HITACHI
Inspire the Next

Job Management Partner 1/Base User's Guide

3020-3-R71(E)

■ Relevant program products

For details about the supported operating systems and the service packs or patches that are required by JP1/Base, see the *Release Notes*.

P-242C-6L97 JP1/Base 09-00 (for Windows Server 2003, Windows Server 2003 (x64), Windows XP Professional)

P-2A2C-6L97 JP1/Base 09-00 (for Windows Vista, Windows Server 2008 Enterprise, Windows Server 2008 Standard)

P-1J2C-6L92 JP1/Base 09-00 (for HP-UX (IPF))

P-9D2C-6L92 JP1/Base 09-00 (for Solaris (SPARC))

P-1M2C-6L92 JP1/Base 09-00 (for AIX)

■ Trademarks

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

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

AMD, AMD Opteron, and combinations thereof, are trademarks of Advanced Micro Devices, Inc.

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

IBM is a trademark of International Business Machines Corporation in the United States, other countries, or both.

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

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

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

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

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

POSIX stands for Portable Operating System Interface for Computer Environment, which is a set of standard specifications published by the Institute of Electrical and Electronics Engineers, Inc.

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

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

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

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

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

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

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

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

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

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

XPG4 stands for X/Open Portability Guide Issue 4, which is a set of specifications published by X/Open Company Limited.

The following program products contain some parts whose copyrights are reserved by Sun Microsystems, Inc.: P-9D2C-6L92 and P-9E2C-6L92

The following program product contains some parts whose copyrights are reserved by UNIX System Laboratories, Inc.: P-9D2C-6L92 and P-9E2C-6L92

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

■ Restrictions

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

■ Edition history

Edition 1 (3020-3-R71(E)): November 2009

■ Copy right

Preface

This manual describes the functionality and operation of Job Management Partner 1/Base. Note that this is a common manual for each OS. If there are OS-specific differences in usage, the differences are specified in the text. In this manual, *Job Management Partner 1* is abbreviated to *JP1*.

Intended readers

This manual is intended for:

- System administrators who are responsible for introducing, building, and running a system that uses JP1 product that requires JP1/Base such as JP1/Integrated Management, JP1/Automatic Job Management System 2 or 3, or JP1/Power Monitor.
- System administrators who are responsible for introducing and running JP1/Base, such as JP1/Integrated Management, JP1/Automatic Job Management System 2 or 3, JP1/Power Monitor.

Organization of this manual

This manual is organized into the following parts:

PART 1: Overview

This part gives an overview and describes the functionality of JP1/Base.

PART 2: Installation and Setup

This part describes how to install and set up JP1/Base. This part also describes how to operate JP1/Base in a cluster system, or how to set up to operate JP1/Base in multiple networks.

PART 3: Installation and Operation

This part describes how to set up and operate JP1/Base functionality.

PART 4: Reference

This part describes the commands used in JP1/Base, JP1/Base definition files, and events output by JP1/Base.

PART 5: Troubleshooting

This part describes the cause and what to do if a problem occurs while you are using JP1/Base.

Related publications

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

- *Job Management Partner 1/Base Messages* (3020-3-R72(E))
- *Job Management Partner 1/Base Function Reference* (3020-3-R73(E))
- *Job Management Partner 1/Integrated Management - Manager Quick Reference* (3020-3-R75(E))
- *Job Management Partner 1/Integrated Management - Manager Overview and System Design Guide* (3020-3-R76(E))
- *Job Management Partner 1/Integrated Management - Manager Configuration Guide* (3020-3-R77(E))
- *Job Management Partner 1/Integrated Management - Manager Administration Guide* (3020-3-R78(E))
- *Job Management Partner 1/Integrated Management - Manager GUI Reference* (3020-3-R79(E))
- *Job Management Partner 1/Integrated Management - Manager Command and Definition file Reference* (3020-3-R80(E))
- *Job Management Partner 1/Integrated Management - Manager Messages* (3020-3-R81(E))
- *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))
- *Job Management Partner 1/Automatic Job Management System 3 Overview* (3020-3-S02(E))
- *Job Management Partner 1/Automatic Job Management System 3 System Design (Configuration) Guide* (3020-3-S03(E))
- *Job Management Partner 1/Automatic Job Management System 3 System Design (Work Tasks) Guide* (3020-3-S04(E))
- *Job Management Partner 1/Automatic Job Management System 3 Configuration Guide 1* (3020-3-S05(E))
- *Job Management Partner 1/Automatic Job Management System 3 Configuration Guide 2* (3020-3-S06(E))
- *Job Management Partner 1/Automatic Job Management System 3 Administration Guide* (3020-3-S07(E))

