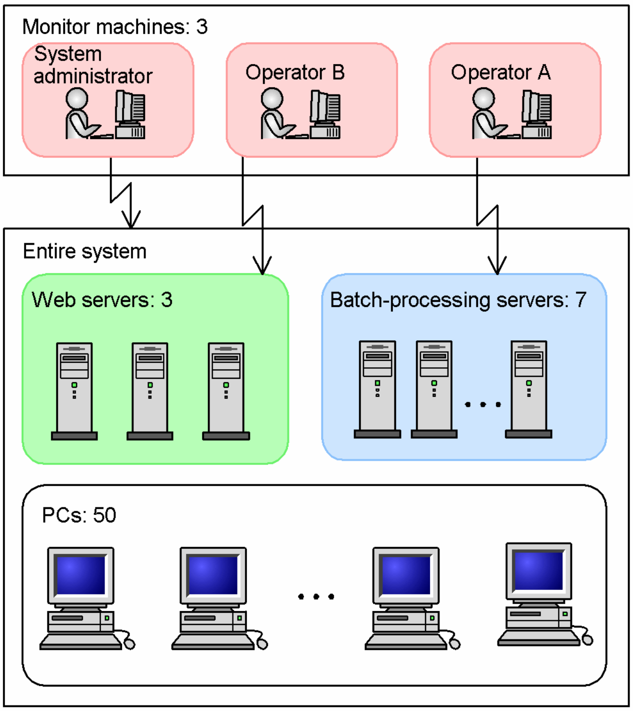
For this reason, you must actually build the integrated monitoring system first, and use it to perform the integrated monitoring tasks for which it is intended. By running the system with a peak load, you can find out if JP1/IM - Manager and JP1/IM - View can execute automated actions and display events in that configuration without delays occurring.

If the processing capacity of the Central Console cannot cope with the peak load, take action to reduce the load. This might entail reducing the number of JP1 events in the system by changing the filter conditions, eliminating redundant automated actions by changing the automated action settings, or increasing the number of base managers.

13.2 Model for performance evaluation

This section uses the example of the business system shown below to give a rough estimate of the increase in memory and disk space requirements incurred when JP1/IM is deployed.

Figure 13–1: Example of business system operation (before JP1/IM deployment)



This system operates as follows:

- Batch processing of work tasks is handled by seven servers.
- Web server functionality is handled by three servers.
- There are 50 user PCs.

Monitoring tasks are divided among three operators (three monitor machines) as follows:

- Operator A monitors the status of batch processing.
- Operator B monitors the status of the Web servers.
- A system administrator monitors the entire system (including end-user PCs).

13.2.1 User requirements

Suppose that JP1/IM is to be deployed in the business system described in *13.2 Model for performance evaluation*, based on the following user requirements (italics indicate JP1/IM keywords).

- A new monitoring server is installed to centrally monitor the business system, and investigate machines where failures occur as necessary.
  -> *System hierarchy (IM configuration)*, *Centralized monitoring using the Central Console*, and *event search*
- The style of monitoring involves three operators, each assigned a specific role as in the existing system.
  -> Applying *event receiver filters*

- Monitoring targets are grouped according to the purpose of the business system.
  -> Using the *Central Scope* (implementing *monitoring range settings*)
- The operator is to be notified automatically when an error requiring immediate attention occurs, even if after hours.
  -> Using *automated actions*
- A history of day-to-day monitoring is kept.
  -> *Saving event list information (CSV snapshot)*

To satisfy these user requirements, the appropriate settings must be made in JP1/IM. For the purposes of this model, the requirements are satisfied by completing the following settings:

System hierarchy (IM configuration)

A new monitoring server is installed to centrally monitor the business system.

-> A system configuration consisting of one manager and 60 agents

Centralized monitoring using the *Central Console*

Events forwarded from agents to the monitoring server are suppressed under the following conditions:

- Events forwarded from a batch-processing server: High priority; forwarded when `Warning` or higher
  -> Assume 20 to 30 such events per server per day
- Events forwarded from a Web server: High priority; forwarded when `Warning` or higher
  -> Assume 10 to 20 such events per server per day
- Events forwarded from a PC: Low priority; forwarded when `Error` or higher
  -> Assume 1 or 2 such events per PC per day

Taking the higher of the two values, you can expect approximately 370 events to be forwarded each day, or 400 when you include the events that occur on the monitoring server (approximately 20 to 30 events with the event level `Warning` or higher). Add a further allowance of 100 to the total, and set the resulting value as the number of events to be stored by JP1/IM - Manager at any one time (the *event buffer size*).

However, supposing that you want to check past events at the same time as recent ones, set the event buffer to 1,000 so that JP1/IM - Manager stores two days' events.

Also, on the assumption that event searches will be carried out as needed from the three monitor machines, set the number of events acquired from machines where errors occurred (the *number of events to acquire in one search*) to 100.

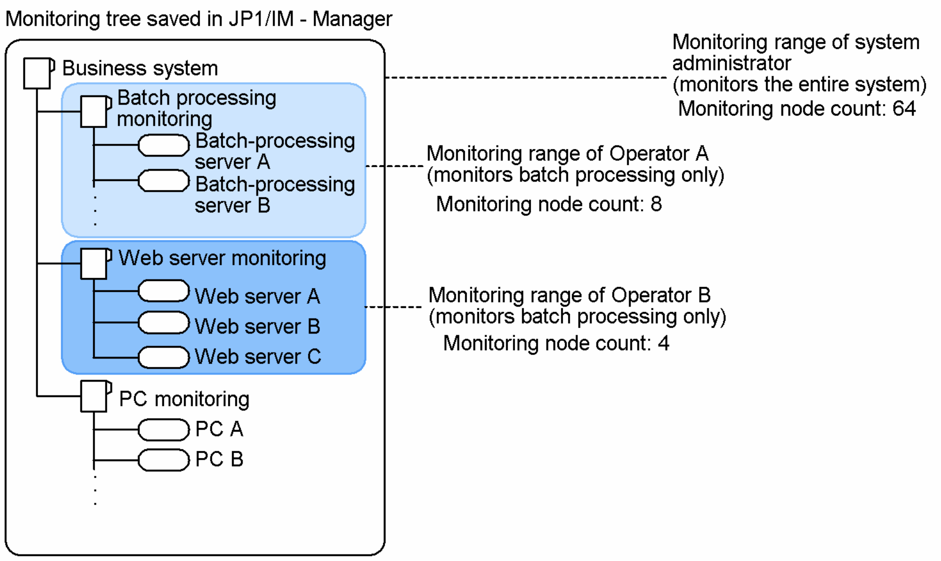
Utilizing *event receiver filters*

Filter the monitored events according to your requirements. Then, calculate the number of events to be saved (the *scroll buffer size*) in the JP1/IM - View for each operator as follows:

- Operator A: Monitors batch-processing servers. Set the scroll buffer size to 500 events ((30 events × 7 servers + 40 event allowance) × 2 days).
- Operator B: Monitors Web servers. Set the scroll buffer size to 200 events ((20 events × 3 servers + 40 event allowance) × 2 days).
- System administrator: Monitors the entire system. Set the scroll buffer size to 1,000, the same as the event buffer size.

Using the *Central Scope* (implementing *monitoring range settings*)

Create the following monitoring tree:


Monitoring tree saved in JP1/IM - Manager
Business system
Batch processing monitoring
Batch-processing server A
Batch-processing server B
Web server monitoring
Web server A
Web server B
Web server C
PC monitoring
PC A
PC B
Monitoring range of system administrator (monitors the entire system)
Monitoring node count: 64
Monitoring range of Operator A (monitors batch processing only)
Monitoring node count: 8
Monitoring range of Operator B (monitors batch processing only)
Monitoring node count: 4

The total number of monitoring nodes in the tree (the total number of monitoring nodes managed in JP1/IM - Manager) is 64, made up of four monitoring groups and 60 monitoring objects.

Implement *monitoring range settings* to restrict the number of monitoring nodes appearing in JP1/IM - View as follows:

- Operator A: One monitoring group, seven monitoring objects
- Operator B: One monitoring group, three monitoring objects
- System administrator: Four monitoring groups, 60 monitoring objects

Automated actions

To enable smooth error detection and basic troubleshooting, 20 automated actions are defined to suit the operating requirements. Of these, five are triggered by multiple conditions joined by an AND condition[#].

#: An event in an AND condition is kept in memory for the specified keep limit (60 minutes by default) or until the AND condition is satisfied. Depending on the situation, assume that in a 60-minute period approximately 30 events will be kept (an estimate obtained by dividing the number of events in a day (500) by 24 hours, and adding 10).

Saving event list information (CSV snapshot)

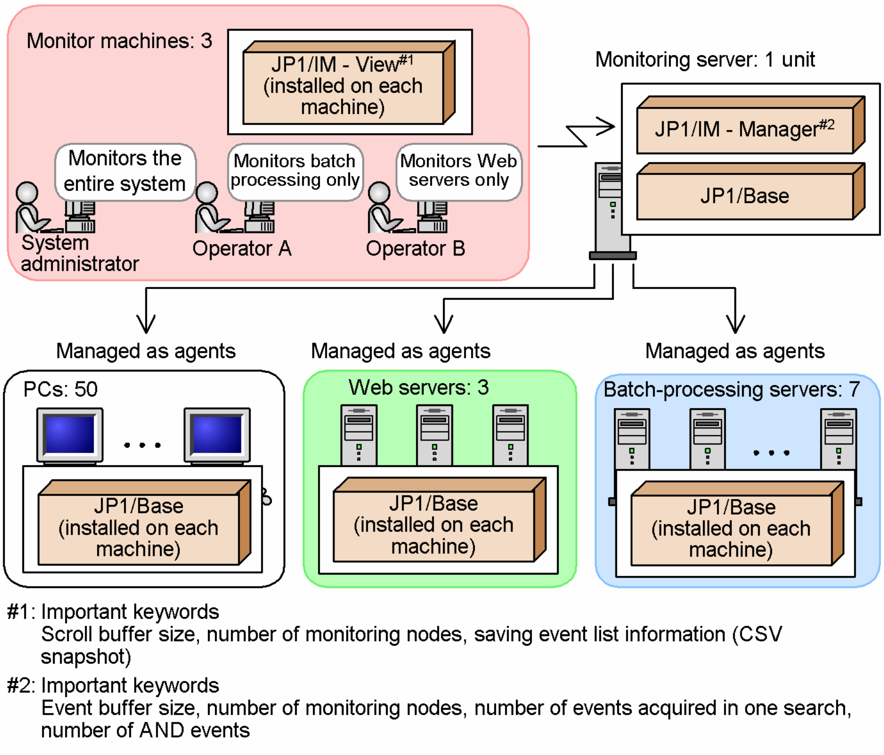
When monitoring is interrupted for some reason, such as at the end of the working day, a CSV snapshot is taken of the event information displayed in JP1/IM - View.

Other

Do not modify settings, such as the log file size, that increase the amount of disk space used. Continue to use the default settings.

The following figure shows the system operation after JP1/IM is deployed.

Figure 13–2: Example of business system operation (after JP1/IM deployment)



Monitor machines: 3
JP1/IM - View#1 (installed on each machine)
Monitors the entire system
Monitors batch processing only
Monitors Web servers only
System administrator
Operator A
Operator B
Monitoring server: 1 unit
JP1/IM - Manager#2
JP1/Base
Managed as agents
Managed as agents
Managed as agents
PCs: 50
JP1/Base (installed on each machine)
Web servers: 3
JP1/Base (installed on each machine)
Batch-processing servers: 7
JP1/Base (installed on each machine)

#1: Important keywords
Scroll buffer size, number of monitoring nodes, saving event list information (CSV snapshot)

#2: Important keywords
Event buffer size, number of monitoring nodes, number of events acquired in one search, number of AND events

Note

The memory required by JP1/IM to monitor the system takes two forms:

1. Memory required by JP1/IM on a constant basis
2. Memory allocated and released for specific purposes during JP1/IM operation

In the above figure, the relevant keywords for the first type of memory are the *event buffer size* and *number of monitoring nodes* for JP1/IM - Manager, and the *scroll buffer size* and *number of (displayed) monitoring nodes* for JP1/IM - View.

The relevant keywords for the second type are *Number of events to acquire in one search* and *Number of AND events* for JP1/IM - Manager, and *Saving event list information (CSV snapshot)* for JP1/IM - View.

When estimating the amount of memory required by JP1/IM, use the sum of the maximum amount of both types of memory.

Estimate your system requirements in terms of this framework. Based on this information, estimate the memory usage and disk space requirements of JP1/IM from the equations in the *Release Notes* for JP1/IM - Manager and JP1/IM - View.

From the results of the equations, make sure that JP1/IM deployment will leave some leeway in the resources of each machine. If you discover that a machine has insufficient memory or disk space, you must consider adding more memory or upgrading the disk. If this cannot be done, you might need to revise your requirements for the system in a way that accommodates your existing hardware.

Also, make sure that a sudden increase in the number of events acquired and processed by JP1/IM due to an unexpected error will not significantly impair performance in terms of displaying events and executing automated actions.

13.2.2 Memory, disk capacity, and database capacity required on a monitoring server

JP1/IM - Manager on a monitoring server has different memory and disk space requirements depending on how JP1/IM is set up. The settings that have the most significant effect on memory and disk usage by JP1/IM - Manager are as follows. For details on the other settings, see the *Release Notes* for JP1/IM - Manager and JP1/IM - View.

- Settings that significantly affect memory usage:
    - Number of event buffers
    - Number of events to acquire in one search
    - Number of monitoring nodes
- Settings that significantly affect disk space usage:
    - Automated action trace log
    - Number of monitoring nodes
    - Number of registered hosts
    - Number of files defined for log trapping

JP1/Base is a prerequisite product when you monitor a system using JP1/IM. For the pertinent information relating to JP1/Base, see the JP1/IM - Base *Release Notes*.

13.2.3 Memory and disk capacity required on a monitor machine

The memory and disk space requirements differ between monitor machines, due to the different monitoring ranges and settings of each operator.

These values vary widely depending on how JP1/IM is set up. The settings that have the most significant effect on memory and disk usage by JP1/IM - View are as follows. For details on the other settings, see the JP1/IM - View *Release Notes*.

- Settings that significantly affect memory usage:
    - Scroll buffer size
    - Number of monitoring nodes
- Settings that significantly affect disk space usage:
    - Number of monitoring nodes
    - Saving event list information (CSV snapshot)#
      #: The amount of disk space used increases with each additional monitoring log saved.

Appendixes

A. Files and Directories

This appendix lists the names of the files and directories used by JP1/IM.

This appendix does not cover the JP1/IM files that you need to back up when changing system settings, or the log files output by JP1/IM. For details on these files, see the following:

- Information about files to back up: See *1.1 Managing the configuration information* in the *JP1/Integrated Management - Manager Administration Guide*.
- Information about log files: See *10.2.4 Log files and directory list* in the *JP1/Integrated Management - Manager Administration Guide*.

In the case of a logical host, the path notation used in the following tables is described in the table below.

Table A–1: Files and folders (or directories) on the shared disk

OS	Internal component	Path notation in the following tables	File or folder (directory) on the shared disk
Windows	Central Console	*console-path*`\conf\`	*shared-folder*`\JP1Cons\conf\`
		console-path`\log\`	*shared-folder*`\JP1Cons\log\`
		console-path`\tmp\`	*shared-folder*`\JP1Cons\tmp\`
		console-path`\operation\`	*shared-folder*`\JP1Cons\operation\`
	Central Scope	*scope-path*`\conf\`	*shared-folder*`\JP1Scope\conf\`
		scope-path`\log\`	*shared-folder*`\JP1Scope\log\`
		scope-path`\tmp\`	*shared-folder*`\JP1Scope\tmp\`
		scope-path`\database\`	*shared-folder*`\JP1Scope\database\`
	IM Configuration Management	*manager-path*`\conf\`	*shared-folder*`\JP1IMM\conf\imcf\`
		manager-path`\log\`	*shared-folder*`\JP1IMM\log\imcf\`
		manager-path`\tmp\`	*shared-folder*`\JP1IMM\tmp\`
UNIX	Central Console	`/etc/opt/jp1cons/conf/`	*shared-directory*`/jp1cons/conf/`
		`/var/opt/jp1cons/log/`	*shared-directory*`/jp1cons/log/`
		`/var/opt/jp1cons/tmp/`	*shared-directory*`/jp1cons/tmp/`
		`/var/opt/jp1cons/operation/`	*shared-directory*`/jp1cons/operation/`
	Central Scope	`/etc/opt/jp1scope/conf/`	*shared-directory*`/jp1scope/conf/`
		`/var/opt/jp1scope/log/`	*shared-directory*`/jp1scope/log/`
		`/var/opt/jp1scope/tmp/`	*shared-directory*`/jp1scope/tmp/`
		`/var/opt/jp1scope/database/`	*shared-directory*`/jp1scope/database/`
	IM Configuration Management	`/etc/opt/jp1imm/conf/`	*shared-directory*`/jp1imm/conf/imcf/`
		`/var/opt/jp1imm/log/`	*shared-directory*`/jp1imm/log/imcf/`
		`/var/opt/jp1imm/tmp/`	*shared-directory*`/jp1imm/tmp/`

For a logical host, read *console-path*`\conf\` as *shared-folder*`\JP1Cons\conf`. For example, *console-path*`\conf\action\actdef.conf` will be *shared-folder*`\JP1Cons\conf\action\actdef.conf`.

For details on the files and directories used by JP1/IM - EG for NNMi, see the manual *Job Management Partner 1/ Integrated Management - Event Gateway for Network Node Manager i Description, User's Guide and Reference*.

A.1 Files and folders of JP1/IM - Manager (for Windows)

This appendix lists the names of the files and folders used by JP1/IM - Manager (for Windows).

(1) JP1/IM - Manager (common to all components)

The tables below show the names of the files and folders used by JP1/IM - Manager (all components). *Ref.* in the tables has the following meaning:

- *Ref.* for a folder: The act of checking what the folder contains
- *Ref.* for a file: The act of opening the file and checking its contents

Table A–2: Files and folders that can be referenced and edited by the user (Windows version of JP1/IM - Manager (all components))

File or folder name	Description	Ref.	Edit
manager-path`\conf\imm_operationlog.conf`	Operation log definition file	Y	Y
manager-path`\conf\imm_operationlog.conf.model`	Model file for the operation log definition file	Y	N
manager-path`\tools\jim_log.bat`	Data collection tool	Y	N

Legend:
Y: Can be performed.
N: Cannot be performed.

Table A–3: Files and folders that do not need to be referenced or edited (Windows version of JP1/IM - Manager (all components))

Folder name	Description
manager-path`\bin\`	Folder for commands
manager-path`\conf\`	Folder for environment settings files
manager-path`\log\`	Log folder
manager-path`\tools\`	Files and folders in the tools folder other than those in the list of files and folders that can be referenced and edited by the user
manager-path`\PATCHLOG.txt`	Patch log file
manager-path`\patch_backup_dir\`	Files and folders in the patch backup folder other than patch utilities mentioned in the patch `RELEASE.TXT`. (This folder is created only when applying a patch.)
system-drive`:\Program Files\jp1common\`#	Folder for program information

#: When the OS is Windows Server 2016, Windows 10, Windows 8.1, Windows 8, Windows Server 2012, Windows 7, or Windows Server 2008 R2, the folder name *system-drive*`:\Program Files` might vary depending on OS environment settings made at the time of installation.

(2) JP1/IM - Manager (Central Console)

The tables below describe the names of the files and folders used by the Windows version of JP1/IM - Manager (Central Console). *Ref.* in the tables has the following meaning:

- *Ref.* for a folder: The act of checking what the folder contains
- *Ref.* for a file: The act of opening the file and checking its contents

Table A–4: Files and folders that can be referenced and edited by the user (Windows version of JP1/IM - Manager (Central Console))

File or folder name	Description	Ref.	Edit
console-path`\bin\`	Folder for commands	Y	N
console-path`\conf\`	Folder for environment settings files	Y	N
console-path`\conf\jp1co_param_V7.conf`	IM parameter definition file	Y	Y
console-path`\conf\jp1co_param_V7.conf.model`	Model IM parameter definition file	Y	N
console-path`\conf\jp1co_service.conf`	Extended startup process definition file	Y	Δ
console-path`\conf\action\actdef.conf`	Automated action definition file	Y	Y
console-path`\conf\action\actnotice.conf`	Automatic action notification definition file	Y	Y
console-path`\conf\action\actnotice.conf.model`	Model automatic action notification definition file	Y	N
console-path`\conf\chsev\jcochsev.conf`	Severity changing definition file	Y	Y
console-path`\conf\chsev\jcochsev.conf.model`	Model Severity changing definition file	Y	N#1
console-path`\conf\mail\jimmail.conf`	Email environment definition file	Y	Y
console-path`\conf\mail\jimmail.conf.model`	Model file for the email environment definition file	Y	N
console-path`\conf\action\event_info_replace.conf`	Configuration file for converting information	Y	Y#2
console-path`\conf\action\attr_list\attr_list.conf`	File that defines which items are displayed for event conditions	Y	Y
console-path`\conf\action\attr_list\attr_list.conf.model`	Model file that defines which items are displayed for event conditions	Y	N
console-path`\conf\action\actdef.conf.model`	Model automated action definition file	Y	N#1
console-path`\conf\console\attribute\`*company-name_product-name*`_attr_en.conf`	Definition file for extended event attributes	Y	Y#2
console-path`\conf\console\attribute\extend`	Folder for definition files for extended event attributes (extended file)	Y	N
console-path`\conf\console\attribute\extend\template_extend_attr_ja.conf`	Definition file for extended event attributes (extended file) for the Japanese language	Y	Y#3
console-path`\conf\console\attribute\extend\template_extend_attr_ja.conf.model`	Model file that defines extended event attributes (extended file) for the Japanese language	Y	N
console-path`\conf\console\attribute\extend\template_extend_attr_en.conf`	Definition file for extended event attributes (extended file) for the English language	Y	Y#3

File or folder name	Description	Ref.	Edit
console-path`\conf\console\attribute\extend\template_extend_attr_en.conf.model`	Model file that defines extended event attributes (extended file) for the English language	Y	N
console-path`\conf\console\attribute\extend\template_extend_attr_zh.conf`	Definition file for extended event attributes (extended file) for the Chinese language	Y	Y#3
console-path`\conf\console\attribute\extend\template_extend_attr_zh.conf.model`	Model file that defines extended event attributes (extended file) for the Chinese language	Y	N
console-path`\conf\console\filter\attr_list\`	Folder for the common-exclusion-conditions display item definition file	Y	N
console-path`\conf\console\filter\attr_list\common_exclude_filter_attr_list.conf`	Common-exclusion-conditions display item definition file	Y	Y
console-path`\conf\console\filter\attr_list\common_exclude_filter_attr_list.conf.model`	Model file for the common-exclusion-conditions display item definition file	Y	N#1
console-path`\conf\console\filter\out_list\common_exclude_filter_auto_list.conf`	Common-exclusion-conditions auto-input definition file	Y	Y
console-path`\conf\console\filter\out_list\common_exclude_filter_auto_list.conf.model`	Model file for the common-exclusion-conditions auto-input definition file	Y	N
console-path`\conf\console\incident\incident.conf`	Definition file for manually registering incidents	Y	Y
console-path`\conf\console\incident\incident.conf.model`	Model file for the incident manual-registration definition file	Y	N
console-path`\conf\console\incident\incident_info.conf`	Configuration file for incident inheritance information	Y	Y
console-path`\conf\console\incident\incident_info.conf.model`	Model file for the configuration file for incident inheritance information	Y	N
console-path`\conf\console\monitor\`*company-name_productname*`_mon.conf`	Definition file for opening monitor windows	Y	Y#2
console-path`\conf\console\object_type\`*company-name_product-name*`_obj.en`	Definition file for object types	Y	Y#2
console-path`\conf\console\performance\performance.conf`	Performance report display definition file	Y	Y
console-path`\conf\console\performance\performance.conf.model`	Model file for the performance report display definition file	Y	N
console-path`\conf\console\profile\.system`	System profile	Y	Δ
console-path`\conf\console\profile\.system.model`	Model file for the system profile	Y	N
console-path`\conf\console\profile\defaultUser`	Default user profile	Y	Δ
console-path`\conf\console\profile\defaultUser.model`	Model file for the default user profile	Y	N
console-path`\conf\console\profile\systemColor.conf`	System color definition file	Y	Y
console-path`\conf\console\profile\systemColor.conf.model`	Model file for the system color definition file	Y	N#1

File or folder name	Description	Ref.	Edit
console-path`\conf\console\profile\profile_`*user-name*	User profile for a specific JP1 user	Y	Δ
console-path`\conf\console\rmtcmd\`	Folder for remote command definitions	Y	N
console-path`\conf\console\rmtcmd\cmdbtn.conf`	Command button definition file	Y	Y
console-path`\conf\console\rmtcmd\cmdbtn.conf.model`	Model file for the command button definition file	Y	N#1
user-specified-folder`\`*file-name*`.conf`	Correlation event generation definition file	Y	Y#2
console-path`\conf\evgen\profile\egs_system.conf`	Correlation event generation system profile	Y	Y
console-path`\conf\evgen\profile\egs_system.conf.model`	Model file for the correlation event generation system profile	Y	N#1
console-path`\conf\console\event_storm\attr_list\event_storm_attr_list.conf`	Display item definition file for the repeated event condition	Y	Y
console-path`\conf\console\event_storm\attr_list\event_storm_attr_list.conf.model`	Model file for the display item definition file for the repeated event condition	Y	N#1
console-path`\conf\console\event_storm\auto_list\event_storm_auto_list.conf`	Auto-input definition file for the repeated event condition	Y	Y
console-path`\conf\console\event_storm\auto_list\event_storm_auto_list.conf.model`	Model file for the auto-input definition file for the repeated event condition	Y	N
console-path`\conf\guide\jco_guide.txt`	Event guide information file	Y	Y#1
console-path`\conf\guide\sample_jco_guide_ja.txt`	Sample event guide information file (Japanese)	Y	N
console-path`\conf\guide\sample_jco_guide_en.txt`	Sample event guide information file (English)	Y	N
console-path`\conf\guide\sample_jco_guide_ja.txt.model`	Model file for the event guide information samples (Japanese)	Y	N
console-path`\conf\guide\sample_jco_guide_en.txt.model`	Model file for the event guide information samples (English)	Y	N
console-path`\conf\health\jcohc.conf`	Health check definition file	Y	Y
console-path`\conf\health\jcohc.conf.model`	Model health check definition file	Y	N
console-path`\conf\hostmap\user_hostmap.conf`	Event-source-host mapping definition file	Y	Y
console-path`\conf\hostmap\user_hostmap.conf.model`	Model file for the event-source-host mapping definition file	Y	N#1
console-path`\conf\processupdate\processupdate.conf`	Status event definition file	Y	Y
console-path`\conf\processupdate\processupdate.conf.model`	Model status event definition file	Y	N
console-path`\default`	Common definitions folder	Y	N
console-path`\default\action.conf.update`	Model automated action environment definition file	Y	N#1

File or folder name	Description	Ref.	Edit
console-path`\default\console.conf.update`	Model communication environment definition file	Y	N#1
user-specified-folder\file-name	Correlation event generation environment definition file	Y	Y#2
console-path`\operation\`	Folder for the operation log	Y	N
console-path`\operation\evgen\egs_discrim{1|2|3}.log`	Correlation event generation history files	Y	N
console-path`\operation\comexclude\comexclude{1|2|3|4|5}.log`	Common exclusion history file	Y	N
console-path`\operation\comexclude\comexcludeDef{1|2|3|4|5}.log`	Common exclusion-conditions definition history file	Y	N
console-path`\www\`	Web-based folder	Y	N
console-path`\www\console_ja.html`	Web-based operation definition file (Japanese)	Y	Δ
console-path`\www\console_ja.html.model`	Model file for the web-based operation definition file for plug-in free mode (Japanese)	Y	N
console-path`\www\plugin\console_ja.html.model.plugin`	Model file for the web-based operation definition file for compatibility mode (Japanese)	Y	N
console-path`\www\console.html`	Web-based operation definition file (English)	Y	Δ
console-path`\www\console.html.model`	Model file for the web-based operation definition file for plug-in free mode (English)	Y	N
console-path`\www\plugin\console.html.model.plugin`	Model file for the web-based operation definition file for compatibility mode (English)	Y	N
console-path`\www\console_zh.html`	Web-based operation definition file (Chinese)	Y	Δ
console-path`\www\console_zh.html.model`	Model file for the web-based operation definition file for plug-in free mode (Chinese)	Y	N
console-path`\www\plugin\console_zh.html.model.plugin`	Model file for the Web-based operation definition file for compatibility mode (Chinese)	Y	N
console-path`\www\console_ja.jnlp`	Web-based startup definition file (Japanese)	Y	Δ
console-path`\www\console_ja.jnlp.model`	Model file for the web-based startup definition file (Japanese)	Y	N
console-path`\www\console.jnlp`	Web-based startup definition file (English)	Y	Δ
console-path`\www\console.jnlp.model`	Model file for the web-based startup definition file (English)	Y	N
console-path`\www\console_zh.jnlp`	Web-based startup definition file (Chinese)	Y	Δ

File or folder name	Description	Ref.	Edit
console-path`\www\console_zh.jnlp.model`	Model file for the web-based startup definition file (Chinese)	Y	N

Legend:

Y: Can be performed.

Δ: Can be partially edited.

N: Cannot be performed.

#1: Use a copy of this file

#2: The following files must be added by the user after JP1/IM - Manager is installed: Configuration file for converting information, definition file for extended event attributes, definition file for objects types, definition file for opening monitor windows, correlation event generation definition file, and correlation event generation environment definition file. For details about the definition file for extended event attributes, definition file for objects types, and definition file for opening monitor windows, see *Definition file for opening monitor windows* in *Chapter 2. Definition Files* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*. For details about the last two files, see the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

#3: When you use the file, delete `template_` from the beginning of the file name.

Table A–5: Files and folders that do not need to be referenced or edited (Windows version of JP1/IM - Manager (Central Console))

Folder name	Description
console-path`\conf\`	Files and folders in the folder for environment settings files other than those in the list of files and folders that can be referenced and edited by the user
console-path`\classes\`	Folder for class files
console-path`\default\`	Files and folders in the common definitions folder other than those in the list of files and folders that can be referenced and edited by the user
console-path`\lib\`	Libraries folder
console-path`\log\`	Logs folder
console-path`\operation\`	Files and folders in the folder for the operation log other than those in the list of files and folders that can be referenced and edited by the user
console-path`\system\`	Folder for Windows initialization files
console-path`\tmp\`	Work folder
console-path`\tools\`	Tools folder
console-path`\www\`	Files and folders in the Web-based folder other than those in the list of files and folders that can be referenced and edited by the user

(3) JP1/IM - Manager (Central Scope)

The tables below describe the names of the files and folders used by the Windows version of JP1/IM - Manager (Central Scope). *Ref.* in the tables has the following meaning:

- *Ref.* for a folder: The act of checking what the folder contains
- *Ref.* for a file: The act of opening the file and checking its contents

Table A–6: Files and folders that can be referenced and edited by the user (Windows version of JP1/IM - Manager (Central Scope))

File or folder name	Description	Ref.	Edit
scope-path`\bin\`	Folder for commands	Y	N

File or folder name	Description	Ref.	Edit
scope-path\conf\action_complete_on.conf *scope-path*\conf\action_complete_off.conf	Settings files for the completed-action linkage function	Y	Y
scope-path\conf\action_complete_on.conf.model *scope-path*\conf\action_complete_off.conf.model	Model settings files for the completed-action linkage function	Y	N
scope-path\conf\auto_dbbackup_on.conf *scope-path*\conf\auto_dbbackup_off.conf	Settings files for automatic backup and recovery of the monitoring object database	Y	Y
scope-path\conf\auto_dbbackup_on.conf.model *scope-path*\conf\auto_dbbackup_off.conf.model	Model settings files for automatic backup and recovery of the monitoring object database	Y	N
scope-path\conf\evhist_warn_event_on.conf *scope-path*\conf\evhist_warn_event_off.conf	Settings files for the maximum number of status change events	Y	Y
scope-path\conf\evhist_warn_event_on.conf.model *scope-path*\conf\evhist_warn_event_off.conf.model	Model settings files for the maximum number of status change events	Y	N
scope-path\conf\guide\	Folder for guide-message files	Y	N
scope-path\conf\jcs_guide_sjis.txt *scope-path*\conf\jcs_guide.txt *scope-path*\conf\jcs_guide_GB18030.txt#	Model guide information files	Y	Y
scope-path\conf\jcs_guide_sjis.txt.model *scope-path*\conf\jcs_guide.txt.model	Model guide information files	Y	N
scope-path\conf\jcs_hosts	Host information file	Y	Y
scope-path\conf\jcs_hosts.model	Model host information file	Y	N
scope-path\conf\jcs_sysprofile_sjis.def *scope-path*\conf\jcs_sysprofile.def *scope-path*\conf\jcs_sysprofile_GB18030.def	Central Scope system profiles	Y	Y
scope-path\conf\jcs_sysprofile_sjis.def.model *scope-path*\conf\jcs_sysprofile.def.model *scope-path*\conf\jcs_sysprofile_GB18030.def.model	Model files for the Central Scope system profiles	Y	N
scope-path\conf\snmpfilter_im_sample.conf	Sample filter definition file for SNMP trap converter (used only when linking with HP NNM version 7.5 or earlier or JP1/Cm2/SSO version 8 or earlier)	Y	N

File or folder name	Description	Ref.	Edit
scope-path`\database\`	Folder for ISAM files	Y	N
scope-path`\database\jcsdb\`	Folder for the monitoring object database	Y	N
scope-path`\database\jcshosts\`	Folder for the host information database	Y	N
scope-path`\sample\`	Sample folder	Y	N
scope-path`\sample\guide\jcs_guide_html_sample_sjis.txt`	Samples of HTML guide information	Y	N
scope-path`\sample\guide\exfile\jcs_guide_html_sample_sjis001.txt`			
scope-path`\sample\guide\exfile\jcs_guide_html_sample.txt`			
scope-path`\sample\guide\exfile\jcs_guide_html_sample001.txt`			

Legend:

Y: Can be performed.

N: Cannot be performed.

#: The user must create this file manually; it is not created automatically during installation.

Table A–7: Files and folders that do not need to be referenced or edited (Windows version of JP1/IM - Manager (Central Scope))

File or folder name	Description
scope-path`\conf\`	Files and folders in the folder for environment settings files other than those in the list of files and folders that can be referenced and edited by the user
scope-path`\database\event\`	Work folder for event collation processing
scope-path`\default\`	Common definitions folder
scope-path`\log\`	Logs folder
scope-path`\system\`	Folder for Windows initialization files
scope-path`\tmp\`	Work folder
scope-path`\tools\`	Tools folder

(4) JP1/IM - Manager (IM Configuration Management)

The tables below describe the names of the files and folders used by the Windows version of JP1/IM - Manager (IM Configuration Management). *Ref.* in the tables has the following meaning:

- *Ref.* for a folder: The act of checking what the folder contains
- *Ref.* for a file: The act of opening the file and checking its contents

Table A–8: Files and folders that can be referenced and edited by the user (Windows version of JP1/IM - Manager (IM Configuration Management))

File or folder name	Description	Ref.	Edit
manager-path`\bin\`	Folder for commands	Y	N

File or folder name	Description	Re f.	Ed it
manager-path\conf\imcf\jp1cf_applyconfig.conf	Apply-IM-configuration-method definition file	Y	Y
manager-path\conf\imcf\jp1cf_applyconfig.conf.model	Model file for the apply-IM-configuration-method definition file	Y	N
manager-path\conf\imcf\jp1cf_profile_manager.conf	Profile management environment definition file	Y	Y
manager-path\conf\imcf\jp1cf_profile_manager.conf.model	Model file for the profile management environment definition file	Y	N
manager-path\conf\imcf\jp1cf_remote_logtrap.conf	Remote log trap environment definition file	Y	Y
manager-path\conf\imcf\jp1cf_remote_logtrap.conf.model	Model file for the remote log trap environment definition file	Y	N

Legend:

Y: Can be performed.

N: Cannot be performed.

Table A–9: Files and folders that do not need to be referenced or edited (Windows version of JP1/IM - Manager (IM Configuration Management))

File or folder name	Description
manager-path\conf\	Files and folders in the folder for environment settings files other than those in the list of files and folders that can be referenced and edited by the user
manager-path\conf\imcf\const\ppinfotemplate.conf	Product information template file
manager-path\conf\imcf\const\ppinfotemplate.conf.update	Product information template update file
manager-path\conf\imcf\const\profile_list0708.csv	Profile list template file
manager-path\conf\imcf\const\profile_listEuropa.csv	
manager-path\conf\imcf\const\jp1base_profile_type_en.csv	Profile type file
manager-path\conf\imcf\const\jp1base_profile_type_jp.csv	
manager-path\conf\imcf\const\jp1base_opiTagList_en.csv	Profile tag list file
manager-path\conf\imcf\const\jp1base_opiTagList_jp.csv	
manager-path\system\default\	Common definitions folder
manager-path\data\	Profile data
manager-path\log\	Logs folder
manager-path\tmp\	Work folder
manager-path\lib\	Libraries folder

A.2 Files and directories of JP1/IM - Manager (for UNIX)

This appendix lists the names of the files and directories used by JP1/IM - Manager (for UNIX).

(1) JP1/IM - Manager (common to all components)

The tables below describe the names of the files and directories used by JP1/IM - Manager (all components). *Ref.* in the tables has the following meaning:

- *Ref.* for a directory: The act of checking what the directory contains
- *Ref.* for a file: The act of opening the file and checking its contents

Table A–10: Files and directories that can be referenced and edited by the user (UNIX version of JP1/IM - Manager (all components))

File or directory name	Description	Ref.	Edit
/etc/opt/jp1imm/conf/imm_operationlog.conf	Operation log definition file	Y	Y
/etc/opt/jp1imm/conf/imm_operationlog.conf.model	Model file for the operation log definition file	Y	N
/opt/jp1imm/tools/jim_log.sh	Data collection tool	Y	N

Legend:

Y: Can be performed.

N: Cannot be performed.

Table A–11: Files and directories that do not need to be referenced or edited (UNIX version of JP1/IM - Manager (all components))

Directory name	Description
/opt/jp1imm/tools/	Files and directories in the tools directory other than those in the list of files and directories that can be referenced and edited by the user
/opt/jp1imm/patch_backup_dir/	Files and directories in the patch backup directory other than patch utilities mentioned in the patch RELEASE.TXT or RELEASE.EUC. (This directory is created only when applying a patch.)
/opt/jp1imm/update.log	Update log file
/opt/jp1imm/patch_history	Patch history file
/var/opt/jp1imm/log/	Logs directory

(2) JP1/IM - Manager (Central Console)

The tables below describe the names of the files and directories used by the UNIX version of JP1/IM - Manager (Central Console). *Ref.* in the tables has the following meaning:

- *Ref.* for a directory: The act of checking what the directory contains
- *Ref.* for a file: The act of opening the file and checking its contents

Table A–12: Files and directories that can be referenced and edited by the user (UNIX version of JP1/IM - Manager (Central Console))

File or directory name	Description	Ref.	Edit
`/etc/opt/jp1cons/jco_start`	Script for starting JP1/IM - Manager automatically	Y	Δ#4
`/etc/opt/jp1cons/jco_start.model`	Model script file for starting JP1/IM - Manager automatically	Y	N#1
`/etc/opt/jp1cons/jco_stop`	Script for stopping JP1/IM - Manager automatically	Y	N#1
`/etc/opt/jp1cons/jco_stop.model`	Model script file for stopping JP1/IM - Manager automatically	Y	N
`/etc/opt/jp1cons/jco_start.cluster`	Script for starting JP1/IM - Manager on a logical host	Y	N
`/etc/opt/jp1cons/jco_stop.cluster`	Script for stopping JP1/IM - Manager on a logical host	Y	N
`/etc/opt/jp1cons/jco_killall.cluster`	Script for forcibly ending JP1/IM - Manager processes in a cluster system	Y	N
`/etc/opt/jp1cons/conf/`	Directory for environment settings files	Y	N
`/etc/opt/jp1cons/conf/jp1co_env.conf`	IM environment definition file	Y	Y
`/etc/opt/jp1cons/conf/jp1co_service.conf`	Extended startup process definition file	Y	Δ
`/etc/opt/jp1cons/conf/jp1co_param_V7.conf`	IM parameter definition file	Y	Y
`/etc/opt/jp1cons/conf/jp1co_param_V7.conf.model`	Model IM parameter definition file	Y	N
`/etc/opt/jp1cons/conf/action/actdef.conf`	Automated action definition file	Y	Y
`/etc/opt/jp1cons/conf/action/actnotice.conf`	Automatic action notification definition file	Y	Y
`/etc/opt/jp1cons/conf/action/actnotice.conf.model`	Model automatic action notification definition file	Y	N
`/etc/opt/jp1cons/conf/chsev/jcochsev.conf`	Severity changing definition file	Y	Y
`/etc/opt/jp1cons/conf/chsev/jcochsev.conf.model`	Model Severity changing definition file	Y	N#1
`/etc/opt/jp1cons/conf/action/event_info_replace.conf`	Configuration file for converting information	Y	Y#2
`/etc/opt/jp1cons/conf/action/attr_list/attr_list.conf`	File that defines which items are displayed for event conditions	Y	Y
`/etc/opt/jp1cons/conf/action/attr_list/attr_list.conf.model`	Model of file that defines which items are displayed for event conditions	Y	N
`/etc/opt/jp1cons/conf/action/actdef.conf.model`	Model automated action definition file	Y	N#1
`/etc/opt/jp1cons/conf/console/attribute/`*company-name_product-name*`_attr_en.conf`	Definition file for extended event attributes	Y	Y#2

File or directory name	Description	Ref.	Edit
`/etc/opt/jp1cons/conf/console/attribute/extend`	Folder for definition files for extended event attributes (extended file)	Y	N
`/etc/opt/jp1cons/conf/console/attribute/extend/template_extend_attr_ja.conf`	Definition file for extended event attributes (extended file) for the Japanese language	Y	Y#3
`/etc/opt/jp1cons/conf/console/attribute/extend/template_extend_attr_ja.conf.model`	Model file that defines extended event attributes (extended file) for the Japanese language	Y	N
`/etc/opt/jp1cons/conf/console/attribute/extend/template_extend_attr_en.conf`	Definition file for extended event attributes (extended file) for the English language	Y	Y#3
`/etc/opt/jp1cons/conf/console/attribute/extend/template_extend_attr_en.conf.model`	Model file that defines extended event attributes (extended file) for the English language	Y	N
`/etc/opt/jp1cons/conf/console/attribute/extend/template_extend_attr_zh.conf`	Definition file for extended event attributes (extended file) for the Chinese language	Y	Y#3
`/etc/opt/jp1cons/conf/console/attribute/extend/template_extend_attr_zh.conf.model`	Model file that defines extended event attributes (extended file) for the Chinese language	Y	N
`/etc/opt/jp1cons/conf/console/filter/attr_list`	Directory for the common-exclusion-conditions display item definition file	Y	N
`/etc/opt/jp1cons/conf/console/filter/attr_list/common_exclude_filter_attr_list.conf`	Common-exclusion-conditions display item definition file	Y	Y
`/etc/opt/jp1cons/conf/console/filter/attr_list/common_exclude_filter_attr_list.conf.model`	Model file for the common-exclusion-conditions display item definition file	Y	N#1
`/etc/opt/jp1cons/conf/console/filter/auto_list/common_exclude_filter_auto_list.conf`	Common-exclusion-conditions auto-input definition file	Y	Y
`/etc/opt/jp1cons/conf/console/filter/auto_list/common_exclude_filter_auto_list.conf.model`	Model file for the common-exclusion-conditions auto-input definition file	Y	N
`/etc/opt/jp1cons/conf/console/incident/incident.conf`	Incident manual-registration definition file	Y	Y
`/etc/opt/jp1cons/conf/console/incident/incident.conf.model`	Model file for the incident manual-registration definition file	Y	N
`/etc/opt/jp1cons/conf/console/incident/incident_info.conf`	Configuration file for incident inheritance information	Y	Y
`/etc/opt/jp1cons/conf/console/incident/incident_info.conf.model`	Model file for the configuration file for incident inheritance information	Y	N
`/etc/opt/jp1cons/conf/console/monitor/`*company-name_product-name*`_mon.conf`	Definition file for opening monitor windows	Y	Y#2
`/etc/opt/jp1cons/conf/console/object_type/`*company-name_product-name*`_obj.en`	Definition file for object types	Y	Y#2
`/etc/opt/jp1cons/conf/console/performance/performance.conf`	Performance report display definition file	Y	Y

File or directory name	Description	Ref.	Edit
`/etc/opt/jp1cons/conf/console/performance/performance.conf.model`	Model file for the performance report display definition file	Y	N
`/etc/opt/jp1cons/conf/console/profile/.system`	System profile	Y	Δ
`/etc/opt/jp1cons/conf/console/profile/.system.model`	Model file for the system profile	Y	N
`/etc/opt/jp1cons/conf/console/profile/defaultUser`	Default user profile	Y	Δ
`/etc/opt/jp1cons/conf/console/profile/defaultUser.model`	Model file for the default user profile	Y	N
`/etc/opt/jp1cons/conf/console/profile/systemColor.conf`	System color definition file	Y	Y
`/etc/opt/jp1cons/conf/console/profile/systemColor.conf.model`	Model file for the system color definition file	Y	N[#1]
`/etc/opt/jp1cons/conf/console/profile/profile_`*user-name*	User profile for a specific JP1 user	Y	Δ
`/etc/opt/jp1cons/conf/console/rmtcmd/`	Directory for remote command definitions	Y	N
`/etc/opt/jp1cons/conf/console/rmtcmd/cmdbtn.conf`	Command button definition file	Y	Y
`/etc/opt/jp1cons/conf/console/rmtcmd/cmdbtn.conf.model`	**Model file for the command button definition file**	**Y**	**N[#1]**
user-specified-directory / *file-name* `.conf`	Correlation event generation definition file	Y	Y[#2]
`/etc/opt/jp1cons/conf/evgen/profile/egs_system.conf`	Correlation event generation system profile	Y	Y
`/etc/opt/jp1cons/conf/evgen/profile/egs_system.conf.model`	Model file for the correlation event generation system profile	Y	N[#1]
`/etc/opt/jp1cons/conf/console/event_storm/attr_list/event_storm_attr_list.conf`	Display item definition file for the repeated event condition	Y	Y
`/etc/opt/jp1cons/conf/event_storm/attr_list/event_storm_attr_list.conf.model`	Model file for the display item definition file for the repeated event condition	Y	N[#1]
`/etc/opt/jp1cons/conf/console/event_storm/auto_list/event_storm_auto_list.conf`	Auto-input definition file for the repeated event condition	Y	Y
`/etc/opt/jp1cons/conf/console/event_storm/auto_list/event_storm_auto_list.conf.model`	Model file for the auto-input definition file for the repeated event condition	Y	N
`/etc/opt/jp1cons/conf/guide/jco_guide.txt`	Event guide information file	Y	Y[#1]
`/etc/opt/jp1cons/conf/guide/sample_jco_guide_ja.txt`	Sample event guide information file (Japanese)	Y	N
`/etc/opt/jp1cons/conf/guide/sample_jco_guide_en.txt`	Sample event guide information file (English)	Y	N
`/etc/opt/jp1cons/conf/guide/sample_jco_guide_ja.txt.model`	Model file for the event guide information samples (Japanese)	Y	N
`/etc/opt/jp1cons/conf/guide/sample_jco_guide_en.txt.model`	Model file for the event guide information samples (English)	Y	N
`/etc/opt/jp1cons/conf/processupdate/processupdate.conf`	Status event definition file	Y	Y

File or directory name	Description	Ref.	Edit
`/etc/opt/jp1cons/conf/processupdate/processupdate.conf.model`	Model status event definition file	Y	N
`/etc/opt/jp1cons/default/`	Common definitions directory	Y	N
`/etc/opt/jp1cons/default/action.conf.update`	Model automated action environment definition file	Y	N#1
`/etc/opt/jp1cons/default/console.conf.update`	Model communication environment definition file	Y	N#1
user-specified-directory/*file-name*	Correlation event generation environment definition file	Y	Y#2
`/etc/opt/jp1cons/conf/health/jcohc.conf`	Health check definition file	Y	Y
`/etc/opt/jp1cons/conf/hostmap/user_hostmap.conf`	Event-source-host mapping definition file	Y	Y
`/etc/opt/jp1cons/conf/hostmap/user_hostmap.conf.model`	Model file for the event-source-host mapping definition file	Y	N#1
`/etc/opt/jp1cons/conf/health/jcohc.conf.model`	Model health check definition file	Y	N
`/opt/jp1cons/bin/`	Commands directory	Y	N
`/opt/jp1cons/tools/`	Tools directory	Y	N
`/opt/jp1cons/www/`	Web-based directory	Y	N
`/opt/jp1cons/www/console_ja.html`	Web-based operation definition file (Japanese)	Y	Δ
`/opt/jp1cons/www/console_ja.html.model`	Model file for the web-based operation definition file for plug-in free mode (Japanese)	Y	N
`/opt/jp1cons/www/plugin/console_ja.html.model.plugin`	Model file for the web-based operation definition file for compatibility mode (Japanese)	Y	N
`/opt/jp1cons/www/console.html`	Web-based operation definition file (English)	Y	Δ
`/opt/jp1cons/www/console.html.model`	Model file for the web-based operation definition file for plug-in free mode (English)	Y	N
`/opt/jp1cons/www/plugin/console.html.model.plugin`	Model file for the web-based operation definition file for compatibility mode (English)	Y	N
`/opt/jp1cons/www/console_zh.html`	Web-based operation definition file (Chinese)	Y	Δ
`/opt/jp1cons/www/console_zh.html.model`	Model file for the web-based operation definition file for plug-in free mode (Chinese)	Y	N
`/opt/jp1cons/www/plugin/console_zh.html.model.plugin`	Model file for the Web-based operation definition file for compatibility mode (Chinese)	Y	N
`/opt/jp1cons/www/console_ja.jnlp`	Web-based startup definition file (Japanese)	Y	Δ

File or directory name	Description	Ref.	Edit
`/opt/jp1cons/www/console_ja.jnlp.model`	Model file for the web-based startup definition file (Japanese)	Y	N
`/opt/jp1cons/www/console.jnlp`	Web-based startup definition file (English)	Y	Δ
`/opt/jp1cons/www/console.jnlp.model`	Model file for the web-based startup definition file (English)	Y	N
`/opt/jp1cons/www/console_zh.jnlp`	Web-based startup definition file (Chinese)	Y	Δ
`/opt/jp1cons/www/console_zh.jnlp.model`	Model file for the web-based startup definition file (Chinese)	Y	N
`/var/opt/jp1cons/operation`	Operation log directory	Y	N
`/var/opt/jp1cons/operation/evgen/egs_discrim{1|2|3}.log`	Correlation event generation history files	Y	N
`/var/opt/jp1cons/operation/comexclude/comexclude{1|2|3|4|5}.log`	Common exclusion history file	Y	N
`/var/opt/jp1cons/operation/comexclude/comexcludeDef{1|2|3|4|5}.log`	Common exclusion-conditions definition history file	Y	N

Legend:

Y: Can be performed.

Δ: Can be partially edited.

N: Cannot be performed.

#1: Use a copy of this file.

#2: The following files must be added by the user after JP1/IM - Manager is installed: Definition file for the extended event attributes, definition file for objects types, definition file for opening monitor windows, correlation event generation definition file, and correlation event generation environment definition file. For details about the first three files, see *Definition file for opening monitor windows* in *Chapter 2. Definition Files* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*. For details about the last two files, see the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

#3: When you use the file, delete `template_` from the beginning of the file name.

#4: Only the lines containing the `LANG` environment variable and `ulimit -c unlimited` can be changed.

Table A–13: Files and directories that do not need to be referenced or edited (UNIX version of JP1/IM - Manager (Central Console))

Directory name	Description
`/etc/opt/jp1cons/conf/`	Files and directories in the directory for environment settings files other than those in the list of files and directories that can be referenced and edited by the user
`/etc/opt/jp1cons/default/`	Files and directories in the common definitions directory other than those in the list of files and directories that can be referenced and edited by the user
`/opt/jp1cons/tools/`	Tools directory
`/opt/jp1cons/classes/`	Directory for class files
`/opt/jp1cons/www/`	Files and directories in the Web-based directory other than those in the list of files and directories that can be referenced and edited by the user
`/opt/jp1cons/lib/`	Directory of library files
`/var/opt/jp1cons/log/`	Logs directory
`/var/opt/jp1cons/operation/`	Files and directories in the directory for the operation log other than those in the list of files and directories that can be referenced and edited by the user

Directory name	Description
/var/opt/jp1cons/tmp/	Work directory

(3) JP1/IM - Manager (Central Scope)

The tables below describe the names of the files and directories used by the UNIX version of JP1/IM - Manager (Central Scope). *Ref.* in the tables has the following meaning:

- *Ref.* for a directory: The act of checking what the directory contains
- *Ref.* for a file: The act of opening the file and checking its contents

Table A–14: Files and directories that can be referenced and edited by the user (UNIX version of JP1/IM - Manager (Central Scope))

File or directory name	Description	Ref.	Edit
/etc/opt/jp1scope/conf/action_complete_on.conf	Settings files for completed-action linkage function	Y	Y
/etc/opt/jp1scope/conf/action_complete_off.conf			
/etc/opt/jp1scope/conf/action_complete_on.conf.model	Model settings files for completed-action linkage function	Y	N
/etc/opt/jp1scope/conf/action_complete_off.conf.model			
/etc/opt/jp1scope/conf/auto_dbbackup_on.conf	Settings files for automatic backup and recovery of the monitoring object database	Y	Y
/etc/opt/jp1scope/conf/auto_dbbackup_off.conf			
/etc/opt/jp1scope/conf/auto_dbbackup_on.conf.model	Model settings files for automatic backup and recovery of the monitoring object database	Y	N
/etc/opt/jp1scope/conf/auto_dbbackup_off.conf.model			
/etc/opt/jp1scope/conf/evhist_warn_event_on.conf	Settings files for the maximum number of status change events	Y	Y
/etc/opt/jp1scope/conf/evhist_warn_event_off.conf			
/etc/opt/jp1scope/conf/evhist_warn_event_on.conf.model	Model settings files for the maximum number of status change events	Y	N
/etc/opt/jp1scope/conf/evhist_warn_event_off.conf.model			
/etc/opt/jp1scope/conf/jcs_guide_sjis.txt	Guide information files#1	Y	Y
/etc/opt/jp1scope/conf/jcs_guide_euc.txt			
/etc/opt/jp1scope/conf/jcs_guide_UTF-8.txt			
/etc/opt/jp1scope/conf/jcs_guide.txt			
/etc/opt/jp1scope/conf/jcs_guide_GB18030.txt#2			
/etc/opt/jp1scope/conf/jcs_guide_sjis.txt.model	Model guide information file#1	Y	N
/etc/opt/jp1scope/conf/jcs_guide_euc.txt.model			
/etc/opt/jp1scope/conf/jcs_guide_UTF-8.txt.model			
/etc/opt/jp1scope/conf/jcs_guide.txt.model			
/etc/opt/jp1scope/conf/jcs_hosts	Host information file	Y	Y

File or directory name	Description	Ref.	Edit
/etc/opt/jp1scope/conf/jcs_hosts.model	Model host information file	Y	N
/etc/opt/jp1scope/conf/jcs_sysprofile_sjis.def	Central Scope system profiles	Y	Y
/etc/opt/jp1scope/conf/jcs_sysprofile_euc.def			
/etc/opt/jp1scope/conf/jcs_sysprofile_UTF-8.def			
/etc/opt/jp1scope/conf/jcs_sysprofile.def			
/etc/opt/jp1scope/conf/jcs_sysprofile_GB18030.def			
/etc/opt/jp1scope/conf/jcs_sysprofile_sjis.def.model	Model files for the Central Scope system profiles	Y	N
/etc/opt/jp1scope/conf/jcs_sysprofile_euc.def.model			
/etc/opt/jp1scope/conf/jcs_sysprofile_UTF-8.def.model			
/etc/opt/jp1scope/conf/jcs_sysprofile.def.model			
/etc/opt/jp1scope/conf/jcs_sysprofile_GB18030.def.model			
/etc/opt/jp1scope/conf/snmpfilter_im_sample.conf	Sample filter definition file for SNMP trap converter (used only when linking with HP NNM version 7.5 or earlier or JP1/Cm2/SSO version 8 or earlier)	Y	N
/etc/opt/jp1scope/sample/	Sample directory	Y	N
/etc/opt/jp1scope/sample/guide/jcs_guide_html_sample_sjis.txt	Samples of HTML guide information#1	Y	N
/etc/opt/jp1scope/sample/guide/jcs_guide_html_sample_euc.txt			
/etc/opt/jp1scope/sample/guide/jcs_guide_html_sample_UTF-8.txt			
/etc/opt/jp1scope/sample/guide/jcs_guide_html_sample.txt			
/etc/opt/jp1scope/sample/guide/exfile/jcs_guide_html_sample_sjis001.txt			
/etc/opt/jp1scope/sample/guide/exfile/jcs_guide_html_sample_euc001.txt			
/etc/opt/jp1scope/sample/guide/exfile/jcs_guide_html_sample_UTF-8-001.txt			
/etc/opt/jp1scope/sample/guide/exfile/jcs_guide_html_sample001.txt			
/opt/jp1scope/bin/	Commands directory	Y	N
/opt/jp1scope/lib/	Directory of library files	Y	N
/opt/jp1scope/lib/$LANG	Message catalog	Y	N
/var/opt/jp1scope/log/JCS_SETUP/jcs_setup.log	Log file to be used at setup	Y	N

Legend:

Y: Can be performed.

N: Cannot be performed.

#1: Only the files for the locale supported by the OS are provided.

#2: The user must create this file manually; it is not created automatically during installation.

Table A–15: Files and directories that do not need to be referenced or edited (UNIX version of JP1/IM - Manager (Central Scope))

File or directory name	Description
`/etc/opt/jp1scope/conf/`	Files and directories in the directory for environment settings files other than those in the list of files and directories that can be referenced and edited by the user
`/etc/opt/jp1scope/default/`	Common definitions directory
`/opt/jp1scope/tools/`	Tools directory
`/var/opt/jp1scope/database/event/`	Work directory for event collation processing
`/var/opt/jp1scope/log/`	Files and directories in the logs directory other than those in the list of files and directories that can be referenced and edited by the user
`/var/opt/jp1scope/tmp/`	Work directory

(4) JP1/IM - Manager (IM Configuration Management)

The tables below describe the names of the files and directories used by the UNIX version of JP1/IM - Manager (IM Configuration Management). *Ref.* in the tables has the following meaning:

- *Ref.* for a directory: The act of checking what the directory contains
- *Ref.* for a file: The act of opening the file and checking its contents

Table A–16: Files and directories that can be referenced and edited by the user (UNIX version of JP1/IM - Manager (IM Configuration Management))

File or directory name	Description	Ref.	Edit
`/opt/jp1imm/bin/`	Commands directory	Y	N
`/etc/opt/jp1imm/conf/imcf/jp1cf_applyconfig.conf`	Apply-IM-configuration-method definition file	Y	Y
`/etc/opt/jp1imm/conf/imcf/jp1cf_applyconfig.conf.model`	Model file for the apply-IM-configuration-method definition file	Y	N
`/etc/opt/jp1imm/conf/imcf/jp1cf_profile_manager.conf`	Profile management environment definition file	Y	Y
`/etc/opt/jp1imm/conf/imcf/jp1cf_profile_manager.conf.model`	Model file for the profile management environment definition file	Y	N
`/etc/opt/jp1imm/conf/imcf/jp1cf_remote_logtrap.conf`	Remote log trap environment definition file	Y	Y
`/etc/opt/jp1imm/conf/imcf/jp1cf_remote_logtrap.conf.model`	Model file for the remote log trap environment definition file	Y	N

Legend:

Y: Can be performed.

N: Cannot be performed.

Table A–17: Files and folders that do not need to be referenced or edited (UNIX version of JP1/IM - Manager (IM Configuration Management))

File or directory name	Description
`/etc/opt/jp1imm/conf/`	Files and folders in the folder for environment settings files other than those in the list of files and folders that can be referenced and edited by the user
`/etc/opt/jp1imm/conf/imcf/const/ppinfotemplate.conf`	Product information template file
`/etc/opt/jp1imm/conf/imcf/const/ppinfotemplate.conf.update`	Product information template update file
`/etc/opt/jp1imm/conf/imcf/const/profile_list0708.csv`	Profile list template file
`/etc/opt/jp1imm/conf/imcf/const/profile_listEuropa.csv`	
`/etc/opt/jp1imm/conf/imcf/const/jp1base_profile_type_en.csv`	Profile list type file
`/etc/opt/jp1imm/conf/imcf/const/jp1base_profile_type_jp.csv`	
`/etc/opt/jp1imm/conf/imcf/const/jp1base_opiTagList_en.csv`	Profile tag list file
`/etc/opt/jp1imm/conf/imcf/const/jp1base_opiTagList_jp.csv`	
`/etc/opt/jp1imm/default/`	Common definitions directory
`/var/opt/jp1imm/data/`	Profile data
`/var/opt/jp1imm/log/`	Logs directory
`/var/opt/jp1imm/tmp/`	Work directory
`/opt/jp1imm/lib/`	Libraries directory

A.3 JP1/IM - View

This appendix lists the names of the files and folders used by JP1/IM - View.

The tables below describe the names of the files and folders used by JP1/IM - View. *Ref.* in the tables has the following meaning:

- *Ref.* for a folder: The act of checking what the folder contains
- *Ref.* for a file: The act of opening the file and checking its contents

Table A–18: Files and folders that can be referenced and edited by the user (JP1/IM - View)

File or folder name	Description	Ref.	Edit
view-path`\Version.txt`	`Version` file	Y	N
view-path`\ProductInfo.txt`	`ProductInfo` file	Y	N
view-path`\bin\`	Folder for commands	Y	N
view-path`\conf\`	Folder for definition files	Y	N

File or folder name	Description	Ref.	Edit
view-path`\conf\appexecute\en\`*company-name_product-name*`_app.conf`	Definition file for executing applications	Y	Y#1, #2
view-path`\conf\appexecute\en\!JP1_CC_APP0.conf.model`	Model definition file for executing applications	Y	N
view-path`\conf\function\en\`*company-name_product-name*`_tree.conf`	Definition file for the Tool Launcher window	Y	Y#1, #2
view-path`\conf\function\en\!JP1_CC_FTREE0.conf.model`	Model definition file for the Tool Launcher window	Y	N
view-path`\conf\tuning.conf`	IM-View settings file	Y	Y
view-path`\conf\tuning.conf.model`	Model IM-View settings file	Y	N
view-path`\conf\jcfview\jcfview.conf`	Operation definition file of the IM configuration management viewer	Y	Y
view-path`\conf\jcfview\jcfview.conf.model`	Model operation definition file of the IM configuration management viewer	Y	N
view-path`\conf\sovsystem\ja\system.conf`	Central Scope viewer system profiles	Y	Y
view-path`\conf\sovsystem\en\system.conf`			
view-path`\conf\sovsystem\zh\system.conf`			
view-path`\conf\sovsystem\ja\system.conf.model`	Model files for the Central Scope viewer system profiles	Y	N
view-path`\conf\sovsystem\en\system.conf.model`			
view-path`\conf\sovsystem\zh\system.conf.model`			
view-path`\conf\sovtoolexec\en\!JP1_CS_APP0.conf`	Start program definition file	Y	Y
view-path`\conf\sovtoolexec\en\!JP1_CS_APP0.conf.model`	Model start program definition file	Y	N
view-path`\conf\sovtoolitem\en\!JP1_CS_FTOOL0.conf`	Toolbar definition file	Y	Y
view-path`\conf\sovtoolitem\en\!JP1_CS_FTOOL0.conf.model`	Model toolbar definition file	Y	N
view-path`\conf\sovtoolitem\en\!JP1_CS_FTREE0.conf`	Icon operation definition file	Y	Y
view-path`\conf\sovtoolitem\en\!JP1_CS_FTREE0.conf.model`	Model icon operation definition file	Y	N
view-path`\conf\webdata\en\hitachi_jp1_`*product-name*`.html`	Web page call definition file	Y	Y
view-path`\conf\webdata\en\hitachi_jp1_`*product-name*`.html.model`	Model Web page call definition file	Y	N
view-path`\default\`	Common definitions folder	Y	N
view-path`\default\view.conf.update`	Model communication environment definition file	Y	N#1
view-path`\default\tree_view.conf.update`	Model communication environment definition file	Y	N#1
view-path`\image\icon\`	Icons folder	Y	Y
view-path`\image\visual\`#3	Visual icons folder	Y	Y
view-path`\image\map\`	Background images folder	Y	Y
view-path`\tools\`	Tools folder	Y	N

File or folder name	Description	Ref.	Edit
view-path\tools\jcoview_log.bat	Data collection tool	Y	N

Legend:

Y: Can be performed.

N: Cannot be performed.

#1: Use a copy of this file.

#2: The definition file for executing applications and definition file for the Tool Launcher window must be added by the user after JP1/IM - View is installed. For details, see *Chapter 2. Definition Files* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

#3: This folder is created by the user after JP1/IM - View is installed.

Table A–19: Files and folders that do not need to be referenced or edited (JP1/IM - View)

Folder name	Description
view-path\conf\	Files and folders in the folder for environment settings files other than those in the list of files and folders that can be referenced and edited by the user
system-drive:\ProgramData\Hitachi\jp1\jp1_default\JP1CoView\conf\#1	
view-path\classes\	Folder for class files
view-path\default\	Files and folders in the common definitions folder other than those in the list of files and folders that can be referenced and edited by the user
view-path\doc\	Help folder
view-path\image\	Files and folders in the folder for image data other than those in the list of files and folders that can be referenced and edited by the user
view-path\log\#2	Logs folder
view-path\patch_backup_dir\	Files and folders in the patch backup folder other than patch utilities mentioned in the patch RELEASE.TXT. (This folder is created only when applying a patch.)
view-path\tools\	Files and folders in the tools folder other than those in the list of files and folders that can be referenced and edited by the user
system-drive:\Program Files\jp1common\#3	Folder for program information

#1: This folder exists only when the OS is Windows. In Windows, some environment settings files are stored in this folder as well as in *view-path*\conf\.

#2: When the OS is Windows, replace the folder name *view-path*\log\ with *system-drive*:\ProgramData\Hitachi\jp1\jp1_default\JP1CoView\log\.

#3: In Windows, the folder name *system-drive*:\Program Files might vary depending on OS environment settings made at the time of installation.

B. List of Processes

This appendix describes JP1/IM processes.

B.1 JP1/IM processes (Windows)

The following shows the process names displayed in the **Processes** page of the Windows Task Manager.

(1) JP1/IM - Manager

The table below describes the JP1/IM - Manager processes. The numbers in parentheses are the number of processes that can be executed concurrently.

Table B–1: JP1/IM - Manager processes (Windows)

Parent process	Functionality	Child process	Functionality
jco_spmd.exe (1)	JP1/IM - Manager process management	jcamain.exe (1)	Automatic Action Service (displayed process name: jcamain)
		evtcon.exe (1)	Event console service (displayed process name: evtcon)
		evflow.exe (1)	Event base service (displayed process name: evflow)
		jcsmain.exe (1)	Central Scope service#1 (displayed process name: jcsmain)
		evgen.exe (2)#2	Correlation event generation service#3 (displayed process name: evgen)
		jcfmain.exe(1)	IM Configuration Management service#4 (displayed process name: jcfmain)
jco_service.exe(1)	Windows service control in JP1/IM - Manager	--	--
jcfmain.exe(1)	IM Configuration Management in JP1/IM - Manager	--	IM Configuration Management service
		jcfallogtrap.exe (0 to 157)#5	Log collection process
pdservice.exe	IM database	--	Windows service control
		pdprcd.exe	Process server process
pdprcd.exe(1)	IM database	--	Process server process
		pdrsvre.exe(3)	Post-processing process. Performs recovery processing when a process terminates abnormally.
		pdmlgd.exe(1)	Message log server process. Controls message output.
		pdrdmd.exe(1)	System manager process. Controls unit starting and stopping and manages connected users.

Parent process	Functionality	Child process	Functionality
		pdstsd.exe(1)	Status server process. Controls I/O operations to unit status files.
		pdscdd.exe(1)	Scheduler process. Distributes transactions among single server processes.
		pdtrnd.exe(1)	Transaction server process. Controls transactions.
		pdtrnrvd.exe(1 to 128)#6	Transaction recovery process. Controls transaction determination and recovery.
		pdlogd.exe(1)	Log server process. Controls acquisition of system logs and log-related processes.
		pd_buf_dfw.exe(1)	Deferred write process. Controls background writing to disks where the database is kept.
		pd_buf_awt.exe(2)	Parallel write process for the deferred write process
		pdlogswd.exe(1)	Log swapper process. Allocates and de-allocates system log-related files, manages I/O operations for system log-related files, and acquires syncpoint dumps.
		pdsds.exe(10 to 32)#7	Single server process. Performs SQL processing.
pdsha.exe (1)	IM database	--	Service for embedded HiRDB in a cluster environment

Legend:

--: None

#1: The process is started only when Central Scope is used. The process is not started by default.

#2: Maximum 2; normally 1. Breakdown as follows:

- Main processes of the event generation service
- Temporary process issued when the event service is connected. The process is generated when the event generation service starts and when an event acquisition filter is updated.

#3: Functionality for correlation event issue (inactive by default). The correlation event generation service is used in systems that do not use the integrated monitoring database.

#4: The process is started when IM Configuration Management is used. The process is not started by default.

#5: When the parent process starts, no child process is started. The number of child processes increases with the number of remotely monitored files. The maximum number of concurrent child processes is 157.

#6: Only one process runs when the system starts, but this number increases temporarily with each abnormal termination of the pdsds.exe process.

#7: 10 instances of this process run at startup, and this number increases with the number of access requests to the IM database. The maximum number of concurrent processes is 32.

When JP1/IM - Manager is used in a cluster system, the above processes are executed on each physical host and logical host. The number of processes that can be executed concurrently is the number of processes in the table multiplied by the number of physical and logical hosts on which the processes are running.

Processes in the above table whose parent process is jco_spmd.exe are controlled by the process management. You can check their status using the jco_spmd_status command.

An example of the display when the processes are running normally is shown below.

```
c:\>jco_spmd_status
```

```
KAVB3690-I Processing to report the status of JP1_CONS has started.

Display the running processes

Process name Process ID

evflow 3672

jcamain 4088

evtcon 4236

jcsmain 4668

evgen 5624

KAVB3691-I All the processes have started.
```

`jcsmain` is listed only when the Central Scope functionality is enabled, `evgen` is listed only when correlation event generation is enabled, and `jcfmain` is listed only when the IM Configuration Management functionality is enabled.

(2) JP1/IM - View

The table below describes JP1/IM - View processes. The numbers in parentheses are the number of processes that can be executed concurrently.

Table B–2: JP1/IM - View processes

Parent process	Functionality	Child process	Functionality
`jcoview.exe` (3 + 3#)	JP1/IM - View process management	`jcoview_evt.exe` (3)	Sends thread dump output events
		`java.exe` (3 + 3#)	JP1/IM - View window control
`jcfview.exe` (3)	IM Configuration Management - View process management	`jcfview_evt.exe` (3)	Sends thread dump output events
		`java.exe` (3 + 3#)	IM Configuration Management - View window control

#: Add when the JP1/IM - View (JP1/IM - Rule Operation linkage function) is active.

B.2 JP1/IM processes (UNIX)

The following shows the process names displayed by the `ps` command.

(1) JP1/IM - Manager

The table below describes the JP1/IM - Manager processes. The numbers in parentheses are the number of processes that can be executed concurrently.

Table B–3: JP1/IM - Manager processes (UNIX)

Parent process	Functionality	Child process	Functionality
jco_spmd (1)#1	Process management	jcamain (1)	Automatic action service (displayed process name: jcamain)
		evtcon (1)#1	Event console service (displayed process name: evtcon)
		evflow (1)	Event base service (displayed process name: evflow)
		jcsmain (1)	Central Scope service#2 (displayed process name: jcsmain)
		evgen (2)#3	Event generation service#4 (displayed process name: evgen)
		jcfmain(1)	IM Configuration Management service#5 (displayed process name: jcfmain)
jcfmain(1)	IM Configuration Management in JP1/IM - Manager	--	IM Configuration Management service
		jcfallogtrap(0 to 157)#6	Log collection process
pdprcd(1)#7	IM database	--	Process server process
		pdrsvre(3)	Post-processing process. Performs recovery processing when a process terminates abnormally.
		pdmlgd(1)	Message log server process. Controls message output.
		pdrdmd(1)	System manager process. Controls unit starting and stopping and manages connected users.
		pdstsd(1)	Status server process. Controls I/O operations to unit status files.
		pdscdd(1)	Scheduler process. Distributes transactions among single server processes.
		pdtrnd(1)	Transaction server process. Controls transactions.
		pdtrnrvd(1 to 128)#8	Transaction recovery process. Controls transaction determination and recovery.
		pdlogd(1)	Log server process. Controls acquisition of system logs and log-related processes.
		pd_buf_dfw(1)	Deferred write process. Controls background writing to disks where the database is kept.
		pd_buf_awt(2)	Parallel write process for the deferred write process
		pdlogswd(1)	Log swapper process. Allocates and de-allocates system log-related files, manages I/O operations for system log-related files, and acquires syncpoint dumps.
		pdsds(10 to 32)#9	Single server process. Performs SQL processing.

Legend:

--: None

#1: The number of processes might increase temporarily.

#2: The process is started only when Central Scope is used. The process is not started by default.

#3: Maximum 2; normally 1. Breakdown as follows:

- Main processes of the event generation service
- Temporary process generated when the event service is connected. The process is generated when the event generation service starts and when an event acquisition filter is updated.

#4: Functionality for correlation event generation (inactive by default). The event generation service is used in systems that do not use the integrated monitoring database.

#5: The process is started when IM Configuration Management is used. The process is not started by default.

#6: When the parent process starts, no child process is started. The number of child processes increases with the number of remotely monitored files. The maximum number of concurrent child processes is 157.

#7: If the IM database is set up, the `pdprcd` process starts at system startup, regardless of whether the automated startup script is enabled.

#8: Only one process runs when the system starts, but this number increases temporarily with each abnormal termination of the `pdsds` process.

#9: 10 instances of this process run at startup, and this number increases with the number of access requests to the IM database. The maximum number of concurrent processes is 32.

When JP1/IM - Manager is used in a cluster system, the above processes are executed on each physical host and logical host. The number of processes that can be executed concurrently is the number of processes in the table multiplied by the number of physical and logical hosts on which the processes are running. Processes running in a cluster system are displayed by the `ps` command shown below. Note that IM database processes (the `pdprcd` process and its child processes) are not displayed for *logical-host-name*.

`jco_spmd -h` *logical-host-name*

`evflow` *logical-host-name*

`jcamain` *logical-host-name*

`evtcon` *logical-host-name startup-option*

`evtcon` *logical-host-name*

`evgen` *logical-host-name*

`jcfmain` *logical-host-name*

`jcsmain` *logical-host-name*

Processes in the above table whose parent process is `jco_spmd` are controlled by the process management. You can check their status using the `jco_spmd_status` command.

An example of the display when the processes are running normally is shown below.

```
# jco_spmd_status

KAVB3690-I Processing to report the status of JP1_CONS has started.

Display the running processes

Process name Process ID

evflow 3672

jcamain 4088

evtcon 4236

jcsmain 4846
```

```
evgen 5624

KAVB3691-I All the processes have started.
```

jcsmain is listed only when the Central Scope functionality is enabled, evgen is listed only when correlation event generation is enabled, and jcfmain is listed only when the IM Configuration Management functionality is enabled.

C. Port Numbers

This appendix lists the port numbers used by JP1/IM. The protocol is TCP/IP.

These port numbers are set when the product is installed.

C.1 Port numbers for JP1/IM

The tables below list the port numbers that JP1/IM uses.

For communication, JP1/IM also uses the port numbers in the range from 1025/tcp to 65535/tcp, which are automatically assigned by the OS. The range of automatically assigned port numbers, however, might vary depending on the OS.

Table C–1: List of port numbers

Service name	Port number	IM-V	IM-M	Description
`jp1imevtcon`	20115/tcp	Y	Y	Used to connect to JP1/IM - Manager (event console service) from JP1/IM - View
`jp1imcmda`	20238/tcp	Y	Y	Used for the following: • Used to execute commands from JP1/IM - View • Used for JP1/IM - Manager (Central Console) to request JP1/Base[#1] to execute automated actions
`jp1imcss`	20305/tcp	Y	Y	Used to connect to JP1/IM - Manager (Central Scope service) from JP1/IM - View
None[#2]	Port number of the IM database[#3]	--	--	Used for internal processing by JP1/IM - Manager (IM database) (for physical hosts)
	Port number of the IM database[#4]	--	--	Used for internal processing by JP1/IM - Manager (IM database) (for logical hosts)
`jp1imcf`	20702/tcp	Y	Y	Used to connect to JP1/IM - Manager (IM Configuration Management service) from JP1/IM - View
`jp1imfcs`	20701/tcp	--	Y	Used for internal processing by JP1/IM - Manager (event base service)
`jp1imegs`	20383/tcp	--	Y	Used for internal processing by JP1/IM - Manager (event generation service)
`jp1rmregistry`	20380/tcp	Y	--	Used to connect to JP1/IM - Rule Operation from JP1/IM - View
`jp1rmobject`	20381/tcp	Y	--	
`jp1cmnaming`	22301/tcp	Y	--	Used to connect to JP1/IM - Central Information Master from JP1/IM - View
`jp1cmsessmgr`	22302/tcp	Y	--	
`jp1cmobjprov`	22303/tcp	Y	--	
`jp1cminfocol`	22304/tcp	Y	--	

Legend:

IM-V: JP1/IM - View
IM-M: JP1/IM - Manager
Y: Registered in the `services` file at installation.

--: Not registered in the `services` file at installation (and does not need to be set).

#1: It refers to JP1/Base on the manager.

#2: Not registered in the `services` file.

#3: This port number is set in the setup information file when the IM database is set up on a physical host. For details about the setup information file, see *Setup information file (jimdbsetupinfo.conf)* (in *Chapter 2. Definition Files*) in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

#4: This port number is set up in the cluster setup information file when the IM database is set up on a logical host. The port number increments with each IM database configured on the logical host. For details about the cluster setup information file, see *Cluster setup information file (jimdbclustersetupinfo.conf)* (in *Chapter 2. Definition Files*) in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

The Web-based JP1/IM - View uses the port numbers shown in the following table.

Service name	Port number	Description
`http`	80/tcp#	Used to connect to the Web server (to download `console.html` from JP1/IM - Manager)
`jp1imevtcon`	20115/tcp	Used to connect to JP1/IM - Manager (event console service) from the Web-based JP1/IM - View (through a Web browser)

#: The port number might differ depending on the Web server settings.

Remotely monitored hosts use the port numbers shown in the following table.

Remotely monitored host	Port number
Remote-monitoring log file trap (SSH connection)	Port number specified in the System Common Settings window of IM Configuration Management
Remote-monitoring log file trap (NetBIOS [NetBIOS over TCP/IP]) connection#1	137/udp, 137/tcp, 138/udp, 139/tcp
Remote-monitoring event log trap (WMI connection)#1	135/tcp and dynamic port numbers that are automatically assigned as needed#2

#1: To collect host information in remote monitoring, WMI and NetBIOS (NetBIOS over TCP/IP) are used for Windows hosts and SSH is used for UNIX hosts.

#2: WMI uses DCOM, and DCOM uses dynamic port allocation. Therefore, set the ports to be used by DCOM so that the lines connected to the ports pass through a firewall.

Standard ranges of the port numbers that are assigned by individual OSs are as follows:

- Windows Server 2008 R2, Windows Server 2012 or Windows Server 2016: 49152 to 65535

C.2 Direction of communication through a firewall

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

Table C–2: Direction of communication through a firewall

Service name	Port number	Direction of communication
`jp1imevtcon`	20115/tcp	JP1/IM - View -> JP1/IM - Manager (Central Console)
`jp1imcmda`	20238/tcp	JP1/IM - View -> JP1/Base#1 JP1/IM - Manager (Central Console) -> JP1/Base#1
`jp1imcss`	20305/tcp	JP1/IM - View -> JP1/IM - Manager (Central Scope)
`jp1rmregistry`	20380/tcp	JP1/IM - View -> JP1/IM - Rule Operation

Service name	Port number	Direction of communication
jp1rmobject	20381/tcp	
jp1imegs	20383/tcp	Firewall setup is unnecessary because all communication takes place on the machine on which JP1/IM - Manager is installed.
None[#2]	Port number of the IM database[#3]	JP1/IM - Manager (physical host) -> JP1/IM - Manager (IM database (physical host))
	Port number of the IM database[#4]	JP1/IM - Manager (logical host) -> JP1/IM - Manager (IM database (logical host))
jp1imcf	20702/tcp	JP1/IM - View -> JP1/IM - Manager (IM Configuration Management)
jp1imfcs	20701/tcp	Firewall setup is unnecessary because all communication takes place on the machine on which JP1/IM - Manager is installed.
jimmail	25/tcp[#5]	JP1/IM - Manager -> mail server (SMTP) (without authentication)
	587/tcp[#5]	JP1/IM - Manager -> mail server (SMTP) (with SMTP-AUTH authentication)
	110/tcp[#5]	JP1/IM - Manager -> mail server (POP3) (with POP-before-SMTP authentication)
http	80/tcp[#6]	Web-based JP1/IM - View (Web browser) -> Web server

Legend:

->: Direction of the connection when established

#1: Refers to JP1/Base on the manager.

#2: Not registered in the services file.

#3: This is the port number for the IM database (physical host) that was set in the setup information file when the IM database was set up on the physical host.

#4: This is the port number for the IM database (logical host) that was set in the cluster setup information file when the IM database was set up on the logical host.

#5: The destination port number might differ depending on which port is used on the destination server.

#6: The port number might differ depending on the HTTP server settings.

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

When JP1/IM is installed on a server host with a firewall, communications within that machine might also be subject to the firewall restrictions. In such a case, set up the firewall so that services can use the port numbers in the table even for communications within the firewall server host.

For details about operation with a firewall, see *8.3 Operating in a firewall environment* in the *JP1/Integrated Management - Manager Configuration Guide*.

(1) Setting the direction in which data passes through the firewall (when remotely monitored host information is collected)

The following connection methods are used to collect remotely monitored host information in JP1/IM - Manager:

In Windows:

SSH, NetBIOS (NetBIOS over TCP/IP), WMI

In UNIX:

SSH

Therefore, when you place JP1/IM - Manager and monitored hosts via a firewall, the data must pass through the firewall as follows:

JP1/IM - Manager (`jcfmain` and `jcfallogtrap`) -> Monitored hosts

Legend: ->: Direction of the connection when established

For an SSH connection

Let the data pass through the firewall using the port number specified for the SSH setting in the System Common Settings window of JP1/IM - Manager.

For a NetBIOS (NetBIOS over TCP/IP) connection

Let the data pass through the firewall using the port used by NetBIOS (NetBIOS over TCP/IP). For details about the configuration, see the manual for the firewall product, or ask the developer of the firewall product.

Note that the connection cannot be separated from other NetBIOS (NetBIOS over TCP/IP) connections.

For a WMI connection

WMI uses DCOM. DCOM uses dynamic port assignment. Therefore, let the data pass through the firewall using the port used by DCOM. For details about the configuration, see the manual for the firewall product, or ask the developer of the firewall product.

Note that the connection cannot be separated from other WMI or DCOM requests.

C.3 Connection status

The following table describes the connection status at each JP1/IM port number.

Table C–3: Connection status

Service name	Port number	Connection status
`jp1imevtcon`	20115/tcp	A connection is established when you log in to the Event Console window from the Login window, and is maintained until you log out. If a communication error occurs or if you forcibly terminate the connection, message KAVB1200-E appears. Click the **OK** button in the message box to re-establish the connection (only if **Automatic refresh** is set to **Apply** in the Preferences window). If **Do not apply** is set for **Automatic refresh** in the Preferences window, you can re-establish the connection by clicking the **Refresh** button in the Event Console window.
`jp1imcmda`	20238/tcp	A connection is established when you launch the Execute Command window and is maintained until you close the window. If a communication error occurs or if you forcibly terminate the connection, message KAVB0414-E appears. To re-establish the connection, re-execute the command in the Execute Command window.
`jp1imcss`	20305/tcp	A connection is established when you log in to the Monitoring Tree window from the Login window, and is maintained until you log out. If a communication error occurs or if you forcibly terminate the connection, message KAVB6241-E or KAVB6251-E appears. Click the **OK** button in the message box to re-establish the connection.
`jp1imegs`	20383/tcp	A connection is established when any of the following commands related to the event generation service or any of the following processes is executed, and is maintained until the command or process completes: • `jcoegschange` command • `jcoegsstatus` command

Service name	Port number	Connection status
		• `jcoegsstart` command • `jcoegsstop` command • Update of an event acquisition filter (using the System Environment Settings window of JP1/IM - View or the `jcochfilter` command) When an event acquisition filter is updated, a connection is established between the event console service and event generation service, and is terminated when the update processing ends.
`jp1rmregistry`	20380/tcp	A connection is established when you log in to JP1/IM - Rule Operation from JP1/IM - View, and is maintained until you log out from JP1/IM Operation from JP1/IM - View.
`jp1rmobject`	20381/tcp	A connection is established when you log in to JP1/IM - Rule Operation from JP1/IM - View, and is maintained until you log out from JP1/IM - Rule Operation from JP1/IM - View.
`JP1/IM-Manager DB Server`	20700/tcp	A connection is established when you start the JP1/IM-Manager service while JP1/IM-Manager DB Server is running, and is maintained until you shut down JP1/IM-Manager.
`jp1imcf`	20702/tcp	A connection is established with the IM Configuration Management service when any of the following services related to JP1/IM - Manager is executed or you log in or execute a command from JP1/IM - View. The connection is maintained until the service, operation, or command is finished. • IM Configuration Management service • A connection is established when you log in to the IM Configuration Management window from the Login window in JP1/IM - View, and is maintained until you log out. • `jcfimport` command • `jcfexport` command If a communication error occurs in a connection to JP1/IM - View or if you forcibly terminate the connection, message KNAN20101-E appears. If this occurs, make sure that the IM Configuration Management service is operating correctly, and click the **OK** button in the message box to re-establish the connection.
`jp1imfcs`	20701/tcp	A connection is established with the event base service when any of the following services or commands related to JP1/IM - Manager is executed, and is maintained until the service or command finishes executing: • Event console service • Automatic action service • Central Scope service • Event generation service • `jcoevtreport` command • `jcohctest` command • `jcoimdef` command • `jcastatus` command • `jcachange` command • `jcoegschange` command • `jcoegsstart` command • `jcoegsstatus` command • `jcoegsstop` command

D. Limits

This appendix shows the limits of JP1/IM.

D.1 Limits when using the Central Console

The tables below describe the limits that apply to JP1/IM - Manager and JP1/IM - View when using the Central Console. The Web-based JP1/IM - View, as a feature of JP1/IM - Manager (Central Console), is subject to the limits for JP1/IM - Manager.

(1) JP1/IM - Manager limits

The following table describes the limits that apply to JP1/IM - Manager and the Web-based JP1/IM - View.

Table D–1: Limits for JP1/IM - Manager

Item	Limit
Number of instances of JP1/IM - View that can connect to one JP1/IM - Manager	64
Number of instances of the Web-based JP1/IM - View that can run on one machine	1
Number of hosts that can be managed by one instance of JP1/IM - Manager (Considering the configuration of agents, this indicates the maximum number of hosts of JP1/IM - Manager and instances of JP1/Base that can be placed directly below JP1/IM - Manager.)	When `close` is specified as the communication type in the event server settings file (`conf`) of JP1/Base on the all agents IM Configuration Management database is set to L size: 2,500 IM Configuration Management database is set to S size or M size: 1,024 When the version of JP1/Base that is placed on the same host as JP1/IM - Manager is 11-10 or earlier, the maximum number of managed hosts is 1,024. If using the IM Configuration Management, you must set the IM Configuration Management database to L size. When there are one or more hosts where a value other than `close` is specified as the communication type in the event server settings file (`conf`) of JP1/Base on the agent In UNIX: 100 In Windows: 62 This value is for a maximum configuration. The number of managed hosts is restricted by the system configuration and network traffic.
Number of hosts that can execute commands from one instance of JP1/IM - Manager	2,500
Event buffer size (number of extracted events that can be buffered from the event database)	2,000
Scroll buffer size (number of events that can be displayed in a window) in the Web-based JP1/IM - View	1,000
Number of events that can be acquired when a window is refreshed in the Web-based JP1/IM - View	200
Number of events that can be acquired in a search in the Web-based JP1/IM - View	1,000

Item	Limit
Maximum length of an event acquisition filter#2 (total size of the event acquisition filters to be applied (total of pass conditions and exclusion-conditions) and the valid common exclusion-condition groups in basic mode)	60 KB When no exclusion-condition group or valid common exclusion-condition group in basic mode is set. 64 KB When an exclusion-condition group or a valid common exclusion-condition group in basic mode is set.
Maximum length of common exclusion conditions#2	Basic mode: 64 kilobytes (total size of the event acquisition filters to be applied (total of pass conditions and exclusion-conditions) and common exclusion-conditions groups) Extended mode: 15 megabytes Note that the following limitations apply to the items that are specified in the common-exclusion-conditions extended definition parameters: • Common exclusion-conditions group name: 1 to 50 bytes • Comments: 1,024 bytes • Number of event conditions: 256 • Total size of event conditions: 64 KB
Maximum length of an event receiver filter#2	1 MB (total size when more than one event receiver filter is set)
Maximum length of a severe events filter#2	64 KB
Maximum length of a view filter#2	1 MB per JP1 user (total size when more than one view filter is set)#3
Maximum length of an event search#2	64 KB#3
Number of event receiver filters	128
Number of conditions that can be set in a filter (applies to passing conditions and exclusion-conditions)	• Event acquisition filter: 30 per filter • Event receiver filter: 30 per filter • Severe events filter: 30 • View filter: 5 per filter • Event search: 5
Maximum length that can be entered in the input field of an item for which multiple attribute values can be specified in a filter window#4 of the Web-based JP1/IM - View	30,000 bytes
Number of filters that can be defined in the list of event acquisition filters	50
Maximum length of a filter name specified in the list of event acquisition filters	50 bytes
Number of common exclusion-conditions that can be defined in the list of event acquisition filters	Basic mode: 30 Extended mode: 2,500
Maximum size of the file containing the list of event acquisition filters	1 MB
Number of queued commands executed by automated actions	65,535
Length of an action definition parameter for an automated action	No limits when using version 09-00 or later. However, the following items specified in an action definition parameter have limit values: • Length of an action name: 1 to 50 bytes

Item	Limit
	- Length of a comment: 1,040 bytes - Length of an event condition: 4,096 bytes - Length of a user name: 31 bytes - Length of *executing-host-name* | *host-group-name*: 255 bytes - Length of a *business-group-name* | *monitoring-group-name*: 2,048 bytes - Length of an action: 4,096 bytes - Length of an environment variable file name: 255 bytes - Size of an automated action definition file: 22 megabytes (23,068,672 bytes)
	When version 08-50 or earlier is used: 5,706 bytes However, the following items specified in an action definition parameter have limit values: - Length of an event monitoring condition: 1,040 bytes - Length of an action: 4,096 bytes - Length of the user name for executing an action: 31 bytes - Length of an environment variable file name: 255 bytes - Length of a target host name: 255 bytes
Length of a target group name	30 bytes
File size of an event guide information file	1 MB
File size of an event-guide message file	1 MB
Total number of items that can be defined in an event guide information file	1,000
Length of an event-guide message after processing of placeholders (variables) and HTML encoding	196,608 characters#5
Length of an event guide-message file name that can be specified in an event guide information file	1,024 characters#5
Number of comparison conditions that can be defined in event guide information	100
Number of correlation event generation conditions that can be defined in a correlation event generation definition file	1,000
Number of filtering conditions for the correlation target range that can be defined in one correlation event generation condition	1
Number of event conditions that can be defined in one correlation event generation condition	10
Timeout period for a correlation event generation condition	1 second to 86,400 seconds (24 hours)
Maximum value that can be specified in the threshold event correlation type	100 events
Number of duplicate attribute value conditions that can be defined in one correlation event generation condition	3
Number of maximum correlation numbers that can be defined in one correlation event generation condition	1
Maximum length of the attribute value used in defining a correlation approval event	2,048 bytes

Item	Limit
Number of sets of JP1 events that can be correlated simultaneously by one correlation event generation condition	1,024 sets
Number of sets of JP1 events that can be correlated simultaneously by all correlation event generation conditions	20,000 sets
Health check timeout period	216,000 seconds (60 hours)
Number of characters that can be specified for a URL in IE	2,046 characters
Number of conditions that can be defined in the List of Repeated Event Conditions window	2,500
Total size of the definitions of repeated event conditions	15 megabytes (15,728,640 bytes)
Length of a definition of repeated event condition	No limit However, there are limits for the following items that are related to specifying a repeated event condition: • **Repeated event condition name**: 1 to 50 bytes • **Comment**: 0 to 1,024 bytes • **Event conditions**: 0 to 256 conditions • Operand of event condition: 65,536 bytes[#6] • **Conditions for same attribute values**: 0 to 3 conditions • Number of seconds as threshold: 1 to 60 • Number of events as threshold: 1 to 200 • **End monitoring period**: 1 to 86,400 seconds • **Time** for **Checks for suppression to continue**: 1 to 86,400 seconds • **Number of events** for **Checks for suppression to continue**: 1 to 1,000,000
Maximum number of email destinations that can be specified at a time by the email notification function of JP1/IM - Manager	20 Multiple destinations cannot be specified over the maximum length of the command line.
Maximum lengths of items with which mail can be sent by the email notification function of JP1/IM - Manager	• Mail address: 256 bytes • Mail subject: 512 bytes • Mail text: 4,096 bytes • One line of mail text: 512 bytes
Number of days that can be specified as the range of events to be collected at login	1 to 31 days
Base time that can be specified for the range of events to be collected at login	0:00 to 23:59
Time that can be specified as the range of events to be collected at login	1 to 744 hours (corresponding to 31 days)
File size of a severity changing definition file	17 MB (17,825,792 bytes)
Number of definitions that can be defined by the severity changing definition function	1,000
Length of one severity changing definition	No limit However, there are limit values for the following items that are related to specifying event conditions for changing severity: • Severity change definition name: 1 to 50 bytes • Comment: 0 to 1,024 bytes • Event conditions: 0 to 256 conditions • Operand of event condition: 0 to 4,096 bytes

Item	Limit
Number of definitions that can be defined by the display message change function	3,000
Length of one display message change definition	No limit However, there are limits for the following items that are related to specifying event conditions for changing display messages: • Display message change definition name: 1 to 50 bytes • Maximum length of a message after change: 1,023 bytes#7 • Comment: 0 to 1,024 bytes • Event conditions: 0 to 256 conditions • Operand of event condition: 0 to 4,096 bytes • Maximum size of a display message change definition file: 22 megabytes (23,068,672 bytes)

#1: The number of file descriptors available to one process is system-dependent.

#2: Because the character string data is stored in Shift-JIS code, the specifiable length of the character string is the same even if JP1/IM - Manager is running in Japanese UTF-8 code.

#3: This limit applies to the Web-based JP1/IM - View.

#4: Filter windows are the Severe Event Definitions window, Event Search Conditions window, Common Exclusion-Conditions Settings window, Settings for View Filter window, and Detailed Settings for Event Receiver Filter window.

#5: Both 1-byte and 2-byte characters are counted as one character. For example, `AAA` is counted as three characters.

#6: For details about the limits other than the size of the operand of the event condition, see *3.4.3(2) Event comparison attributes that can be specified in repeated event conditions*.

#7: The message length is based on the encoding settings for JP1/IM - Manager.

(2) JP1/IM - View limits

The following table describes the limits that apply to JP1/IM - View.

Table D–2: Limits for JP1/IM - View

Item	Limit
Number of instances of JP1/IM - View that can be started within a single session (per process#1)	3#2
Scroll buffer size (number of events that can be displayed in a window)	2,000
Number of events that can be acquired when a window is refreshed	200
Number of events that can be acquired in a search	2,000
Maximum length of a filter#3	• View filter: 1 MB per JP1 user (total size when more than one view filter is set) • Event search: 64 KB
Number of view filters	50
Maximum length of a name of a view filter	50 bytes
Number of condition groups that can be set in a filter (applies to passing conditions and exclusion-conditions)	• Event acquisition filter: 30 per filter • Event receiver filter: 30 per filter • Severe events filter: 30 • View filter: 5 per filter • Event search: 5

Item	Limit
Maximum length that can be entered in the input field of an item for which multiple attribute values can be specified in a filter window#4	30,000 bytes
Number of instances of the ｜ special character that can be specified when regular expressions are used to specify conditions	1,000 per input field
Number of filters that can be defined in the list of event acquisition filters	50 (when connected to Central Console)
Number of common exclusion-condition groups that can be defined in the list of event acquisition filters	Basic mode: 30 Extended mode: 2,500
Longest environment variable file name that can be specified in the Execute Command window#5	255 bytes
Longest target host name that can be specified in the Execute Command window	255 bytes
Longest action definition parameter for an automated action definition	When connected to JP1/IM - Manager 09-00 or later: No limits when using version 09-00 or later. However, the following items specified in an action definition parameter have limit values: • Length of an action name: 1 to 50 bytes • Length of a comment: 1,040 bytes • Length of an event condition: 4,096 bytes • Length of a user name: 31 bytes • Length of *executing-host-name* ｜ *host-group-name*: 255 bytes • Length of a *business-group-name* ｜ *monitoring-group-name*: 2,048 bytes • Length of an action: 4,096 bytes • Length of an environment variable file name: 255 bytes When version 08-50 or earlier is used: 5,706 bytes The following limits apply to the individual items specified in the action definition parameter: • Length of an event monitoring condition: 1,040 bytes • Length of an action: 4,096 bytes • Length of the user name for executing an action: 31 bytes • Length of an environment variable file name: 255 bytes • Length of a target host name: 255 bytes
	When connecting to JP1/IM - Manager version 08-00 to 08-50: 5,706 bytes The following limits apply to the individual items specified in the action definition parameter: • Length of an event monitoring condition: 1,040 bytes • Length of an action: 4,096 bytes • Length of the user name for executing an action: 31 bytes • Length of an environment variable file name: 255 bytes
Number of lines of execution results to display in the Execute Command window that can be specified in the Preferences window	100 to 10,000 lines
Size of text data that can be copied to the clipboard	6 MB

Item	Limit
Number of conditions that can be defined in the List of Repeated Event Conditions window	2,500
Total size of the definitions of repeated event conditions	15 megabytes (15,728,640 bytes)
Length of a definition of repeated event condition	No limit However, there are limits for the following items that are related to specifying a repeated event condition: • **Repeated event condition name**: 1 to 50 bytes • **Comment**: 0 to 1,024 bytes • **Event conditions**: 0 to 256 conditions • Operand of event condition: 65,536 bytes[#6] • **Conditions for same attribute values**: 0 to 3 conditions • Number of seconds as threshold: 1 to 60 • Number of events as threshold: 1 to 200 • **End monitoring period**: 1 to 86,400 seconds
Number of days that can be specified as the range of events to be collected at login	1 to 31
Base time that can be specified for the range of events to be collected at login	0:00 to 23:59
Time that can be specified as the range of events to be collected at login	1 to 744 hours (corresponding to 31 days)
Number of definitions that can be defined by the severity changing definition function	1,000
Number of definitions that can be specified for a manager host in the non-encryption communication host configuration file for encrypted communication	1,024
Maximum length (in characters) of a manager host name in the non-encryption communication host configuration file for encrypted communication	255 characters
Number of definitions that can be defined by the display message change function	3,000
Length of one display message change definition	No limit However, there are limits for the following items that are related to specifying event conditions for changing a display message: • Display message change definition name: 1 to 50 bytes • Maximum length of a message after change: 1,023 bytes[#7] • **Comment**: 0 to 1,024 bytes • **Event conditions**: 0 to 256 conditions • Operand of event condition: 0 to 4,096 bytes • Maximum size of a display message change definition file: 22 megabytes (23,068,672 bytes)

#1: The following viewers and windows are started for each process:

- Central Console viewer and Central Scope viewer
- IM Configuration Management viewer
- Monitoring Tree (Editing) window

#2: The larger the number of active instances of JP1/IM - View, the greater the memory and disk space requirements.

#3: Because character string data is stored in Shift-JIS code, the specifiable length of a character string is the same even if JP1/IM - Manager is running in Japanese UTF-8 code.

#4: Filter windows are the Severe Event Definitions window, Event Search Conditions window, Common Exclusion-Conditions Settings window, Settings for View Filter window, and Detailed Settings for Event Receiver Filter window.

#5: The total size of all fields must be no more than 2,305 bytes (For example, if five conditions are set, the total size of the five attribute values must be no more than 2,305 bytes).

#6: For details about the limits other than the size of the operand of the event condition, see *3.4.3(2) Event comparison attributes that can be specified in repeated event conditions*.

#7: The message length is based on the encoding settings for JP1/IM - Manager.

D.2 Limits when using the Central Scope

The following tables describe the limits that apply to JP1/IM - Manager and JP1/IM - View when using the Central Scope.

(1) JP1/IM - Manager limits

The following table describes the limits that apply to JP1/IM - Manager.

Table D–3: Limits for JP1/IM - Manager

Item	Limit
Number of instances of JP1/IM - View that can connect to one JP1/IM - Manager	64
Number of hosts that can be monitored by one instance of the Central Scope	5,000 This value includes all hosts being monitored from the Central Scope, such as JP1/AJS - Agent hosts and hosts being monitored using the SNMP trap converter of JP1/Base, in addition to hosts configured under JP1/IM - Manager.
Number of Monitoring Tree windows that can be managed by JP1/IM - Manager	1
Longest monitoring node name that can be set in a configuration file for a monitoring tree	255 bytes#1
Longest basic information for a monitoring node that can be set in a configuration file for a monitoring tree	Attribute value: 1,023 bytes#1, #2
Longest status change condition name that can be set in a configuration file for a monitoring tree	63 bytes
Longest value specifiable for individual conditions in a configuration file for a monitoring tree	Attribute value: 1,023 bytes#1, #2
File size of a guide information file	1 MB
File size of a guide-message file	1 MB

#1: If JP1/IM - Manager is running in UTF-8 code, character string data is stored in Japanese UTF-8 code. Therefore, the specifiable length of a character string becomes shorter.

#2: The total for all fields is a maximum of 1,280 bytes. (For example, if five conditions are set, the total size of the five attribute values must not exceed 1,280 bytes.)

(2) JP1/IM - View limits

The following table describes the limits that apply to JP1/IM - View.

Table D–4: Limits for JP1/IM - View

Item	Limit
Number of instances of JP1/IM - View that can be started within a single session (per process#1)	3#2
Number of monitoring nodes that can be monitored in a Monitoring Tree window	50,000
Length of a monitoring node name	255 bytes#3
Number of basic information items that can be set for one monitoring node	5
Number of characters that can be entered in a basic information field	Attribute name: 32 bytes#3 Attribute value: 1,023 bytes#3, #4
Number of status change conditions that can be set for one monitoring node	8
Length of a status change condition name	63 bytes
Number of individual conditions that can be set in one status change condition for monitoring objects	5
Percentage value that can be set as a comparison condition in one status change condition for monitoring groups	100
Maximum count that can be set as a comparison condition in one status change condition for monitoring groups	50,000
Number of characters that can be entered in an individual condition field	Attribute name: 32 bytes#3 Attribute value: 1,023 bytes#3, #4
Number of JP1 events that can be issued by one monitoring node	7
Number of status change event logs that can be kept by each monitoring node	100
File name length of a background image that can be set in a monitoring group	260 bytes#3
File name length of an image file used as an icon for a monitoring node (for the normal and expanded status, and Visual Icon)	260 bytes#3
Number of common conditions that can be added by the user	191
Length of the common condition name set in the Common Condition Detailed Settings window	63 bytes#3
Number of characters that can be entered in a **Common condition details** field (other than the **Extended attribute** area) of the Common Condition Detailed Settings window	1,023 bytes#3
Number of characters that can be entered in a **Common condition details** field (**Extended attribute** area) of the Common Condition Detailed Settings window	Attribute name: 32 bytes#3 Attribute value: 1,023 bytes#3, #4
Length of the file name of the background image in a Visual Monitoring window	260 bytes#3
Number of monitoring nodes that can be placed in one Visual Monitoring window	128
Number of Visual Monitoring windows that users can create	64
Length of the name set for a Visual Monitoring window	63 bytes#3

Item	Limit
Length of a comment about a Visual Monitoring window	80 bytes#3
Number of definitions that can be specified for a manager host in the non-encryption communication host configuration file for encrypted communication	1,024 definitions
Maximum length (in characters) of a manager host name in the non-encryption communication host configuration file for encrypted communication	255 characters

#1: The following viewers and windows are started for each process:

- Central Console viewer and Central Scope viewer
- IM Configuration Management viewer
- Monitoring Tree (Editing) window

#2: The larger the number of active instances of JP1/IM - View, the greater the memory and disk space requirements.

#3: If JP1/IM - Manager is running in UTF-8 code, character string data is stored in Japanese UTF-8 code. Therefore, the specifiable length of a character string becomes shorter.

#4: The total for all fields is a maximum of 1,280 bytes. (For example, if five conditions are set, the total size of the five attribute values must not exceed 1,280 bytes.)

D.3 Limits when using IM Configuration Management

The tables below describe the limits that apply to JP1/IM - Manager and IM Configuration Management - View when using IM Configuration Management.

(1) JP1/IM - Manager limits

The following table describes the limits that apply to JP1/IM - Manager.

Table D–5: Limits for JP1/IM - Manager

Item	Limit
Number of instances of JP1/IM - IM Configuration Management - View that can connect to one JP1/IM - Manager	64#1
Number of hosts one JP1/IM - Manager can manage (total number of the JP1/IM - Manager hosts, the JP1/Base instances that can be placed directly below JP1/IM - Manager, and the remotely monitored hosts in the system configuration, regardless of IPv4 hosts, IPv6 hosts, or IPv4/IPv6 hosts)	2,500
Number of hosts that can be monitored from one instance of IM Configuration Management (regardless of IPv4 hosts, IPv6 hosts, or IPv4/IPv6 hosts)	10,000 2,499 agents can be configured directly under IM Configuration Management
Number of tiers in the system hierarchy (IM configuration) that can be monitored by one IM Configuration Management instance	3 levels (assuming the integrated manager as being in the first level)
Maximum number of files that can be monitored remotely#2	1,024
Maximum number of log file trap processes that can be managed by one host	100#3
Number of standby hosts that can be set up on one logical host	4
Number of IP addresses that can be displayed for one host	8

Item	Limit
Number of alias host names that can be displayed for one host	4
Total number of business groups and monitoring groups	100
Maximum number of hosts that can be set for one business group or one monitoring group	2,500
Number of tiers for business groups	1 level
Number of tiers for monitoring groups	9 levels

#1: When AIX is used, a maximum of 16 JP1/IM - View instances can be connected simultaneously to one JP1/IM - Manager to operate (collect and apply) profiles, collect host information, and execute virtualization configuration information. If this limit is exceeded or if you perform remote monitoring, set the `max_thread_proc` kernel parameter to 300 or more.

#2: This is the total of the number of log files monitored by remote log file traps and the number of servers monitored by remote event log traps.

#3: If 101 or more log trap files are active, the message KNAN22411-W is output and the first 100 are collected.

(2) JP1/IM - View limits

The following table describes the limits that apply to JP1/IM - View.

Table D–6: Limits for JP1/IM - View

Item	Limit
Number of instances of JP1/IM - View that can be started within a single session (per process#1)	3#2
Number of definitions that can be specified for a manager host in the non-encryption communication host configuration file for encrypted communication	1,024 definitions
Maximum length (in characters) of a manager host name in the non-encryption communication host configuration file for encrypted communication	255 characters

#1: The following viewers and windows are started for each process:

- Central Console viewer and Central Scope viewer
- IM Configuration Management viewer
- Monitoring Tree (Editing) window

#2: The larger the number of active instances of JP1/IM - View, the greater the memory and disk space requirements.

D.4 Remote monitoring configuration limits

Table D–7: Limits for remote monitoring configuration

Item	Limit
Maximum number of log files that can be specified for one remote-monitoring log file trap	32
Maximum number of remote-monitoring log file traps that can be defined on one host	10
Maximum number of hosts that can be remotely monitored by one JP1/IM - Manager	1,024
Maximum number of remote-monitoring log file traps that can be monitored by one JP1/IM - Manager	1,024

Item	Limit
Maximum number of remote-monitoring event log traps that can be monitored by one JP1/IM - Manager	1,024
Maximum number of log files that can be remotely monitored by one JP1/IM - Manager	1,024
Monitoring interval for remote-monitoring log file traps and remote-monitoring event log traps	60 second to 86,400 seconds

E. Operating Permissions

Operating permissions are assigned to each JP1 user. There are six JP1 permission levels, as follows:

- `JP1_Console_Admin`
  Allows the JP1 user to perform all operations (system settings, system operations, viewing operations, setting the user environment, and starting linked products) in the Central Console and Central Scope.
- `JP1_Console_Operator`
  Allows the JP1 user to perform system operations, viewing operations, set the user environment, and start linked products in the Central Console and Central Scope.
- `JP1_Console_User`
  Allows the JP1 user to perform viewing operations, set the user environment, and start linked products in the Central Console and Central Scope.
- `JP1_CF_Admin`
  Allows the JP1 user to perform all IM Configuration Management operations (change and apply the system hierarchy, change and apply profiles).
- `JP1_CF_Manager`
  Allows the JP1 user to perform the following IM Configuration Management operations: Register host information, change and apply profiles, reference configuration information and host settings, and collect information.
- `JP1_CF_User`
  Allows the JP1 user to perform the following IM Configuration Management operations: View configuration information and host information.

Note 1: JP1/IM - Manager (Central Console)

`JP1_Console_Operator` permission is assumed if no JP1 permission level has been set.

Note 2: JP1/IM - Manager (Central Scope)

`JP1_Console_User` permission is assumed if no JP1 permission level has been set.

Note 3: JP1/IM - Manager (IM Configuration Management)

- `JP1_Console_User` permission is assumed if no JP1 permission level has been set.
- If multiple JP1 permission levels are assigned to a JP1 user, where one permission allows a certain operation but another permission denies the same operation, the JP1 permission level that allows the operation takes priority.
- In JP1/IM - View windows, menus and buttons that are used for functions that are not allowed by JP1 permission levels are unavailable.
- JP1 users can check which JP1 permission levels are granted to them only when they log in. After a JP1 user logs in, if JP1 permission levels for the JP1 user are changed on the authentication server, the new permission levels will be enabled when the user logs in the next time.

E.1 Operating permissions required for system monitoring using the Central Console

Operating permissions required for system monitoring using the Central Console differs depending on whether restrictions on viewing and operating business groups are enabled.

(1) Operating permissions required when restrictions on viewing and operating business groups are disabled

The following table lists and describes operating permissions required when restrictions on viewing and operating business groups are disabled.

Table E–1: Operating permissions required when restrictions on viewing and operating business groups are disabled

Type of operation			JP1 permission level			
Category	Operation	Description	Admin	Operator	User	None
System settings	Set the system environment	Set the JP1/IM - Manager environment in the following windows: • System Environment Settings window • Event Acquisition Settings window • Common Exclusion-Conditions Settings window • Common Exclusion-Condition Settings (Extended) window	Y	--	--	--
	Define for changing the event severity	Change the severity of JP1 events that satisfy conditions by using the following windows: • Severity Change Definition Settings window • Add Severity Change Definition Settings window	Y	--	--	--
	Define severe events	Define severe events in the Severe Event Definitions window.	Y	--	--	--
	Set an event receiver filter	Set an event receiver filter in the following windows: • Settings for Event Receiver Filter window • Detailed Settings for Event Receiver Filter window	Y	--	--	--
	Set automated actions	Set automated actions in the following windows: • Action Parameter Definitions window • Action Parameter Detailed Definitions window • Action Parameter Detailed Definitions (for compatibility) window • Action Parameter Detailed Definitions (Extended Event Information) window	Y	--	--	--
	Set event information mapping	Set event information mapping in the following windows: • Event-Information Mapping Definitions window	Y	--	--	--

Type of operation			JP1 permission level			
Category	Operation	Description	Admin	Operator	User	None
		• Event-Information Mapping Detailed Definitions window				
	Set repeated event conditions	Set repeated event conditions in the following windows: • List of Repeated Event Conditions window • Repeated Event Condition Settings window	Y	--	--	--
	Set display message change	Set the display message change definition in the following windows: • Display Message Change Definitions window • Display Message Change Definition Settings window	Y	--	--	--
System operations	Change the response status of severe events	Change the response status of JP1 events.	Y	Y	--	Y
	Release a severe event	Change a JP1 event displayed on the Severe Events page to a non-severe event.	Y	--	--	--
	Clear status notification suppression	Re-enable notification of automated action errors when the notification function is suppressed during delay monitoring or status monitoring.	Y	Y	--	Y
	Cancel an automated action	Request the cancellation of an automated action in `Wait`, `Queue`, or `Running` status (by clicking the **Cancel Action** button in the Action Log window, Action Log Details window, or List of Action Results window).	Y	Y	--	Y
	Re-execute an automated action	Re-execute an automated action in `Error` or `Ended` status (by clicking the **Re-execute** button in the Action Log window, Action Log Details window, or List of Action Results window).	Y	Y	--	Y
	Execute commands	Execute commands on managed hosts in the Execute Command window.	Y	Y	--	Y
	Respond to response-waiting events	Enter responses for response-waiting events in the Enter Response window.	Y	Y	--	Y
	Release response-waiting events from the hold-and-accumulate state	Release response-waiting events from the hold-and-accumulate state on the Response-Waiting Events page of the Event Console window.	Y	Y	--	Y
	Restore monitoring of the accumulation of response-waiting events	Restore the function that notifies the user when the number of accumulated response-waiting events exceeds the upper limit.	Y	--	--	--

Type of operation			JP1 permission level			
Category	Operation	Description	Admin	Operator	User	None
	Edit memo entries	Set memo entries in the following window: • Edit Event Details window	Y	Y	--	Y
Viewing operations	View JP1 events	View JP1 events on the **Monitor Events** page and **Severe Events** page of the Event Console window.	Y	Y	Y	Y
		View JP1 event details in the Event Details window				
		View related events in the Related Events window.				
	View the results of automated actions	View the results of automated actions in the following windows: • Action Log window • Action Log Details window • List of Action Results window • Conditions for Updating List of Action Results window	Y	Y	Y	Y
	Search for events	Search for events in the following windows and display the results on the **Search Events** page of the Event Console window: • Event Search Conditions window • Event Search Conditions (Program-Specific Information in Extended Attribute) window • Event Search Detailed Conditions (Program-Specific Information in Extended Attribute) window	Y	Y	Y	Y
	Use a view filter	Set conditions for the JP1 events displayed on the **Monitor Events** and **Severe Events** pages of the Event Console window.	Y	Y	Y	Y
		Switch between view filters.				
	Display event guide information	Check guide information in the Event Details window.	Y	Y	Y	Y
Set the user environment	Set the user environment	Open the Preferences window and set the user environment.	Y	Y	Y	Y
Start linked products	Launch the GUI of another application	Launch the application that reported a JP1 event, and view or manipulate information.	Y	Y	Y	Y
	Open the Tool Launcher window	Use the Tool Launcher window to start linked products.	Y	Y	Y	Y
	Launch the Rule Operation viewer GUI	Launch the Rule Log Details window of JP1/IM - Rule Operation from the Action Log window, Action Log Details window, or List of Action Results window.	Y	Y	Y	Y

Legend:

Admin: `JP1_Console_Admin`

Operator: JP1_Console_Operator

User: JP1_Console_User

Y: Can perform the operation.

--: Cannot perform the operation.

Notes:

- When a JP1 user is granted two or more JP1 permission levels, and a particular operation is permitted by one level but prohibited by another, the operation is permitted.
- Menus and buttons for functions that are not permitted under the various permission levels are unavailable in the JP1/IM - View windows.
- Functions that cannot be performed in the Web-based Event Console window are unavailable regardless of the JP1 permission level.
- The assigned JP1 permission level is checked only when the JP1 user logs in. If the JP1 permission level is subsequently changed on the authentication server, the new permission level takes effect the next time the JP1 user logs in.

(2) Operating permissions required when restrictions on viewing and operating business groups are enabled

The following table lists and describes operating permissions required when restrictions on viewing and operating business groups are enabled.

Table E–2: Operating permissions required for Central Console operations

Type of operation			JP1 resource group								
			JP1_Console or *				Other than JP1_Console				Not specified
			JP1 permission level								
Category	Operation	Description	Admin	Operator	User	None	Admin	Operator	User	None	None
System settings	Set the system environment	Set the JP1/IM - Manager environment in the following windows: • System Environment Settings window • Event Acquisition Settings window • Common Exclusion-Conditions Settings window • Common Exclusion-Condition Settings (Extended) window	Y	--	--	--	--	--	--	--	--
	Define for changing	Change the severity of JP1 events that	Y	--	--	--	--	--	--	--	--

Type of operation			JP1 resource group								
			`JP1_Console` or *				Other than `JP1_Console`				Not specified
			JP1 permission level								
Category	Operation	Description	Admin	Operator	User	None	Admin	Operator	User	None	None
	the event severity	satisfy conditions by using the following windows: - Severity Change Definition Settings window - Add Severity Change Definition Settings window									
	Define severe events	Define severe events in the Severe Event Definitions window.	Y	--	--	--	--	--	--	--	--
	Set an event receiver filter	Set an event receiver filter in the following windows: - Settings for Event Receiver Filter window - Detailed Settings for Event Receiver Filter window	Y	--	--	--	--	--	--	--	--
	Set automated actions	Set automated actions in the following windows: - Action Parameter Definitions window - Action Parameter Detailed Definitions window - Action Parameter Detailed Definitions (for compatibility) window - Action Parameter Detailed Definitions (Extended Event Information) window	Y	--	--	--	--	--	--	--	--
	Set event information mapping	Set event information mapping in the following windows:	Y	--	--	--	--	--	--	--	--

Type of operation			JP1 resource group								
			JP1_Console or *				Other than JP1_Console				Not specified
			JP1 permission level								
Category	Operation	Description	Admin	Operator	User	None	Admin	Operator	User	None	None
		• Event-Information Mapping Definitions window • Event-Information Mapping Detailed Definitions window									
	Set repeated event conditions	Set repeated event conditions in the following windows: • List of Repeated Event Conditions window • Repeated Event Condition Settings window	Y	--	--	--	--	--	--	--	--
	Set display message change	Set the display message change definition in the following windows: • Display Message Change Definitions window • Display Message Change Definition Settings window	Y	--	--	--	--	--	--	--	--
System operations	Change the response status of severe events	Change the response status of JP1 events.	Y	Y	--	--	Y	Y	--	--	--
	Release a severe event	Change a JP1 event displayed on the Severe Events page to a non-severe event.	Y	--	--	--	Y	--	--	--	--
	Clear status notification suppression	Re-enable notification of automated action errors when the notification function is suppressed during	Y	Y	--	--	--	--	--	--	--

Type of operation			JP1 resource group								
			JP1_Console or *				Other than JP1_Console				Not specified
			JP1 permission level								
Category	Operation	Description	Admin	Operator	User	None	Admin	Operator	User	None	None
		delay monitoring or status monitoring.									
	Cancel an automated action	Request the cancellation of an automated action in Wait, Queue, or Running status (by clicking the **Cancel Action** button in the Action Log window, Action Log Details window, or List of Action Results window).	Y	Y	--	--	--	--	--	--	--
	Re-execute an automated action	Re-execute an automated action in Error or Ended status (by clicking the **Re-execute** button in the Action Log window, Action Log Details window, or List of Action Results window).	Y	Y	--	--	--	--	--	--	--
	Execute commands	Execute commands on managed hosts in the Execute Command window.	Y	Y	--	--	Y#	Y#	--	--	--
	Respond to response-waiting events	Enter responses for response-waiting events in the Enter Response window.	Y	Y	--	--	Y	Y	--	--	--
	Release response-waiting events from the hold-and-accumulate state	Release response-waiting events from the hold-and-accumulate state on the Response-Waiting Events page of the Event Console window.	Y	Y	--	--	Y	Y	--	--	--
	Restore monitoring of the accumulation of response-waiting events	Restore the function that notifies the user when the number of accumulated response-waiting events exceeds the upper limit.	Y	--	--	--	Y	--	--	--	--

Type of operation			JP1 resource group								
			`JP1_Console` or *				Other than `JP1_Console`				Not specified
			JP1 permission level								
Category	Operation	Description	Admin	Operator	User	None	Admin	Operator	User	None	None
	Edit memo entries	Set memo entries in the following window: • Edit Event Details window	Y	Y	--	--	Y	Y	--	--	--
Viewing operations	View JP1 events	View JP1 events on the **Monitor Events** page and **Severe Events** page of the Event Console window.	Y	Y	Y	--	Y#	Y#	Y#	--	--
		View JP1 event details in the Event Details window									
		View related events in the Related Events window.									
	View the results of automated actions	View the results of automated actions in the following windows: • Action Log window • Action Log Details window • List of Action Results window • Conditions for Updating List of Action Results window	Y	Y	Y	--	--	--	--	--	--
	Search for events	Search for events in the following windows and display the results on the **Search Events** page of the Event Console window: • Event Search Conditions window • Event Search Conditions (Program-Specific Information in Extended Attribute) window	Y	Y	Y	--	Y#	Y#	Y#	--	--

Type of operation			JP1 resource group								
			`JP1_Console` or *				Other than `JP1_Console`				Not specified
			JP1 permission level								
Category	Operation	Description	Admin	Operator	User	None	Admin	Operator	User	None	None
		• Event Search Detailed Conditions (Program-Specific Information in Extended Attribute) window									
	Use a view filter	Set conditions for the JP1 events displayed on the **Monitor Events** and **Severe Events** pages of the Event Console window.	Y	Y	Y	--	Y	Y	Y	--	--
		Switch between view filters.									
	Display event guide information	Check guide information in the Event Details window.	Y	Y	Y	--	Y	Y	Y	--	--
Set the user environment	Set the user environment	Open the Preferences window and set the user environment.	Y	Y	Y	--	Y	Y	Y	--	--
Start linked products	Launch the GUI of another application	Launch the application that reported a JP1 event, and view or manipulate information.	Y	Y	Y	--	Y	Y	Y	--	--
	Open the Tool Launcher window	Use the Tool Launcher window to start linked products.	Y	Y	Y	--	Y	Y	Y	--	--
	Launch the Rule Operation viewer GUI	Launch the Rule Log Details window of JP1/IM - Rule Operation from the Action Log window, Action Log Details window, or List of Action Results window.	Y	Y	Y	--	--	--	--	--	--

Legend:

Admin: `JP1_Console_Admin`

Operator: `JP1_Console_Operator`

User: `JP1_Console_User`

Y: Can perform the operation.

--: Cannot perform the operation.

Notes:

The assigned JP1 permission level is checked only when the JP1 user logs in. If the JP1 permission level is subsequently changed on the authentication server, the new permission level takes effect the next time the JP1 user logs in.

#:

Operations for the hosts in the business group, or JP1 events generated in the business group can be displayed.

E.2 Operating permissions required for system monitoring using the Central Scope

User operations related to system monitoring using the Central Scope can be broadly classified into two types:

- Monitoring: Operations performed while monitoring the system using the Monitoring Tree window or Visual Monitoring window
- Editing: Operations for creating or editing the system monitoring environment using the Monitoring Tree (Editing) window or Visual Monitoring (Editing) window

The operating permissions required for each type of operation are described below.

(1) Monitoring permissions (Monitoring Tree window and Visual Monitoring window)

The following table describes the operating permissions required for monitoring operations.

Table E–3: Operating permissions required for Central Scope operations (in the Monitoring Tree window)

Type of operation			JP1 resource group	JP1 permission level			
Category	Operation	Description		Admin	Operato r	User	None
System settings	Add, change, and delete common conditions	Add, change, and delete common conditions in JP1/IM - Manager.	`JP1_Console`	Y	--	--	--
System operations and viewing (when the monitoring range settings are enabled)	Change monitoring node attributes	Change the following attributes of a monitoring node: • Monitoring node name • Icon • Visual Icon • Status • Monitoring status • Basic information • Status change condition# • Event generation condition	JP1 resource group for the particular node	Y	Y	--	--
			`JP1_Console`	Y	--	--	--

Type of operation			JP1 resource group	JP1 permission level			
Category	Operation	Description		Admin	Operato r	User	None
		#: Excluding adding or changing a common condition in JP1/IM - Manager.					
	View monitoring nodes	View monitoring nodes in the Monitoring Tree window.	JP1 resource group for the particular node	Y	Y	Y	--
			`JP1_Console`	Y	--	--	--
	Search for monitoring nodes	Search for monitoring nodes in the Search window.	JP1 resource group for the particular node	Y	Y	Y	--
			`JP1_Console`	Y	--	--	--
	Display monitoring node attributes	Check the attributes of a monitoring node in the Properties window.	JP1 resource group for the particular node	Y	Y	Y	--
			`JP1_Console`	Y	--	--	--
	Perform visual monitoring	Monitor nodes in the Visual Monitoring window.	JP1 resource group for the particular node	Y	Y	Y	--
			`JP1_Console`	Y	--	--	--
	Display guide information	Check guide information in the Guide window.	JP1 resource group for the particular node	Y	Y	Y	--
			`JP1_Console`	Y	--	--	--
	Search for status change events	Search for JP1 events that triggered a status change.	JP1 resource group for the particular node	Y	Y	Y	--
			`JP1_Console`	Y	--	--	--
System operations and viewing (when the monitoring range settings are disabled)	Changing monitoring node attributes	Change the following attributes of a monitoring node: • Monitoring node name • Icon • Visual Icon • Status • Monitoring status • Basic information	`JP1_Console`	Y	Y	--	--

Type of operation			JP1 resource group	JP1 permission level			
Category	Operation	Description		Admin	Operator	User	None
		• Status change condition# • Event generation condition #: Excluding adding or changing a common condition in JP1/IM - Manager.					
	View monitoring nodes	View monitoring nodes in the Monitoring Tree window.	`JP1_Console`	Y	Y	Y	Y
	Search for monitoring nodes	Search for monitoring nodes in the Search window.	`JP1_Console`	Y	Y	Y	Y
	Display monitoring node attributes	Check the attributes of a monitoring node in the Properties window.	`JP1_Console`	Y	Y	Y	Y
	Perform visual monitoring	Monitor nodes in the Visual Monitoring window.	`JP1_Console`	Y	Y	Y	Y
	Display guide information	Check guide information in the Guide window.	`JP1_Console`	Y	Y	Y	Y
	Search for status change events	Search for JP1 events that triggered a status change.	`JP1_Console`	Y	Y	Y	Y
Toggle between **Detailed view** and **Icon view**		Toggle between **Detailed view** and **Icon view** in the detailed view area of the Monitoring Tree window. In **Icon view**, draw a selection rectangle and arrange icons evenly.	`JP1_Console`	Y	Y	Y	Y
View tree editing		View the Monitoring Tree (Editing) window.	`JP1_Console`	Y	Y	Y	Y
List login users		View the Login User List window.	`JP1_Console`	Y	Y	Y	Y
Display the event console		View the Event Console window.	`JP1_Console`	Y	Y	Y	Y
Open the Tool Launcher window		View the Tool Launcher window.	`JP1_Console`	Y	Y	Y	Y
Save monitoring trees locally		Save monitoring trees to the local host.	`JP1_Console`	Y	Y	Y	Y

Legend:

Admin: `JP1_Console_Admin`

Operator: `JP1_Console_Operator`

User: `JP1_Console_User`

Y: Can perform the operation.

--: Cannot perform the operation.

Notes:

- When a JP1 user is granted two or more JP1 permission levels, and a particular operation is permitted by one level but prohibited by another, the operation is permitted.
- Menus and buttons for functions that are not permitted under the various permission levels are unavailable in the JP1/IM - View windows.
- The assigned JP1 permission level is checked only when the JP1 user logs in. If the JP1 permission level is subsequently changed on the authentication server, the new permission level takes effect the next time the JP1 user logs in.

Table E–4: Operating permissions required for Central Scope (Visual Monitoring window)

Type of operation			JP1 resource group	JP1 permission level			
Category	Operation	Description		Admin	Operato r	User	None
System settings	Add, change, and delete common conditions	Add, change, and delete common conditions in JP1/IM - Manager.	JP1_Conso le	Y	--	--	--
System operations and viewing (when the monitoring range settings are enabled)	Change monitoring node attributes	Change the following attributes of a monitoring node: • Monitoring node name • Icon • Visual Icon • Status • Monitoring status • Basic information • Status change condition# • Event generation condition #: Excluding adding or changing a common condition in JP1/IM - Manager.	JP1 resource group for the particular node	Y	Y	--	--
			JP1_Conso le	Y	--	--	--
	Display a monitoring tree	Select nodes in a Visual Monitoring window and display them in the Monitoring Tree window.	JP1 resource group for the particular node	Y	Y	Y	--
			JP1_Conso le	Y	--	--	--
	Search for monitoring nodes	Search for monitoring nodes in the Search window.	JP1 resource group for the particular node	Y	Y	Y	--
			JP1_Conso le	Y	--	--	--
	Display monitoring node attributes	Check the attributes of a monitoring node in the Properties window.	JP1 resource group for the particular node	Y	Y	Y	--
			JP1_Conso le	Y	--	--	--
	Display guide information	Check guide information in the Guide window.	JP1 resource group for the particular node	Y	Y	Y	--
			JP1_Conso le	Y	--	--	--
	Search for status change events	Search for JP1 events that triggered a status change.	JP1 resource group for the particular node	Y	Y	Y	--

Type of operation			JP1 resource group	JP1 permission level			
Category	Operation	Description		Admin	Operato r	User	None
			`JP1_Console`	Y	--	--	--
System operations and viewing (when the monitoring range settings are disabled)	Changing monitoring node attributes	Change the following attributes of a monitoring node: • Monitoring node name • Icon • Visual Icon • Status • Monitoring status • Basic information • Status change condition# • Event generation condition #: Excluding adding or changing a common condition in JP1/IM - Manager.	`JP1_Console`	Y	Y	--	--
	Display a monitoring tree	Select nodes in a Visual Monitoring window and display them in the Monitoring Tree window.	`JP1_Console`	Y	Y	Y	Y
	Search for monitoring nodes	Search for monitoring nodes in the Search window.	`JP1_Console`	Y	Y	Y	Y
	Display monitoring node attributes	Check the attributes of a monitoring node in the Properties window.	`JP1_Console`	Y	Y	Y	Y
	Display guide information	Check guide information in the Guide window.	`JP1_Console`	Y	Y	Y	Y
	Search for status change events	Search for JP1 events that triggered a status change.	`JP1_Console`	Y	Y	Y	Y

Legend:

Admin: `JP1_Console_Admin`

Operator: `JP1_Console_Operator`

User: `JP1_Console_User`

Y: Can perform the operation.

--: Cannot perform the operation.

(2) Editing operations (Monitoring Tree (Editing) window and Visual Monitoring (Editing) window)

No special JP1 user operations are involved in editing the Monitoring Tree window or Visual Monitoring window of the Central Scope. Any user who can log in to the OS can perform editing.

However, operations such as automatically generating a monitoring tree or saving edited information to JP1/IM - Manager require connection to JP1/IM - Manager.

To log in to JP1/IM - Manager in such cases, you must have JP1 user permissions.

The following table describes edit operations and required operating permissions.

Table E–5: Operating permissions required for Central Scope operations (in the Monitoring Tree (Editing) window)

Type of operation			JP1 resource group	JP1 permission level			
Category	Operation	Description		Admin	Operator	User	None
Operations that include login processing	Automatically generate a tree	Collect monitoring tree information from the system through JP1/IM - Manager.	`JP1_Console`	Y	--	--	--
	Acquire a tree from the server	Acquire monitoring tree data from JP1/IM - Manager.	`JP1_Console`	Y	--	--	--
	Update server data	Export edited data to JP1/IM - Manager.	`JP1_Console`	Y	--	--	--
	Acquire the latest definitions	Acquire a list of common conditions managed by JP1/IM - Manager.	`JP1_Console`	Y	--	--	--
	Rearrange or delete listed Visual Monitoring windows	Change the display order of the Visual Monitoring windows managed by JP1/IM - Manager, or delete a Visual Monitoring window from the list.	`JP1_Console`	Y	--	--	--
Operations without login processing	Move monitoring nodes	Move monitoring nodes.	Not required	Not required	Not required	Not required	Not required
	Add and delete monitoring nodes, and change node attributes	Add and delete monitoring nodes, and change node attributes.# #: Defining a status change condition involves setting a common condition, which requires login to JP1/IM - Manager (`JP1_Console_Admin` permission required).	Not required	Not required	Not required	Not required	Not required
	Add, change, and delete common conditions	Add, change, and delete common conditions.	Not required	Not required	Not required	Not required	Not required
	Save monitoring trees locally	Save monitoring trees to the local host.	Not required	Not required	Not required	Not required	Not required
	Acquire local monitoring trees	Acquire monitoring tree data saved to the local host.	Not required	Not required	Not required	Not required	Not required
	Search for monitoring nodes	Search for monitoring nodes in the Search window.	Not required	Not required	Not required	Not required	Not required
	Display visual monitoring (editing)	Display the Visual Monitoring (Editing) window.	Not required	Not required	Not required	Not required	Not required

Legend:

Admin: `JP1_Console_Admin`

Operator: JP1_Console_Operator

User: JP1_Console_User

Y: Can perform the operation.

--: Cannot perform the operation.

Not required: Any user who can log in to the OS can perform the operation.

Table E–6: Operating permissions required for Central Scope operations (in the Visual Monitoring (Editing) window)

Type of operation			JP1 resource group	JP1 permission level			
Category	Type of operation	Description		Admin	Operator	User	None
Operations that include login processing	Acquire data from the server	Acquire information about the Visual Monitoring windows managed by JP1/IM - Manager.	JP1_Console	Y	--	--	--
	Update server data	Export edited data to JP1/IM - Manager.	JP1_Console	Y	--	--	--
Operations without login processing	Arrange monitoring nodes	Drag-and-drop monitoring nodes from the Monitoring Tree (Editing) window.	Not required	Not required	Not required	Not required	Not required
	Delete monitoring nodes	Delete monitoring nodes placed in the Monitoring Tree (Editing) window.	Not required	Not required	Not required	Not required	Not required
	Change the background image	Change the background image.	Not required	Not required	Not required	Not required	Not required
	Save data locally	Save data to the local host.	Not required	Not required	Not required	Not required	Not required
	Acquire local data	Acquire data from the local host.	Not required	Not required	Not required	Not required	Not required

Legend:

Admin: JP1_Console_Admin

Operator: JP1_Console_Operator

User: JP1_Console_User

Y: Can perform the operation.

--: Cannot perform the operation.

Not required: Any user who can log in to the OS can perform the operation.

E.3 Operating permissions required for IM Configuration Management

The following table describes the operating permissions required for IM Configuration Management.

Table E–7: Operating permissions required for IM Configuration Management

Type of operation			JP1 permission level		
Category	Operation	Description	Admin	Manager	User
Host management	Register hosts	Register managed hosts (JP1/Base hosts or VMM hosts) with IM Configuration Management.	Y	Y	--
	Collect host information	Collect and store host and product information from managed hosts.	Y	Y	--
	Edit host information	Edit host and product information in a host list	Y	Y	--
	Delete hosts	Delete hosts from a host list.	Y	Y	--
	View hosts	View a list of registered hosts.	Y	Y	Y
IM configuration	Collect	Collect IM configuration information.	Y	Y	--
	Display	Display IM configuration information.	Y	Y	Y
	Edit information and acquire exclusive rights	Edit IM configuration information and acquire exclusive rights.	Y	--	--
	Apply	Apply edited IM configuration information to the system.	Y	--	--
Profiles	Collect	Collect valid configuration information and configuration file contents from agents (JP1/Base).	Y	Y	--
	Display	Display valid configuration information and configuration file contents for each host in the profile list.	Y	Y	Y
	Edit information and acquire exclusive rights	Edit configuration files for each host in the profile list and acquire exclusive rights.	Y	Y	--
	Apply	Apply edited configuration file contents to the system.	Y	Y	--
	List	View a list of information about registered profiles.	Y	Y	Y
Services	Status display	View the activity status of services on an agent (JP1/Base).	Y	Y	Y
Release of exclusive rights	IM configuration	Clear update rights set for an IM configuration.	Y	--	--
	Profiles	Clear exclusive rights set for a profile.	Y	Y	--

Legend:

Admin: `JP1_CF_Admin`

Manager: `JP1_CF_Manager`

User: `JP1_CF_User`

Y: Can perform the operation.

--: Cannot perform the operation.

Notes:

The JP1 resource group for JP1/IM is `JP1_Console`. Assign the JP1 permission level for operating IM Configuration Management to the JP1 resource group `JP1_Console`.

F. Support for Changing Communication Settings

In JP1/Base, which is the prerequisite program for JP1/IM - Manager, the communication settings can be changed to support a variety of network configurations. This allows you to use JP1/IM - Manager even in network configurations that have special requirements, such as the following:

- Specific communication network

  The JP1/IM - Manager and JP1/Base hosts are connected to multiple LANs, but you require them to communicate over a specific LAN only (using IP addresses other than those associated with the host names).

- Separate network

  The JP1/IM - Manager and JP1/Base hosts are connected to multiple LANs, but you do not want them to communicate across LANs (they cannot communicate using the IP address associated with the destination host name).

To change the communication settings, use the JP1/Base `jp1hosts` definition file, `jp1hosts2` definition file, and communication protocol settings file. For details on communication settings, see the description of JP1/Base communication settings for various network configurations in the *JP1/Base User's Guide*.

The following table describes the communication settings that can be entered in these two files for the functionality provided by JP1/IM - Manager and JP1/Base.

Table F–1: JP1/IM functions and support for communication settings (for viewer-manager communication)

Function	Communication setting		
	jp1hosts definition file	jp1hosts2 definition file	Communication protocol settings file
Command execution (JP1/IM - View -> JP1/Base)	Y	Y	Y
Event monitoring (JP1/IM - View -> JP1/IM - Manager (Central Console))	Y	Y	Y
Object status monitoring (JP1/IM - View -> JP1/IM - Manager (Central Scope))	Y	Y	Y
IM Configuration Management (JP1/IM - View -> JP1/IM - Manager (IM Configuration Management))	Y	Y	Y
Rule management (JP1/IM - View -> JP1/IM - Rule Operation)	Y	N	Y
Login (JP1/IM - View -> JP1/IM - Manager (Central Console))#	N	N	N

Legend:

Y: The communication setting can be changed, allowing JP1/IM - Manager to be used in a network configuration with special requirements.

N: The communication setting cannot be used because it is not supported.

(*product* -> *product*): Required product-to-product connection.

#: Depends on the OS's name resolution.

Table F–2: JP1/IM functions and support for communication settings (for manager-agent communication)

Function	Communication setting		
	jp1hosts definition file	jp1hosts2 definition file	Communication protocol settings file
Configuration management (JP1/Base -> JP1/Base)	Y	Y	Y
Command execution (JP1/Base -> JP1/Base)	Y	Y	Y
Event search (JP1/IM - Manager -> JP1/Base)	N	N	N
Definition collection and distribution (JP1/Base -> JP1/Base)	Y	Y	Y
IM Configuration Management (JP1/IM - Manager -> JP1/Base)	Y	Y	Y

Legend:

Y: The communication setting can be changed, allowing JP1/IM - Manager to be used in a network configuration with special requirements.

N: It might not be possible to use JP1/IM - Manager in a network configuration with special requirements even if the communication settings are changed.

(*product* -> *product*): Required product-to-product connection.

G. Regular Expressions

In JP1/IM, regular expressions can be used in various conditional expressions, such as an execution condition for an automated action or a search condition for finding JP1 events or monitoring nodes. (A *regular expression* is a means of representing a particular character string by the use of a special character when performing a search or replacing text.) Care is required, however, as the regular expressions you can use in JP1/IM depend on your operating system and the particular JP1/IM function in which the regular expression is used.

The following describes regular expressions that can be used in JP1/IM.

G.1 Types of regular expressions

The regular expressions available in JP1/IM differ according to the operating system and the function in which the regular expression is interpreted. This is because the various JP1/IM functions and operating systems support different types of regular expressions. These differences mean differences in the syntax of the available regular expressions. For details, see *G.2 Syntax of regular expressions*.

The types of regular expressions are as follows:

JP1-specific regular expressions (Windows)

Special characters that can be used as regular expressions, defined specifically in JP1.

You can change the JP1/IM and JP1/Base settings to operate with XPG4-compliant extended regular expressions, but this might result in unintended behavior. You should therefore review the defined conditional expressions and redefine them to comply with the extended regular expressions.

XPG4-compliant extended regular expressions (Windows)

Regular expressions (special characters) additional to the preset JP1-specific regular expressions.

XPG4 basic regular expressions (AIX)

XPG4 basic regular expressions provided by UNIX (for details, see the OS *regexp(5)*).

Care is required as the range of basic regular expressions you can use is dependent on the computer model and OS.

You can change the JP1/Base settings to operate with XPG4-compliant extended regular expressions, but this might result in unintended behavior. You should therefore review the existing settings and redefine them to comply with the extended regular expressions.

XPG4 extended regular expressions (AIX)

XPG4 extended regular expressions provided by UNIX (for details, see the OS *regexp(5)*). These are basically XPG4 basic regular expressions plus a number of additional regular expressions (special characters), but with some XPG4 basic regular expressions deleted.

Care is required as the range of extended regular expressions you can use is dependent on the computer model and OS.

The table below describes the functions in which regular expressions can be used and the types of regular expressions that each function supports.

POSIX1003.2 basic regular expressions (Linux)

POSIX1003.2 basic regular expressions provided by Linux (for details, see the OS *regex*). Care is required as the range of basic regular expressions you can use is dependent on the OS. You can change the JP1/Base settings to operate with POSIX1003.2 extended regular expressions, but this might result in unintended behavior. You should therefore review the existing settings and redefine them to comply with the extended regular expressions.

POSIX1003.2 extended regular expressions (Linux)

POSIX1003.2 extended regular expressions provided by Linux (for details, see the OS *regexp(7)*). Care is required as the range of extended regular expressions you can use is dependent on the OS.

Table G–1: Regular expressions that can be used in JP1/IM functions

Function	Description	Windows		AIX		Linux	
		Default	Can be set	Default	Can be set	Default	Can be set
Search for events from JP1/IM - View	Regular expressions can be used in JP1 event search conditions. The types of regular expressions that can be used depend on the JP1/Base settings on the target host.	JP1-specific regular expressions	Extended regular expressions (XPG4-compliant)	Basic regular expressions (XPG4)	Extended regular expressions (XPG4)	Basic regular expressions (POSIX1003.2)	Extended regular expressions (POSIX1003.2)
Search for monitoring nodes from JP1/IM - View	Regular expressions can be used in monitoring node search conditions. The types of regular expressions are fixed.	Extended regular expressions (XPG4-compliant)	--	Extended regular expressions (XPG4)	--	Extended regular expressions (POSIX1003.2)	--
Display event guide information	Regular expressions can be used in conditions for displaying event guide information. The types of regular expressions are fixed.	Extended regular expressions (XPG4-compliant)	--	Extended regular expressions (XPG4)	--	Extended regular expressions (POSIX1003.2)	--
Change monitoring node status and display guide information	Regular expressions can be used in the common conditions and individual conditions of monitoring node status change conditions, and in conditions for displaying guide information. The types of regular expressions are fixed.	Extended regular expressions (XPG4-compliant)	--	Extended regular expressions (XPG4)	--	Extended regular expressions (POSIX1003.2)	--
Automated actions	Regular expressions can be used in conditions for executing automated actions. In Windows, the types of regular expressions that can be used depend on the settings in the JP1/IM - Manager that executes the automated action. (Fixed in UNIX.)	Extended regular expressions (XPG4-compliant)	JP1-specific regular expressions	Extended regular expressions (XPG4)	--	Extended regular expressions (POSIX1003.2)	--
Issue correlation events	Regular expressions can be used in the event attribute specified in a correlation event generation condition. The types of regular expressions are fixed.	Extended regular expressions (XPG4-compliant)	--	Extended regular expressions (XPG4)	--	Extended regular expressions (POSIX1003.2)	--
Filtering • Event receiver filter • Severe events filter • View filter	Regular expressions can be used in conditions for displaying JP1 events in the Event Console window. The types of regular expressions are fixed in both Windows and UNIX.	Extended regular expressions (XPG4-compliant)	--	Basic regular expressions (XPG4)	--	Extended regular expressions (POSIX1003.2)	--

Function	Description	Windows		AIX		Linux	
		Default	Can be set	Default	Can be set	Default	Can be set
- Event acquisition filter - Common exclusion-condition (basic mode)	Regular expressions can be used in conditions for JP1 event acquisition by JP1/IM - Manager from JP1/Base on the manager. The types of regular expressions that can be used depend on the settings in JP1/Base on the manager.	JP1-specific regular expressions	Extended regular expressions (XPG4-compliant)	Basic regular expressions (XPG4)	Extended regular expressions (XPG4)	Basic regular expressions (POSIX1003.2)	Extended regular expressions (POSIX1003.2)
Severity changing	Regular expressions can be used in event conditions for which you change the severity levels using the severity changing function. The types of regular expressions are fixed in both Windows and UNIX.	Extended regular expressions (XPG4-compliant)	--	Extended regular expressions (XPG4)	--	Extended regular expressions (POSIX1003.2)	--
Display message change function	Regular expressions can be used in event conditions for JP1 events whose display message is to be changed. The types of regular expressions are fixed in both Windows and UNIX.	Extended regular expressions (XPG4-compliant)	--	Extended regular expressions (XPG4)	--	Extended regular expressions (POSIX1003.2)	--
Common exclusion-condition (extended mode)	Regular expressions can be used in conditions for excluding events in common exclusion-condition (extended mode). The types of regular expressions are fixed in both Windows and UNIX.	Extended regular expressions (XPG4-compliant)	--	Extended regular expressions (XPG4)	--	Extended regular expressions (POSIX1003.2)	--
Event-source-host mapping	Regular expressions can be used when the event source host name is specified in the function corresponding to the **Event source host name** attribute. The types of regular expressions are fixed in both Windows and UNIX.	Extended regular expressions (XPG4-compliant)	--	Extended regular expressions (XPG4)	--	Extended regular expressions (POSIX1003.2)	--
Repeated event condition	Regular expressions can be used in the repeated event conditions specified for repeated-event monitoring suppression. The types of regular expressions are fixed in both Windows and UNIX.	Extended regular expressions (XPG4-compliant)	--	Extended regular expressions (XPG4)	--	Extended regular expressions (POSIX1003.2)	--
Remote monitoring	Regular expressions can be used in the log conditions that are converted into JP1 events by remote monitoring. The types of regular expressions are fixed in both Windows and UNIX.	Extended regular expressions (XPG4-compliant)	--	Extended regular expressions (XPG4)	--	Extended regular expressions (POSIX1003.2)	--

Legend:

--: Cannot be changed because extended regular expressions are used by default.

As shown above, under the default settings, the types of regular expressions used in JP1/IM differ according to the function and operating system used. You need to be aware of these differences when using regular expressions.

If you prefer to use regular expressions transparently, you can change the settings and use extended regular expressions compliant with the XPG4 standard in Windows, or extended regular expressions according to XPG4 in UNIX. We recommend changing the settings because you can then use regular expressions without regard to OS-based or function-based differences in usage.

For details on JP1/IM settings, see *Automated action environment definition file (action.conf.update)* in *Chapter 2. Definition Files* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference*.

For details on the JP1/Base functions that can use regular expressions, and the types of regular expressions used in JP1/Base, see the chapter on JP1/Base installation and setup in the *JP1/Base User's Guide*.

G.2 Syntax of regular expressions

The following regular expressions can be used in JP1/IM. Use them in accordance with the coding conventions explained below.

> **Important**
>
> We advise against using regular expressions other than those described here because the specifications differ according to the computer model and operating system. Use only the regular expressions described below.

(1) Ordinary characters

An *ordinary character* is one that requires a complete match with itself when specified as the search target in a regular expression. The only characters not handled as ordinary characters are control codes and special characters.

(2) Special characters

Special characters are the following: `^ $ . * + ? | ( ) { } [ ] \`. These special characters are explained below.

`^`

The caret (`^`) means the first characters (match the start). The caret is a special character only when used as the first character in a regular expression. When used elsewhere, the caret is handled as an ordinary character.

When a caret is specified as a special character, lines beginning with the specified string make a match.

`$`

The dollar sign (`$`) means the last characters (match the end). It is a special character only when used as the last character in a regular expression. When used elsewhere, the dollar sign is handled as an ordinary character.

When a dollar sign is specified as a special character, lines ending with the specified string make a match. When `$` and `^` are used together, lines containing only the specified string make a match.

`.` (period)

The period (`.`) means any single character.

When a period is specified as a special character, any single character other than a linefeed character makes a match.

`*`

The asterisk (`*`) means zero or more occurrences of the preceding character.

+

In JP1-specific regular expressions and basic regular expressions, the plus sign (+) is handled as an ordinary character.

As a special character, + means one or more occurrences of the preceding character.

?

In JP1-specific regular expressions and basic regular expressions, the question mark (?) is handled as an ordinary character.

As a special character, ? means zero or one occurrence of the preceding character.

|

In JP1-specific regular expressions and basic regular expressions, the vertical bar (|) is handled as an ordinary character.

As a special character, | means an OR condition between the regular expressions on either side. It is used in combination with the special characters ( ).

( )

In JP1-specific regular expressions and basic regular expressions, left and right parentheses are handled as ordinary characters.

As special characters, ( ) group the enclosed regular expression.

Parentheses are used to explicitly indicate to the program that the enclosed characters are a regular expression. They are mainly used with a vertical bar (|). (See *G.4 Tips on using regular expressions*.)

{ }

In JP1-specific regular expressions and basic regular expressions, curly brackets are handled as ordinary characters.

As special characters, { } mean that the preceding character occurs repeatedly for the number of times specified inside the curly brackets.

[ ]

In JP1-specific regular expressions and basic XPG4 regular expressions, square brackets are handled as ordinary characters.

As special characters, [ ] mean a match with any of the characters enclosed in the square brackets (or with any character *not* enclosed if a caret (^) is the first character).

\

The backslash (\) cancels a special character (^ $. * + ? | ( ) { } [ ] \).#

A special character preceded by a backslash is handled as an ordinary character. Use the backslash only to cancel a special character. You can sometimes use an alphanumeric character as a regular expression indicating a control code (linefeed code or tab character, for example) by prefixing it with a backslash. However, this can lead to unintended behavior as the regular expression will be handled differently according to the operating system and product.

#

In JP1-specific regular expressions and basic XPG4 regular expressions, the following are handled as ordinary characters: + ? | ( ) { } [ ]

In basic POSIX 1003.2 regular expressions, the following are handled as ordinary characters: + ? | ( ) { }

G.3 Comparison between types of regular expressions

The following table describes the differences in the types of regular expressions that can be used in Windows and other operating systems.

Table G–2: Comparison between types of regular expressions

Expression	Meaning	Windows		AIX		Linux	
		JP1	Extd XPG4	Basic	Extd	Basic POSIX	Extd POSIX
String	Matches lines containing the specified string.	Y	Y	Y	Y	Y	Y
^*string*	Matches the specified string at the beginning of a line.	Y	Y	Y	Y	Y	Y
string$	Matches the specified string at the end of a line.	Y	Y	Y	Y	Y	Y
^*string*$	Combination of ^ and $. Matches lines containing only the specified string.	Y	Y	Y	Y	Y	Y
^$	Combination of ^ and $. Matches empty lines.	Y	Y	Y	Y	Y	Y
. (period)	Matches any single character.	Y	Y	Y	Y	Y	Y
*char**	Matches strings of zero or more occurrences of the preceding character.	Y	Y	Y	Y	Y	Y
.*	Combination of a period (.) and asterisk (*). Matches any character string.	Y	Y	Y	Y	Y	Y
char+	Matches strings of one or more occurrences of the preceding character.	N	Y	N	Y	N	Y
char?	Matches strings of zero or one occurrence of the preceding character.	N	Y	N	Y	N	Y
regex | *regex*	Matches either regular expression.	N	Y	N	Y	N	Y
(*regex*)	Groups a regular expression. Used to explicitly indicate to the program that the specified characters are a regular expression. Used mainly with a vertical bar (|). (See *G.4 Tips on using regular expressions*.)	N	Y	N	Y	N	Y
char{*n*}	Matches strings in which the preceding character occurs *n* times.	N	Y	N	Y	N	Y
char{*n*,}	Matches strings in which the preceding character occurs at least *n* times.	N	Y	N	Y	N	Y
char{*n*,*m*}	Matches strings in which the preceding character occurs at least *n* times but no more than *m* times.	N	Y	N	Y	N	Y
[*string*]	Matches any character specified in the string enclosed in square brackets.	N	Y	N	Y	N	Y
[^*string*]	Matches any character not specified in the string enclosed in square brackets.	N	Y	N	Y	Y	Y

Expression	Meaning	Windows		AIX		Linux	
		JP1	Extd XPG4	Basic	Extd	Basic POSIX	Extd POSIX
[*char*-*char*]	Matches any character in the range, in ascending order of the character codes.	N	Y	N	Y	Y	Y
[^*char*-*char*]	Matches any character not in the specified range, in ascending order of the character codes.	N	Y	N	Y	Y	Y
\special-char	Handles the special character as an ordinary character.	N	Y	N	Y	N	Y

Legend:

JP1: JP1-specific regular expression

Extd XPG4: XPG4-compliant extended regular expression

Basic: XPG4 basic regular expression

Extd: XPG4 extended regular expression

Basic POSIX: POSIX 1003.2-compliant basic regular expression

Extd POSIX: POSIX 1003.2-compliant extended regular expression

Y: Can be used.

N: Cannot be used.

G.4 Tips on using regular expressions

- To use extended regular expressions by extending JP1-specific regular expressions (Windows), XPG4 basic regular expressions (AIX), or POSIX1003.2 basic regular expressions (Linux), you must review the existing settings and redefine them to comply with the extended regular expressions, so as to avoid unintended behavior.
- Control codes (linefeed codes, tab characters, and so on) might be handled differently depending on the product and operating system. For this reason, you should not include control codes in a regular expression used to specify a condition for a message.
- A period followed by an asterisk (`.*`) matches any character. If you make frequent use of this regular expression, it might take a long time to find matches. When defining a condition to match a long message, for example, use the period-and-asterisk combination only where required in the search string.

  In an environment that supports extended regular expressions, you can use the combination `[^ ]*` instead of the period-and-asterisk combination to match non-null characters. This reduces the search time.
- When the regular expression "`.*`" is used for a condition of partial match, the condition is the same regardless of whether "`.*`" is specified at the beginning and end of the condition.

  For example, examples 1 and 2 below specify the same condition.

  (Example 1) Regular expression that matches the character string that includes `A001 Δ:ΔWeb server`.

  ```
  .*A001Δ:ΔWeb server.*
  ```

  (Example 2) Regular expression that matches the character string that includes `A001Δ:ΔWeb server`.

  ```
  A001Δ:ΔWeb server
  ```

  Therefore, do not specify "`.*`" at the beginning and end of the string, as it might increase the search time.

  For the event guide information file (`jco_guide.txt`), by default, a condition using a regular expression is satisfied only when the specified string makes a complete match. Note that, in this case, the search results will differ depending on whether "`.*`" is specified at the beginning and end of the string.

- The vertical bar (`|`) represents an OR condition. Note the following when using this OR condition in a regular expression:

  Because a vertical bar (`|`) has low precedence in a regular expression, you must specify the range of the OR condition explicitly; otherwise, it might work erroneously or not at all. You can specify the range of an OR condition by enclosing it in parentheses. An example of specifying the conditions for a source event server name as an OR condition is shown below.

  Example: JP1 events issued by `work` or `host`

  ```
  ^.*Δ.*Δ.*Δ.* Δ.*Δ(work|host)Δ.*Δ.*Δ.*Δ.*$
  ```

- Spaces before or after the vertical bar (`|`) special character are treated as characters. Do not enter a space unless you want it to be included in the OR condition.
- When an extended regular expression is used, if square brackets (`[]`), curly brackets (`{}`), or parentheses (`()`) are not properly paired, a syntax error occurs. If you want to use a square bracket, curly bracket, or parenthesis as an ordinary character, place a backslash (`\`) immediately before the character so that the character is not used as a special character.

  The following shows an example of this case:

  Example: When you want to use a left parenthesis (`(`) as an ordinary character:

  ```
  \(
  ```

G.5 Examples of using regular expressions

The following table describes examples of using regular expressions.

Table G–3: Examples of using regular expressions

Expression	Meaning	String specified as a regular expression	Example pattern	Match (Y) or No match (N)
string	Matches lines containing the specified string.	`spring`	**spring** has come.	Y
			winter-summer-autumn-**spring**	Y
			-----**spring**-----	Y
^*string*	Matches the specified string at the beginning of a line.	`^spring`	**spring** has come.	Y
			winter-summer-autumn-spring	N
			-----spring-----	N
string$	Matches the specified string at the end of a line.	`spring$`	spring has come.	N
			winter-summer-autumn-**spring**	Y
			-----spring-----	N
^*string*$	Matches lines containing only the specified string.	`^spring$`	spring has come.	N
			winter-summer-autumn-spring	N
			spring	Y
			spring	N
^$	Matches empty lines.	`^$`		Y
			spring	N

Expression	Meaning	String specified as a regular expression	Example pattern	Match (Y) or No match (N)
. (period)	Matches any single character.	`in.e`	w**inte**r has come.	Y
			mother of **inve**ntion	Y
			life is **in e**verything	Y
			eight nine ten	N
			increasing population	N
		`s..ing`	picnic in **spring**	Y
			skiing in winter	Y
[*string*] #1, #2	Matches any character specified in the string enclosed in square brackets.	`[pr]`	s**pr**ing has come.	Y
			today is monday.	N
[*char*-*char*] #1, #2	Matches any character in the range, in ascending order of the character codes.	`[a-i]`	spr**i**n**g** **ha**s **c**om**e**.	Y
[^*char*-*char*] #1, #2	Matches any character not in the specified range, in ascending order of the character codes.	`[^a-i]`	**spr**i**n**g ha**s** **com**e.	Y
*char**	Matches strings of zero or more occurrences of the preceding character.	`ro*m`	te**rm**inal	Y
			cd-**rom**	Y
			living **room**	Y
		`h.*n`	T**his is a pen**.	Y
			T**hat is an** apple.	Y
regex | *regex* #1, #2, #3	Matches either regular expression.	`[0-9]+|apple`	That is an **apple**.	Y
			spring in **2003**	Y
\special-char #1, #2, #3	Handles the special character as an ordinary character.	`o\.h`	<stdi**o.h**>	Y
			another man	N
(*regex*) #1, #2, #3	Groups a regular expression. Used to explicitly indicate to the program that the specified characters are a regular expression. Used mainly with a vertical bar (|). (See *G.4 Tips on using regular expressions*.)	`i(n.e|ng)`	w**inte**r has come.	Y
			interest**ing** book	Y

Legend:

Bold type: String matching the specified regular expression.

Y: The example pattern is a match.

N: The example pattern is not a match.

#1: Cannot be specified as a JP1-specific regular expression.

#2: Cannot be specified as a basic XPG4 regular expression.

#3: Cannot be specified as a basic POSIX1003.2 regular expression.

H. Connectivity with Previous Versions

This appendix describes restrictions when connecting different versions of JP1/IM products or different versions of JP1/Base on agents.

H.1 Connectivity with version 11 products

The following describes restrictions that are placed when JP1/IM - View 11-50 is connected to JP1/IM - Manager 11-00 to 11-10 and when JP1/IM - View 11-00 to 11-10 is connected to JP1/IM - Manager 11-50.

(1) Restrictions placed when JP1/IM - View 11-50 is connected to JP1/IM - Manager 11-00 to 11-10 (common to all components)

Table H–1: Restrictions placed when JP1/IM - View 11-50 is connected to JP1/IM - Manager 11-00 to 11-10 (common to all components)

JP1/IM - Manager version	Restrictions#
	1
11-00	Y
11-01	Y
11-10	--

Legend: Y: Applicable --: Not applicable

#: The restriction number corresponds to the number in the following table.

Table H–2: List of restrictions

No.	Details
1	Operation log data cannot be output.

(2) Restrictions placed when JP1/IM - View 11-50 is connected to JP1/IM - Manager 11-00 to 11-10 (when using the Central Console)

Table H–3: Restrictions placed when JP1/IM - View 11-50 is connected to JP1/IM - Manager 11-00 to 11-10 (when using the Central Console)

JP1/IM - Manager version	Restrictions#	
	1 to 4	5 to 10
11-00	Y	Y
11-01	Y	Y
11-10	--	Y

Legend: Y: Applicable --: Not applicable

#: The restriction number corresponds to the number in the following table.

Table H–4: List of restrictions

No.	Details
1	The **Suppressed event ID** field and the **Read Suppressed Event ID From Selected Event** button are not displayed in the following windows: • Event Search Conditions window • Settings for View Filter window
2	Performance reports of event-source hosts cannot be displayed because the **Display Performance** menu and the **Display Performance** button are not displayed in the following pages and windows: • **Monitor Events** page • **Severe Events** page • **Search Events** page • **Response-Waiting Events** page • Related Events window • Event Details window • Edit Event Details window
3	The event attribute values to be inherited by automated actions cannot be Base64 encoded or URL encoded.
4	The JP1/AJS - Web Console monitor window cannot be displayed from the event guide by using single sign-on.
5	You cannot set more than 1,025 repeated event conditions.
6	You cannot set more than 1,025 condition groups in the common exclusion-conditions in extended mode.
7	You cannot specify the status (enabled, disabled) of automated action definitions.
8	When automated action definitions are applied, you cannot inherit the suppression status and the status of satisfied conditions of the AND-joined conditions unless the action definition is edited.
9	You cannot specify items for **Target for exclusion** in the Common Exclusion-Condition Settings (Extended) window.
10	You cannot inherit arbitrary event attributes and character strings in incident manual-registration to JP1/Service Support from JP1/IM - View.

(3) Restrictions placed when JP1/IM - View 11-50 is connected to JP1/IM - Manager 11-00 to 11-10 (when using the Central Scope)

There are no restrictions on connecting JP1/IM - View 11-50 to JP1/IM - Manager 11-00 to 11-10 (when using the Central Scope).

(4) Restrictions placed when JP1/IM - View 11-50 is connected to JP1/IM - Manager 11-00 to 11-10 (when using IM Configuration Management)

Table H–5: Restrictions placed when JP1/IM - View 11-50 is connected to JP1/IM - Manager 11-00 to 11-10 (when using IM Configuration Management)

JP1/IM - Manager version	Restrictions#	
	1 to 5	6
11-00	Y	Y
11-01	Y	Y
11-10	--	Y

Legend: Y: Applicable --: Not applicable

#: The restriction number corresponds to the number in the following table.

Table H–6: List of restrictions

No.	Details
1	No notification that agent settings for log file trap information might have been changed is sent while the Display/Edit Profiles window is being used.
2	The enable/disable setting for starting processes automatically when the log file trap service is started cannot be changed in the Display/Edit Profiles window.
3	Log file trap information for non-cluster operation cannot be applied by file transmission in the Display/Edit Profiles window.
4	Host information cannot be collected unless the remote monitoring of the host whose host information is to be collected is stopped.
5	In the Remote Monitoring Settings window, SSH connections cannot be set up for individual hosts.
6	You cannot set more than 1,025 hosts in a single business or monitoring group.

(5) Restrictions placed when JP1/IM - View 11-00 to 11-10 is connected to JP1/IM - Manager 11-50 (common to all components)

There are no restrictions (common to components) on connecting JP1/IM - View 11-00 to 11-10 to JP1/IM - Manager 11-50.

(6) Restrictions placed when JP1/IM - View 11-00 to 11-10 is connected to JP1/IM - Manager 11-50 (when using the Central Console)

Table H–7: Restrictions placed when JP1/IM - View 11-00 to 11-10 is connected to JP1/IM - Manager 11-50 (when using the Central Console)

JP1/IM - View version	Restrictions#	
	1 to 3	4 to 6
11-00	Y	Y
11-01	Y	Y
11-10	--	Y

Legend: Y: Applicable --: Not applicable

#: The restriction number corresponds to the number in the following table.

Table H–8: List of restrictions

No.	Details
1	The **Suppressed event ID** field and the **Read Suppressed Event ID From Selected Event** button are not displayed in the following windows: • Event Search Conditions window • Settings for View Filter window
2	Performance reports of event-source hosts cannot be displayed because the **Display Performance** menu and the **Display Performance** button are not displayed in the following pages and windows: • **Monitor Events** page • **Severe Events** page • **Search Events** page • **Response-Waiting Events** page • Related Events window • Event Details window

No.	Details
	- Edit Event Details window
3	The JP1/AJS - Web Console monitor window cannot be displayed from the event guide by using single sign-on.
4	The Action Parameter Definitions window cannot be displayed if you are using an action definition file where DESC_VERSION is 4.
5	If automated actions are set to be excluded in the common exclusion-conditions in extended mode, the following operations cannot be done: - Displaying the System Environment Settings window - Setting additional common exclusion-conditions
6	You cannot inherit arbitrary event attributes and character strings in incident manual-registration to JP1/Service Support from JP1/IM - View.

(7) Restrictions placed when JP1/IM - View 11-00 to 11-10 is connected to JP1/IM - Manager 11-50 (when using the Central Scope)

There are no restrictions on connecting JP1/IM - View 11-00 to 11-10 to JP1/IM - Manager 11-50 (when using the Central Scope).

(8) Restrictions placed when JP1/IM - View 11-00 to 11-10 is connected to JP1/IM - Manager 11-50 (when using IM Configuration Management)

Table H–9: Restrictions placed when JP1/IM - View 11-00 to 11-10 is connected to JP1/IM - Manager 11-50 (when using IM Configuration Management)

JP1/IM - View version	Restrictions#	
	1 to 6	7
11-00	Y	Y
11-01	Y	Y
11-10	--	Y

Legend: Y: Applicable --: Not applicable

#: The restriction number corresponds to the number in the following table.

Table H–10: List of restrictions

No.	Details
1	No notification that agent settings for log file trap information might have been changed is sent while the Display/Edit Profiles window is being used.
2	The enable/disable setting for starting processes automatically when the log file trap service is started cannot be changed in the Display/Edit Profiles window.
3	Log file trap information for non-cluster operation cannot be applied by file transmission in the Display/Edit Profiles window.
4	Host information cannot be collected unless the remote monitoring of the host whose host information is to be collected is stopped.
5	In the Remote Monitoring Settings window, SSH connections cannot be set up for individual hosts.
6	When an agent configuration is applied by using the differential distribution method, the confirmation dialog box displays `KNAN20440-Q`, not `KNAN20441-Q` (the agent configuration is applied by the differential distribution method).
7	You cannot set more than 1,025 hosts in a single business or monitoring group.

H.2 Connectivity with version 10 products

The following describes restrictions that are placed when JP1/IM - View 11-50 is connected to JP1/IM - Manager 10-00 to 10-50 and when JP1/IM - View 10-00 to 10-50 is connected to JP1/IM - Manager 11-50.

(1) Restrictions placed when JP1/IM - View 11-50 is connected to JP1/IM - Manager 10-00 to 10-50 (common to all components)

Table H–11: Restrictions placed when JP1/IM - View 11-50 is connected to JP1/IM - Manager 10-00 to 10-50 (common to all components)

JP1/IM - Manager version	Restrictions#
	1 to 3
10-00	Y
10-10	Y
10-50	Y

Legend: Y: Applicable

#: The restriction numbers correspond to the numbers in the following table.

Table H–12: List of restrictions

No.	Details
1	Encrypted communication cannot be established with JP1/IM - Manager.
2	Connection cannot be established with JP1/IM - Manager in a different language environment.
3	Operation log data cannot be output.

(2) Restrictions placed when JP1/IM - View 11-50 is connected to JP1/IM - Manager 10-00 to 10-50 (when using the Central Console)

Table H–13: Restrictions placed when JP1/IM - View 11-50 is connected to JP1/IM - Manager 10-00 to 10-50 (when using the Central Console)

JP1/IM - Manager version	Restrictions#		
	1 to 3	4 to 8	9 to 22
10-00	Y	Y	Y
10-10	--	Y	Y
10-50	--	--	Y

Legend: Y: Applicable --: Not applicable

#: The restriction numbers correspond to the numbers in the following table.

Table H–14: List of restrictions

No.	Details
1	Repeated event conditions cannot be defined.
2	Repeated events for which monitoring is suppressed by repeated event monitoring suppression cannot be displayed in consolidated format.

No.	Details
3	Single sign-on cannot be used to connect to JP1/Navigation Platform.
4	The range of automated-action suppression and the issuance of the event to notify that suppression will continue cannot be specified.
5	Additional severity changing definitions cannot be registered, or severity changing definitions cannot be defined in the Severity Change Definition Settings window.
6	View filters cannot be used on the **Severe Events** page.
7	Events cannot be highlighted on the **Severe Events** page.
8	The range of events to be collected at login cannot be set.
9	Display message change settings cannot be specified.
10	Program-specific extended attributes cannot be displayed in the events list in the Event Console window.
11	Program-specific extended attributes cannot be specified in event conditions in the following definitions: • Severe event definition • Event acquisition filter • Common exclusion conditions • View filter • Event receiver filter
12	Program-specific extended attributes cannot be specified as item names in event conditions in the following definitions (program-specific extended attributes can be specified as attribute names): • Automated action definition • Common exclusion conditions extended definition file • Severity changing definition file • Display item definition file for repeated event conditions • Event search condition • Event-information mapping definitions
13	The **Suppressed event ID** field and the **Read Suppressed Event ID From Selected Event** button are not displayed in the following windows: • Event Search Conditions window • Settings for View Filter window
14	Performance reports of event-source hosts cannot be displayed because the **Display Performance** menu and the **Display Performance** button are not displayed in the following pages and windows: • **Monitor Events** page • **Severe Events** page • **Search Events** page • **Response-Waiting Events** page • Related Events window • Event Details window • Edit Event Details window
15	The event attribute values to be inherited by automated actions cannot be Base64 encoded or URL encoded.
16	The JP1/AJS - Web Console monitor window cannot be displayed from the event guide by using single sign-on.
17	You cannot set more than 1,025 repeated event conditions.
18	You cannot set more than 1,025 condition groups in the common exclusion-conditions in extended mode.
19	You cannot specify the status (enabled, disabled) of automated action definitions.
20	When automated action definitions are applied, you cannot inherit the suppression status and the status of satisfied conditions of the AND-joined conditions unless the action definition is edited.

No.	Details
21	You cannot specify items for **Target for exclusion** in the Common Exclusion-Condition Settings (Extended) window.
22	You cannot inherit arbitrary event attributes and character strings in incident manual-registration to JP1/Service Support from JP1/IM - View.

(3) Restrictions placed when JP1/IM - View 11-50 is connected to JP1/IM - Manager 10-00 to 10-50 (when using the Central Scope)

Table H–15: Restrictions placed when JP1/IM - View 11-50 is connected to JP1/IM - Manager 10-00 to 10-50 (when using the Central Scope)

JP1/IM - Manager version	Restrictions#
	1 to 5
10-00	Y
10-10	Y
10-50	--

Legend: Y: Applicable --: Not applicable

#: The restriction numbers correspond to the numbers in the following table.

Table H–16: List of restrictions

No.	Details
1	Margins of monitoring node icon and monitoring node name cannot be hidden.
2	Transmission factor cannot be set for monitoring node icons.
3	Status colors of monitoring node and monitoring node name cannot be changed.
4	Moving of monitoring node icon cannot be suppressed in the Monitoring Tree and Visual Monitoring windows.
5	Timing of the flashing alarm lamp cannot be changed.

(4) Restrictions placed when JP1/IM - View 11-50 is connected to JP1/IM - Manager 10-00 to 10-50 (when using IM Configuration Management)

Table H–17: Restrictions placed when JP1/IM - View 11-50 is connected to JP1/IM - Manager 10-00 to 10-50 (when using IM Configuration Management)

JP1/IM - Manager version	Restrictions#	
	1 to 2	3 to 9
10-00	Y	Y
10-10	--	Y
10-50	--	Y

Legend: Y: Applicable --: Not applicable

#: The restriction numbers correspond to the numbers in the following table.

Table H–18: List of restrictions

No.	Details
1	Virtualization management information about KVM or HCSM cannot be set or displayed.
2	Information about a host that holds virtualization management information about KVM or HCSM cannot be edited or deleted. In addition, `Unknown` is displayed as the host type.
3	Event IDs and log file trap names cannot be set in the event log trap action definitions and remote-monitoring event log trap action definitions.
4	No notification that agent settings for log file trap information might have been changed is sent while the Display/Edit Profiles window is being used.
5	The enable/disable setting for starting processes automatically when the log file trap service is started cannot be changed in the Display/Edit Profiles window.
6	Log file trap information for non-cluster operation cannot be applied by file transmission in the Display/Edit Profiles window.
7	Host information cannot be collected unless the remote monitoring of the host whose host information is to be collected is stopped.
8	In the Remote Monitoring Settings window, SSH connections cannot be set up for individual hosts.
9	You cannot set more than 1,025 hosts in a single business or monitoring group.

(5) Restrictions placed when JP1/IM - Manager 11-50 is connected to JP1/IM - View 10-00 to 10-50 (common to all components)

Table H–19: Restrictions placed when JP1/IM - Manager 11-50 is connected to JP1/IM - View 10-00 to 10-50 (common to all components)

JP1/IM - View version	Restrictions#
	1 to 2
10-00	Y
10-10	Y
10-50	Y

Legend: Y: Applicable

#: The restriction numbers correspond to the numbers in the following table.

Table H–20: List of restrictions

No.	Details
1	Encrypted communication cannot be established with JP1/IM - View.
2	Connection cannot be established from JP1/IM - View in a different language environment.

(6) Restrictions placed when JP1/IM - View 10-00 to 10-50 is connected to JP1/IM - Manager 11-50 (when using the Central Console)

Table H–21: Restrictions placed when JP1/IM - View 10-00 to 10-50 is connected to JP1/IM - Manager 11-50 (when using the Central Console)

JP1/IM - View version	Restrictions#		
	1 to 3	4 to 8	9 to 18
10-00	Y	Y	Y
10-10	--	Y	Y
10-50	--	--	Y

Legend: Y: Applicable --: Not applicable

#: The restriction numbers correspond to the numbers in the following table.

Table H–22: List of restrictions

No.	Details
1	Repeated event conditions cannot be defined.
2	Repeated events for which monitoring is suppressed by repeated event monitoring suppression cannot be displayed in consolidated format.
3	Single sign-on cannot be used to connect to JP1/Navigation Platform.
4	The range of automated-action suppression and the issuance of the event to notify that suppression will continue cannot be specified.
5	Additional severity changing definitions cannot be registered, or severity changing definitions cannot be defined in the Severity Change Definition Settings window.
6	View filters cannot be used on the **Severe Events** page.
7	Events cannot be highlighted on the **Severe Events** page.
8	The range of events to be collected at login cannot be set.
9	Display message change settings cannot be specified and the messages after change cannot be displayed.
10	Program-specific extended attributes cannot be displayed in the events list in the Event Console window.
11	Program-specific extended attributes cannot be specified in event conditions in the following definitions: • Severe event definition • Event acquisition filter • Common exclusion conditions • View filter • Event receiver filter
12	Program-specific extended attributes cannot be specified as item names in event conditions in the following definitions (program-specific extended attributes can be specified as attribute names): • Automated action definition • Common exclusion conditions extended definition file • Severity changing definition file • Display item definition file for repeated event conditions • Event search conditions • Event-information mapping definitions
13	The **Suppressed event ID** field and the **Read Suppressed Event ID From Selected Event** button are not displayed in the following windows:

No.	Details
	• Event Search Conditions window • Settings for View Filter window
14	Performance reports of event-source hosts cannot be displayed because the **Display Performance** menu and the **Display Performance** button are not displayed in the following pages and windows: • **Monitor Events** page • **Severe Events** page • **Search Events** page • **Response-Waiting Events** page • Related Events window • Event Details window • Edit Event Details window
15	The JP1/AJS - Web Console monitor window cannot be displayed from the event guide by using single sign-on.
16	The Action Parameter Definitions window cannot be displayed if you are using an action definition file where `DESC_VERSION` is `4`.
17	If automated actions are set to be excluded in the common exclusion-conditions in extended mode, the following operations cannot be done: • Displaying the System Environment Settings window • Setting additional common exclusion-conditions
18	You cannot inherit arbitrary event attributes and character strings in incident manual-registration to JP1/Service Support from JP1/IM - View.

(7) Restrictions placed when JP1/IM - View 10-00 to 10-50 is connected to JP1/IM - Manager 11-50 (when using the Central Scope)

Table H–23: Restrictions placed when JP1/IM - View 10-00 to 10-50 is connected to JP1/IM - Manager 11-50 (when using the Central Scope)

JP1/IM - View version	Restrictions#
	1 to 5
10-00	Y
10-10	Y
10-50	--

Legend: Y: Applicable --: Not applicable

#: The restriction numbers correspond to the numbers in the following table.

Table H–24: List of restrictions

No.	Details
1	Margins of monitoring node icon and monitoring node name cannot be hidden.
2	Transmission factor cannot be set for monitoring node icons.
3	Status colors of monitoring node and monitoring node name cannot be changed.
4	Moving of monitoring node icon cannot be suppressed in the Monitoring Tree and Visual Monitoring windows.
5	Timing of the flashing alarm lamp cannot be changed.

(8) Restrictions placed when JP1/IM - View 10-00 to 10-50 is connected to JP1/IM - Manager 11-50 (when using IM Configuration Management)

Table H–25: Restrictions placed when JP1/IM - View 10-00 to 10-50 is connected to JP1/IM - Manager 11-50 (when using IM Configuration Management)

JP1/IM - View version	Restrictions#	
	1 to 2	3 to 9
10-00	Y	Y
10-10	--	Y
10-50	--	Y

Legend: Y: Applicable --: Not applicable

#: The restriction numbers correspond to the numbers in the following table.

Table H–26: List of restrictions

No.	Details
1	Virtualization management information about KVM or HCSM cannot be set or displayed.
2	Information about a host that holds virtualization management information about KVM or HCSM cannot be edited or deleted. In addition, `Unknown` is displayed as the host type.
3	No notification that agent settings for log file trap information might have been changed is sent while the Display/Edit Profiles window is being used.
4	The enable/disable setting for starting processes automatically when the log file trap service is started cannot be changed in the Display/Edit Profiles window.
5	Log file trap information for non-cluster operation cannot be applied by file transmission in the Display/Edit Profiles window.
6	Host information cannot be collected unless the remote monitoring of the host whose host information is to be collected is stopped.
7	In the Remote Monitoring Settings window, SSH connections cannot be set up for individual hosts.
8	When an agent configuration is applied by using the differential distribution method, the confirmation dialog box displays `KNAN20440-Q`, not `KNAN20441-Q` (the agent configuration is applied by the differential distribution method).
9	You cannot set more than 1,025 hosts in a single business or monitoring group.

H.3 Connectivity with version 9 products

The following describes restrictions that are placed when JP1/IM - View 11-50 is connected to JP1/IM - Manager 09-00 to 09-50 and when JP1/IM - View 09-00 to 09-50 is connected to JP1/IM - Manager 11-50.

(1) Restrictions placed when JP1/IM - View 11-50 is connected to JP1/IM - Manager 09-00 to 09-50 (common to all components)

Table H–27: Restrictions placed when JP1/IM - View 11-50 is connected to JP1/IM - Manager 09-00 to 09-50 (common to all components)

JP1/IM - Manager version	Restrictions#
	1 to 3
09-00	Y
09-01	Y
09-10	Y
09-50	Y

Legend: Y: Applicable

#: The restriction numbers correspond to the numbers in the following table.

Table H–28: List of restrictions

No.	Details
1	Encrypted communication cannot be established with JP1/IM - Manager.
2	Connection cannot be established with JP1/IM - Manager in a different language environment.
3	Operation log data cannot be output.

(2) Restrictions placed when JP1/IM - View 11-50 is connected to JP1/IM - Manager 09-00 to 09-50 (when using the Central Console)

Table H–29: Restrictions placed when JP1/IM - View 11-50 is connected to JP1/IM - Manager 09-00 to 09-50 (when using the Central Console)

JP1/IM - Manager version	Restrictions#	
	1 to 2	3 to 25
09-00	Y	Y
09-01	Y	Y
09-10	Y	Y
09-50	--	Y

Legend:

Y: Applicable

--: Not applicable

#: The restriction numbers correspond to the numbers in the following table.

Table H–30: List of restrictions

No.	Details
1	Common exclusion-conditions (extended mode) cannot be defined.
2	A business group or monitoring group cannot be specified for an event condition or command execution host.
3	Additional common exclusion-conditions cannot be registered.

No.	Details
4	In the Command Execution window, commands on the viewer host cannot be executed.
5	In the Command Execution window, event inheritance information cannot be specified for the contents of the command to be executed.
6	Repeated event conditions cannot be defined.
7	Repeated events for which monitoring is suppressed by repeated event monitoring suppression cannot be displayed in consolidated format.
8	Single sign-on cannot be used to connect to JP1/Navigation Platform.
9	The range of automated-action suppression and the issuance of the event to notify that suppression will continue cannot be specified.
10	Additional severity changing definitions cannot be registered, or severity changing definitions cannot be defined in the Severity Change Definition Settings window.
11	View filters cannot be used on the **Severe Events** page.
12	Events cannot be highlighted on the **Severe Events** page.
13	The range of events to be collected at login cannot be set.
14	Display message change settings cannot be specified.
15	Program-specific extended attributes cannot be displayed in the events list in the Event Console window.
16	Program-specific extended attributes cannot be specified in event conditions in the following definitions: • Severe event definition • Event acquisition filter • Common exclusion conditions • View filter • Event receiver filter
17	Program-specific extended attributes cannot be specified as item names in event conditions in the following definitions (program-specific extended attributes can be specified as attribute names): • Automated action definition • Common exclusion conditions extended definition file • Event search conditions • Event-information mapping definitions
18	The **Suppressed event ID** field and the **Read Suppressed Event ID From Selected Event** button are not displayed in the following windows: • Event Search Conditions window • Settings for View Filter window
19	Performance reports of event-source hosts cannot be displayed because the **Display Performance** menu and the **Display Performance** button are not displayed in the following pages and windows: • **Monitor Events** page • **Severe Events** page • **Search Events** page • **Response-Waiting Events** page • Related Events window • Event Details window • Edit Event Details window
20	The event attribute values to be inherited by automated actions cannot be Base64 encoded or URL encoded.
21	The JP1/AJS - Web Console monitor window cannot be displayed from the event guide by using single sign-on.
22	You cannot specify the status (enabled, disabled) of automated action definitions.

No.	Details
23	When automated action definitions are applied, you cannot inherit the suppression status and the status of satisfied conditions of the AND-joined conditions unless the action definition is edited.
24	You cannot specify items for **Target for exclusion** in the Common Exclusion-Condition Settings (Extended) window.
25	You cannot inherit arbitrary event attributes and character strings in incident manual-registration to JP1/Service Support from JP1/IM - View.

(3) Restrictions placed when JP1/IM - View 11-50 is connected to JP1/IM - Manager 09-00 to 09-50 (when using the Central Scope)

Table H–31: Restrictions placed when JP1/IM - View 11-50 is connected to JP1/IM - Manager 09-00 to 09-50 (when using the Central Scope)

JP1/IM - View version	Restrictions#
	1 to 5
09-00	Y
09-01	Y
09-10	Y
09-50	Y

Legend: Y: Applicable

#: The restriction numbers correspond to the numbers in the following table.

Table H–32: List of restrictions

No.	Details
1	Margins of monitoring node icon and monitoring node name cannot be hidden.
2	Transmission factor cannot be set for monitoring node icons.
3	Status colors of monitoring node and monitoring node name cannot be changed.
4	Moving of monitoring node icon cannot be suppressed in the Monitoring Tree and Visual Monitoring windows.
5	Timing of the flashing alarm lamp cannot be changed.

(4) Restrictions placed when JP1/IM - View 11-50 is connected to JP1/IM - Manager 09-00 to 09-50 (when using IM Configuration Management)

Table H–33: Restrictions placed when JP1/IM - View 11-50 is connected to JP1/IM - Manager 09-00 to 09-50 (when using IM Configuration Management)

JP1/IM - Manager version	Restrictions#			
	1	2 to 4	5 to 7	8 to 17
09-00	Y	Y	Y	Y
09-01	--	Y	Y	Y
09-10	--	--	Y	Y
09-50	--	--	--	Y

Legend:

Y: Applicable

--: Not applicable

#: The restriction numbers correspond to the numbers in the following table.

Table H–34: List of restrictions

No.	Details
1	In the IM Configuration Management window, the following items cannot be selected from the **Operation** menu: • **Virtualization Configuration**>**Collect Virtualization Configuration** • **Virtualization Configuration**>**Batch Collect Virtualization Configurations** • **Virtualization Configuration**>**Apply to Central Scope Monitoring Tree**
2	In the Display/Edit Profiles window, the following items cannot be selected from the menu: • **Edit**>**Add Profile** • **Edit**>**Delete Profile** • **Operation**>**Start Process** • **Operation**>**Stop Process** • **Operation**>**Save/Apply Profiles**>**Apply by Restarting** • **Operation**>**Save/Apply Profiles**>**Apply by Sending File**
3	In the Display/Edit Profiles window, **Startup options** is not displayed.
4	In the Display/Edit Profiles window, the following items cannot be selected from the **Application method** radio button. • **Restart** • **Send a file**
5	In the IM Configuration Management window, the following menu items are unavailable: • **Edit**>**System Common Settings** • **Edit**>**Business Group** • **Edit**>**Edit Remote Monitoring Configuration** • **Operation**>**Business Group**
6	In the Register Host window, the item **Remote communication type** is unavailable.
7	In the IM Configuration Management window, the **Business Group** page is not displayed.
8	In the IM Configuration Management window, hosts managed by IPv6 addresses cannot be registered.
9	Virtualization management information about KVM or HCSM cannot be set or displayed.
10	Information about a host that holds virtualization management information about KVM or HCSM cannot be edited or deleted. In addition, `Unknown` is displayed as the host type.
11	Event IDs and log file trap names cannot be set in the event log trap action-definitions and remote-monitoring event log trap action-definitions.
12	No notification that agent settings for log file trap information might have been changed is sent while the Display/Edit Profiles window is being used.
13	The enable/disable setting for starting processes automatically when the log file trap service is started cannot be changed in the Display/Edit Profiles window.
14	Log file trap information for non-cluster operation cannot be applied by file transmission in the Display/Edit Profiles window.
15	Host information cannot be collected unless the remote monitoring of the host whose host information is to be collected is stopped.
16	In the Remote Monitoring Settings window, SSH connections cannot be set up for individual hosts.
17	You cannot set more than 1,025 hosts in a single business or monitoring group.

(5) Restrictions placed when JP1/IM - Manager 11-50 is connected to JP1/IM - View 09-00 to 09-50 (common to all components)

Table H–35: Restrictions placed when JP1/IM - Manager 11-50 is connected to JP1/IM - View 09-00 to 09-50 (common to all components)

JP1/IM - View version	Restrictions#
	1 to 2
09-00	Y
09-01	Y
09-10	Y
09-50	Y

Legend: Y: Applicable

#: The restriction numbers correspond to the numbers in the following table.

Table H–36: List of restrictions

No.	Details
1	Encrypted communication cannot be established with JP1/IM - View.
2	Connection cannot be established from JP1/IM - View in a different language environment.

(6) Restrictions placed when JP1/IM - View 09-00 to 09-50 is connected to JP1/IM - Manager 11-50 (when using the Central Console)

Table H–37: Restrictions placed when JP1/IM - View 09-00 to 09-50 is connected to JP1/IM - Manager 11-50 (when using the Central Console)

JP1/IM - View version	Restrictions#	
	1 to 6	7 to 28
09-00	Y	Y
09-01	Y	Y
09-10	Y	Y
09-50	--	Y

Legend:

Y: Applicable

--: Not applicable

#: The restriction numbers correspond to the numbers in the following table.

Table H–38: List of restrictions

No.	Details
1	Common exclusion-conditions (extended mode) cannot be defined.
2	Command buttons are not displayed.
3	Incidents cannot be manually registered in JP1/Service Support.

No.	Details
4	The event source host attribute is not displayed (the event source host attribute can be specified for event conditions as an extended attribute).
5	If restrictions are enabled on viewing and operating business groups, users cannot log in.
6	Business groups and monitoring groups cannot be specified for event conditions and the command execution host.
7	Additional common exclusion-conditions cannot be registered.
8	The command buttons for which commands on a viewer host are specified, and for which event inheritance information is specified cannot be displayed.
9	Repeated event conditions cannot be defined.
10	Repeated events for which monitoring is suppressed by repeated event monitoring suppression cannot be displayed in consolidated format.
11	Single sign-on cannot be used to connect to JP1/Navigation Platform.
12	The range of automated-action suppression and the issuance of the event to notify that suppression will continue cannot be specified.
13	Additional severity changing definitions cannot be registered, or severity changing definitions cannot be defined in the Severity Change Definition Settings window.
14	View filters cannot be used on the **Severe Events** page.
15	Events cannot be highlighted on the **Severe Events** page.
16	The range of events to be collected at login cannot be set.
17	Display message change settings cannot be specified and the messages after change cannot be displayed.
18	Program-specific extended attributes cannot be displayed in the events list in the Event Console window.
19	Program-specific extended attributes are specified in event conditions in the definitions listed below, but the definitions cannot be applied to JP1/IM - Manager. Also, program-specific extended attributes are specified in event conditions in the following definitions, but the event conditions cannot be displayed in windows (windows open with no event condition entered): • Severe event definition • Event acquisition filter • Common exclusion conditions • Event receiver filter
20	Program-specific extended attributes cannot be specified in event conditions in the following definitions: • Severe event definition • Event acquisition filter • Common exclusion conditions • View filter • Event receiver filter
21	Program-specific extended attributes cannot be specified as item names in event conditions in the following definitions (program-specific extended attributes can be specified as attribute names): • Automated action definition • Common exclusion conditions extended definition file • Event search conditions • Event-information mapping definitions
22	The **Suppressed event ID** field and the **Read Suppressed Event ID From Selected Event** button are not displayed in the following windows: • Event Search Conditions window • Settings for View Filter window

No.	Details
23	Performance reports of event-source hosts cannot be displayed because the **Display Performance** menu and the **Display Performance** button are not displayed in the following pages and windows: • **Monitor Events** page • **Severe Events** page • **Search Events** page • **Response-Waiting Events** page • Related Events window • Event Details window • Edit Event Details window
24	The JP1/AJS - Web Console monitor window cannot be displayed from the event guide by using single sign-on.
25	You cannot set more than 1,025 condition groups in the common exclusion-conditions in extended mode.
26	The Action Parameter Definitions window cannot be displayed if you are using an action definition file where `DESC_VERSION` is `4`.
27	If automated actions are set to be excluded in the common exclusion-conditions in extended mode, the System Environment Settings window cannot be displayed.
28	You cannot inherit arbitrary event attributes and character strings in incident manual-registration to JP1/Service Support from JP1/IM - View.

(7) Restrictions placed when JP1/IM - View 09-00 to 09-50 is connected to JP1/IM - Manager 11-50 (when using the Central Scope)

Table H–39: Restrictions placed when JP1/IM - View 09-00 to 09-50 is connected to JP1/IM - Manager 11-50 (when using the Central Scope)

JP1/IM - View version	Restrictions#
	1 to 5
09-00	Y
09-01	Y
09-10	Y
09-50	Y

Legend: Y: Applicable

#: The restriction numbers correspond to the numbers in the following table.

Table H–40: List of restrictions

No.	Details
1	Margins of monitoring node icon and monitoring node name cannot be hidden.
2	Transmission factor cannot be set for monitoring node icons.
3	Status colors of monitoring node and monitoring node name cannot be changed.
4	Moving of monitoring node icon cannot be suppressed in the Monitoring Tree and Visual Monitoring windows.
5	Timing of the flashing alarm lamp cannot be changed.

(8) Restrictions placed when JP1/IM - View 09-00 to 09-50 is connected to JP1/IM - Manager 11-50 (when using IM Configuration Management)

Table H–41: Restrictions placed when JP1/IM - View 09-00 to 09-50 is connected to JP1/IM - Manager 11-50 (when using IM Configuration Management)

JP1/IM - View version	Restrictions#			
	1 to 2	3 to 5	6 to 9	10 to 18
09-00	Y	Y	Y	Y
09-01	--	Y	Y	Y
09-10	--	--	Y	Y
09-50	--	--	--	Y

Legend:

Y: Applicable

--: Not applicable

#: The restriction numbers correspond to the numbers in the following table.

Table H–42: List of restrictions

No.	Details
1	**Virtual Manager Type** is not displayed as an attribute of a host.
2	For a host for which **Virtual Manager Type** is set as an attribute, the menu item **Edit Host Properties** cannot be executed.
3	In the Display/Edit Profiles window, the following items cannot be selected from the menu: • **Edit**>**Add Profile** • **Edit**>**Delete Profile** • **Operation**>**Start Process** • **Operation**>**Stop Process** • **Operation**>**Save/Apply Profiles**>**Apply by Restarting** • **Operation**>**Save/Apply Profiles**>**Apply by Sending File**
4	In the Display/Edit Profiles window, **Startup options** is not displayed.
5	In the Display/Edit Profiles window, the following items cannot be selected from the **Application method** radio button. • **Restart** • **Send a file**
6	Information about the remote monitoring configuration is not displayed. • On the **IM Configuration** page in the IM Configuration Management window, the hosts that are only included in the remote monitoring configuration are not displayed. • On the **IM Configuration** page in the IM Configuration Management window, icons that indicate whether the hosts are included in the agent configuration or in the remote monitoring configuration are not displayed in the tree display area. • In the host attribute **Configuration type**, *Remote*, *Base manager, Remote*, *Relay manager, Remote*, and *Agent, Remote* are not displayed.
7	The following attributes of a host are not displayed: • **Collection status (Remote)** • **Authentication information category** • **Remote communication type** • **Group name**
8	In the Display/Edit Profiles window, **Remote Monitoring** is not displayed in the tree display area.
9	The following Business Group menu items and page cannot be displayed or edited:

No.	Details
	• In the IM Configuration Management window, the **Business Group** page is not displayed. • In the IM Configuration Management window, **Business Group** is not displayed in the **Edit** menu. • In the IM Configuration Management window, **Business Group** is not displayed in the **Operation** menu.
10	Virtualization management information about KVM or HCSM cannot be set or displayed.
11	Information about a host that holds virtualization management information about KVM or HCSM cannot be edited or deleted. In addition, `Unknown` is displayed as the host type.
12	No notification that agent settings for log file trap information might have been changed is sent while the Display/Edit Profiles window is being used.
13	The enable/disable setting for starting processes automatically when the log file trap service is started cannot be changed in the Display/Edit Profiles window.
14	Log file trap information for non-cluster operation cannot be applied by file transmission in the Display/Edit Profiles window.
15	Host information cannot be collected unless the remote monitoring of the host whose host information is to be collected is stopped.
16	In the Remote Monitoring Settings window, SSH connections cannot be set up for individual hosts.
17	When an agent configuration is applied by using the differential distribution method, the confirmation dialog box displays `KNAN20440-Q`, not `KNAN20441-Q` (the agent configuration is applied by the differential distribution method).
18	You cannot set more than 1,025 hosts in a single business or monitoring group.

H.4 Connectivity with previous versions of JP1/Base

(1) Restrictions on event searches in JP1/Base 09-00 to 11-10 from JP1/IM - View 11-50

There are no restrictions on event searches from JP1/IM - View 11-50 to JP1/Base 09-00 or 11-10.

(2) Restrictions on managing JP1/Base 09-00 to 11-10 from JP1/IM - Manager 11-50 (when using IM Configuration Management)

Table H–43: Restrictions on managing JP1/Base 09-00 to 11-10 from JP1/IM - Manager 11-50 (when using IM Configuration Management)

JP1/Base version#1	Restrictions#2		
	1	2	3 to 6
09-00	Y	Y	Y
09-10 to 10-50	--	Y	Y
11-00 to 11-10	--	--	Y

Legend:

Y: Applicable

--: Not applicable

#1: Refers to the version of JP1/Base on the search target host.

#2: The restriction numbers correspond to the numbers in the following table.

Table H–44: List of restrictions

No.	Details
1	You cannot perform the following operations for log file traps on the monitored hosts: • Add profiles • Delete profiles • Start a process • Stop a process • Apply information by restarting • Apply information by sending files
2	Event IDs and log file trap names cannot be set in the event log trap action definitions on monitored hosts.
3	When a managed host is a site manager, IM configuration cannot be applied to the agents under the site manager by using the differing-components application method.
4	No notification that agent settings for log file trap information might have been changed is sent while the Display/Edit Profiles window is being used.
5	The enable/disable setting for starting processes automatically when the log file trap service is started cannot be changed in the Display/Edit Profiles window.
6	Log file trap information for non-cluster operation cannot be applied by file transmission in the Display/Edit Profiles window.

(3) Restrictions when the manager host uses JP1/IM - Manager version 11-50 and JP1/Base version 11-00 to 11-10 (when using IM Configuration Management)

Table H–45: Restrictions when the manager host uses JP1/IM - Manager version 11-50 and JP1/Base version 11-00 to 11-10 (when using IM Configuration Management)

JP1/Base version	Restrictions#	
	1 to 3	4
11-00	Y	Y
11-10	--	Y

Legend: Y: Applicable --: Not applicable

#: The restriction numbers correspond to the numbers in the following table.

Table H–46: List of restrictions

No.	Details
1	In remote-monitoring event log traps, the retry count for event log collection cannot be adjusted.
2	In remote-monitoring event log traps, the retry interval and the monitoring interval for event log collection cannot be adjusted individually.
3	When **Apply Agent Configuration** is run in the Edit Agent Configuration window, the differing-components application method cannot be used.
4	You cannot set more than 1,025 agent hosts directly under JP1/IM - Manager in the agent configuration.

(4) Connectivity for monitoring JP1/Base on agent hosts from JP1/IM - Manager (with the Central Console functionality)

Table H–47: Connectivity for monitoring JP1/Base on agent hosts from JP1/IM - Manager

JP1/Base (agent) version[#1]	JP1/IM - Manager (JP1/IM - Console) version[#1]					
	06-00 to 06-71	07-00 to 07-51	08-00 to 08-50	09-00 to 09-50	10-00 to 10-50	11-00 to 11-50
06-00 to 06-71	Y	Y	Y	E	E	E
07-00 to 07-51	Y	Y	Y	Y	E	E
08-00 to 08-50	E[#2]	E[#2]	Y	Y	Y	E
09-00 to 09-50	E[#2]	E[#2]	Y	Y	Y	Y
10-00 to 10-50	E[#2]	E[#2]	Y	Y	Y	Y
11-00 to 11-50	E[#2]	E[#2]	E	Y	Y	Y

Legend:

Y: Supported

E: Only event forwarding from JP1/Base to JP1/IM - Manager is supported.

#1

Functions provided by both JP1/Base and JP1/IM - Manager are supported. For details about connectivity and compatibility between JP1/IM - Manager (JP1/IM - Console) and JP1/Base, see the documentation for the applicable product version.

#2

JP1/IM - Manager and JP1/IM - Console cannot process normally JP1 events issued in a UTF-8 locale environment. A compatible encoding mode must be set on the event-forwarding source JP1/Base.

I. Performance and Estimation

This appendix describes the memory and disk space requirements of JP1/IM, and traffic volumes on the network.

I.1 Memory requirements

For details on JP1/IM memory requirements, see the *Release Notes* for JP1/IM - Manager and JP1/IM - View.

I.2 Disk space requirements

For details on JP1/IM disk space requirements, see the *Release Notes* for JP1/IM - Manager and JP1/IM - View.

I.3 Network traffic volumes

The following describes traffic volumes generated at communication based on the Central Console and Central Scope. Traffic arising from other types of communication is minimal and is not covered in this explanation.

(1) Amount of data generated during communication based on the Central Console

The following describes the amounts of data generated during communication based on the Central Console.

(a) Estimated traffic volumes between JP1/IM - View and JP1/IM - Manager (Central Console)

Table I–1: Traffic volumes between JP1/IM - View and JP1/IM - Manager (Central Console)

Activity	Estimated data transferred (bytes)
Display events in the Event Console window.	((5,000 + {average data size per event}#1 × 1.5) × (number of events acquired when window refreshed)#2 + 2,500) × ({number of events generated since window was last refreshed}#3 / {number of events acquired when window refreshed}#2)
Open the Event Search Conditions window, or click the **OK** button in the Event Search Conditions window.	Data transferred = {total size of condition groups}#4 + ({name of search target host} × 1.5) {condition group} = (400 bytes + {total of attribute values specified for the condition group} + ({condition group name} × 1.5))
Perform an event search.	((5,000 + {average data size per event}#1 × 1.5) × (number of events acquired when window refreshed)#2 + 2,500) × ({number of retrieved events}#5 / {number of events acquired when window refreshed}#2)
Open the Event Details window.	20,000 + {total byte size of the attribute names defined in the definition file for the extended event attributes for the event in question} × 1.5 + {average data size per event}#1 × 1.5 + {length of event-guide messages (max. 409,600)}

Activity	Estimated data transferred (bytes)
Open the System Environment Settings window, or click the **Apply** button in the System Environment Settings window.	Data transferred = {total event acquisition filter data} + {data of active event acquisition filters} + {data of common exclusion-condition groups} + 1,200 {event acquisition filter data} = {total size of condition groups}#4 + ({length of event acquisition filter name} × 1.5) {condition group} = (400 bytes + {total of attribute values specified for the condition group} + ({condition group name} × 1.5)) {common exclusion-condition groups} = (400 bytes + {total of attribute values specified for common exclusion-condition groups} + ({condition group name} × 1.5))
Open the Settings for Event Receiver Filter window, or click the **Apply** button in the Settings for Event Receiver Filter window.	Data transferred = {total event receiver filter data} {event receiver filter data} = {total size of condition groups}#4 + ({length of event receiver filter name} × 1.5) + ({user names associated with filter} × 1.5) {condition group} = (410 bytes + {total of attribute values specified for the condition group} + ({condition group name} × 1.5))
Open the Severe Event Definitions window, or click the **OK** button in the Severe Event Definitions window.	Data transferred = {total size of condition groups}#4 {condition group} = (400 bytes + {total of attribute values specified for the condition group} + ({condition group name} × 1.5))
Click the **OK** button in the Settings for View Filter window, or click the **OK** button in the View List of Filters window.	Data transferred = {total size of view filters} {view filter} = {total size of condition groups}#4 + ({view filter names} × 1.5) {condition group} = (400 bytes + {total of attribute values specified for the condition group} + ({condition group name} × 1.5))
Apply the settings in the Preferences window.	6,000
Open the Action Parameter Definitions window.	1,750 + ({byte size of one action definition} + 140) × (number of action definitions)
Click the **Apply** button in the Action Parameter Definitions window.	3,200 + (({byte size of one action definition} + 140) × (number of action definitions)) × 2
Open the Action Log window.	2,400 + ({byte size of the action command} + {length of the messages displayed in the Action Log Details window})
Open the List of Action Results window.	1,850 + (500 + {byte size of the action command} + {length of the messages displayed in the Action Log Details window}) × (number of displayed actions)
Click the **OK** button in the Conditions for Updating List of Action Results window, or close the List of Action Results window.	1,600

#1: Example of calculating the average data size per event

To find the average data size per event:

1. Using the `jevexport` command, output all the events generated during a set period of time to a CSV file. For details on the `jevexport` command, see the *JP1/Base User's Guide*.

2. Find the total number of bytes in the output CSV file.

3. Divide the total byte count by the number of generated events.

If events that generate data greater than the average size are output in close succession, the above estimation might be exceeded.

#2: This is the value set in **Num. of events to acquire at update** in the Preferences window. The default is 20 events.

#3: Find the number of events issued since window was last refreshed using the equation given below.

#4: A *condition group* is a pass condition group or exclusion-condition group.

#5: This is the value set in **Num. of events to acquire in 1 search** in the Preferences window. The default is 20 events.

Equation for {number of events generated since window was last refreshed}

- When **Apply** is set for **Automatic refresh** in the Preferences window:

Number of events generated since window was last refreshed =
{value set in **Interval** (default 5 sec.)}
× {number of events generated per second}

- When **Do not apply** is set for **Automatic refresh** in the Preferences window:
  Number of events generated since window was last refreshed =
  {interval at which user refreshes Event Console (sec.)}
  × {number of events generated per second}

(b) Estimated traffic volumes between JP1/IM - View and JP1/Base (manager)

Table I–2: Traffic volumes between JP1/IM - View and JP1/Base (manager)

Activity	Estimated data transferred (bytes)
Execute a command from the Execute Command window.	(928 + {command length}) × (4# + {number of lines in the execution result})

#: The number increases if a warning message (KAVB2*xxx*-W) is output about the command execution, but this is an exceptional case and is not counted in the estimate.

(c) Estimated traffic volumes between JP1/IM - Manager (Central Console) and JP1/Base

Table I–3: Traffic volumes between JP1/IM - Manager (Central Console) and JP1/Base

Activity	Estimated data transferred (bytes)
Execute a command in an automated action (data relayed between JP1/IM - Manager (Central Console) and JP1/Base on the same host).	(5,024 × 4#1)#2
Click **Event Search Conditions** on the **Search Events** page to search for events (data relayed between JP1/IM - Manager (Central Console) and JP1/Base on the target host).	140#3 + (600#4 × {number of JP1 events matching the search conditions})

#1: The number increases if a warning message (KAVB2*xxx*-W) is output about the command execution, but this is an exceptional case and is not counted in the estimate.

#2: Maximum amount of data for one automated action request issued to JP1/Base 08-00 or later.

#3: Amount of data when the name of the destination event server is 16 bytes and the event ID is the only search condition.

#4: Data size of the JP1 event issued when a character string of about 100 bytes is trapped by the log file trapping function.

(d) Estimated traffic volumes between JP1/Base and JP1/Base

Table I–4: Traffic volumes between JP1/Base and JP1/Base

Activity	Estimated data transferred (bytes)
Execute a command from the Execute Command window or execute a command in an automated action (data relayed among JP1/Base that received the request, JP1/Base on the relay host, and JP1/Base on the target host).	5,540#1 + (1,700 × (3#2 + {number of lines in the execution result}))#3

#1: Maximum amount of data for a command execution request.

#2: The number increases if a warning message (KAVB2*xxx*-W) is output about the command execution, but this is an exceptional case and is not counted in the estimate.

#3: Maximum amount of data in the command execution result. You can adjust the amount of data using the `jcocmddef` command. For details on this command, see the chapter on commands in the *JP1/Base User's Guide*.

(2) Central Scope traffic

The following describes the amounts of data generated during communication based on the Central Scope.

(a) Estimated traffic volumes between JP1/IM - View and JP1/IM - Manager (Central Scope)

Table I–5: Traffic volumes between JP1/IM - View and JP1/IM - Manager (Central Scope)

Activity	Estimated data transferred (bytes)
Update of the data being monitored in the Visual Monitoring window since the last poll (where polling takes place at 5-second intervals).	500 + (number of nodes) × 40
Change in the status or monitoring status of nodes being monitored in the Monitoring Tree window since the last poll (where polling takes place at 5-second intervals).	64 + (number of nodes whose status or monitoring status has changed since the last poll) × 20
During monitoring from the Monitoring Tree window of JP1/IM - Manager (Central Scope), updating of tree configuration information since the last poll (where polling takes place at 5-second intervals).	Sum of the data amount for each monitoring object#1 + sum of the data amount for each monitoring group#2 + sum of the data amount for each common condition#3
Display the Guide window by choosing **View** and then **Guide** in the Monitoring Tree window, or by choosing **Guide** from the pop-up menu in the Visual Monitoring window.	1,400 + size of the guide-message
Search for status change events by choosing **View** and then **Search Status-Change Events** in the Monitoring Tree window.	90 × number of status change events for the selected monitoring node
Add or change a common condition in the Common Condition Detailed Settings window. Note that no communication is entailed when the Common Condition Detailed Settings window is opened from the Monitoring Tree (Editing) window.	100 + data amount for the common condition#3
Apply tree configuration information to JP1/IM - Manager (Central Scope) by choosing **File** and then **Update Server Tree** in the Monitoring Tree (Editing) window.	100 + sum of the data amount for each monitoring object#1 + sum of the data amount for each monitoring group#2 + sum of the data amount for each common condition#3
Acquire all common conditions from JP1/IM - Manager (Central Scope) by choosing **Options** and then **Acquire Latest Definition** in the Monitoring Tree (Editing) window.	100 + sum of the data amount for each common condition#3
Apply visual monitoring data to JP1/IM - Manager (Central Scope) by clicking the **Update the Visual Monitoring Data of**	500 + (number of nodes) × 40

Activity	Estimated data transferred (bytes)
Server button in the Visual Monitoring (Editing) window.	

#1: Data amount for each monitoring object =
200 + {length of monitoring node name} + {length of icon file name (when sent)}
+ {length of icon file name (when expanded)} + {length of background image file name}
+ {sum of attribute name lengths} + {sum of attribute value lengths}
+ {sum of individual condition attribute name lengths}
+ {sum of individual condition attribute name values}
+ {sum of lengths of status change condition names in monitoring group}

#2: Data amount for each monitoring group =
200 + {length of monitoring node name} + {length of icon file name (when sent)}
+ {length of icon file name (when expanded)} + {length of background image file name}
+ {sum of attribute name lengths} + {sum of attribute value lengths}
+ {sum of lengths of status change condition names in monitoring group}
+ {number of status change conditions in monitoring group} × 40

#3: Data amount for each common condition =
250 + {length of common condition name} + 10 × {number of specified event levels}
+ {sum of lengths of source event server names} + {length of object type}
+ {sum of lengths of object names} + {length of root object name}
+ {length of occurrence name} + {sum of user name lengths} + {message length}
+ {product name length} + {event ID} × 10
+ {sum of lengths of extended attribute names}
+ {sum of lengths of extended attribute values}

(b) Estimated traffic volumes between JP1/IM - Manager (Central Scope) and JP1/Base on a managed host

Table I–6: Traffic volumes between JP1/IM - Manager (Central Scope) and JP1/Base on a managed host

Activity	Estimated data transferred (bytes)
Select the **Generate**, **Show Differences**, or **Add** button in the Auto-generation - Select Configuration window.	For work-oriented or server-oriented trees: JP1/AJS data amounts# + JP1/PFM data amounts# + Data amounts of JP1/Cm2/SSO version 8 or earlier# + Cosminexus data amounts#

#: Estimate these data amounts using the tables below.

- Estimating JP1/AJS data amounts

Table I–7: JP1/AJS data amounts

Equation	Item	Estimated data transferred for each item (bytes)
200 + sum of *a* + sum of *b* + sum of *c* + sum of *d*	*a*: Scheduler service	10 + length of the scheduler service name + length of the character code
	b: Job group	20 + length of the scheduler service name + length of the full name of the unit + length of the job group name

Equation	Item	Estimated data transferred for each item (bytes)
		+ length of the comment name
	c: Root jobnet	20 + length of the scheduler service name + length of the full name of the unit + length of the jobnet name + length of the comment name
	d: Execution agent	10 + length of the scheduler service name + length of the root jobnet path + length of the job execution agent name

- Estimating JP1/PFM data amounts

Table I–8: JP1/PFM data amounts

Equation	Item	Estimated data transferred for each item (bytes)
200 + sum of *e*	*e*: Service	310 + length of host name + length of instance name

- Estimating data amounts of JP1/Cm2/SSO version 8 or earlier

Table I–9: JP1/Cm2/SSO data amounts

Equation	Item	Estimated data transferred for each item (bytes)
400 + sum of *f* + sum of g	*f*: Server that performs monitoring with threshold value	50 + length of host name
	g: Application to be monitored	20 + length of host name + length of application name

- Estimating Cosminexus data amounts

Table I–10: Cosminexus data amounts

Equation	Item	Estimated data transferred for each item (bytes)
200 + sum of *h* + sum of *i* + sum of *j* + sum of *k* + sum of *l* + sum of *m* + sum of *n* + sum of *o* + sum of *p* + sum of *q* + sum of *r* + sum of *s* + sum of *t* + sum of *u* + sum of *v*	*h*: Operations management domain	10 + length of operations management domain name + length of operations management domain display name
	i: Host	10 + length of operations management domain name + length of the name or IP address of the operations management agent machine + length of host display name
	j: Logical J2EE server	320 + length of operations management domain name + length of logical server name × 7 + length of host name + length of logical server display name + length of logical server name of the logical naming service being used

Equation	Item	Estimated data transferred for each item (bytes)
		+ length of logical server name of the logical OTS being used + length of logical server name of the logical CTM being used + length of logical server name of the logical TCS being used + length of logical server name of the logical performance tracer being used + length of logical server name of the logical SFO being used
	k: Logical naming service	70 + length of operations management domain name + length of logical server name + length of host name + length of logical server display name + length of logical server name of the logical smart agent being used
	l: Logical smart agent	20 + length of operations management domain name + length of logical server name + length of host name + length of logical server display name
	m: Logical OTS	70 + length of operations management domain name + length of logical server name + length of host name + length of logical server display name + length of logical server name of the logical smart agent being used
	n: Logical TCS	70 + length of operations management domain name + length of logical server name + length of host name + length of logical server display name + length of logical server name of the logical TCS being used
	o: Logical CTM domain manager	120 + length of operations management domain name + length of logical server name + length of host name + length of logical server display name + length of logical server name of the logical smart agent being used + length of logical server name of the logical performance tracer being used
	p: Logical CTM	70 + length of operations management domain name + length of logical server name + length of host name + length of logical server display name + length of logical server name of the logical CTM domain manager being used
	q: Logical performance tracer	20 + length of operations management domain name + length of logical server name + length of host name + length of logical server display name

Equation	Item	Estimated data transferred for each item (bytes)
	r: Logical SFO	70 + length of operations management domain name + length of logical server name + length of host name + length of logical server display name + length of logical server name of the logical performance tracer being used
	s: Logical Web server	70 + length of operations management domain name + length of logical server name × 2 + length of host name + length of logical server display name + length of logical server name of the logical performance tracer being used
	t: J2EE application	20 + length of operations management domain name + length of display name of J2EE application properties
	u: Imported J2EE application	50 + length of display name of J2EE application properties + length of logical server name of imported logical J2EE server
	v: J2EE server mapping definition	50 + length of logical server name of the logical Web server + length of logical server name of mapped logical J2EE server

J. Kernel Parameters

To use JP1/IM in a UNIX environment, adjust the OS kernel parameters to allocate the resources needed to run JP1/IM.

For details about the kernel parameters you need to adjust, see the JP1/IM - Manager *Release Notes*.

K. Operation Log Output

The operation log of JP1/IM - Manager contains log information about the login and logout history, including who attempted login or logout when and where, and whether the attempt was successful or failed. The operation log is used to find the cause of security problems such as unauthorized access, and to collect information necessary to ensure secure system operation.

An operation log is a text file output in CSV format. By periodically saving operation logs and processing them by using spreadsheet software, you can use the operation log data as analysis data.

Data is not output to the operation log in initial settings. If JP1/IM - Manager is running in a Chinese environment, English data is output to the operation log.

Note that integrated management of data recorded in operation logs is possible by using JP1/Audit to collect data.

This appendix describes the information recorded in the operation log, and how to specify the settings necessary for outputting data to operation logs.

K.1 Types of events recorded in the operation log

The table below shows the types of events recorded in the operation log and the trigger conditions for JP1/IM - Manager to output operation log data. An event type is an identifier used in the operation log to classify the events recorded in the operation log.

Table K–1: Types of events recorded in the operation log

Event type	Description	Trigger conditions for JP1/IM - Manager to output log data
Authentication	This event indicates one of the following events: • Login successful • Login failed • Logout successful • Logout failed	• An attempt to log in was successful. • An attempt to log in failed. • An attempt to log out was successful. • An attempt to log out failed.

K.2 Storage format of operation log output

Operation log data is output to the operation log file (`imm_operation.log`), which is a sequential file (SEQ2). When the size of the log file reaches a specified value (the initial value is 5 megabytes), the file is renamed to `imm_operation`*n*`.log` (*n:* decimal number in the range from 1 to 16) and saved. Then, a file with the same name before the change is created, and then log data is written to this file.

You can use the operation log definition file (`imm_operationlog.conf`) to change when to switch the file, the output destination of files, and the maximum number of files that can be saved. For details about how to specify the operation log definition file, see *K.5 Settings for outputting operation logs*.

K.3 Operation log output format

This section describes the output format and output destination of operation logs, and the output items in operation logs.

(1) Output format

common-specification-identifier common-specification-revision-number, *output-item-1*=*value-1*, *output-item-2*=*value-2*, ..., *output-item-n*=*value-n*

(2) Output destination

The output destination of the operation log file is specified in the operation log definition file (`imm_operationlog.conf`). The initial value of the output destination is as follows:

In Windows:

Manager-path`\log\operationlog\imm_operation[`*n*#`].log`

In UNIX:

`/var/opt/jp1imm/log/operationlog/imm_operation[`*n*#`].log`

#

n is a decimal number in the range from 1 to 16.

(3) Output items

There are two types of output items as follows:

- Common output items
  Items that are output by all JP1 products that output operation logs
- Fixed output items
  Items that are output individually by each JP1 product that output operation logs

(a) Common output items

Table K–2: Common output items in operation logs

No.	Output item		Value	Description
	Item name	Output attribute name		
1	Common specification identifier	--	`CALFHM`	Log format identifier
2	Common specification revision number	--	`1.0`	Revision number for managing the log format
3	Sequence number	`seqnum`	*sequence-number*	Sequence number of a operation log record (assigned to each process)
4	Message ID	`msgid`	`KNAN3`*xxxx-x*	Message ID of the product[#1]
5	Date and time	`date`	*YYYY-MM-DD*T*hh*:*mm*:*ss.sss*`TZD`[#2]	Operation log output date and time, and time zone
6	Generated program name	`progid`	`JP1IMM`	Name of the program in which the event occurred
7	Generated component	`compid`	• `CentralConsole` • `CentralScope`	Name of the component in which the event occurred

No.	Output item		Value	Description
	Item name	Output attribute name		
			• `Configuration`	
8	Generated process ID	`pid`	• *evtcon-process-ID* • *jcsmain-process-ID* • *jcfmain-process-ID*	ID of the process in which the event occurred
9	Generated location (host name)	`ocp:host`	• *host-name-in-JP1/IM - Manager* • *logical-host-name-in-JP1/IM - Manager*	Name of the host in which the event occurred
10	Event type	`ctgry`	`Authentication`	Category name for classifying the events that are output to operation logs
11	Event result	`result`	• `Success` (success) • `Failure` (failure)	Result of the event
12	Subject identification information	`subj:uid`	*JP1-user-name-in-JP1/IM - View*	Name of the JP1 user who caused the event

Legend:

--: No attribute names are output.

#1: The message ID of the message indicated in the free description in the fixed output items is output.

#2: `T` that follows *YYYY*-*MM*-*DD* separates the date from the time. *TZD* is the time zone identifier. One of the following is output:

- `+`*hh*`:`*mm*: Indicates that the local time is ahead of UTC by *hh*:*mm*.
- `-`*hh*`:`*mm*: Indicates that the local time is behind UTC by *hh*:*mm*.
- `Z`: Indicates that the local time is the same as UTC.

(b) Fixed output items

Table K–3: Fixed output items in operation logs

No.	Output item		Value	Description
	Item name	Output attribute name		
1	Object information	`obj`	`Session`	Operation target
2	Operation information	`op`	• `Login` • `Logout`	Operation details
3	Request sender host	`from:ipv4`	*IPv4-address-in-JP1/IM - View*	IP address of the request sender
4	Free description	`msg`	*message-output-to-the-operation log*	Message indicating the contents of the event#

#: The message text for the message ID in the common output items is output.

(4) Output example

Information that is output to the operation log when a user logs in to the Central Console:

```
CALFHM 1.0, seqnum=2, msgid=KNAN30000-I,
date=2015-10-27T14:00:05.155+09:00, progid=JP1IMM, compid=CentralConsole,
pid=1452, ocp:host=hostname, ctgry=Authentication, result=Success,
subj:uid=System, obj=Session, op=LOGIN, from:ipv4=198.1.1.1, msg="A login
operation was successful"
```

(5) Note

If a user opens the operation log file while JP1/Audit is monitoring the operation log data, a lock error might occur. If you want to check the contents of the operation log file during linkage with JP1/Audit, copy the operation log file to any location, and then check the copy.

K.4 Trigger conditions for operation log output

If you want to see the message text output for each message ID, see the manual *JP1/Integrated Management - Manager Messages*.

Table K–4: Trigger conditions for operation log output and message IDs

Trigger conditions			Message ID
Operation	Results	Cause	
Login to Central Console	Successful	Login authentication is successful.	KNAN30000-I
	Failed	• Login authentication failed. • Communication error with the authentication server	KNAN30001-W
Logout from Central Console	Successful	Logout authentication is successful.	KNAN30002-I
	Failed	Communication error with the authentication server	KNAN30003-W
Login to Central Scope	Successful	Login authentication is successful.	KNAN30000-I
	Failed	• Login authentication failed. • Communication error with the authentication server	KNAN30001-W
Logout from Central Scope	Successful	Logout authentication is successful.	KNAN30002-I
	Failed	Communication error with the authentication server	KNAN30003-W
Login to IM Configuration Management	Successful	Login authentication is successful.	KNAN30000-I
	Failed	• Login authentication failed. • Communication error with the authentication server	KNAN30001-W
Logout from IM Configuration Management	Successful	Logout authentication is successful.	KNAN30002-I
	Failed	Communication error with the authentication server	KNAN30003-W

K.5 Settings for outputting operation logs

To output data to the operation log, log output must be specified in the operation log definition file (`imm_operationlog.conf`). For details about the operation log definition file (`imm_operationlog.conf`), see *Operation log definition file (imm_operationlog.conf) Chapter 2. Definition Files* in the manual *JP1/Integrated Management - Manager Command and Definition File Reference.*

(1) Procedure for specifying the settings for outputting data to operation logs

(a) For physical hosts

1. Edit the operation log definition file (`imm_operationlog.conf`).

   1-1 Specify the `ENABLE` parameter.

   Open the operation log definition file (`imm_operationlog.conf`) by using an editor, and then change the `ENABLE` parameter as follows:

   - Before the change (initial setting)
     `"ENABLE"=dword:00000000`
   - After the change
     `"ENABLE"=dword:00000001`

   1-2 If you want to change the initial setting of the operation log output destination, specify the `LOGFILEDIR` parameter.

   Change the `LOGFILEDIR` parameter as follows:

   In Windows

   - Before the change (initial setting)
     `"LOGFILEDIR"="`*Manager-path*`\log\operationlog"`
   - After the change
     `"LOGFILEDIR"="`*any-output-destination*`"`

   IN UNIX

   - Before the change (initial setting)
     `"LOGFILEDIR"="/var/opt/jp1imm/log/operationlog"`
   - After the change
     `"LOGFILEDIR"="`*any-output-destination*`"`

   1-3 If necessary, specify the size of the log file (`LOGSIZE`) and the maximum number of log files that can be saved (`LOGFILENUM`).

2. Execute the `jbssetcnf` command.

   The settings you specified are applied to the common definition information.

3. Enable the settings.

   Restart JP1/IM - Manager to enable the settings.

(b) For logical hosts

1. Edit the operation log definition file (`imm_operationlog.conf`) on the shared disk.

   1-1 Specify the logical host name for the key name in the environment settings.

   Open the operation log definition file (`imm_operationlog.conf`) by using an editor, and then change the `[JP1_DEFAULT\JP1IMM\OPERATION]` parameter as follows:

   - Before the change (initial setting)

`[JP1_DEFAULT\JP1IMM\OPERATION]`

- After the change
  `[`*logical-host-name*`\JP1IMM\OPERATION]`

1-2 Specify the `ENABLE` parameter.

Specify the `ENABLE` parameter as follows:

- Before the change (initial setting)
  `"ENABLE"=dword:00000000`
- After the change
  `"ENABLE"=dword:00000001`

1-3 Specify the operation log output destination.

Specify the output destination for the `LOGFILEDIR` parameter. Specify an existing write-enabled directory for the output destination. We recommend that you specify the operation log output for the logical host to the shared disk.

Setting example in Windows:

- Before the change (initial setting)
  `"LOGFILEDIR"="`*Manager-path*`\log\operationlog"`
- After the change
  `"LOGFILEDIR"="`*shared-folder*`\JP1IMM\log\operationlog"`

Setting example in UNIX:

- Before the change (initial setting)
  `"LOGFILEDIR"="/var/opt/jp1imm/log/operationlog"`
- After the change
  `"LOGFILEDIR"="`*shared-directory*`/jp1imm/log/operationlog"`

1-4 If necessary, specify the size of the log file (`LOGSIZE`) and the maximum number of log files that can be saved (`LOGFILENUM`).

2. Execute the `jbssetcnf` command on the primary node.
   The definition file settings you specified are applied to the common definition information.
3. Apply the settings of the primary node to the secondary node.
   If you are using a cluster system, you must match the common definition information on all the servers. For details, see *6.7.1 Changing settings in files (for Windows)* or *7.7.1 Changing settings in files (for UNIX)* in the *JP1/Integrated Management - Manager Configuration Guide*.
4. Enable the settings.
   Restart JP1/IM - Manager from the cluster software to enable the settings.

K.6 Operation log messages

The messages that can be output to operation logs are listed below. For details about each message, see the manual *JP1/Integrated Management - Manager Messages*.

- KNAN30000-I
- KNAN30001-W
- KNAN30002-I

- KNAN30003-W

L. Version Changes

This appendix describes the changes between versions.

L.1 Changes in version 11-50

(1) Changes in the manuals 3021-3-A06-30(E), 3021-3-A07-30(E), 3021-3-A08-30(E), 3021-3-A09-30(E), 3021-3-A10-30(E), 3021-3-A11-30(E), and 3021-3-A12-30(E)

- For linkage with JP1/Service Support, a new incident registration mode was added to allow any event attributes or character strings to be inherited.
- A common exclusion-condition in extended mode can now exclude a JP1 event that satisfies the condition from automated-action execution.
- A description was added for the common exclusion history file that logs the exclusion processes of common exclusion-conditions.
- A description was added for the common exclusion-conditions definition history file that logs the definition history of common exclusion-conditions.
- A note was added for the common exclusion-conditions.
- The maximum number of repeated event conditions was increased to 2,500. The total size of the definitions of repeated event conditions was increased to 15 MB.
- Saving event listings (CSV snapshot) now includes action-excluded events.
- Saving event information from the integrated monitoring database (output of an event report) now includes the following event attributes:
    - Common exclude conditions group ID (`E.JP1_IMCOMEXCLUDE_ID`)
    - Common exclude conditions group name (`E.JP1_IMCOMEXCLUDE_NAME`)
    - Common exclude conditions group target-for-exclusion (`E.JP1_IMCOMEXCLUDE_TARGET`)
- Defined automated actions can now be enabled or disabled by using the Action Parameter Definitions window or the `jcachange` command.
- A note was added for cases where the automated action function requests a large number of agents at once to execute a command.
- For automated action definitions, the status of execution conditions can now be retained unless their definitions are changed.
- A consideration on maintenance was added for excluding error events that are caused by maintenance work from action execution.
- The maximum number of hosts that can be managed by one instance of JP1/IM - Manager was increased to 2,500.
- The following files were added to the list of files and folders:
    - Configuration file for incident inheritance information
    - Model file for the configuration file for incident inheritance information
    - Common exclusion history file
    - Common exclusion-conditions definition history file

- The maximum number of hosts on which commands can be executed from one instance of JP1/IM - Manager was increased 2,500.
- The maximum number of defined common exclusion-conditions groups (in extended mode) was increased to 2,500. The maximum filter length of the common exclusion-conditions groups (in extended mode) was increased to 15 MB.
- The maximum number of hosts that can be set in a business group or monitoring group was increased to 2,500.
- A description was added to explain that the automated action definition file must be updated when JP1/IM - Manager is upgraded from versions earlier than 11-10.
- A common exclusion-conditions group (extended) can now be set to exclude a collected JP1 event from automated-action execution.
- Exclusion processing caused by common exclusion-conditions and update processing of common exclusion-conditions definition are now logged into history files.
- For the procedure to link with JP1/Service Support, a step was added for cases where the incident registration mode is set to 3.
- The configuration file for incident inheritance information was added to the list of files to back up.
- A description about the exclusion history and definition history of common exclusion-conditions was added to the section about using historical reports.
- The detailed information of JP1 events displayed in the Event Details window now includes the following items:
  - Common exclude conditions group ID
  - Common exclude conditions group name
  - Common exclude conditions group target-for-exclusion
- The following files were added to the lists of log files and directories:
  - Common exclusion history file
  - Common exclusion-conditions definition history file
- The following files were added to the lists of data to be collected for troubleshooting:
  - Common exclusion history file
  - Common exclusion-conditions definition history file
- A corrective action for cases where a common exclusion-condition is used in extended mode was added to the actions to take when no JP1 event is displayed in the Event Console window.
- A description was added for actions to take when an automated action is not executed.
- In the Event Console window, the **Action** column now shows an icon indicating that the event is excluded from action execution by a common exclusion-condition (action execution).
- The configuration file for incident inheritance information (`incident_info.conf`) was added to the relation definition files of the Event Details window and the Edit Event Details window.
- For common exclusion-conditions in extended mode, in the System Environment Settings window, the **Type** column of the **General** page now shows an icon indicating that the common exclusion-condition excludes a collected event from action execution.
- For common exclusion-conditions in extended mode, in the Event Acquisition Conditions List window, the **Type** column of the **Common exclusion-conditions groups** list now shows an icon indicating that the common exclusion-condition excludes a collected event from action execution.
- In the Common Exclusion-Condition Settings (Extended) window, you can now specify the exclusion target.
- The event list in the Event Console window can now show the following items:

    - Common exclude conditions group ID
    - Common exclude conditions group name
    - Common exclude conditions group target-for-exclusion
- You can now enable or disable automated action definitions in the Action Parameter Definitions window.
- When you apply changes in the Action Parameter Definitions window, you can now retain the suppression status and the status of satisfied conditions of the AND-joined conditions unless the action definition is edited.
- You can now specify an action ID of the action execution condition in the Action Parameter Detailed Definitions window.
- A note was added for cases where a large number of agents are requested at once to execute a command.
- For the `jcachange` command, the following options were added: `-e`, `-on`, `-off`, and `-st`.
- The `jcadefconv` command can now convert an action definition file from a version earlier than 11-50 (the `DESC_VERSION` value is less than `4`) to version 11-50 or later (the `DESC_VERSION` value is `4`).
- The following definition file was added:
    - Configuration file for incident inheritance information (`incident_info.conf`)
- The following files were added to lists of data collected with the data collection tool:
    - Common exclusion history file
    - Common exclusion-conditions definition history file
- For the automated action environment definition file (`action.conf.update`), the default value of the `ACTIONINFSIZE` parameter was changed to `dword:00001000` (4,096 KB).
- For the automated action definition file (`actdef.conf`), the parameters `aid` and `valid` were added. Additionally, the `DESC_VERSION` parameter can now take a new file version of `4`.
- For the automated action definition file (`actdef.conf`) (for conversion), the `DESC_VERSION` parameter now can take a file version of `4`.
- The definitions for the following items were added to the default definition file for extended event attributes:
    - Common exclude conditions group ID
    - Common exclude conditions group name
    - Common exclude conditions group target-for-exclusion
- For the common exclusion-conditions extended definition file, the `ex-target` parameter was added. Additionally, the `DESC_VERSION` parameter can now take a new file version of `2`.
- For linkage with JP1/Service Support, a new incident registration mode was added to allow any event attributes to be inherited.
- The following messages were added:

  KAVB0518-E, KAVB0759-E, KAVB0762-E, KAVB0763-E, KAVB1604-E to KAVB1608-E, KAVB1873-W, KAVB1874-E, KAVB3173-W, KAVB3180-W, KAVB3181-W, KAVB3185-I, KAVB4026-E to KAVB4029-E, KAVB4148-E, KAVB4155-E, KAVB4451-E, KAVB4452-E, KAVB4714-E, KAVB4715-E, KAVB5112-E, KAVB5505-W, KAVB5506-W, KAVB5559-W to KAVB5561-W, KAVB5760-W to KAVB5762-W, KAVB8821-E, KNAN22533-E, KNAN22534-E
- The output destination of the following message was corrected:

  KAVA1821-E, KAVB1115-W
- The actions for the following messages were changed:

  KAVB1591-E, KAVB1858-E, KAVB2605-E, KAVB5105-W, KNAN22017-E, KNAN22823-E

- For the following messages, the message output lines were added. The actions were also changed.
  KAVB3118-E, KAVB3119-E
- For the following messages, the message description was changed.
  KAVB1869-E, KAVB4450-E
- For the following message, the message description was changed. The actions were also changed.
  KAVB5109-W

L.2 Changes in version 11-10

(1) Changes in the manuals 3021-3-A06-20(E), 3021-3-A07-20(E), 3021-3-A08-20(E), 3021-3-A09-20(E), 3021-3-A10-20(E), 3021-3-A11-20(E), and 3021-3-A12-20(E)

- Windows Server 2016 is now supported.
- A JP1/PFM - Web Console report window that indicates the performance of a selected event-source-host at the time of an event can now be directly displayed (single sign-on).
- By clicking the URL of the JP1/AJS - Web Console that is displayed in the event guide information, the user now can directly display the JP1/AJS - Web Console monitor window that corresponds to a JP1/AJS job or jobnet (single sign-on).
- The JP1/AJS - Web Console monitor window can now be displayed from a sent email by specifying the URL of the JP1/AJS - Web Console monitor window that corresponds to the JP1/AJS job or jobnet in the email text.
- Values of event inheritance information for automated actions can now be URL encoded or Base64 encoded.
- Remote monitoring can now be continued even when host information is collected during remote monitoring.
- The differential distribution method was added to the methods for applying the system hierarchy. With this method, the configuration definition information can be deleted from or distributed to only those hosts that have been changed in the current agent configuration.
- Log information that has been output on a host subject to remote monitoring can now be collected between the time remote monitoring stopped and the time remote monitoring is restarted.
- The maximum size of log information that can be collected per monitoring interval during remote monitoring can now be changed.
- A description about the maximum amount of log data that can be collected by one JP1/IM - Manager was added.
- For profile management, the method that uses IM Configuration Management can now be combined with the method that uses JP1/Base commands.
- When log file trapping is stopped from IM Configuration Management, the log file trap information for agents is no longer deleted.

  With this change, the log file trap information for agents can now be deleted when profiles are deleted in IM Configuration Management.
- The following configuration files can now be applied as a batch operation by IM Configuration Management:
  - Log-file trap action definition files
  - Log-file trap startup definition files
- The user can now specify whether to start the process automatically when the log file trap service starts.
- The retry count and retry interval can now be changed for remote-monitoring event log traps.

- JP1/IM - View can now be used concurrently from multiple sessions by using Remote Desktop Connection.
- The following files were added to the lists of files and directories:
    - Performance report display definition file
    - Model file for the performance report display definition file
    - Profile management environment definition file
    - Model file for the profile management environment definition file
    - Remote log trap environment definition file
    - Model file for the remote log trap environment definition file
    - Model file for the web-based operation definition file for plug-in free mode
    - Model file for the web-based operation definition file for compatibility mode
    - Web-based startup definition file
    - Model file for the web-based startup definition file
- Limitations on connecting JP1/IM - Manager 11-10 and JP1/IM - View 11-10 to earlier versions of products were added.
- A description about specifying access permissions for monitored log files was added to the description of the settings for monitoring logs on remotely monitored hosts.
- The procedure for the SEQ2 log file output format was changed in the description of the settings for monitoring logs on remotely monitored hosts.
- Additions and changes were made to the settings for the sizes of logs and event logs that can be collected per monitoring interval.
- IM Configuration Management can now compare the contents of profiles collected previously by the manager and the contents of the most recent profiles of agents to check for inconsistency.
- Changes were made to the method for configuring SSH communication for monitored hosts running on UNIX when remotely monitored hosts are added.
- Because the differential distribution method was added, the description of the methods for applying the system hierarchy was changed.
- Conditions for using both profile management in IM Configuration Management and profile management in JP1/Base were added to the prerequisites for specifying profiles for agents.
- The settings for using the web-based version of JP1/IM - View in plug-in free mode were added.
- The remote log trap environment definition file (`jp1cf_remote_logtrap.conf`) was added as a file whose common definition information must be copied from the active server (whose settings are changed) to the standby server in a cluster system.
- A description about the settings for linking with JP1/AJS was added.
- A description about the settings for linking with JP1/PFM was added.
- Changes were made to the procedure for resetting the date/time of a monitored host in a remote monitoring configuration after intentionally changing the date/time to a point in the future.
- The procedure for displaying performance reports for JP1 events was added.
- Data to be collected when using the web-based version of JP1/IM - View in plug-in free mode was added.
- Changes were made to the actions to take when IM Configuration Management fails to apply the system hierarchy.
- The following corrective actions were added to troubleshooting:

    - Actions to take when events cannot be collected because the trace log for the Central Console viewer or Central Scope viewer wraps around (and overwrites an earlier log file)
    - Actions to take when events cannot be collected because the trace log for IM Configuration Management wraps around (and overwrites an earlier log file)
- **Display Performance** was added to the menu items in the Event Console window.
- A **Display Performance** button was added to the following windows:
    - The Event Details window
    - The Edit Event Details window
- You can now configure different information for each host when you select the SSH UNIX connection in the Remote Monitoring Settings window.
- A **Start the process automatically when the log file trap service starts** check box was added to the **Configuration File** page in the Display/Edit Profiles window.
- Shift-JIS encoding can now be displayed when the agent host OS is SUSE Linux. This can be selected using an option in the **Startup locale** drop-down list on the **Configuration File** page of the Display/Edit Profiles window.
- The following item was added to the log file trapping information in the **Configuration File** page in the Display/Edit Profiles window:
    - Start the process automatically when the log file trap service starts (SKIP option)
- The following items were added to the displayed information regarding trapping of entries from the remote event log on the **Configuration File** page of the Display/Edit Profiles window:
    - `open-retry-times`
    - `open-retry-interval`
- A description was added to indicate that network paths cannot be specified as output file names or output destinations.
- Information about the following definition files were added:
    - Web-based startup definition file (`console_`*`xx`*`.jnlp`)
    - Profile management environment definition file (`jp1cf_profile_manager.conf`)
    - Remote log trap environment definition file (`jp1cf_remote_logtrap.conf`)
    - Performance report display definition file (`performance.conf`)
- A description of the encoding for event inheritance information was added.
- A description of how to switch between plug-in free mode and compatibility mode of the web-based version of JP1/IM - View was added. Model files for plug-in free mode and for compatibility mode were also added.
- Cross-references about URLs for linking with JP1/AJS were added.
- Information about the following event IDs were added:
  `00003FC6`, `00003FC7`, `00003FC8`, `00003FC9`, `00003FD6`, `00003FD7`, `00003FD8`, `00003FD9`, `00003FDA`, `00003FDB`, `00003FDC`
- The following messages were added:
  KAVB0687-I, KAVB0688-E, KAVB1983-I to KAVB1985-E, KNAN20241-Q, KNAN20242-Q, KNAN20441-Q, KNAN21187-W, KNAN21405-W to KNAN21412-E, KNAN22274-I, KNAN22464-I, KNAN22465-E, KNAN22502-I, KNAN22530-E to KNAN22532-E, KNAN26143-W, KNAN26339-W to KNAN26346-I, KNAN26350-W to KNAN26354-E, KNAN29099-W
- The following messages were changed:
  KAVB0685-E, KAVB8203-E, KAVB8204-E, KAVB8303-W to KAVB8305-W, KNAN21170-W, KNAN21400-W, KNAN21402-E to KNAN21404-E, KNAN22220-E, KNAN22223-E, KNAN22245-E, KNAN22250-E,

KNAN22403-E, KNAN22422-E, KNAN22426-E, KNAN22466-E, KNAN22500-E, KNAN22503-E, KNAN26063-E, KNAN26081-E, KNAN26095-E, KNAN26140-W, KNAN26142-W, KNAN26163-E, KNAN26187-E, KNAN26208-E, KNAN26338-E

L.3 Changes in version 11-01

(1) Changes in the manuals 3021-3-A06-10(E), 3021-3-A07-10(E), 3021-3-A08-10(E), 3021-3-A09-10(E), 3021-3-A10-10(E), 3021-3-A11-10(E), and 3021-3-A12-10(E)

- A description was added indicating that you can search for repeated events consolidated in a consolidation event by specifying the suppressed event ID as a search condition.
- A description of the flow of issuing events after display messages changed was added.
- The operation log definition file and the model file for the operation log definition file were added to the lists of files and folders that can be referenced and edited by the user.
- Restrictions on connecting JP1/Integrated Management - Manager 11-01 and JP1/Integrated Management - View 11-01 to previous versions of products were added.
- It is now possible to output the history of login and logout information to action logs.
- In the Settings for View Filter window, suppressed event IDs can now be set and the **Read Suppressed Event ID From Selected Event** button was added.
- The `jco_spmd_reload` command can now be used to apply the definition files.
- The operation log definition file (`imm_operationlog.conf`) was added to the files whose common definition information must be copied from the active server (whose settings are changed) to the standby server in a cluster system.
- A description was added indicating that you can search for repeated events consolidated in a consolidation event by specifying the suppressed event ID for the search condition.
- The suppressed event ID was added as an item that can be specified in the Event Search Conditions window. In addition, the **Read Suppressed Event ID From Selected Event** button was added.
- Operation log was added as a type of log information.
- Information for the following log files was added:
  - Operation log file
  - Managed-node count (`jimnodecount` command) log file
- A description of RAS information that is collected if a problem occurs during remote monitoring was added.
- In the Event Search Conditions window, the **Read Suppressed Event ID From Selected Event** button and **Suppressed event ID** area were added.
- A note on specifying the suppressed event ID was added for the **Item name** drop-down list in the Event Search Detailed Conditions (Program-Specific Information in Extended Attribute) window.
- In the Settings for View Filter window, the **Read Suppressed Event ID From Selected Event** button and **Suppressed event ID** area were added.
- A note on executing the `jcadefconv` command with the `-i` or `-o` option specified was added.
- The definition file for opening monitor windows was added as a definition file that is enabled when the `jco_spmd_reload` command is executed.

- A note on the handling of control characters when the `jimmail` command (Windows-specific command) is executed was added.
- The `jimnodecount` command, which counts the number of nodes managed by JP1/IM - Manager, was added.
- The operation log definition file (`imm_operationlog.conf`), which defines whether to output operation log data, the output destination, log file size, and number of files, was added.
- A description stating that the definitions in the definition file for opening monitor windows are applied when the `jco_spmd_reload` command is executed for the file was added.
- The following JP1 event ID was added:
  00003F7C
- The following messages were added:
  KAVB0112-E, KAVB1979-E, KAVB1981-I, KAVB1982-E, KAVB8201-E, KAVB8202-E, KAVB8203-E, KAVB8204-E, KAVB8205-E, KAVB8206-E, KAVB8207-E, KAVB8208-E, KAVB8301-W, KAVB8302-W, KAVB8303-W, KAVB8304-E, KAVB8305-W, KAVB8306-E, KAVB8307-W, KNAN30000-I, KNAN30001-W, KNAN30002-I, KNAN30003-W
- The following messages were changed:
  KAVB1689-W, KAVB4627-W, KNAN11202-I, KNAN11207-I

L.4 Changes in version 11-00

(1) Changes in the manuals 3021-3-A06(E), 3021-3-A07(E), 3021-3-A08(E), 3021-3-A09(E), 3021-3-A10-01(E), 3021-3-A11(E), and 3021-3-A12(E)

- The following operating systems are now supported:
  - Windows 10
  - Linux 7
  - SUSE Linux 12
  - Oracle Linux 7, Oracle Linux 6
  - CentOS 7, CentOS 6
- The following operating systems are no longer supported:
  - Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008
  - Solaris
  - HP-UX (IPF)
  - Linux 5
- The user can now group JP1 events in desired units and manage them (addition of program-specific attributes).
- SSL communication is now supported between a host and a manager host (communication encryption function).
- Program-specific extended attributes of JP1 events can now be displayed under any item names in the events list in the Event Console window and output to event reports (program-specific extended attribute display function).
- Desired item names can now be used when program-specific extended attributes are specified in event conditions, such as view filters and event receiver filters (program-specific extended attribute specification function).
- JP1 event messages can now be converted to a predefined message display format (display message change function).
- The OpenStack base and virtual machines and physical servers on OpenStack can now be monitored for failures.

- The REST API of JP1/AO can now be used to perform operations, such as changing monitoring settings and adding users.
- Notes have been added regarding system configurations in which multiple sites are monitored.
- Descriptions have been added for the `LANG` language environment settings to indicate that the SJIS encoding can be used only in SUSE Linux in a Linux environment.
- Descriptions have been added to the preparations for using functions.
- JP1 events can now be issued so that JP1 event messages that have been changed by the display message change function can be referenced by user programs (events issued after display message change) (JP1/IM - MO compatibility function).
- Descriptions of how to update and recover the IM database have been added.
- Descriptions of the relationship between JP1 events that are issued by BJEX or JP1/AS and JP1/IM apply only to response-waiting events, as Windows versions now support response-waiting events.
- The data to be collected in the event of an error has been added and changed.
- The default or initial value for the following window items was changed:
  - In the Preferences window, the default value for **Scroll buffer** on the **Monitor Events** page was changed from 500 to 2,000.
  - In the Preferences window, the default value for **Num. of events to acquire in 1 search** on the **Monitor Events** page was changed from 20 to 100.
  - In the Preferences window, the initial value for the check box **Save the page that was displayed when the window was closed, and the application state of the view filter** on the **Event Attributes** page was changed from disabled to enabled.
  - In the Preferences window, the initial value for **Coloring** on the **Event Attributes** page was changed from disabled to enabled.
  - In the Preferences window, the initial value for the **Include the Severe Events page** radio button under **Coloring** on the **Event Attributes** page was changed from disabled to enabled.
  - In the Preferences window, the default value for **Action Log** on the **Command Execution** page was changed from 100 to 10,000.
  - In the System Environment Settings window (**General** page), the default value for **Event buffer** was changed from 500 to 2,000.
  - In the Conditions for Updating List of Action Results window, the default value for **Update method** was changed from **Update manually** to **Update automatically**.
  - In the Conditions for Updating List of Action Results window, the default value for **Num. to display** was changed from 20 to 200.
- The default values for the following command options and definition parameters were changed:
  - The default value for `-cmdbtn` in the `jcoimdef` command was changed from `OFF` to `ON`.
  - Previously, the menu for starting the IM Configuration Management viewer was not registered by specifying `-i` in the `jcovcfsetup` command during installation, but the menu is now registered during installation.
  - The default value for `EventCount` (number of event buffers) in the system profile (`.system`) was changed from 500 to 2,000.
  - The default value for a timeout in the communication environment definition file (`console.conf.update`) was changed from 2,500 to 60,000 milliseconds.
  - The on-memory mode of the status change condition that is specified in the definition file for the on-memory mode of the status change condition was changed from disabled to enabled.

- The following JP1 event IDs have been added:
  `00003F6A`, `00003F76`, `00003F77`, `00003F78`, `00006400`
- The following messages have been added:
  KAVB0233-Q, KAVB0517-W, KAVB1192-E, KAVB1596-W to KAVB1598-Q, KAVB1936-E to KAVB1965-E, KAVB1969-W to KAVB1978-E, KAVB2567-E, KAVB2626-E, KAVB2630-E to KAVB2640-W, KAVB3164-E to KAVB3172-W, KAVB3915-E to KAVB3918-E, KAVB4620-W to KAVB4641-W, KAVB4803-I, KAVB5759-W, KAVB5800-I to KAVB5804-E, KAVB5806-E, KAVB5809-E to KAVB5810-E, KAVB5820-W to KAVB5822-W, KAVB6601-E to KAVB6604-W, KAVB6610-E to KAVB6616-E, KAVB7580-E to KAVB7586-E, KAVB7810-E, KAVB7812-E to KAVB7814-E, KAVB7818-E, KAVB8608-W to KAVB8610-W, KAVB8810-I to KAVB8820-W, KAVB9251-E to KAVB9252-E, KAVB9255-E, KAVB9256-E, KNAN11204-E to KNAN11210-W, KNAN20121-E to KNAN20124-W, KNAN20131-E to KNAN20137-E, KNAN20141-E to KNAN20144-W, KNAN20151-E to KNAN20157-E, KNAN24150-E to KNAN24151-E, KNAN24153-E, KNAN24155-E, KNAN29090-E to KNAN29091-E, KNAN29093-E to KNAN29095-E, KNAN29097-W to KNAN29098-E
- The following messages have been changed:
  KAVB0013-E to KAVB0015-E, KAVB0106-E, KAVB0108-E, KAVB0111-E, KAVB0121-E, KAVB0229-I to KAVB0231-E, KAVB0311-W, KAVB0411-E, KAVB0413-E, KAVB0535-I to KAVB0536-I, KAVB0872-E, KAVB1202-E to KAVB1203-E, KAVB1205-E, KAVB1509-E, KAVB1535-E, KAVB1541-E, KAVB1652-E, KAVB1682-E, KAVB1686-E to KAVB1688-W, KAVB2002-I, KAVB2003-E, KAVB2027-E, KAVB2051-I, KAVB2071-W, KAVB2103-E, KAVB2239-E, KAVB2323-E, KAVB2557-W, KAVB2605-E to KAVB2608-E, KAVB2614-E, KAVB2618-E to KAVB2621-E, KAVB3078-E, KAVB3093-E, KAVB3101-E, KAVB3107-E, KAVB3149-E, KAVB3156-W, KAVB3158-E, KAVB3647-E, KAVB3828-E, KAVB4253-W, KAVB6210-E, KAVB6251-E, KAVB7003-E, KAVB7155-E, KAVB7204-E, KAVB7607-E, KAVB8060-E, KAVB8428-W, KAVB8454-W, KNAN11173-E, KNAN11197-I to KNAN11200-I, KNAN20102-E, KNAN20228-E, KNAN21002-E, KNAN22012-E, KNAN22267-E, KNAN22701-E to KNAN22702-E, KNAN22805-E to KNAN22806-E, KNAN23003-E, KNAN29002-E, KNAN29007-E, KNAN29082-E
- The following message has been deleted:
  KAVB0012-W

L.5 Changes in version 10-50

- Additions have been made in the procedures for installing and setting up JP1/IM and JP1/Base.
- Descriptions have been narrowed down to the procedure for customizing the settings of event forwarding with IM Configuration Management.
- A procedure for monitoring records in application log files by JP1/IM has been added.
- A procedure for monitoring Windows event logs by JP1/IM has been added.
- The method to change the severity levels of events has been changed from a definition file to a window.
- A setting procedure has been added in order to send email by the email notification function.
- The description of how to know the range of impact of system failures by visual monitoring has been moved from former chapter 1 in this manual.
- The description of how to monitor the system for each business group has been moved from the former chapter 1 in the *Job Management Partner 1/Integrated Management - Manager Quick Reference*.
- An explanation has been added to generally describe the functions related to the measures taken to handle a large number of events.
- View filters are now available on the **Severe Events** page.
- Descriptions have been added in figures to indicate that view filters can be set for the **Severe Events** page.

- Suppression of repeated event monitoring is now described as separate items according to the usages below. Also, some considerations for the suppression of repeated event monitoring have been added.
  - Suppressing the display of repeated events by using a repeated event condition without a threshold.
  - Suppressing the display of a large number of events and the execution of automated actions.
- Issuance of an event to notify that suppression will continue has been added to the function to suppress monitoring of repeated events.
- The description of the consolidated display of repeated events has been moved. Also, the differences between the consolidated display of repeated events and the suppression of repeated-event display are now listed in a table.
- Specification of the range for suppression of the execution of automated actions has been added to the function to suppress monitoring of repeated events.
- The maximum end monitoring period for suppressing display of repeated events and suppressing monitoring of large numbers of events was extended to 86,400 seconds.
- Descriptions and considerations have been added for the suppression of the forwarding of a large number of events.
- The Severity Change Definition Settings window has been added as a window you can reference when using the severity changing function.
- The range of events to be collected at login can now be set.
- Descriptions of the mechanisms to send a notification email by automated action at the occurrence of an error and the comparison of the notification by email between JP1/IM - Manager and TELstaff have been added.
- Customizing the settings of monitoring-target nodes in the Central Scope has been added as a function and some considerations related to this function have been added.
- The following files have been added to the list of files and directories:
  - System profile of Central Scope
  - Model file for the system profile of Central Scope
  - System profile of the Central Scope viewer
  - Model file for the system profile of the Central Scope viewer
- Restrictions applying when JP1/Integrated Management - Manager 10-50 and JP1/Integrated Management - View 10-50 are connected to lower-version products have been added.
- The range of events to be collected at login can now be set.
- View filters are now available on the **Severe Events** page.
- Background colors can now be set on the **Severe Events** page.
- Descriptions have been added to explain how to set up the email notification function of JP1/IM - Manager. In addition, notes on the use of the function and directions on passing through the firewall have been added.
- A procedure for setting severity changes using a window has been added as a setting method for the severity changing function.
- A procedure for customizing the monitoring node settings in the Central Scope has been added.
- Additions have been made to describe the backup files added because of the addition of the email notification function, points to be noted when the host name and IP address are changed. Additions have also been added to describe how to locate errors when mail cannot be sent and the actions to be taken against individual errors.
- Background colors can now be set on the **Severe Events** page.
- View filters are now available on the **Severe Events** page.

- A procedure for selecting the range of suppressing the execution of actions has been added to the procedure for suppressing the automated actions triggered by repeated events by using the suppression of repeated event monitoring. Also, added is a procedure for specifying the issuance of an event to notify that suppression will continue.
- A procedure for suppressing forwarding of a large number of events has been added.
- The range of events to be collected at login can now be set.
- A description has been added to let users see the Job Management Partner 1/Integrated Management - Manager Configuration Guide for details about the event display during a specified period.
- Because view filters are now available on the **Severe Events** page, the description explaining that view filters are applied only on the **Monitor Events** page has been deleted.
- Procedures for changing the severity levels of events using a window has been added.
  - Setting the severity levels at system configuration
  - Setting the severity levels during system operation
  - Registering an added severity change definition as a regular severity change definition
- The following OSs have been added to the list of applicable OSs:
  - Windows 8.1
  - Windows Server 2012 R2
- The Severity Change Definition Settings window has been added to enable users to set event conditions for severity changing definitions.
- The View Severity Change Definitions window has been added to enable users to list the event conditions for severity changing definitions.
- The following menu items have been added to the Event Console window:
  - **Add Severity Change Definition Settings**
  - **Severity Change Definitions**
- View filter settings have been added on the **Severe Events** page.
- Background color settings have been added on the **Severe Events** page.
- The **Display** page has been added to enable users to set the range of events to be collected at login.
- **Suppress actions for the following events** has been added as an item to select the range of suppressing automated actions under **Suppression items** on the **Basic Settings** page of the Repeated Event Condition Settings window.
- Checks for suppression to continue and processing for when suppression continues have been added as items to make sure that the suppression of repeated-event monitoring continues and perform processing on the **Options** page of the Repeated Event Condition Settings window.
- When closing a window, users can now select whether to save the page being displayed and the status of the view filter application.
- The `jimmail` command for sending email to a specified email address has been added.
- The `jimmailpasswd` command for setting a password for POP-before-SMTP or SMTP-AUTH authentication in the email environment definition file has been added.
- `42` has been added as a return value of the `jcsdbsetup` command.
- The email environment definition file has been added.
- `cmt`, `defin`, and `addflag` have been added as parameters for the severity changing definition file.
- A file (`chsev_attr_list.conf`) has been added to enable users to specify the items of severity changing definitions to be displayed in the **Attribute name** column in the Severity Change Definition Settings window.

- A file (`chsev_auto_list.conf`) to define automatic input of severity changing definitions has been added to enable users to define the JP1 event attributes that are set automatically. The attributes are set automatically, when you choose (after selecting a JP1 event in the event list of the Event Console window) **View** and then **Add Severity Change Definition Settings** to open the Severity Change Definition Settings window.
- The system profile of Central Scope and system profile of the Central Scope viewer have been added.
- The following JP1 event IDs have been added:
  00003F02, 00003F60, 00003F65, and 00003F71
- Monitoring ID and monitoring name have been added as extended attributes of the JP1 event whose *event ID is the value specified in the ACTDEF parameter*.
- The following messages have been added:
  KAVB0232-W, KAVB1191-E, KAVB1536-E, KAVB1538-W to KAVB1544-W, KAVB1917-E to KAVB1935-W, KAVB4678-I, KAVB4679-I, KAVB4802-I, KAVB6581-W, KAVB7464-W, KAVB8701-E to KAVB8741-E
- The following messages have been deleted:
  KAVB1402-W, KAVB1403-E
- The description of the administrator's action to be taken when a problem occurs during system operation has been separated as an independent topic.
- The explanation of message description format has been moved from Chapter 1 to Chapter 2.
- The corrective actions to be taken for the following messages have been changed:
  KAVB1899-E, KNAN11140-E, KNAN21400-W, KNAN21402-E, KNAN21403-E, KNAN26039-E, KNAN26187-E, KNAN26328-E
- The operations of the system for the following messages have been changed:
  KAVB4602-W
- The following message has been changed:
  KAVB4677-I

L.6 Changes in version 10-10

- The following OSs have been added to the list of applicable OSs:
  - Windows 8
  - Windows Server 2012
  - Linux 5
- The events that meet user-specified conditions among the events having occurred in large numbers can now be consolidated into a single event in the display by the suppression of repeated-event monitoring.
- The actions to be taken for the JP1 events displayed on the Central Console can now be made clear in linkage with JP1/IM - Navigation Platform.
- JP1/Integrated Management - Navigation Platform has been added as an Integrated Management product that can be linked to JP1/Integrated Management - Manager.
- Suppression of repeated-event monitoring has been added as functionality for consolidating and displaying repeated events and suppressing unnecessary actions when many repeated events matching a specified condition have occurred. Accordingly, the consolidated display of repeated events and the suppression of repeated-event monitoring are described separately in *3.4 Monitoring repeated events*.
- IM Configuration Management can now manage the virtualization configuration information of the following virtualization software and virtualization environment management software:

- HCSM
- KVM

- An event ID (B.IDBASE) has been added as an attribute of the JP1 event that can be registered as an incident in JP1/Integrated Management - Service Support.
- Customizing JP1/Integrated Management - View operation is now described as two separate items: customization that uses the Central Console viewer or Central Scope viewer and customization that uses IM Configuration Management viewer.
- Restrictions applying when JP1/Integrated Management - Manager 10-10 and JP1/Integrated Management - View 10-10 are connected to previous product versions have been added.
- Section *4.13 Customizing the JP1/IM - View operation* in the *JP1/Integrated Management - Manager Configuration Guide* has been moved and its title has been changed to *Customizing operation of JP1/IM - View (Central Console viewer and Central Scope viewer)*.
- A description has been added to explain how to customize the IM Configuration Management - View operation to specify the JP1 JP1/IM - View operation.
- When the OS is Solaris, UTF-8 can now be specified as a character code in the LANG environment variable of JP1/IM.
- A procedure has been added to enable a function (suppression of repeated-event monitoring) to suppress monitoring when the events that match user-specified conditions occur repeatedly.
- A description has been added to explain how to link to JP1/IM - Navigation Platform.
- A procedure has been added to suppress monitoring when the events that match user-specified conditions occur repeatedly (suppression of repeated-event monitoring).
- A procedure has been added to consolidate the events that have the same attributes and occur successively and display them (consolidated display of repeated events).
- Procedures have been added to check repeated events and consolidated events and change their action status.
- A procedure has been added to view the job contents (operating procedures) by linking to JP1/IM - Navigation Platform.
- The virtualization configuration information of the following virtualization software and virtualization environment management software can now be imported and exported as the management information of IM Configuration Management.
    - HCSM
    - KVM
- Instructions to make sure that KVM and HCSM have been set up and are running have been added as the actions to be taken when IM Configuration Management fails to collect virtualization system configurations.
- The Repeated Event Condition Settings window has been added as a means of setting repeated event conditions to suppress the monitoring of repeated events.
- The Extended Attribute (Common Information/Specific Information) Settings window has been added as a means of specifying common extended attribute names or program-specific (or user-specific) extended attribute names.
- The List of Repeated Event Conditions window has been added as a means of listing repeated event conditions that are set to suppress the monitoring of repeated events.
- The following menu items have been added to the Event Console window:
    - **Suppress by Repeated Event Conditions**
    - **Repeated Event Condition Settings**

- A description has been added to explain that the Related Events (Summary) window can display only the first 100 events and indicates other events in the **Events that cannot be displayed** field at the bottom of the window.
- Repeated events can now be specified in the following windows:
    - Event Search Conditions window
    - Settings for View Filter window
- When the OS is Solaris, `ja_JP.eucJP` can now be selected as a `LANG` value for the EUC encoding from the **Startup locale** drop-down list in the Display/Edit Profiles window of IM Configuration Management.
- UTF-8 has been added as a value that can be specified as a character code for log files when the OS to be monitored by remote-monitoring log file trapping is UNIX.
- The `jcfcolvmhcsm` command, which obtains virtualization configuration information from HCSM and outputs it to a virtualization configuration information file, has been added.
- The `jcfcolvmkvm` command, which obtains virtualization configuration information from KVM and outputs it to a virtualization configuration information file, has been added.
- The `-storm` option, which specifies whether to enable the suppression of repeated-event monitoring, has been added to the `jcoimdef` command.
- The maximum number of serial numbers you can specify in the `jcochstat` command has been changed to 100.
- A parameter that suppresses the display of the name of logged-in JP1 user has been added to the following definition files:
    - Web-based operation definition file (`console_ja.html`)
    - Operation definition file for IM Configuration Management - View (`jcfview.conf`)
- In the section for event guide information file, the information about the *URL used to link with JP1/IM - Navigation Platform* has been added for the HTML tag that specifies a linkage-target URL. The information has been added under the table *HTML tags that can be used in the event guide message file*.
- For all OSs, C, EUCJIS, SJIS, and UTF-8 can now be selected as the character code to be used in the definition file for extended event attributes and the definition file for opening monitor windows.
- A display item definition file for repeated event conditions (`event_storm_attr_list.conf`) has been added to specify the items to be displayed in the **Attribute name** column in the Repeated Event Condition Settings window.
- The auto-input definition file for repeated event conditions (`event_storm_auto_list.conf`) has been added to define the JP1 event attributes to be set automatically when the Repeated Event Condition Settings window opens. The window opens when you choose (after selecting a JP1 event in the event list of the Event Console window) **View** and then **Suppress by Repeated Event Conditions**.
- The parameters and registration mode (`SS_MODE`) used to link three products (Central Console, JP1/IM - Service Support, and JP1/IM - Navigation Platform) have been added to the definition file for registering incidents manually. Accordingly, a list of parameters that cannot be specified in this definition file has been added to the version information, and a note on the settings has been added to the description of `SS_URL=http://`*JP1/IM - Service Support-host*`:`*port-number*.
- The following parameters have been added to the IM-View settings file:
    - Suppressing the display of the names of the last JP1 users who logged in (`LOGIN_USER_HISTORY_MAX`)
    - Suppressing the display of the names of logged-in JP1 users (`SCREEN_TITLE_LOGININFO`)
- HCSM and KVM have been added as virtualization management types of the host information that is exported. Also, port number and private key path have been added as host information items that are exported.
- UTF-8 has been added as a Japanese character code that can be specified in the components of the statements in definition files.

- The following JP1 events have been added:
  00003F56, 00003F57, 00003F58, 00003F59
- The following messages have been added:
  KAVB0252-E, KAVB0253-Q, KAVB0684-I to KAVB0686-W, KAVB1148-Q, KAVB1190-E, KAVB1689-W, KAVB1884-W to KAVB1899-E, KAVB4670-W to KAVB4677-I, KAVB7146-E, KAVB7415-W, KNAN22072-E, KNAN22073-E, KNAN24070-W, KNAN26338-E
- The output destinations of the following messages have been changed:
  KNAN20020-W, KNAN20021-W, KNAN22066-E, KNAN22802-E, KNAN24009-E
- The following messages have been changed:
  KAVB0806-E, KAVB4053-I, KAVB4602-W, KAVB4604-W to KAVB4606-W, KAVB4608-W, KAVB4609-W, KAVB4612-W to KAVB4614-W, KAVB8417-I, KAVB8424-I, KNAN22016-E, KNAN22249-E, KNAN22315-E, KNAN22499-E, KNAN24006-E, KNAN24010-E, KNAN24033-W, KNAN24036-W, KNAN24038-W, KNAN24039-E, KNAN24063-W, KNAN26095-E, KNAN26142-W, KNAN26187-E, KNAN26329-E, KNAN26330-E, KNAN26334-E, KNAN29085-W, KNAN29086-W
- The corrective actions to be taken for the following messages have been changed:
  KAVB1131-W to KAVB1135-E, KAVB1137-W to KAVB1141-E,KAVB1153-E, KAVB1159-W to KAVB1162-W, KAVB1636-E, KAVB1639-E, KAVB1651-E, KAVB4603-W, KAVB4607-W, KAVB4610-E, KAVB4611-E, KAVB4615-E, KAVB4616-E, KAVB4664-E, KNAN22058-E, KNAN22066-E, KNAN22206-E, KNAN22249-E, KNAN22449-I, KNAN22823-E, KNAN22824-E, KNAN22830-E, KNAN22831-E, KNAN22842-E, KNAN24002-E, KNAN24009-E, KNAN24035-W, KNAN26138-E, KNAN29012-E
- The operations of the system for the following messages have been changed:
  KAVB5104-W, KNAN11012-I, KNAN11064-W, KNAN11066-I, KNAN11108-I, KNAN11118-E, KNAN11151-I, KNAN11154-I, KNAN11159-I, KNAN11161-I, KNAN11162-I, KNAN11180-I to KNAN11183-I, KNAN11186-I, KNAN11189-I, KNAN11198-I, KNAN11200-I to KNAN11202-I

L.7 Changes in version 10-00

- By selecting JP1 events being monitored, exclusion-conditions can now be defined when the attribute names and values of the events have been entered (additional common exclusion-conditions).
- Commands can now be executed on client hosts (viewer hosts) (client application execution function).
- Event information displayed in the Event Console window can now be automatically specified for the contents of a command to be executed (event information inheritance function).
- When a monitored host uses HP-UX, Solaris, or AIX, UTF-8 can now be specified as the locale for monitoring by the log file trap or remote-monitoring log file trap.
- When the names of monitored hosts are managed in FQDN format, the method of controlling event-source-host mapping can now be changed.
- Hosts with IPv6 addresses can now be monitored.
- Linkage with JP1/Advanced Shell is now possible.
- A procedure has been added to explain what order manuals should be read in.

L.8 Changes in version 09-50

- Grouping monitoring on the business viewpoint (business group monitoring) is now available.

- The following contents have been added, relating to how to specify business groups:
  - Prerequisites when the path name is used to specify a business group
  - Applying business groups and monitoring groups also applies the names on the Central Console.
  - Deleting business groups or monitoring groups will disable the specified contents.
- Mapping statuses for the following cases have been added:
  - When conditions are not matched.
  - When the values have been already set.
- The description of IM host accounts has been changed.
- Actions to be taken in the following case have been added:
  - In the agent configuration, when the system hierarchy in the tree display area on the **IM Configuration** page is displayed in gray.
- The following descriptions have been added:
  - If an agent configuration is applied after the system hierarchies are synchronized, information on the base managers is cleared.
  - An agent configuration must be applied when a remote monitoring configuration is used.
- The operations related to exclusion control for virtualization configuration information have been changed as follows:
  - Virtualization configuration information on the same host cannot be edited concurrently from different IM configuration management viewers.
  - Virtualization configuration information for the different hosts can be edited concurrently from different IM configuration management viewers.
- Configuration files that can be collected for individual JP1/Base versions are now organized in one place.
- The statuses of applied configuration files and hosts have been added.
- Descriptions of predefined filters, which filter log files and event logs that are collected from remotely monitored hosts, have been added.
- The following contents have been added:
  - If a log file is output while other log files are being collected, the same log file might be trapped twice.
  - Conditions of log files
- A description that log information is not collected when JP1/IM - Manager is stopped has been added. Also, a description that the maximum number of retries for a remote-monitoring event log trap is three times has been added.
- The following description has been added regarding the JP1 events issued by remote monitoring: the event-source-host mapping function is required to display and define a monitored host name as the event source host.
- The number of files to be exported has been changed.
- An example of the total number of business groups and monitoring groups has been added to the examples of system scale for database size.
- IM Configuration Management of JP1/IM - Manager has been added to the descriptions about processes.
- Direction of communication through a firewall when information about remotely monitored hosts is collected has been added.
- The limits that apply to JP1/IM - Manager when using IM Configuration Management have been updated.
  - The limit of the number of remotely monitored hosts has been deleted.
  - The total number of business groups and monitoring groups has been added.

    - The maximum number of hosts that can be set for a business group or a monitoring group has been added.
    - The limits of the number of tiers for business groups and monitoring groups have been added.
    - For AIX or HP-UX, the maximum number of IM Configuration Management viewers that can be connected to one JP1/IM - Manager has been added.
- The required operating permissions are now separately described for when restrictions on viewing and operating business groups are enabled and for when they are disabled.
- Restrictions when JP1/IM - Manager 09-50 and JP1/IM - View 09-50 are connected to the previous versions of products have been added.
- The following types of monitoring and management are now available for the hosts in the remote monitoring configuration (with the remote communication settings):
    - Messages in log files and Windows event logs that are generated on a host on which JP1/Base has not been installed can now be remotely monitored.
    - Definition information (profiles) set on remotely monitored hosts can now be checked or edited.
    - The IM Configuration Management window has been divided into the Edit Agent Configuration window (for editing the agent configuration) and the Edit Remote Monitoring Configuration window (for editing the remote monitoring configuration).
- Multiple monitored hosts can now be grouped from the business viewpoint so that individual business groups can be monitored separately.
- The event source host for an event that caused a JP1 event can now be displayed and defined by using event-source-host mapping.
- Extended mode has been added to common exclusion-conditions, the number of definitions for condition groups and the number of specifiable attributes have been increased, and event conditions can now be compared by specifying date and time.
- The following method has been added to the methods for executing commands in JP1/IM - View: frequently used commands can be registered as command buttons and executed when the buttons are clicked.
- How to convert event inheritance information into JP1 event information has been added.
- Notes for the configuration file names for log file trap information have been added.
- JP1 events can now be manually registered as incidents in JP1/IM - Service Support.
- A description has been added for the connection method when JP1/IM - View is used for Remote Desktop Connection.
- When setting the event guide by using variables (placeholder strings), URL-encoded character strings or Base64-encoded UTF-8 character strings can now be output in event guide messages.
- The following files have been added to the files and folders that can be referenced or edited by the user:
    - Folder for the common-exclusion-conditions display item definition file
    - Common-exclusion-conditions display item definition file
    - Model file for the common-exclusion-conditions display item definition file
    - System color definition file
    - Model file for the system color definition file
    - Folder for remote command definitions
    - Command button definition file
    - Model file for the command button definition file
    - Event-source-host mapping definition file

    - Model file for the event-source-host mapping definition file
- The following items have been added to the table of regular expressions that can be used in JP1/IM functions:
    - Severity changing function
    - Common exclusion-conditions (extended mode)
    - Event-source-host mapping function
- A procedure has been added for monitoring remote-monitoring event traps for monitored hosts on which Windows 7, Windows Server 2008, Windows Server 2008 (x64), Windows Server 2008 R2 (x64), or Windows Vista is running even when the user is logged off.
- Procedures for setting local security are now separately described for JP1/IM - Manager hosts and monitored hosts.
- A procedure for editing the registry has been added.
- A procedure for setting the `UseDNS` or `LookupClientHostnames` item has been added to the procedures for setting up SSH servers.
- The user who logs in to the monitored hosts when the following operations are performed under the SHH setting has been changed to the user who can remotely monitor the target host:
    - Create keys (for Windows)
    - Place the secret keys on the JP1/IM - Manager hosts (for Windows)
    - Place the public keys on the remotely monitored hosts (for Windows)
- The following description has been added: to display **Event source host name** after JP1/IM - Manager is upgraded, `E.JP1_SOURCEHOST` must be added to the file that defines which items are displayed for event conditions.
- Notes when hosts are registered in IM Configuration Management have been added.
- The following description has been added: in the agent configuration, if on the **IM Configuration** page, the system hierarchy in the tree display area is displayed in gray due to the change of host names or mismatch of configuration definition information, the configuration must be applied again.
- The following description has been added: if the profiles have not been applied, all the profiles that have not been applied and saved on the server will be deleted.
- The following description has been added: the agent configuration must be applied when the remote monitoring configuration is used.
- Item name **Assigned JP1 resource group name** in the Create Business Group window and the Edit Business Group Basic Information window has been changed.
- The following description has been added: if business groups and monitoring groups are applied, the names of the business groups and monitoring groups specified in the definitions on the Central Console are also changed to the latest names.
- A procedure for deleting files and folders (directories) after deleting the IM Configuration Management database has been added.
- Prerequisites for the settings of individual databases have been added.
- Commands can now be registered to command buttons and executed. A procedure has been added for this.
- A function for monitoring logs on the remotely monitored hosts has been added. A description of the procedure for setting this function has been added.
- Remotely monitored hosts can now be monitored. Related descriptions have been added to the following functions:
    - Register hosts.
    - Change host information.

- IM configuration was divided into agent configuration and the remote monitoring configuration. Descriptions have been changed accordingly.
- A function restricting viewing and operating business groups has been added. A description of the procedure for setting business groups has been added accordingly.
- A procedure for acquiring exclusive edit rights has been added.
- A procedure for setting profiles on remotely monitored hosts has been added.
- **Event source host name** has been added to the items that can be set and displayed.
- Common exclusion-conditions are now divided into the basic mode and the extended mode. Descriptions have been changed accordingly.
- A procedure for setting the display colors of JP1 events has been added.
- An event-source-host mapping function has been added. A procedure for using this function has been added accordingly.
- A description that the font size can be changed in the Event Console window has been added.
- A function restricting viewing and operating business groups has been added. A procedure for setting this function has been added accordingly.
- A description of services has been added to the prerequisites for the physical host environment.
- Conditions for physical host names and logical host names have been added to the prerequisites for cluster operations.
- The following description has been added: if JP1/IM - MO is used, the JP1/IM - Message Optimizer service on the connection source host must be stopped.
- A procedure for suppressing error reports to Microsoft has been added.
- A procedure for deleting only logical hosts on a JP1/IM - Manager host has been added.
- Because the events managed by JP1/IM - Manager can be manually registered as incidents in JP1/IM - Service Support, a description of the procedures for setting up the linkage between JP1/IM - Manager and JP1/IM - Service Support has been added.
- The following files have been added to the files to be backed up:
    - Common-exclusion-conditions display item definition file
    - System color definition file
    - Command button definition file
    - Event-source-host mapping definition file
- The log file trap (remote) and event log trap (remote) have been added to the command that collects the service status.
- *Log files and directory list* has been updated.
- Causes and corrective actions have been added to the descriptions of problems when remote-monitoring log file traps are running.
- The cause and corrective actions have been added for when a dialog box remains displayed while the IM configuration management viewer is being processed.
- How to operate when JP1/IM - MO is used has been added.
- The Files to be backed up when the remote monitoring configuration is used have been added.
- A description of the tasks required when the passwords for the manager and the remotely monitored hosts are changed in the remote monitoring configuration has been added.

- The differences in the agent configuration and the remote monitoring configuration when the monitoring configuration is changed in the system configuration have been added. Also, related notes have been added.
- **Event source host name** has been added to the display items and display names in the event list.
- A description of the difference between event information mapping and event-source-host mapping has been added.
- Restrictions when restrictions are enabled on viewing and operating business groups have been added.
- A procedure for calling the Select the process work board as the registration target window of JP1/IM - Service Support has been added because JP1 events can be registered as incidents.
- Descriptions and examples of the following options of the `jcochfilter` command have been added to the description of activating or deactivating common exclusion-conditions:
    - `-on`
    - `-off`
    - `-e`
- How to execute commands by using the command buttons has been added.
- The versions of the functions displayed in the Tool Launcher window have been clarified.
- A description of the Edit Remote Monitoring Configuration window used for remote monitoring has been added.
- A description of the management of business groups has been added.
- A description of remote monitoring operations has been added.
- The following items have been added to the information to be exported or imported:
    - Remote authentication information
    - Business group information
    - Monitoring group information
- In troubleshooting, actions to be taken when a business group or monitoring group is specified for the target host have been added to the actions to be taken when commands cannot be executed.
- Actions to be taken for remote monitoring problems have been added.
- The following description has been added: In **Search host** in the Event Search Conditions window and **Target host** in the Execute Command window, the name of a host belonging to the business group that can be viewed by the logged-in JP1 user must be entered.
- The causes of some display items in the IM configuration management viewer becoming different or disabled have been added.
- **System Common Settings** has been added to the Edit menu in the IM Configuration Management window.
- Detailed information displayed for remote monitoring has been added.
- The following description has been added to the description of **Host name** in the Edit Host Properties window: if a host is registered in a business group, **Host name** cannot be changed.
- A description for when hosts are deleted from the agent configuration has been added to the description for the Edit Agent Configuration window.
- A description has been added explaining that, in the following windows, it is mandatory to fill in the **User name** and **Password** fields if characters are entered in any other fields.
    - Remote Monitoring Settings window
    - **WMI/NetBIOS** page in the System Common Settings window
    - **IM Host Account** page in the System Common Settings window

- Notes have been added about deleting hosts from the remote monitoring configuration and reapplying when in the Edit Remote Monitoring Configuration window.
- The following contents have been added to the **Configuration File** page of the Display/Edit Profiles window:
    - Details about the individual statuses have been added to the displayed **Application status** item.
    - The following description has been added: when log file trap information or remote-monitoring event log trap information is selected, predefined filters can be set.
    - The following descriptions have been added to the items displayed in **Configuration File**:

      - Restrictions on characters that can be used in **Monitoring log file** have been added to the description of start options.

      - A description for when **Apply by Restarting** must be executed has been added to the description of saving and applying settings.
    - A description has been added to explain the `Startup Options` to be displayed when remote-monitoring event log trap information is selected in the tree display area while WMI/NetBIOS (NetBIOS over TCP/IP) connection is used.
- The Common Exclusion-Condition Settings (Extended) window has been added. This window can be used to set JP1 event exclusion-conditions and their validity periods for an event acquisition filter.
- The IM Configuration Management window has renamed to the Edit Agent Configuration window.

  Also, the following contents in the Edit Agent Configuration window have been corrected:
    - The menu items have been renamed.
    - **Remote communication type** (which is used to display the communication method of remote monitoring) and **Configuration type** (which is used to display configuration type) have been added.
- The Remote Monitoring Settings window has been added to set information for remote monitoring.
- The Edit Remote Monitoring Configuration window has been added to enable editing of the remote monitoring configuration managed by IM Configuration Management.
- The Create Business Group window has been added to enable creation of business groups.
- The Edit Business Group Basic Information window has been added to enable editing of basic information about business groups.
- The Create Monitoring Group window has been added to enable creation of monitoring groups.
- The Edit Monitoring Group window has been added to enable editing of basic information about monitoring groups.
- The Add/Delete Monitoring Group Hosts window has been added to enable registering or release of registration of hosts for business groups or monitoring groups.
- The Change Monitoring Group Name window has been added to enable changing monitoring group names.
- The System Common Settings window has been added to enable saving and managing the values of setting items as common setting values.
- For the registration of incidents, the Select the process work board as the registration target window of JP1/IM - Service Support can now be called from JP1/IM - Manager by clicking the **Register Incident** button.
- The following contents have been added to the Event Details window and the Edit Event Details window:
    - The **Execute Command** button has been added. It displays the Execute Command window for command execution.
    - For the registration of incidents, a JP1/IM - Service Support window can now be called by clicking the **Register Incident** button.

- When a correlation event on a host other than the one to which the user logged in from JP1/IM - View is displayed under **Display Items** in the Related Events (Correlation) window, incident registration in JP1/IM - Service Support is disabled.
- The following contents have been added to the Severe Event Definitions window, the Event Search Conditions window, the Settings for View Filter window, and the Detailed Settings for Event Receiver Filter window:
    - **Event source host name** can now be specified in event conditions.
    - When the `-ignorecasehost` option of the `jcoimdef` command is specified as `ON`, if an option other than **Regular expression** is selected for **Source host** and **Event source host name**, now the character string is not case sensitive.
    - The path name for a business group name can now be specified for **Source host** and **Event source host name**.
- The mode of common exclusion-conditions can now be selected from basic mode and extended mode. Accordingly, descriptions for individual modes have been added to the **General** page of the System Environment Settings window and to the **Common exclusion-conditions groups** in the Event Acquisition Conditions List window.
- The Preferences window has been changed to a tabbed view and the display size of fonts can be specified.
- The following contents have been added to the **Action Condition** page of the Action Parameter Detailed Definitions window:
    - **Event source host name** can now be specified in event conditions.
    - When the `-ignorecasehost` option of the `jcoimdef` command is specified as `ON`, if an option other than **Regular expression** is selected for **Source host** and **Event source host name**, now the character string is not case sensitive.
    - A business group name can now be specified as the path name when **Source host** and **Event source host name** are specified for the character string to be edited.
    - A business group name and monitoring group name can now be specified as the path name in **Target host**.
- In the Conditions for Updating List of Action Results window, a business group name and monitoring group name can now be specified as the path name in **Host**.
- The following contents have been added to the Execute Command window:
    - Commands can now be executed by clicking the command buttons.
    - A business group name or monitoring group name can now be specified as the path name in **Target host**.
- Agent configurations, remote monitoring configurations, and business groups can now be monitored. Accordingly, the menu items in the IM Configuration Management window have been changed.
- A **Business Group** page (**Business Group** tab) has been added to the IM Configuration Management window. It displays the configuration of business groups and monitoring groups.
- On the **Host List** page of the IM Configuration Management window, the following items have been added to the items displayed in low-level host information:
    - **Collection status**
    - **Remote communication type**
    - **Business Group**
    - **Monitoring Group**
- The remote monitoring configuration can now be monitored. Accordingly, **Remote monitoring settings** has been added to the items displayed in **Basic Information** on the **Host List** page of the IM Configuration Management window.

    Also, a display item in **Detailed Information** has been changed as follows:

    - **Collection status** -> **Information collection result**

- The following contents have been added on the **IM Configuration** page of the IM Configuration Management window:
  - Icons that indicate agent monitoring and remote monitoring have been added.
  - Remote (Base manager) and Remote (Integrated manager) have been added to the relationship between the host type and display information.
- **Remote communication settings** can now be specified in the Register Host window and the Edit Host Properties window.
- Profiles for remote-monitoring log file traps can now be added in the Add Profile window.
- **Editing business group** has been added to the items displayed in the Login User List window.
- Descriptions of the number of commands that can be executed at the same time have been added to the functional overview of the following commands:
  - `jcfaleltdef` command (for Windows only)
  - `jcfaleltreload` command (for Windows only)
  - `jcfaleltstart` command (for Windows only)
  - `jcfaleltstat` command (for Windows only)
  - `jcfaleltstop` command (for Windows only)
  - `jcfallogdef` command
  - `jcfallogreload` command
  - `jcfallogstart` command
  - `jcfallogstat` command
  - `jcfallogstop` command
  - `jcfexport` command
  - `jcfimport` command
  - `jcfvirtualchstat` command
- The `-filter` option has been added to the following commands:
  - `jcfaleltdef` command (for Windows only)
  - `jcfaleltstart` command (for Windows only)
  - `jcfallogdef` command
  - `jcfallogstart` command
- Descriptions of the return values for the following commands have been changed:
  - `jcfaleltdef` command (for Windows only) (Return value: 21)
  - `jcfaleltreload` command (for Windows only) (Return value: 12, 21)
  - `jcfaleltstart` command (for Windows only) (Return value: 21)
  - `jcfaleltstat` command (for Windows only) (Return value: 1, 21)
  - `jcfaleltstop` command (for Windows only) (Return value: 12, 21)
  - `jcfallogdef` command (Return value: 8, 21)
  - `jcfallogreload` command (Return value: 21)
  - `jcfallogstart` command (Return value: 8, 21)

    - jcfallogstat command (Return value: 1, 21)
    - jcfallogstop command (Return value: 12, 15, 21)
    - jcfexport command (Return value: 21)
    - jcfimport command (Return value: 21)
    - jcfview command (for Windows only) (Return value: 5)
    - jcfvirtualchstat command (Return value: 21)
- Descriptions of the return values for the following commands have been deleted:
    - jcfaleltdef command (for Windows only) (Return value: 13)
    - jcfaleltstat command (for Windows only) (Return value: 10, 13)
    - jcfaleltstop command (for Windows only) (Return value: 16)
    - jcfallogdef command (Return value: 13)
    - jcfallogreload command (Return value: 8)
    - jcfallogstat command (Return value: 10, 13)
    - jcfallogstop command (Return value: 16)
- The following description has been added to the description for the jcfaleltreload command: if the start options are changed by the jcfaleltdef command or in the Display/Edit Profiles window, they are not applied even after reloading.
- Descriptions of the -o option for the following commands have been changed:
    - jcfaleltstart command (for Windows only)
    - jcfallogdef command
    - jcfallogstart command
- A description for deleting profiles has been added to the functional overview of the jcfallogdef command.
- Descriptions of the -r option for the following commands have been changed:
    - jcfallogdef command
    - jcfallogstart command
- The following description has been added to the description for the jcfallogreload command: if a value of any parameter other than the MARKSTR and ACTDEF parameters is changed by the jcfaleltdef command or in the Display/Edit Profiles window, it is not applied even after reloading.
- A description of the files to be deleted after the jcfdbunsetup command is executed has been added.
- A description about "while remote monitoring is performed" has been added to the functional overview of the jcfimport command.
- The apply-IM-configuration-method definition file (jp1cf_applyconfig.conf), which is automatically generated when JP1/IM - Manager is installed, has been added.
- A description about the maximum character string size has been added to HEADLINE in the remote-monitoring log file trap action-definition file.

  Also, definition examples have been added.
- An example of definitions in the remote-monitoring event log trap action-definition file has been added.
- IMDBHOSTNAME has been added to the setup information file (jimdbsetupinfo.conf).
- JP1 events have been added.

- Event occurrence of JP1 events and messages have been changed.
  00003FD3
- Log type has been deleted from the details of event ID 00003FD0.
- The following items have been added to the details about event ID 00003FD2:
  - API where error occurred
  - Monitored host name
- The following item has been added to the details about event ID 00003FD3:
  - Monitored host name
- The `jimdbupdate` command has been added so that the IM database can be updated.
- The following description has been added to the functional description of the `jcfmkcsdata` command: generating import files for the Central Scope for which the monitoring tree information of a business group has been added.
- The following commands have been added so that remotely monitored hosts can be managed:
  - `jcfaleltdef` command (for Windows only)
  - `jcfaleltreload` command (for Windows only)
  - `jcfaleltstart` command (for Windows only)
  - `jcfaleltstat` command (for Windows only)
  - `jcfaleltstop` command (for Windows only)
  - `jcfallogdef` command
  - `jcfallogreload` command
  - `jcfallogstart` command
  - `jcfallogstat` command
  - `jcfallogstop` command
- The `jcochcefmode` command has been added so that the operation mode of common exclusion-conditions can be changed.
- The description of the `-d` option of the `jcashowa` command has been changed. Also, the description of how to specify the option by seconds has been added.
- Notes for the following commands have been added:
  - `jcfdbsetup`
  - `jcfdbunsetup`
  - `jcodbsetup`
  - `jcodbunsetup`
- The `-r` and `-g` options have been added to the following commands:
  - `jcfexport`
  - `jcfimport`
- The `-g` option has been added to the `jcfmkcsdata` command. Also, return value `11` has been added.
- The following files have been added to the definition files that are enabled when the `jco_spmd_reload` command is executed:
  - A file that defines which items are displayed for event conditions (`attr_list.conf`)

    - Common-exclusion-conditions display item definition file (common_exclude_filter_attr_list.conf)

- Notes at system startup and when JP1/IM - Manager is manually started have been added to the functional description of the jco_start command (UNIX only).
- Notes when JP1/IM - Manager is manually stopped have been added to the functional description of the jco_stop command (UNIX only).
- The following options have been added to the jcochfilter command:
    - -on
    - -off
    - -ef
    - -check
- A cross reference for CSV output format has been added to the functional description of the jcoevtreport command and the operand name of the -f option has been changed.
- The following options have been added to the jcoimdef command:
    - -cmdbtn
    - -hostmap
    - -bizmonmode
    - -ignorecasehost
- Notes about when JP1/IM - MO is used have been added to the descriptions for the following commands:
    - jimdbbackup
    - jimdbrecovery
    - jimdbrorg
    - jimdbstop
- The remote-monitoring log file trap action-definition file has been added to define actions of the remote-monitoring log file trap function.
- The remote-monitoring event log trap action-definition file has been added to define actions of the remote-monitoring event log trap function.
- The event-source-host mapping definition file (user_hostmap.conf) has been added. This file is used to define the conditions and the mapping source for a JP1 event to which the event source host is mapped by using the event source host mapping function.
- The values that can be specified for "ACTIONLIMIT"=dword:*hexadecimal-value* in the automated action environment definition file (action.conf.update) have been added.
- The system color definition file (systemColor.conf) has been added to define the settings of the colors used in the event list.
- The common-exclusion-conditions extended definition file has been added to define event conditions and applicable periods of common exclusion-conditions in extended mode.
- The common-exclusion-conditions display item definition file (common_exclude_filter_attr_list.conf) has been added to define items displayed in the **Attribute name** display area in the Common Exclusion-Condition Settings (Extended) window.
- The command button definition file (cmdbtn.conf) has been added to define the command buttons displayed in the Execute Command window.

- **Event source host name**, which is used for event-source-host mapping, has been added to the attribute names that can be specified for event conditions for the following files:
  - Automated action definition file (`actdef.conf`)
  - User profiles (`defaultUser | profile_`*user-name*)
  - Event guide information file (`jco_guide.txt`)
  - Correlation event generation definition file
  - severity changing definition file (`jcochsev.conf`)
  - Definition file for opening monitor windows
- The business group name and monitoring group name have been added to the items that can be specified for the host name in the automated action definition file (`actdef.conf`).
- The comments in the table of variables that can be used for action definitions in the automated action definition file (`actdef.conf`) have been changed.
- **Event source host name**, which is used for event-source-host mapping, has been added to the display items that can be specified in the file that defines which items are displayed for event conditions (`attr_list.conf`).
- A description for the configuration file for converting information (`event_info_replace.conf`) has been added.
- A description for when an error is detected by the health check function has been added to the description of `FAILOVER` in the health check definition file (`jcohc.conf`).
- The description of `DESC_VERSION` and `EV_FILE` in the event guide information file (`jco_guide.txt`) has been changed.
- `EV_USER` has been added in the event guide information file (`jco_guide.txt`).

  Also, descriptions of replacing characters for event guide messages have been added.
- The maximum sizes of the attribute values for the correlation event generation definition file have been added.
- The description of extended attributes that cannot be specified as attribute names in the correlation event generation definition file has been changed.
- The description of the correlation approval events for the correlation event generation definition file has been added.
- A description of linking with JP1/IM - Service Support has been added in the incident manual-registration definition file (`incident.conf`).
- The versions of the products that can link with JP1/IM - Manager and the supported OSs have been added to the list in the Web page call definition file (`hitachi_jp1_`*product-name*`.html`).
- In the description of the operation definition file of the IM configuration management viewer (`jcfview.conf`), the Edit IM Configuration window has been changed to the Edit Agent Configuration window.

  Also, descriptions of the Edit Remote Monitoring Configuration window have been added.
- Descriptions about the active host name have been added to the description of `ONLINEHOSTNAME` in the cluster setup information file (`jimdbclustersetupinfo.conf`).
- The description of item names in the item file has been changed.
- The description of attribute names, operators, and operands that can be specified for event conditions in the filter file has been added.
- The following messages have been added:

  KAVB0012-W to KAVB0015-W, KAVB0110-E, KAVB0267-E, KAVB0354-I, KAVB0415-E to KAVB0419-E, KAVB0422-E to KAVB0424-E, KAVB0682-I, KAVB0683-E, KAVB0760-W, KAVB0761-W, KAVB0888-E to KAVB0891-E, KAVB0893-E to KAVB0900-E, KAVB0902-W, KAVB0903-E, KAVB0961-E, KAVB0962-W, KAVB1012-E to KAVB1021-W, KAVB1104-W, KAVB1105-W, KAVB1136-W to KAVB1141-E, KAVB1533-E, KAVB1534-E, KAVB1593-W to KAVB1688-W, KAVB1692-W, KAVB1694-E, KAVB1851-I to KAVB1872-W, KAVB4016-W, KAVB4440-W to KAVB4445-E, KAVB4507-W, KAVB4508-W, KAVB4650-I to KAVB4664-E, KAVB4666-W to KAVB4669-E, KAVB4706-W to KAVB4708-W, KAVB4710-I to KAVB4713-E, KAVB4790-W, KAVB8450-I to KAVB8457-E, KAJV0016-W, KAJV0017-W, KAJV0500-I to KAJV0503-E, KAJV0600-I to KAJV0614-E, KAJV0616-W to KAJV0619-E, KAJV2016-W, KAJV2017-W, KAJV2500-I to KAJV2503-E, KNAN11197-I to KNAN11202-I, KNAN20009-I, KNAN20045-Q, KNAN20046-E, KNAN20048-W, KNAN20057-I, KNAN20238-Q, KNAN20240-Q, KNAN20303-Q, KNAN20364-I, KNAN20365-I, KNAN20418-Q to KNAN20433-E, KNAN20437-Q, KNAN20438-Q, KNAN20440-Q, KNAN21185-E, KNAN21186-E, KNAN21300-E to KNAN21311-E, KNAN21400-W to KNAN21404-E, KNAN22032-E, KNAN22033-E, KNAN22265-E to KNAN22267-E, KNAN22270-E to KNAN22273-I, KNAN22307-I to KNAN22321-E, KNAN22413-E to KNAN22415-E, KNAN22451-E, KNAN22452-E, KNAN22454-E, KNAN22462-E, KNAN22529-E, KNAN22700-E to KNAN22702-E, KNAN22861-W, KNAN22862-E, KNAN22870-I to KNAN22874-E, KNAN22890-E, KNAN26000-I to KNAN26003-E, KNAN26006-I, KNAN26008-E, KNAN26010-E, KNAN26025-W to KNAN26028-E, KNAN26039-E, KNAN26050-I, KNAN26055-I to KNAN26059-E, KNAN26063-E to KNAN26065-E, KNAN26069-E, KNAN26072-W, KNAN26073-W, KNAN26078-I, KNAN26081-E, KNAN26091-I to KNAN26095-E, KNAN26097-E to KNAN26110-W, KNAN26117-E, KNAN26119-E, KNAN26121-I, KNAN26123-E, KNAN26131-I, KNAN26132-E, KNAN26138-E, KNAN26140-W, KNAN26142-W, KNAN26153-E, KNAN26155-E, KNAN26163-E, KNAN26181-E, KNAN26182-E, KNAN26187-E, KNAN26189-E, KNAN26196-E, KNAN26206-E, KNAN26208-E to KNAN26212-E, KNAN26214-I, KNAN26216-I, KNAN26217-I, KNAN26223-Q to KNAN26226-I, KNAN26230-I, KNAN26239-I, KNAN26243-E, KNAN26247-E, KNAN26249-I, KNAN26251-I, KNAN26252-I, KNAN26256-I, KNAN26258-E, KNAN26261-I, KNAN26265-E to KNAN26267-E, KNAN26269-I, KNAN26271-I, KNAN26274-I, KNAN26276-I, KNAN26278-I, KNAN26279-I, KNAN26281-I, KNAN26283-I, KNAN26285-I, KNAN26287-I, KNAN26292-E to KNAN26298-E, KNAN26317-I to KNAN26323-E, KNAN26325-E to KNAN26332-E, KNAN26334-E, KNAN26336-E, KNAN29087-E, KNAN29088-E, KNAN11203-I

- The output destinations of the following messages have been changed:

  KAVB8430-E, KNAN20354-Q, KNAN20362-Q, KNAN20520-I, KNAN20810-I, KNAN20816-E, KNAN20821-I, KNAN21180-E, KNAN21181-E, KNAN22267-E, KNAN22270-E to KNAN22272-I, KNAN22529-E, KNAN22819-E, KNAN22832-E, KNAN22846-E, KNAN22861-W, KNAN26003-E, KNAN26039-E, KNAN26050-I, KNAN26058-E, KNAN26063-E, KNAN26069-E, KNAN26072-W, KNAN26073-W, KNAN26078-I, KNAN26092-E, KNAN26097-E, KNAN26138-E, KNAN26153-E, KNAN26163-E, KNAN26187-E, KNAN26196-E, KNAN26208-E, KNAN26209-E, KNAN26211-E, KNAN26317-I, KNAN26318-I to KNAN26320-E

- Dialog boxes were added to the table of output destinations for messages related to IM Configuration Management (part 3).

- The following messages have been deleted:

  KNAN22870-I to KNAN22874-E, KNAN24100-I to KNAN24107-I, KNAN26008-E, KNAN26010-E, KNAN26059-E, KNAN26064-E, KNAN26065-E, KNAN26117-E, KNAN26121-I, KNAN26123-E, KNAN26131-I, KNAN26132-E, KNAN26180-E, KNAN26265-E, KNAN26292-E, KNAN26295-E, KNAN26298-E, KNAN26325-E

- The corrective actions to be taken for the following messages have been changed:

  KAVB0422-E, KAVB0423-E, KAVB1586-W, KAVB1587-E, KNAN11122-E, KNAN11123-E, KNAN11144-W, KNAN20000-E, KNAN20105-E, KNAN20230-Q, KNAN21400-W, KNAN21402-E, KNAN21403-E, KNAN22012-E, KNAN22058-E, KNAN22201-E, KNAN22205-E, KNAN22249-E, KNAN22253-E, KNAN22265-E, KNAN22403-E, KNAN22406-E, KNAN22407-E, KNAN22422-E, KNAN22424-E, KNAN22426-E, KNAN22466-E, KNAN22468-E, KNAN22500-E, KNAN22526-W, KNAN22701-E, KNAN22702-E, KNAN22806-E, KNAN22823-E, KNAN22824-E, KNAN24005-E, KNAN26002-E, KNAN26027-I, KNAN26039-E, KNAN26057-E, KNAN26063-E, KNAN26081-E, KNAN26095-E, KNAN26097-E, KNAN26099-E, KNAN26119-E, KNAN26163-E, KNAN26187-E, KNAN26208-E, KNAN26209-E, KNAN26296-E, KNAN26328-E, KNAN29041-E, KNAN11141-E

- The following messages have been changed:

  KAVB0682-I, KAVB0683-E, KNAN20040-E to KNAN20042-E, KNAN20222-Q, KNAN20226-Q, KNAN20227-Q, KNAN20230-Q, KNAN20326-Q, KNAN20354-Q, KNAN20362-Q, KNAN20437-Q, KNAN20438-Q, KNAN20440-Q, KNAN22012-E, KNAN22015-E, KNAN22200-I to KNAN22206-E, KNAN22208-E, KNAN22209-I, KNAN22249-E, KNAN22263-E, KNAN22271-I, KNAN22272-I, KNAN22407-E, KNAN22500-E, KNAN22823-E, KNAN22824-E, KNAN24005-E, KNAN26097-E, KNAN26099-E, KNAN26187-E, KNAN26196-E, KNAN26281-I, KNAN26328-E, KNAN29922-E

- The explanations of the following messages have been changed:

  KAVB0246-E, KAVB1513-W, KNAN20048-W, KNAN20222-Q, KNAN20230-Q, KNAN20238-Q, KNAN20303-E, KNAN20354-Q, KNAN20362-Q, KNAN20364-I, KNAN20365-I, KNAN21300-E to KNAN21310-E, KNAN22033-E, KNAN22200-I to KNAN22206-E, KNAN22208-E, KNAN22209-I, KNAN22263-E, KNAN22266-E, KNAN22267-E, KNAN22270-E to KNAN22272-I, KNAN22406-E, KNAN22407-E, KNAN22498-E, KNAN22500-E, KNAN22701-E, KNAN22861-W, KNAN24005-E, KNAN26000-I, KNAN26027-I, KNAN26039-E, KNAN26050-I, KNAN26063-E, KNAN26092-E, KNAN26093-I, KNAN26095-E, KNAN26098-E, KNAN26100-E, KNAN26103-I to KNAN26105-W, KNAN26108-I to KNAN26110-W, KNAN26119-E, KNAN26138-E, KNAN26187-E, KNAN26211-E, KNAN26212-E, KNAN26214-I, KNAN26216-I, KNAN26217-I, KNAN26226-I, KNAN26230-I, KNAN26249-I, KNAN26251-I, KNAN26252-I, KNAN26256-I, KNAN26261-I, KNAN26269-I, KNAN26271-I, KNAN26274-I, KNAN26276-I, KNAN26278-I, KNAN26279-I, KNAN26281-I, KNAN26283-I, KNAN26285-I, KNAN26287-I, KNAN26293-E, KNAN26294-E, KNAN26322-E, KNAN26323-E, KNAN26326-I to KNAN26330-E

- The operations of the system for the following messages have been changed:

  KNAN20048-W, KNAN20303-E, KNAN20330-E, KNAN20530-W, KNAN21307-E, KNAN21310-E, KNAN22266-E, KNAN22267-E, KNAN22270-E to KNAN22272-I, KNAN22506-W, KNAN22514-W, KNAN22515-W, KNAN22517-W, KNAN22528-W, KNAN22861-W, KNAN26000-I, KNAN26039-E, KNAN26081-E, KNAN26095-E, KNAN26163-E, KNAN26208-E, KNAN26294-E

- The following message IDs have been changed:

  KNAN20303-Q to KNAN20303-E

  KNAN21308-E to KNAN21308-Q

  KNAN22518-W to KNAN22518-E

  KNAN26025-W to KNAN26025-E

  KNAN26098-W to KNAN26098-E

L.9 Changes in version 09-10

- Windows 7 has been added to the OSs supported by JP1/Integrated Management - View.
- A list of JP1/IM - Manager services has been added.
- A description about the flow of processing after JP1 events are acquired has been added.
- The description of severe event filters is now separately described in the display of severe event filtering and in the judgement of severe event filtering.
- The description for when the host type cannot be changed has been changed.
- Descriptions and notes about actions when **Rebuild Profile Tree** is executed have been added.
- Operating permissions and notes for cluster operations have been added.
- Notes when a host name is specified in the Register Host window have been added.

- The following note has been added to the notes for variables: if JP1 event information contains characters that can be regarded as a command, those characters must be converted by the configuration file for converting information.
- The following description has been added: the log-file trap action definition files and log-file trap startup definition files that can be collected depends on the JP1/Base version.
- Profiles can now be added and deleted in the IM configuration management viewer.
- Log file traps can now be started and stopped in the IM configuration management viewer.
- Actions to be taken when the menu items are unavailable in the IM configuration management viewer have been changed.
- A list of configuration files that can be edited in IM Configuration Management has been added.
- The cross-references for the following procedures have been changed from the *Job Management Partner 1/ Integrated Management - Manager Overview and System Design Guide* to the *Job Management Partner 1/Integrated Management - Manager Configuration Guide*:
    - Apply the configuration files to each host
    - Batch-apply the configuration files to all hosts
- The files and the range of information that can be exported and imported have been changed.
- Among the virtualization software and virtualization environment management software to be collected, JP1/SC/CM and vCenter are now supported in a UNIX environment. Therefore, *Windows only* has been deleted from the descriptions.
- A description that the `pdprcd` process is started regardless of whether the automated startup script settings are enabled has been added.
- A description about the `pdprcd` process has been added.
- The maximum length of an action definition parameter in automatic action definitions has been changed.
- The maximum sizes of the automatic action definition file and the severity changing definition file have been added to *Limits*.
- Restrictions when JP1/IM - Manager 09-10 or JP1/IM - View 09-10 is connected to previous versions of products have been added.
- The log-file trap startup definition file has been added to the following items:
    - Definition information of the event service to be collected and distributed
    - Configuration files that can be saved and applied
    - Files that can be specified in the Display/Edit Profiles window
- The log-file trap action definition file and the log-file trap startup definition file have been added to the following items:
    - Files to be exported and imported
    - Output destination of the definition information exported by the `jcfexport` command
- The following description has been added: JP1/Base must be upgraded to use the log file trapping function.
- A description when log file traps are set for cluster has been added.
- Procedures for applying edited information in the configuration files by restarting the log file trap and by sending files have been added. Then the configuration has been changed accordingly.
- Procedures for setting and deleting JP1/IM - Manager (IM database) have been changed.
- The settings file for the consolidated display of repeated events and the file that defines which items are displayed for event conditions have been added to the files to be backed up.

- A procedure for backing up and recovering the IM database has been changed.
- A description about migration of management information of JP1/IM - Manager (IM Configuration Management) has been added.
- The causes of a host information collection failure in IM Configuration Management have been added.
- The Add Profile window has been added.
- A description of **Specified display event period** has been added to the **Severe Events** page.
- The following menu items have been added to the Display/Edit Profiles window:
    - **Add Profile**
    - **Delete Profile**
    - **Apply by Restarting**
    - **Apply by Sending File**
    - **Start Process**
    - **Stop Process**
- Descriptions of the items displayed in the **Configuration File** page when log file trap information is selected have been added.
- Descriptions of items for individual configuration files that can be operated on in the Display/Edit Profiles window have been changed.
- The `SpmSetSvcCon` command has been added so that dependencies between the JP1/IM - Manager service and the JP1/Base Event service can be set.
- Among the types of virtualization software and virtualization environment management software to be collected, JP1/SC/CM, vCenter, and Hitachi Compute Blade logical partitioning feature are now supported in a UNIX environment. Therefore, *Windows only* has been deleted from the descriptions.
- The commands below are now supported in a UNIX environment. Therefore, descriptions about UNIX have been added, and *Windows only* has been deleted from the descriptions.
    - `jcfcolvmvc` command
    - `jcfcolvmvirtage` command
    - `jcfvirtualchstat` command
- The description for the `jcacancel` command has been changed.
- The `-dbntcpos` option has been deleted from the list of options that can be immediately applied by the `-i` option of the `jcoimdef` command.
- The event occurrence of the `-dbntc` and `-dbntcpos` options has been changed in the table that shows when definitions of the `jcoimdef` command are enabled.
- Notes when the following commands are used in a UNIX environment have been added:
    - `jcfdbsetup` command
    - `jcodbsetup` command
- Notes when the commands below are used in a Windows environment and UNIX environment have been added. Also, notes regarding the service status have been added.
    - `jcfdbunsetup` command
    - `jcodbunsetup` command
- Example definitions have been added.

    - Automated action definition file (`actdef.conf`)
    - Automated action definition file (`actdef.conf`) (for compatibility)
    - Configuration file for converting information (`event_info_replace.conf`)
- `DESC_VERSION` of the system profile (`.system`) has been changed.
- Descriptions have been added indicating that the `NNMI_FAMILY_UK` extended attribute is set in JP1 events whose NNMi incidents have been converted.
- Descriptions have been added indicating that the following messages are for dummy events:
  KAVB0246-E, KAVB0248-E, KAVB0251-E, KAVB1513-W, KAVB1516-W, KAVB1527-E
- The output destinations of the following messages have been changed:
  KAVB8108-E, KNAN20020-W, KNAN20021-W, KNAN20234-I, KNAN21171-E to KNAN21177-E, KNAN22031-E, KNAN22058-E, KNAN22068-E, KNAN22301-E, KNAN22302-E, KNAN22304-E to KNAN22306-E, KNAN22857-E, KNAN22858-E
- The following messages have been added:
  KNAN20302-Q, KNAN20352-Q to KNAN20360-E, KNAN20362-Q, KNAN20363-I, KNAN20416-Q, KNAN21180-E, KNAN21181-E, KNAN21183-E, KNAN21184-E, KNAN22069-E to KNAN22071-W, KNAN22264-E, KNAN22492-E, KNAN22500-E, KNAN22501-E, KNAN22503-E, KNAN22505-I to KNAN22507-W, KNAN22510-I, KNAN22511-I, KNAN22514-W, KNAN22515-W, KNAN22517-W, KNAN22518-W, KNAN22520-E, KNAN22521-I, KNAN22523-I, KNAN22524-E, KNAN22526-W to KNAN22528-W, KNAN22860-W
- The corrective actions to be taken for the following messages have been changed:
  KAVB3613-W, KAJV2321-E, KNAN21174-E, KNAN22058-E, KNAN22301-E, KNAN22304-E to KNAN22306-E, KNAN22403-E, KNAN22412-E, KNAN22422-E, KNAN22426-E, KNAN22466-E, KNAN22859-E
- The following message has been changed:
  KNAN20231-Q

L.10 Changes in version 09-01

- Virtualization management information can now be set in the IM configuration management viewer. Accordingly, the Register Host window has been changed.
- A description that the virtualization system configuration can be managed in IM Configuration Management has been added.
- The position of the severe event filter is now described separately in the display of severe events filtering and in the judgement of severe events filtering.
- The types of virtualization software and virtualization environment management software that can manage a virtualization system configuration in IM Configuration Management have been added. The following types of software have been added:
    - Virtualization environment management software that can be used for virtualization system management hosts:
      JP1/SC/CM, SCVMM, and vCenter
    - Virtualization software that can be used for VMM hosts:
      Hyper-V and Hitachi Compute Blade logical partitioning feature
- Virtualization configuration information has been added to the host information that can be exported from IM Configuration Management.
- The virtualization system configuration can now be collected from the IM configuration management viewer.

- Contents of managing the virtualization system configuration have been added to the considerations for managing the system hierarchy.
- Restrictions on IM Configuration Management when JP1/IM - View 09-01 is connected to JP1/IM - Manager 09-00 and when JP1/IM - View 09-00 is connected to JP1/IM - Manager 09-01 have been added.
- Notes when a host is registered in IM Configuration Management have been added.
- The following commands, which collect virtualization configuration management information, have been added:
    - For SCVMM: `jcfcolvmscvmm` command
    - For vCenter: `jcfcolvmvc` command
    - For Hitachi Compute Blade logical partitioning feature: `jcfcolvmvirtage` command
- A description of the prerequisites for managing virtualization configuration has been added.
- A description of how to register virtual hosts has been moved from the *Job Management Partner 1/Integrated Management - Manager Administration Guide* to the *Job Management Partner 1/Integrated Management - Manager Configuration Guide*.
- A procedure for searching virtual hosts has been added.
- A function for applying virtualization configuration information of the IM configuration management viewer to the monitoring tree of the Central Scope has been added. The following menus have been added to the IM Configuration Management window:

  Operation>**Virtualization Configuration**>**Apply to Central Scope Monitoring Tree**
- A description of the ports for `jp1imcf` required when JP1/IM - Manager (IM Configuration Management) is used for communication between the viewer and the manager, has been added.
- A procedure for re-creating the event database when JP1/Base version 09-00 or later is running on the manager, has been added.
- The procedure for changing back the date and time of the system on the manager host when the date and time of the system is changed while JP1/IM is running, has been changed.
- A description related to the IM database when the system time is made forwarded while JP1/IM is running has been added.
- The following functions in the *Job Management Partner 1/Integrated Management - Manager Administration Guide* are now cross-referenced to the *Job Management Partner 1/Integrated Management - Manager Configuration Guide*:
    - Manage hosts.
    - Manage the system hierarchy.
    - Manage profiles.
    - Register hosts on virtualization systems.
- The items below have been added to the output items that can be exported to the host input information file. Also, output examples have been added.
    - Virtual Manager Type
    - User name
    - Password
    - Domain name
    - Communication type
    - Virtualization management former host name

- A table of environment variables for the character codes that can be exported to the host input information file and the host collection information file has been added.
- The items below have been added to the output items that can be exported to the host collection information file. Also, output examples have been added.
  - Host name
  - Virtual Manager Type
  - Version
- Items of host information that are manually imported have been added. Also, the ranges of the values have been changed. The added item names are as follows:
  - IP address
  - Virtual Manager Type
  - User name
  - Password
  - Domain name
  - Communication type
  - Virtualization management former host name
- *Actions to take when virtualization system configuration cannot be obtained in IM Configuration Management* has been added to *Corrective actions*.
- The cause and corrective actions for KNAN20102-E have been changed in *Corrective actions*.
- The figure illustrating the transition of the IM Configuration Management windows has been changed.
- The **Virtualization Configuration** menu item has been added to the IM Configuration Management window.
- **Virtual Manager Type** has been added to the items displayed in **Lower Host Information** on the **Host List** page.
- **Virtualization Configuration information** has been added to the items displayed in **Basic Information** on the **Host List** page.
- **Virtual Manager Type**, **Version**, **User name**, **Communication type**, and **Domain name** have been added to the items displayed in **Detailed Information** on the **Host List** page.
- A description when **Physical host** is selected in the Register Host window has been changed.
- A description when **Virtual host** is selected in the Register Host window has been changed.
- A description when **Unknown** is selected in the Register Host window has been changed.
- The Virtual Manager Settings window has been added.
- A description when **Physical host** is selected in the Edit Host Properties window has been changed.
- A description when **Virtual host** is selected in the Edit Host Properties window has been changed.
- A description when **Unknown** is selected in the Edit Host Properties window has been changed.
- **Virtual Manager Type** has been added to the items displayed in the **Lower Host Information** in the IM Configuration Management window.
- The `jcfcolvmscvmm` command has been added so that virtualization configuration information is acquired from SCVMM and output to the virtualization configuration information file.
- The `jcfcolvmvc` command has been added so that virtualization configuration information is acquired form vCenter and output to the virtualization configuration information file.

- The jcfcolvmvirtage command has been added so that virtualization configuration information is acquired from Hitachi Compute Blade logical partitioning feature and output to the virtualization configuration information file.
- The jcfvirtualchstat command has been added so that the virtualization configuration of the specified host can be updated.
- Execution permissions for the jcoview_log.bat command have been changed.
- The format and output example of the virtualization configuration information file output by executing the jcfcolvmesx command has been changed.
- The -r option was added to the jcfmkcsdata command to specify whether the virtualization system configuration tree contained in the export file of the JP1/IM - Manager (Central Scope) specified in the argument is to be used.
- Notes about upgrading from IM Configuration Management version 09-00 or earlier have been added to the description for the jcfmkhostsdata command.
- A list of options that are enabled when the -i option is specified with the jcoimdef command has been added.
- The status when automatic action service starts, which is set by the -r option of the jcoimdef command, has been added.
- A table of event occurrences for which the definition of the jcoimdef command is enabled has been added.
- The following messages have been added:

  KAVB8106-E to KAVB8109-E, KNAN20231-Q, KNAN20232-Q, KNAN20233-Q, KNAN20234-I, KNAN20301-Q, KNAN22029-E, KNAN22030-E, KNAN22050-I to KNAN22058-E, KNAN22060-E to KNAN22068-E, KNAN22300-I to KNAN22306-E, KNAN22854-E, KNAN22857-E to KNAN22859-E, KNAN24018-E, KNAN24040-I to KNAN24042-I, KNAN24060-W to KNAN24063-W, KNAN29085-W, KNAN29086-W, KNAN29900-I to KNAN29907-E, KNAN29909-E to KNAN29914-E, KNAN29920-I to KNAN29924-E, KNAN29926-I, KNAN29927-I
- The following messages have been deleted:

  KNAN20334-E, KNAN20804-E, KNAN20805-E, KNAN21054-E, KNAN22434-E
- The corrective actions to be taken for the following messages have been changed:

  KAVB1661-E, KAVB1664-E, KAVB5301-W, KNAN21170-W, KNAN22220-E, KNAN22403-E, KNAN22422-E, KNAN22426-E, KNAN22466-E
- The following messages have been changed:

  KNAN20006-E, KNAN20044-E, KNAN20051-E, KNAN20101-E, KNAN20102-E, KNAN20404-Q, KNAN21055-E, KNAN21165-E, KNAN21168-E, KNAN21170-W, KNAN21171-E, KNAN21175-E, KNAN21177-E, KNAN21179-E, KNAN22011-E, KNAN22022-E, KNAN22031-E, KNAN22103-E, KNAN22243-E, KNAN22245-E, KNAN22250-E, KNAN22412-E, KNAN22468-E, KNAN24005-E, KNAN24006-E, KNAN24012-E

L.11 Changes in version 09-00

- Event levels of events received from JP1/Base can now be changed according to predefined conditions, and the events can be managed by JP1/IM - Manager under the new event level (function for changing the severity level of JP1 events).
- A dedicated database for JP1/IM - Manager (the *IM database*) can now be created.
- A maximum of 1,500,000 events can now be managed (when using the IM database).
- Memo entries can now be added to events (when using the IM database) (addition of memo entries).

- An event can be issued when a correlation event fails to establish a correlation (event generation).
- Action definitions can now be set from a GUI (Action Parameter Detailed Definitions window) (simplified automatic action function).
- By specifying a date and time or by moving the slider, users can limit the range of events displayed in the event list (addition of event display start-time specification area).
- Managed hosts can now be registered, deleted, and viewed in list form from IM Configuration Management - View, allowing centralized management of information related to registered hosts (host management).
- The system hierarchy can be centrally managed from IM Configuration Management - View (system hierarchy management).
- IM Configuration Management - View can be used to centrally manage the profiles in JP1/Base on the hosts (profile management).
- Activity information about the JP1/Base services running on each host can be checked from IM Configuration Management - View (management of service activity information).
- Commands are now available for exporting and importing management information associated with IM Configuration Management (import and export of IM Configuration Management information).
- System hierarchies that incorporate virtual hosts can now be managed in IM Configuration Management - View. Also, information about a system hierarchy that has virtual hosts can be imported and used in the Central Scope (virtualization configuration management).
- Troubleshooting data can be collected by the data collection tool.
- Actions can now be performed locally by JP1/Base on a stand-alone basis.
- JP1/IM can be linked with JP1/AJS3.
- NNMi incidents generated by HP NNMi can now be converted into JP1 events by JP1/IM - EG for NNMi and be monitored by JP1/IM.
- Messages can now be displayed in a unified format by the linkage with JP1/IM - MO.
- Messages have been added, deleted, and changed.
- JP1 events have been added.

  Event IDs: `3F15`, `3F16`
- The JP1/IM - Manager manuals have been reorganized.

M. Reference Material for this Manual

M.1 Related publications

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

Integrated management-related

- *JP1 Version 11 JP1/Base User's Guide* (3021-3-A01(E))
- *JP1 Version 11 JP1/Base Messages* (3021-3-A02(E))
- *JP1 Version 11 JP1/Base Function Reference* (3021-3-A03(E))
- *JP1 Version 11 Integrated Management: Getting Started (Integrated Console)* (3021-3-A06(E))
- *JP1 Version 11 JP1/Integrated Management - Manager Overview and System Design Guide* (3021-3-A07(E))
- *JP1 Version 11 JP1/Integrated Management - Manager Configuration Guide* (3021-3-A08(E))
- *JP1 Version 11 JP1/Integrated Management - Manager Administration Guide* (3021-3-A09(E))
- *JP1 Version 11 JP1/Integrated Management - Manager GUI Reference* (3021-3-A10(E))
- *JP1 Version 11 JP1/Integrated Management - Manager Command and Definition File Reference* (3021-3-A11(E))
- *JP1 Version 11 JP1/Integrated Management - Manager Messages* (3021-3-A12(E))
- *Job Management Partner 1/Integrated Management - Event Gateway for Network Node Manager i Description, User's Guide and Reference* (3020-3-R82(E))
- *Job Management Partner 1/Integrated Management - Rule Operation System Configuration and User's Guide* (3020-3-K10(E))
- *Job Management Partner 1/Integrated Management - Rule Operation GUI Reference* (3020-3-K11(E))

JP1-related

- *JP1 Version 11 JP1/Service Support Configuration and Administration Guide* (3021-3-A22(E))
- *JP1 Version 11 JP1/Service Support Operator's Guide* (3021-3-A23(E))
- *JP1 Version 11 JP1/Performance Management Planning and Configuration Guide* (3021-3-A37(E))
- *JP1 Version 11 JP1/Performance Management User's Guide* (3021-3-A38(E))
- *JP1 Version 11 JP1/Automatic Operation Overview and System Design Guide* (3021-3-A87(E))
- *JP1 Version 11 JP1/Automatic Operation Administration Guide* (3021-3-A89(E))
- *JP1 Version 11 JP1/Automatic Operation Command and API Reference* (3021-3-A91(E))
- *JP1 Version 11 JP1/Automatic Operation Service Template Reference* (3021-3-A92(E))
- *JP1 Version 11 JP1/Automatic Job Management System 3 Linkage Guide* (3021-3-B20(E))
- *JP1 Version 11 JP1/Automatic Job Management System 3 Messages* (3021-3-B21(E))
- *JP1 Version 11 JP1/Advanced Shell Description, User's Guide, Reference, and Operator's Guide* (3021-3-B32(E))
- *Job Management Partner 1/Software Distribution Setup Guide* (3020-3-S80(E)), for Windows$^{(R)}$ systems
- *Job Management Partner 1/Software Distribution Administrator's Guide Volume 1* (3020-3-S81(E)), for Windows$^{(R)}$ systems

- *Job Management Partner 1/Software Distribution Administrator's Guide Volume 2* (3020-3-S82(E)), for Windows(R) systems
- *Job Management Partner 1/Software Distribution Client Description and User's Guide* (3020-3-S85(E)), for UNIX(R) systems
- Job Management Partner 1/Performance Management - Analysis Description, Operator's Guide and Reference (3020-3-K77(E))

Navigation Platform-related

- *Hitachi Navigation Platform Setup and Operations Guide* (3021-3-023(E))

Cosminexus-related

- *uCosminexus Application Server System Setup and Operation Guide* (3020-3-Y02(E))

HiRDB-related

- *HiRDB Version 9 Installation and Design Guide* (3000-6-452(E)), for UNIX(R) systems
- *HiRDB Version 9 Installation and Design Guide* (3020-6-452(E)), for Windows(R) systems
- *HiRDB Version 9 System Definition* (3000-6-453(E)), for UNIX(R) systems
- *HiRDB Version 9 System Definition* (3020-6-453), for Windows(R) systems

M.2 Conventions: Abbreviations

This manual uses the following abbreviations for the names of Hitachi products and other products:

Abbreviation		Full name or meaning
AIX#1		AIX(R) 6.1
		AIX(R) 7.1
BJEX		uCosminexus Batch Job Execution Server
Cosminexus	Cosminexus Application Server	Cosminexus Application Server Enterprise Version 6
		uCosminexus Application Server Standard Version 6
		uCosminexus Application Server Enterprise
		uCosminexus Application Server Standard
		uCosminexus Service Platform
HCSM		Hitachi Compute Systems Manager
HNTRLib		Hitachi Network Objectplaza Trace Library
HNTRLib2		Hitachi Network Objectplaza Trace Library 2
HP-UX	HP-UX (IPF)	HP-UX 11i V3 (IPF)
JP1/AJS	JP1/AJS2 - Advanced Manager	JP1/Automatic Job Management System 2 - Advanced Manager
	JP1/AJS - Agent	JP1/Automatic Job Management System 2 - Agent
		JP1/Automatic Job Management System 3 - Agent
	JP1/AJS - Manager	JP1/Automatic Job Management System 2 - Manager
		JP1/Automatic Job Management System 3 - Manager

Abbreviation			Full name or meaning
	JP1/AJS - View	JP1/AJS2 - View	JP1/Automatic Job Management System 2 - View
		JP1/AJS3 - View	JP1/Automatic Job Management System 3 - View
	JP1/AJS - Web Console		JP1/Automatic Job Management System 3 - Web Console
JP1/AJS2 - Scenario Operation View			JP1/Automatic Job Management System 2 - Scenario Operation View
JP1/AJS2 - View for Mainframe			JP1/Automatic Job Management System 2 - View for Mainframe
JP1/AO			JP1/Automatic Operation
JP1/AS			JP1/Advanced Shell
JP1/Audit			JP1/Audit Management - Manager[#2]
JP1/ESA			JP1/Cm2/Extensible SNMP Agent
			JP1/Extensible SNMP Agent
JP1/FTP			JP1/File Transmission Server/FTP[#2]
JP1/Integrated Management or JP1/IM	JP1/IM - Central Console or JP1/IM - CC		JP1/Integrated Manager - Central Console
	JP1/IM - Central Scope or JP1/IM - CS		JP1/Integrated Manager - Central Scope
	JP1/IM - Event Gateway for Network Node Manager i or JP1/IM - EG for NNMi		JP1/Integrated Management - Event Gateway for Network Node Manager i[#3]
	JP1/IM - Manager		JP1/Integrated Management - Manager
	JP1/IM - Message Optimizer Assistant or JP1/IM - MO		JP1/Integrated Management - Message Optimizer[#2, #3]
			JP1/Integrated Management - Message Optimizer Assistant[#2, #3]
	JP1/IM - Rule Operation or JP1/IM - RL		JP1/Integrated Management - Rule Operation[#3]
	JP1/IM - View		JP1/Integrated Management - View
JP1/IM - Central Information Master			JP1/Integrated Manager - Central Information Master
JP1/IM - Console			JP1/Integrated Manager - Console View
			JP1/Integrated Manager - Central Console
			JP1/Integrated Manager - Satellite Console
			JP1/Integrated Manager - SDK for Console
JP1/Navigation Platform or JP1/NP	JP1/IM - Navigation Platform or JP1/IM - NP		JP1/Integrated Management - Navigation Platform[#3]
	JP1/Navigation Platform or JP1/NP		JP1/Navigation Platform[#3]
JP1/NetInsight II - Facility Manager			JP1/NetInsight(R) II - Facility Manager[#2]
			JP1/NetInsight(R) II - Facility Manager Standard[#2]
			JP1/NetInsight(R) II - Facility Manager Upgrade License[#2]
JP1/NPS			JP1/Network Printing System
JP1/PAM	JP1/PA - Adaptor		JP1/Performance Analysis - Adaptor

Abbreviation		Full name or meaning
		JP1/Performance Management - Analysis Adaptor
	JP1/PA - Manager	JP1/Performance Analysis - Manager
		JP1/Performance Management - Analysis Manager
	JP1/PA - View	JP1/Performance Analysis - View
		JP1/Performance Management - Analysis View
JP1/PFM	JP1/PFM - Agent	JP1/Performance Management - Agent for Platform, and other agent product names
	JP1/PFM - Manager	JP1/Performance Management - Manager
	JP1/PFM - View	JP1/Performance Management - View
	JP1/PFM - Web Console	JP1/Performance Management - Web Console
JP1/PFM/SSO - Agent for Process		JP1/Performance Management/SNMP System Observer - Agent for Process
JP1/PFM/SSO for Application Server		JP1/Performance Management/SNMP System Observer for Application Server
JP1/SC/CM		JP1/ServerConductor/Control Manager#2
JP1/ServerConductor	JP1/ServerConductor	JP1/ServerConductor/Advanced Agent#2
		JP1/ServerConductor/Agent#2
		JP1/ServerConductor/Blade Server Manager#2
		JP1/ServerConductor/Blade Server Manager Plus#2
		JP1/ServerConductor/Server Manager#2
	ServerConductor	ServerConductor/Advanced Agent
		ServerConductor/Agent
		ServerConductor/Blade Server Manager
		ServerConductor/Server Manager
	System Manager	System Manager - Advanced Agent
		System Manager - Management Console
		System Manager - Server Agent
		System Manager - Server Agent for HP-UX
JP1/Service Support	JP1/IM - Service Support	JP1/Integrated Management - Service Support#3
	JP1/Service Support	JP1/Service Support#3
JP1/SES		JP1/System Event Service
JP1/SSO	JP1/PFM/SSO	JP1/Performance Management/Distributed SNMP System Observer#2
		JP1/Performance Management/SNMP System Observer#2
	JP1/SSO	JP1/Distributed Server System Observer
		JP1/Server System Observer

Abbreviation		Full name or meaning
JP1/TELstaff	JP1/IM - TELstaff	JP1/Integrated Manager - TELstaff[#2, #3]
		JP1/Integrated Manager - TELstaff Alarm View[#2, #3]
Linux[#1]	CentOS 6 (x64)	CentOS 6 (x64)
	CentOS 7	CentOS 7
	Linux 6 (x64)	Red Hat Enterprise Linux(R) Server 6 (64-bit x86_64)
	Linux 7	Red Hat Enterprise Linux(R) Server 7
	Oracle Linux 6 (x64)	Oracle Linux(R) Operating System 6 (x64)
	Oracle Linux 7	Oracle Linux(R) Operating System 7
	SUSE Linux 12	SUSE Linux(R) Enterprise Server 12
NNM	HP NNM	HP Network Node Manager Software version 6 or earlier
		HP Network Node Manager Starter Edition Software version 7.5 or earlier
	JP1/Cm2/NNM	JP1/Cm2/Network Node Manager version 7 or earlier[#2]
		JP1/Cm2/Network Node Manager Starter Edition 250 version 8 or earlier[#2]
		Job Management Partner 1/Cm2/Network Node Manager Starter Edition Enterprise 8 or earlier[#2]
NNMi	HP NNMi	HP Network Node Manager i Software v8.10
	JP1/NNMi	JP1/Cm2/Network Node Manager i 09-00 or earlier
		JP1/Network Node Manager i 11-00 or later
SCIM	JP1/SCIM	JP1/Security Integrated Manager[#2]
Solaris		Solaris 10(SPARC)
		Solaris 11(SPARC)
vCenter		VMware vCenter Server
VMware		VMware(R) ESX 3.5

#1: *UNIX* is sometimes used generically, referring to Solaris, AIX, and Linux.

#2: These products run only in a Japanese environment.

#3: For these products, this manual provides only an overview of the functions related to JP1/IM - Manager and JP1/IM - View.

M.3 Acronyms

This manual also uses the following abbreviations:

Abbreviation	Full name or meaning
ASCII	American Standard Code for Information Interchange
CMT	Container-Managed Transaction
CN	Common Name

Abbreviation	Full name or meaning
CRLF	Carriage Return/Line Feed
CSV	Comma Separated Value
CUI	Character User Interface
DB	Database
DBMS	Database Management System
DNS	Domain Name System
FQDN	Fully Qualified Domain Name
GMT	Greenwich Mean Time
GUI	Graphical User Interface
HTML	Hyper Text Markup Language
HTTP	HyperText Transfer Protocol
IP	Internet Protocol
ISAM	Indexed Sequential Access Method
J2EE	Java^{TM}2 Platform Enterprise Edition
Java VM	Java^{TM} Virtual Machine
JDBC	Java^{TM} DataBase Connectivity
JIS	Japanese Industrial Standards
KVM	Kernel-based Virtual Machine
LAN	Local Area Network
NAT	Network Address Translator
NIC	Network Interface Card
NTP	Network Time Protocol
OTS	Object Transaction Service
POSIX	Portable Operating System Interface for UNIX
SAN	Subject Alternative Name
SFO	Session Fail Over
SNMP	Simple Network Management Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
SPMD	Single Program Multiple Data
TXT	Text
UAC	User Account Control
UCS	Universal Multiple-Octet Coded Character Set
UNC	Universal Naming Convention
URL	Uniform Resource Locator
UTC	Universal Time Coordinated

Abbreviation	Full name or meaning
UTF	UCS Transformation Format
VMM	Virtual Machine Monitor
WAN	Wide Area Network
WWW	World Wide Web

M.4 Conventions: KB, MB, GB and TB

This manual uses the following conventions:

- 1 KB (kilobyte) is 1,024 bytes.
- 1 MB (megabyte) is $1{,}024^2$ bytes.
- 1 GB (gigabyte) is $1{,}024^3$ bytes.
- 1 TB (terabyte) is $1{,}024^4$ bytes.

N. Glossary

action-excluded event

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

additional common exclusion-conditions

Exclusion-conditions you can define by using monitored JP1 events while the system is running. You can exclude unnecessary JP1 events during monitoring. These conditions remain defined until the system is reconfigured. You can define these conditions in the Common Exclusion-Condition Settings (Extended) window.

additional repeated event conditions

New repeated event conditions you define during system operation when you want to suppress the monitoring of specific repeated events. Additional repeated event conditions enable you to suppress the monitoring of repeated events that occur while the system is running. You can define the additional conditions in the Repeated Event Condition Settings window.

agent

In JP1/IM, a host managed by a manager, or a program managed by a manager program.

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

Each agent runs JP1/Base, which provides the core functionality for the JP1/IM system.

agent configuration

A JP1/IM system configuration that consists of a manager on which JP1/Base is running and monitored agents.

auto-generation

A function that automatically generates a monitoring tree in the JP1/IM Central Scope.

By generating a tree automatically, and then customizing it to suit your mode of operation, you can easily set up an environment to perform system monitoring based on a monitoring tree.

A monitoring tree represents the system to be monitored by JP1/IM in tree format, with the nodes to be monitored arranged upon it. Every node in the tree needs to be defined, and the JP1/IM auto-generation function can produce this huge amount of definition information automatically. Using this function, you can automatically collect definition information from the hosts to be monitored by JP1/IM, and automatically create a monitoring tree. If the system is reconfigured, you can extract the differences between the new and existing monitoring trees as difference information.

automated actions

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

Using an automated action, you can, for example, execute a command to inform the system administrator of an important event that occurred while JP1/IM was monitoring the system. In an automated action definition, you can specify conditions for executing the action and the command to be executed as the action.

basic attribute

Information (an attribute) held by all JP1 events.

See also *JP1 event*.

basic information

Basic information held by the monitoring nodes that make up a monitoring tree in the JP1/IM Central Scope.

In the case of a monitoring group, the name that identifies the group is basic information.

For example, you can assign a group name such as *Daily accounting routines* or *Database server group* to jobs or servers grouped according to the monitoring objectives.

In the case of a monitoring object, the information for identifying the object is basic information.

For example, you can define a combination of information, such as a jobnet name together with a host name, for identifying the monitoring object within the system.

Basic information can be used, for example, when searching for monitoring nodes or in the conditions (individual conditions in a status change condition) for identifying the node concerned when a JP1 event occurs in the job or resource being monitored.

BJEX

A batch job execution system used for the batch processing of the data collected for a specific period of time.

business group

A unit of monitored hosts that are grouped by using JP1/IM - IM Configuration Management based on a certain purpose, such as units of systems used for individual businesses or the scope of monitoring targets for individual system administrators. For each business group, you can manage the scope of JP1 events that can be viewed in the Event Console window (Central Console) or the Monitoring Tree window (Central Scope), and the scope of monitoring settings that can be operated.

Central Console

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

In the Central Console, events occurring on the various hosts in the system are managed using JP1 events. The more important JP1 events, which need to be managed or dealt with in some way, are forwarded to a manager where they can be centrally managed. By monitoring these JP1 events in a viewer (the Event Console window), the user can monitor the whole system.

The Central Console also supports automated actions that execute a command automatically in response to specific JP1 events, and provides functionality for operating on the system from a viewer.

These features of the Central Console enable the user to efficiently perform the monitoring, error investigation, and troubleshooting tasks involved in system management.

Central Scope

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

In the Central Scope, the hosts, programs, jobs, and other system resources that need to be monitored are displayed in a tree view in a Monitoring Tree window. Because the relationships between the monitored objects are presented visually, the user has a clear picture of the likely impact of any problem in the system.

The Visual Monitoring window lets you display key resources and functions that you need to watch closely in a map view. You can arrange the monitoring points as icons on a map, organizational chart, or other background image. This allows the administrator to centrally monitor the system, no matter how large, from the required viewpoints.

certificate

Electronic information that validates the identity of the communication target when information is exchanged in an open corporate information system. Identify fraud by third parties is avoided by using encryption technology. Certificates are issued by certification authorities. JP1/IM - Manager supports the X509 PEM format.

Certificate Signing Request

A request for certificate signing for issuance of a server certificate. A CSR contains information about a public key and other information, such as organization name and location. The certification authority signs the submitted CSR and then issues it as a server certificate.

client application

A command executed on a client host (viewer) by using the client application execution function.

See also *client application execution function*.

client application execution function

A function that allows you to execute commands on a client host (viewer) in the Execute Command window.

cluster system

A system in which multiple servers work together as a single system.

A cluster system is designed to ensure uninterrupted job processing and to enhance availability by having another server continue processing if a failure occurs. The processing of another server taking over processing is known as *failover*.

If the active server (primary node) fails, the standby server (secondary node) takes over. Because the job processing is switched from the active to the standby node, a cluster system is also called a *node switching system*.

Cluster systems include load-sharing systems with multiple servers that perform parallel processing. In this manual, however, *cluster system* refers only to failover functionality for preventing interruption of job processing.

command execution log

A generic name for the database in which an execution log is recorded when a command is executed from JP1/IM - View or a command is executed in an automated action.

The logs for command execution from JP1/IM - View and for command execution in automated actions are managed separately. The file names generated in practice are as follows.

- Command execution logs for command execution from JP1/IM - View: `CMDISAMLOGV8.*`

- Command execution logs for command execution in automated actions: `ACTISAMLOGV8.*`

common condition

A status change condition that applies to all monitoring objects of the same type in the JP1/IM Central Scope.

See also *status change condition*.

common definition information

A database containing the definition parameters for the JP1 execution environment.

Common definition information is managed by JP1/Base and is used by JP1/Base, JP1/IM, JP1/AJS, and JP1/Power Monitor 06-02 or later. The database resides on a local disk of each server, and the definition parameters are sorted according to the physical host or logical host to which they apply.

When JP1 is used in a cluster system, the logical host settings in the common definition information residing on the primary and secondary servers must be identical. For this reason, after completing the setup and environment settings on the primary server, you must copy the defined parameters to the secondary server.

common exclusion-conditions

Conditions that form part of an event acquisition filter for selecting JP1 events monitored by JP1/IM, and that consist of a group of conditions to prevent JP1 events from being monitored or exclude them from automated-action execution.

configuration definition

Information defining the configuration of the system managed by JP1/IM.

A configuration definition defines the hierarchy of managers and agents in JP1/IM. Managers can be defined at different levels. For example, you can define lower-level base managers under a higher-level integrated manager.

Configuration definitions are managed by the JP1/IM configuration management functionality.

The information about the host relationships defined in a configuration definition can be used in JP1/IM to specify the hosts to which important JP1 events should be forwarded, for example, or to define the target host for executing a command in an automated action.

configuration management

Information that defines the system hierarchy managed by JP1/IM (IM configuration).

You can manage the system configuration by using IM Configuration Management, or by editing the definition files directly.

Configuration definition information is used to manage the hosts.

See also *IM Configuration Management* and *configuration definition*.

consolidated display of repeated events

A function that summarizes identical JP1 events received in succession by JP1/IM - View into a single JP1 event for display on the **Monitor Events** page or **Severe Events** page of the Event Console window. By using this function, you can prevent other important JP1 events from being overlooked.

consolidation completion event

An event for which consolidation has been completed.

consolidation event

An event into which JP1 events have been consolidated.

consolidation start event

Of JP1 events that have been consolidated, the first JP1 event that JP1/IM - View receives.

correlation event

A JP1 event issued by correlation processing. JP1/IM can issue a new JP1 event as a correlation event whenever a related JP1 event is issued. The correlation event and the association between the JP1 events can be defined by the user as a *correlation event generation definition*.

correlation event generation definition

A definition for issuing correlation events, specifying which types of JP1 events to associate, and the nature of the issued correlation event. A correlation event generation definition consists of a correlation event generation condition name, a filtering condition for the correlation target range, one or more event conditions, a timeout period, an event correlation type, a duplicate attribute value condition, a maximum correlation number, a correlation approval event, and a correlation failure event.

correlation source event

A JP1 event that triggers issue of a correlation event. Correlation source events can be listed in the Related Events (Correlation) window.

See also *correlation event*.

Cosminexus

A core product used to build application server-based systems for developing and running business applications that provide high performance and reliability.

cross root certificate

A certificate that enables a server certificate issued by an intermediate certificate authority to be verified from its root certificate authority.

CSR

-> See *Certificate Signing Request*.

delay monitoring

Monitoring of the execution time of an automated action, from start to completion. Delay monitoring is able to detect and notify the user of any automated action that fails to complete within a set time.

error color

A status color that appears when the monitoring node status is other than Initial.

-> See *status* and *status color*.

event acquisition filter

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

You can use an event acquisition filter to acquire events in JP1/SES format or to suppress acquisition of specific JP1 events.

event being consolidated

An event for which consolidation is still in progress.

event buffer

An area of memory used by JP1/IM - Manager (Central Console) to store JP1 events extracted from the event service of JP1/Base.

JP1 events are stored in the event buffer when:

- JP1/IM - Manage (Central Console) starts
- JP1 events are stored in the event database of JP1/Base

JP1/IM - View acquires events from the event buffer, not directly from the event service of JP1/Base.

Event Console window

A JP1/IM - View window that shows the JP1 events received by the Central Console in a time series. The Event Console window is the first window that appears when you log in to Central Console.

JP1/IM centrally manages the events generated on the various hosts by recording them as JP1 events and forwarding the more important ones to a JP1/IM manager. By viewing these JP1 events in the Event Console window, you can centrally monitor events occurring in the system.

event display start-time specification

When you use the integrated monitoring database, you can change the JP1 events listed in the Event Console window of JP1/IM - View by specifying a date and time or by moving the slider in the **event display start-time specification** area.

event generation condition

A condition that determines the type of status change in a monitoring node in the JP1/IM Central Scope that will cause the node to issue a JP1 event.

A monitoring node manages the status of the job or resource it is monitoring based on JP1 events issued by that job or resource. By defining an event generation condition, a JP1 event can be issued when a monitoring node changes status (that is, when a problem of some kind occurs in the job or resource being monitored), enabling early detection and swift response to any problems.

The JP1 event issued as a result of this condition has the event ID 00003FB0.

event guide function

A function that displays guide information in the JP1/IM Central Console for investigating and resolving JP1 events that occur during system monitoring.

By displaying troubleshooting procedures and other advice on handling JP1 events that could impact on the system, you can reduce the system administrator's workload when a problem occurs.

The event guide function displays guidance targeted to a specific JP1 event. The JP1/IM Central Scope provides a similar function, but targeted to a specific monitoring node.

See also *guide function*.

event ID

One of the attributes of a JP1 event. An event ID is an identifier indicating the program that issued the event and the nature of the JP1 event. It is a basic attribute and has the attribute name `B.ID`.

Event IDs are hexadecimal values, such as 7FFF8000.

Event IDs are uniquely assigned by each of the programs in the JP1 series. For details on the JP1 events issued by a specific program, see the documentation for the product concerned.

The values from 0 to 1FFF, and from 7FFF8000 to 7FFFFFFF, are available as user-specifiable event IDs.

A JP1 event is an 8-byte number consisting of a basic code (upper four bytes) and extended code (lower four bytes). Usually only the basic code is used, representing a 4-byte event ID. The extended code is `0`, except in special cases, as when set by the user in the API. When both the basic and extended codes need to be included, they are joined with a colon (:) and appear as `7FFF8000:0`, for example.

event inheritance function

A function that allows you to specify JP1 event information displayed in the Event Console window as a variable for the following items related to the contents of a command to be executed:

- The name of the host on which the command is to be executed
- The command to be executed
- Environment variable file

For example, when you execute a command for investigating or resolving a problem, you do not have to directly enter the values for the command arguments. You can use variables that specify JP1 event IDs and messages you want to investigate.

event level

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

The event level is common information in the extended attributes of a JP1 event, and the attribute name is `E.SEVERITY`.

Event levels are `Emergency`, `Alert`, `Critical`, `Error`, `Warning`, `Notice`, `Information`, and `Debug`.

event receiver filter

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

Use an event receiver filter when you want to restrict the JP1 events that can be viewed by a particular user who performs operational tasks.

event source host

The host where the event that caused the JP1 event occurred.

exclusion-condition

A filter condition that filters out JP1 events that match the condition. An exclusion-condition can be specified in an event acquisition filter, view filter, severe events filter, event receiver filter, or event search.

extended attribute

Information (an attribute) held by a JP1 event, optionally set by the source program when issuing a JP1 event.

See also *JP1 event*.

failover

Uninterrupted JP1 processing by transferring JP1 operations to another server when a failure occurs on the active server. Or, switching by the system administrator of the server that is currently executing JP1 processing.

Because the server on a secondary node takes over from the server on the primary node, failover is also known as *node switching*.

forwarding filter

A filter set on each JP1/IM host, specifying conditions for the JP1 events to be forwarded from that host and the destination manager to which they are sent.

These settings are registered with the JP1/Base event service, and are known as a *forwarding filter* in JP1/IM.

In JP1/IM, events occurring in the system are centrally managed as JP1 events. To enable centralized management, JP1 events are forwarded to JP1/IM managers. The particular types of JP1 events to be forwarded are defined in a forwarding filter.

general monitoring object

A monitoring object whose target can be set by the user. A system-monitoring object when edited becomes a general monitoring object.

The monitoring node type is *User Monitoring Object*.

See also *monitoring object*.

guide function

A function that displays error causes and action procedures in the JP1/IM Central Scope relating to problems occurring in the system.

By displaying troubleshooting procedures and other advice on handling problems arising during system monitoring, you can reduce the system administrator's workload at the initial response stage.

The guide function displays guidance targeted to a specific monitoring node. The JP1/IM Central Console provides a similar function, but targeted to a specific JP1 event.

See also *event guide function*.

HCSM

See *Hitachi Compute Systems Manager*.

health check function

A function that informs the user, by means of a JP1 event or notification command, when a hangup occurs in a JP1/IM or JP1/Base process.

The JP1/IM health check function can detect hangups in JP1/IM - Manager processes# and in the JP1/Base event service on managers. Detection is reported via a JP1 event or notification command.

The JP1/Base health check function can detect hangups in JP1/Base processes on the local host and on remote hosts. Detection is reported via a JP1 event.

By using the JP1/IM and JP1/Base health check functions in conjunction, you can quickly detect and respond to process errors in JP1/IM or in any instance of JP1/Base configured in the JP1/IM system.

#

The central scope service, IM Configuration Management service, and IM database service are not supported.

HiRDB

A database management system (DBMS) product for building a relational database scalable to business operations.

Hitachi Compute Blade logical partitioning feature

A product (made by Hitachi, Ltd.) that configures a virtualization environment.

Hitachi Compute Systems Manager

A Hitachi product for managing and operating IT system resources.

HP NNM

A generic name for a suite of integrated network management tools for managing the network configuration, performance, and failures.

IM Configuration

A system hierarchy managed by IM Configuration Management. There are two types of system hierarchy: agent configuration and remote monitoring configuration.

See also *agent configuration* and *remote monitoring configuration*.

IM Configuration Management

A function that centrally manages the system hierarchy managed by JP1/IM (IM configuration) and the settings of the hosts that compose the system, by using the configuration management function of JP1/IM - Manager from the IM configuration management viewer. By using IM Configuration Management, you can check JP1/Base service activity information and manage the status of the JP1/Base profiles on each host.

See also *configuration management*.

IM Configuration Management database

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

IM database

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

See also *IM Configuration Management database* and *integrated monitoring database*.

incident

A single occurrence of an event that can lower the quality of an IT service or impede normal system operation.

individual condition

A status change condition defined for a specific monitoring object in the JP1/IM Central Scope.

See also *status change condition*.

initial status

The status when the JP1/IM Central Scope has no information about the status of a monitoring node in the monitoring tree.

See also *status*.

integrated monitoring database

A database provided by JP1/IM - Manager for use with the Central Console functionality.

intermediate CA certificate

A certificate issued by an intermediate certification authority.

IPv4 host

A host for which only an IPv4 address has been set.

IPv4/IPv6 host

A host for which both an IPv4 address and an IPv6 address have been set.

IPv6 host

A host for which only an IPv6 address has been set.

JP1/AJS

A program for running jobs automatically.

Using JP1/AJS, you can execute processing in order according to a set schedule, or initiate processing when a specific event occurs.

JP1/AS

A product that creates and executes shell scripts for batch jobs. JP1/Advanced Shell can be split into JP1/Advanced Shell and JP1/Advanced Shell - Developer. JP1/Advanced Shell executes shell scripts for batch jobs. In a narrow sense, JP1/Advanced Shell is called an execution environment. JP1/Advanced Shell makes it possible for the same shell script for a job to be executed on both Windows and UNIX.

JP1/Audit

A program that manages evidential trace information for IT systems in a company, and supports evaluation and audit of internal controls.

JP1/Base

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

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

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

JP1/Cm2/SSO

A program that collects and manages server resources on a network and that monitors processes.

JP1 common definition information

See *common definition information*.

JP1 event

Information for managing events occurring in the system within the JP1 framework.

The information recorded in a JP1 event is categorized by attribute as follows:

- Basic attributes
  Held by all JP1 events.
  The basic attribute name for an event ID, for example, is written as `B.ID` (or simply `ID`).
- Extended attributes
  Attributes that are optionally set by the program that issued the JP1 event. An extended attribute consists of the following common information and program-specific information:
  - Common information (extended attribute information in a standard format for all JP1 events)
  - Program-specific information (other information in a format specific to the program issuing the event)
  The extended attribute name for an event level, for example, is written as `E.SEVERITY` (or simply `SEVERITY`).

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

jp1hosts information

Host information that associates JP1-specific host names with IP addresses.

This information can be used for customizing JP1 communication procedures in an environment with interconnected networks, for example. `jp1hosts` information is managed by JP1/Base and is used by programs such as JP1/Base, JP1/IM, and JP1/AJS.

`jp1hosts` information does not support communication using IPv6 addresses. To use IPv6 addresses for communication, you must set `jp1hosts2` information.

See also *jp1hosts2 information*.

When `jp1hosts` information has been defined, the settings take precedence in JP1 communication over the OS `hosts` file settings. This allows you to associate host names and IP addresses differently from the OS settings, specifically for JP1 communication.

jp1hosts2 information

Host information that associates JP1-specific host names with IP addresses.

This information can be used for customizing JP1 communication procedures in an environment with inter-connected networks, for example. `jp1hosts2` information is managed by JP1/Base and is used by programs such as JP1/Base, JP1/IM, and JP1/AJS.

To use IPv6 addresses for communication, you must set `jp1hosts2` information.

When `jp1hosts2` information has been defined, the settings take precedence in JP1 communication over the OS `hosts` file settings. This allows you to associate host names and IP addresses differently from the OS settings, specifically for JP1 communication.

JP1/IM - Manager

A program that enables integrated system management by providing centralized monitoring and operation across all system resources.

JP1/IM - Manager consists of three components: the *Central Console*, the *Central Scope*, and *IM Configuration Management*.

JP1/IM - Rule Operation

A program that supports rapid failure recovery by predefining recovery procedures or *rules* for the errors that might occur in the system, and executing them automatically.

JP1/IM - View

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

The same JP1/IM - View is used with both JP1/IM - Manager and JP1/IM - Rule Operation. It can be connected to either program as required, for monitoring and managing the system.

This manual does not cover the use of JP1/IM - View connected to JP1/IM - Rule Operation.

See also *viewer*.

JP1/Navigation Platform

A product that visualizes the flow of jobs and operating procedures. JP1/Navigation Platform brings together as a unit dispersed procedures and the technical knowledge and skills of many persons that can be shared in an organization to improve the accuracy and efficiency of work.

JP1/PFM/SSO

The name of JP1/Cm2/SSO version 7.

See also *JP1/Cm2/SSO*.

JP1/ServerConductor

Software that centrally manages servers and client PCs from a management console on the network. JP1/ServerConductor can manage hardware asset information and problems, and control turning on and off of servers and client PCs.

JP1/SES event

An event that was output by an obsolete JP1 product or by a product that does not support JP1 event output. JP1/SES events have basic attributes only (whereas JP1 events also have extended attributes).

JP1/Software Distribution

A generic name for a system that performs software distribution and client management as batch operations over a network.

JP1/SSO

The name of JP1/Cm2/SSO version 6.

See also *JP1/Cm2/SSO*.

KVM

A virtualization platform that is a standard part of Linux kernel 2.6.20 and later.

log file trap name

A name assigned to a monitored target in log file trapping, event log trapping, remote monitoring log file trapping, or remote monitoring event log trapping.

logical host

A logical server that provides the JP1 execution environment for running JP1 in a cluster system. If a failure occurs, a failover between logical hosts takes place.

Each logical host has a logical IP address and a shared disk, which are inherited at failover. A logical host consists of JP1 programs and other applications which run using the logical IP address and the shared disk.

At failover, the secondary node takes over the logical IP address and shared disk, and JP1 continues running. Thus, even if the physical server running JP1 is switched, other hosts can access the server using the same IP address and it appears that one host is operating continuously.

manager

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

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

The managers run JP1/Base, which provides the core functionality, and JP1/IM - Manager.

memo entry setting function

When you use the integrated monitoring database, this functionality allows users to set additional information about a JP1 event displayed in the Event Console window.

monitoring group

There are following two types in monitoring group:

- Monitoring group in the Central Scope

  Monitoring groups in the Central Scope is used to group monitoring objects. An icon that is displayed in the Event Tree window and indicates a group of monitoring objects is also called a monitoring group.

  Monitoring groups can be tailored to objectives. For example, you can define a job group or host group, depending on what you want to monitor.

  The status of a monitoring group changes according to the highest severity among the statuses passed from the lower-level monitoring objects and groups it contains, or according to the conditions defined in a status change condition.

- Monitoring group in IM Configuration Management

  Groups of hosts in a business group. Hosts in a business group set in IM Configuration Management can be further grouped to monitoring groups from the viewpoint of monitoring a business system. Monitoring groups can also be made in multiple tiers. These types of monitoring groups can also be applied to the Monitoring Tree window (Central Scope).

monitoring node

A generic name for any monitoring object or monitoring group that is part of a monitoring tree in the JP1/IM Central Scope.

See also *monitoring object* and *monitoring group*.

monitoring object

An object that you monitor using the JP1/IM Central Scope, or an icon in the Monitoring Tree window showing the status of an object being monitored.

When the Central Scope receives a JP1 event from an object being monitored, the event is judged using a *status change condition*, and the status of the monitoring object is displayed accordingly. (For example, a status change condition might set the status to `Emergency` on receipt of a JP1 event of `Emergency` level.) This allows you to manage the status of the various operations and resources being monitored in the system.

monitoring status

An attribute that determines whether to monitor the status of a monitoring node in the JP1/IM Central Scope.

There are two monitoring statuses: **Monitor** and **Do not monitor**.

When **Monitor** is set for a node, that node will react to any change in the status of whatever it is monitoring. In the case of a monitoring object, its status changes on receipt of a JP1 event that matches the monitoring conditions defined in a status change condition. In the case of a monitoring group, its status changes according to the highest severity among the statuses passed from its lower-level monitoring objects and groups (any status change in a monitoring node is always passed to the higher-level node), or according to the conditions defined in a status change condition. In JP1/IM - View, icons are color-coded to show the status of each monitoring node.

When **Do not monitor** is set for a node, its status does not change regardless of any JP1 event received from the job or host being monitored, or any status passed from a lower-level node. In JP1/IM - View, the icons of **Do not monitor** nodes are grayed out. You can set **Do not monitor** for a node when you need to maintain the resource it is monitoring, or when an automatically generated node does not need to be monitored.

monitoring tree

Functionality provided by the JP1/IM Central Scope for managing the objects being monitored in the system in form of a tree, drawn according to the viewpoints required by the system administrator. *Monitoring tree* might also be used to refer to the Monitoring Tree window in JP1/IM - View which provides this functionality.

See also *Central Scope*.

node switching system

See *cluster system*.

non-consolidation event

An empty consolidation event because no repeated events have occurred.

pass conditions

A set of conditions for JP1 events that you want to display (acquire). A pass condition can be specified in an event acquisition filter, view filter, severe events filter, event receiver filter, or event search.

physical host

A physical server configured in a cluster system in which JP1 operates. The term *physical host* is used in contrast with *logical host* (a logical server that can be failed over independently of the physical servers).

private key

A key (private key) used for data decryption and for creating electronic signatures to be used in public key encryption. It is also called a nonpublic key. A private key is managed securely by its owner.

When encrypted data is received, the recipient uses the recipient's own private key to decrypt the data. A sender can create an electronic signature by using the sender's own private key and then affixing the sender's electronic signature to the data to be sent.

remotely monitored host

A host that is set for remote communication and is to be monitored. You can manage JP1 events which are converted from events collected by remote monitoring, such as the messages in the log files generated on hosts on which JP1/Base has not been installed and such as Windows event logs.

remote monitoring

Connecting to a monitored host remotely and monitoring it. This functionality enables you to monitor remote hosts without having to install JP1/Base on the monitored hosts.

remote monitoring configuration

A configuration in which remotely connected hosts are monitored. You must set the hosts to be monitored for remote communication in advance.

repeated event conditions

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

repeated-event monitoring suppression

Functionality that prevents a large number of repeated events from being displayed in the event list of the Event Console window and that prevents the actions corresponding to repeated events from being executed. Suppression occurs when a large number of repeated events matching a specified condition occur.

repeated events

For the suppression of repeated-event monitoring:

Repeated events are JP1 events that match a condition specified by the user.

For the consolidated display of repeated events:

Repeated events are JP1 events that are received after a consolidation start event and that have the same content as the consolidation start event.

repeated start event

The repeated event the manager host received first among the repeated events subject to suppression.

-> See *repeated events*.

root certificate

A certificate issued by a root certification authority.

scroll buffer

An area of memory used by JP1/IM - View to store JP1 events extracted from the event buffer of JP1/IM - Manager.

A scroll buffer is kept for each of the **Monitor Events** page, **Severe Events** page, and **Search Events** page.

The JP1 events that JP1/IM - View displays on each page is determined by the contents of the scroll buffer for that page.

JP1 events are stored in the scroll buffer of the **Monitor Events** page, **Severe Events** page when:

- JP1/IM - View starts#
- The page is automatically refreshed#
- The user selects **Refresh** in a menu or the toolbar

#: If **Apply** is selected for **Automatic refresh** in the Preferences window.

At the above times, JP1/IM - View communicates with JP1/IM - Manager as long as unacquired events are present in the event buffer. The number of events acquired in one transmission is determined by the value set in **Num. of events to acquire at update** in the Preferences window.

JP1 events are stored in the scroll buffer of the **Search Events** page when a user runs an event search.

The number of events acquired in one search is determined by the value set in **Num. of events to acquire in 1 search** in the Preferences window. To display the events that could not be acquired in one search, click **Search for Next Event**.

server certificate

A digital certificate obtained from a certification authority that proves the identity of the user and that is used for encrypting SSL communication.

ServerConductor

See also *JP1/ServerConductor*.

severe events filter

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

A *severe event* is a particularly important JP1 event that needs to be addressed, such as a failure of some sort. JP1/IM provides a **Severe Events** page so that users can reliably detect and deal with every severe event. On this page, as well as listing up only severe events, you can also manage the response status of each one.

severity level changing function

A function that lets users freely change the event level of a JP1 event, so that JP1 events can be managed in accordance with the system's operating environment.

status

The status of a resource being managed by a monitoring node in the JP1/IM Central Scope.

A monitoring node can have any of the following statuses: `Emergency`, `Alert`, `Critical`, `Error`, `Warning`, `Normal`, `Debug`, or `Initial`. `Initial` status means that the Central Scope does not yet have any information about the status of the resource being monitored.

For example, if a failure occurs and the node issues a JP1 event of `Emergency` level, the Central Scope will manage the event according to the status of the monitoring node.

status change condition

A condition that determines when to change the status of a monitoring object or monitoring group in the JP1/IM Central Scope.

- Status change condition for a monitoring object

  Defines the types of JP1 events in the job or resource being monitored that will cause the monitoring object to change status. A status change condition for a monitoring object consists of one or more common conditions and individual conditions, and the resulting status when the status change condition is satisfied.

  A *common condition* is one that applies to all monitoring objects of the same type. For example, an event ID indicating that a job has ended abnormally is used for all monitoring objects that monitor jobs. A condition of this nature is defined as a common condition.

  An *individual condition* is one whose value is specific to the monitoring object concerned. For example, an individual condition might identify what is being monitored by a value such as the name of the job or the name of the host that executes the job. Conditions of this nature are defined as individual conditions. In the case of a system-monitoring object, the same attribute as specified in the basic information of the monitoring object is defined in the individual condition contained in a status change condition.

- Status change condition for a monitoring group

  Defines the status of a lower-level node that will cause the monitoring group to change status. A status change condition for a monitoring group consists of a child node status, a comparison condition, and the resulting status when the status change condition is satisfied.

Child node status refers to the status of a monitoring node at the next level below (immediately under) the monitoring group. When the child node status is set as `Alert`, for example, applicable statuses will include `Emergency`, which has higher priority than `Alert`.

The *comparison condition* calculates lower-level nodes whose status has changed to the defined child node status, by a percentage or a count. The former is calculated as the number of child nodes in the specified status, as a percentage (%) of the total number of child nodes in the monitoring group. The latter is the number of child nodes in the specified status.

status color

The background color of monitoring node or the font color of monitoring node name. Status colors are associated with the statuses (for example, Warning and Error) of monitoring node.

-> See *status*.

status monitoring

Monitoring for abnormal termination of an automated action. Status monitoring is able to detect and notify the user of any abnormally ended automated action whose status has changed to `Fail`, `Error`, or `Error (Miss).`

system information management

A structure for realizing integrated management of a system by centrally managing information about the system's myriad resources.

System Manager

See also *JP1/ServerConductor*.

system-monitoring object

A monitoring object provided by the JP1/IM Central Scope.

Each system-monitoring object contains predefined basic settings for monitoring a particular product in the JP1 series. The use of such objects facilitates environment setup.

See also *monitoring object*.

Tool Launcher window

A JP1/IM - View window for registering and launching applications of the user's choice.

By registering applications needed for job processing in the Tool Launcher window, you can integrate operations under JP1/IM - View in running your JP1/IM system.

The Tool Launcher window has preset links for launching the GUI of products in the JP1 series.

variable binding

A variable binding of an SNMP trap. When a SNMP trap is converted into a JP1 event in JP1/Base, the variable bindings are read into the program-specific information contained in the extended attributes of the JP1 event.

As basic information, an SNMP trap indicates the source program (enterprise name) and the trap type (generic or specific). In addition, when detailed trap-specific information needs to be included, variable bindings (also written as `VarBind`) are appended to the SNMP trap when it is issued.

A variable binding contains an object identifier (OID) and data. For example, when JP1/Cm2/SSO monitors an application, if an error is detected, an SNMP trap is issued with a variable binding to which the application name is added as detailed information.

For details on SNMP traps, see RFC1157 and other network-related documentation. For details on the information contained in the variable bindings, see the manual for the specific program that issues SNMP traps.

vCenter

See also *VMware vCenter Server*.

viewer

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

A viewer connects to the Central Console, Central Scope, IM Configuration Management, and Rule Management managers to perform system monitoring and management tasks.

view filter

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

Use a view filter when you want to temporarily restrict an event listing to specific JP1 events only.

virtualization environment management software

Software that can be used on a virtualization system management host running vCenter, JP1/SC/CM, SCVMM, or HCSM.

virtualization software

Software that can be used on a VMM host running Hyper-V, KVM, Hitachi Compute Blade logical partitioning feature, or VMware ESX.

virtual root node

Appears only when the monitoring range settings are enabled for the monitoring tree.

Unlike a monitoring object or monitoring group, the information in a virtual root node cannot be edited (in the Properties window). Neither can you change the node status or perform any other direct operations on the virtual root node. (Its status changes accordingly when the status of a monitoring node below it changes, but you cannot change the virtual root node status directly. To change its status, you must change the status of a lower-level monitoring node.)

Visual Icon

An icon displayed in the JP1/IM Central Scope which can be any size and based on any image. A visual icon is set as an attribute of a monitoring node. Because a visual icon can be any size, this feature offers the user a greater degree of freedom when creating monitoring windows. Visual Icon is displayed only in map view and in the Visual Monitoring window.

visual monitoring

Functionality provided by the JP1/IM Central Scope for displaying the objects in the system that need to be monitored particularly closely as icons arranged on a map, organizational chart, or other image. *Visual monitoring* might also be used to refer to the Visual Monitoring window in JP1/IM - View which provides the map view functionality.

See also *Central Scope*.

VMware vCenter Server

A product providing a platform that centrally manages a virtualization environment.

Web-based JP1/IM - View

A light version of JP1/IM - View, forming part of JP1/IM - Manager (Central Console). The program has a number of functional limitations, such as not being able to open the Tool Launcher window or Execute Command window. To use the Web-based JP1/IM - View, in addition to a Web browser, the Java Runtime Environment (JRE) and its accompanying plug-ins are required on the viewer. For details, see the *Release Notes* for JP1/IM - Manager. A Web server is required on the manager.

Web page

A generic name for the GUI provided by another product and viewed in a Web browser (refers to the Web-based JP1/IM - View in the JP1/IM context).

Index

Hitachi, Ltd.

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