- *Job Management Partner 1/Automatic Job Management System 3 Troubleshooting* (3020-3-S08(E))
- *Job Management Partner 1/Automatic Job Management System 3 Operator's Guide* (3020-3-S09(E))
- *Job Management Partner 1/Automatic Job Management System 3 Command Reference 1* (3020-3-S10(E))
- *Job Management Partner 1/Automatic Job Management System 3 Command Reference 2* (3020-3-S11(E))
- *Job Management Partner 1/Automatic Job Management System 3 Linkage Guide* (3020-3-S12(E))
- *Job Management Partner 1/Automatic Job Management System 3 Messages 1* (3020-3-S13(E))
- *Job Management Partner 1/Automatic Job Management System 3 Messages 2* (3020-3-S14(E))
- *Job Management Partner 1/Software Distribution Description and Planning Guide* (3020-3-S79(E)), for Windows systems
- *Job Management Partner 1/Software Distribution Setup Guide* (3020-3-S80(E)), for Windows systems
- *Job Management Partner 1/Software Distribution Administrator's Guide Volume 1* (3020-3-S81(E)), for Windows systems
- *Job Management Partner 1/Software Distribution Administrator's Guide Volume 2* (3020-3-S82(E)), for Windows systems
- *Job Management Partner 1/Software Distribution Client Description and User's Guide* (3020-3-S85(E)), for UNIX systems
- *Job Management Partner 1/Automatic Job Management System 2 Description* (3020-3-K21(E))
- *Job Management Partner 1/Automatic Job Management System 2 Planning and Administration Guide* (3020-3-K22(E))
- *Job Management Partner 1/Automatic Job Management System 2 Setup Guide* (3020-3-K23(E))
- *Job Management Partner 1/Automatic Job Management System 2 Operator's Guide* (3020-3-K24(E))
- *Job Management Partner 1/Automatic Job Management System 2 Command Reference* (3020-3-K25(E))
- *Job Management Partner 1/Automatic Job Management System 2 Linkage Guide* (3020-3-K27(E))

- *Job Management Partner 1/Automatic Job Management System 2 Messages* (3020-3-K28(E))
- *Job Management Partner 1/Power Monitor Description, User's Guide and Reference* (3020-3-K54(E))
- *Job Management Partner 1/Software Distribution Manager Description and Administrator's Guide* (3000-3-841(E))
- *Job Management Partner 1/Software Distribution SubManager Description and Administrator's Guide* (3020-3-L42(E)), for UNIX systems
- *Job Management Partner 1/Performance Management/SNMP System Observer Description, Operator's Guide and Reference* (3020-3-F69(E))
- *VOS3 Job Management Partner 1/Open Job Entry* (6190-3-365(E))
- *MVS Job Management Partner 1/Open Job Entry Description, User's Guide and Reference* (9000-3-365(E))
- *OSIV/MSP Job Management Partner 1/Open Job Entry Description, User's Guide and Reference* (9000-3-366(E))

JP1/Base manual organization

The JP1/Base documentation is divided into three manuals. Read the manual appropriate to your goals, referring to the content of each manual shown in the following table.

Manual	Content
Job Management Partner 1/Base User's Guide	• Overview of JP1/Base functionality • Setup of each function • Commands, definition files, JP1 events • Troubleshooting • Processes, port numbers, operational logs
Job Management Partner 1/Base Messages	Messages
Job Management Partner 1/Base Function Reference	• Methods for issuing or acquiring JP1 events by using user applications or JP1 programs. • Functions

Conventions: Abbreviations

This manual uses the following abbreviations for product names:

Abbreviation		Full name or meaning
AIX	AIX 5L	AIX 5L V5.3
	AIX	AIX V6.1

Abbreviation		Full name or meaning
HNTRLib2		Hitachi Network Objectplaza Trace Library 2
HP-UX	HP-UX (IPF)	HP-UX 11i V2 (IPF)
		HP-UX 11i V3 (IPF)
JP1/AJS	JP1/AJS	Job Management Partner 1/Automatic Job Scheduler
	JP1/AJS - Agent	Job Management Partner 1/Automatic Job Management System 2 - Agent
		Job Management Partner 1/Automatic Job Management System 3 - Agent
	JP1/AJS - Manager	Job Management Partner 1/Automatic Job Management System 2 - Manager
		Job Management Partner 1/Automatic Job Management System 3 - Manager
	JP1/AJS - View	Job Management Partner 1/Automatic Job Management System 2 - View
		Job Management Partner 1/Automatic Job Management System 3 - View
JP1/AJS2 for Mainframe	JP1/AJS2 - Agent for Mainframe	Job Management Partner 1/Automatic Job Management System 2 - Agent for Mainframe
	JP1/AJS2 - Manager for Mainframe	Job Management Partner 1/Automatic Job Management System 2 - Manager for Mainframe
	JP1/AJS2 - View for Mainframe	Job Management Partner 1/Automatic Job Management System 2 - View for Mainframe
JP1/AJS - EE		Job Management Partner 1/Automatic Job Scheduler - Enterprise Edition
JP1/AOM		Job Management Partner 1/Automatic Operation Monitor
JP1/AOM - EE		Job Management Partner 1/Automatic Operation Monitor - Enterprise Edition
JP1/Base		Job Management Partner 1/Base
JP1/Cm2/OAA		Job Management Partner 1/Cm2/Operations Assist Agent
JP1/Cm2/OAM		Job Management Partner 1/Cm2/Operations Assist Manager

Abbreviation		Full name or meaning
JP1/Integrated Management or JP1/IM	*Products after version 8*	
	JP1/IM - Manager	Job Management Partner 1/Integrated Management - Manager
	JP1/IM - Rule Operation	Job Management Partner 1/Integrated Management - Rule Operation
	JP1/IM - View	Job Management Partner 1/Integrated Management - View
	Version 7 and earlier products	
	JP1/IM - Central Console	Job Management Partner 1/Integrated Manager - Central Console
	JP1/IM - Central Scope	Job Management Partner 1/Integrated Manager - Central Scope
	JP1/IM - View	Job Management Partner 1/Integrated Manager - View
JP1/OJE		Job Management Partner 1/Open Job Entry
JP1/PFM/SSO		Job Management Partner 1/Performance Management/SNMP System Observer
JP1/SES		Job Management Partner 1/System Event Service
JP1/Software Distribution		Job Management Partner 1/Software Distribution Client
		Job Management Partner 1/Software Distribution Manager
Microsoft Cluster Server		Microsoft(R) Cluster Server
Microsoft Internet Explorer		Microsoft(R) Internet Explorer(R)
NNM	HP NNM	HP Network Node Manager Starter Edition software version 7.5
Solaris	Solaris (SPARC)	Solaris 9/10 (SPARC)
Visual C++		Microsoft(R) Visual C++(R)
Windows NT		Microsoft(R) Windows NT(R) Server Network Operating System Version 4.0
		Microsoft(R) Windows NT(R) Server Enterprise Edition Version 4.0

Abbreviation		Full name or meaning
		Microsoft(R) Windows NT(R) Workstation Operating System Version 4.0
Windows Server 2003	Windows Server 2003	Microsoft(R) Windows Server(R) 2003, Enterprise Edition
		Microsoft(R) Windows Server(R) 2003, Standard Edition
	Windows Server 2003 (x64)	Microsoft(R) Windows Server(R) 2003, Datacenter x64 Edition
		Microsoft(R) Windows Server(R) 2003, Enterprise x64 Edition
		Microsoft(R) Windows Server(R) 2003, Standard x64 Edition
Windows Server 2008	Windows Server 2008 Enterprise	Microsoft(R) Windows Server(R) 2008 Enterprise
		Microsoft(R) Windows Server(R) 2008 Enterprise without Hyper-V
	Windows Server 2008 Standard	Microsoft(R) Windows Server(R) 2008 Standard
		Microsoft(R) Windows Server(R) 2008 Standard without Hyper-V
Windows Vista		Microsoft(R) Windows Vista(R) Business
		Microsoft(R) Windows Vista(R) Enterprise
		Microsoft(R) Windows Vista(R) Ultimate
Windows XP	Windows XP Professional	Microsoft(R) Windows(R) XP Professional Operating System

- *Windows* is sometimes used generically, referring to Windows Server 2003, Windows Server 2008, Windows Vista, and Windows XP Professional.
- *UNIX* is sometimes used generically, referring to AIX, HP-UX, and Solaris.
- Note that executing program products might display or output the abbreviations, such as in messages, rather than the full name of a program product.

This manual also uses the following abbreviations:

Abbreviation	Full name or meaning
AMD	Advanced Micro Devices

Abbreviation	Full name or meaning
API	Application Programming Interface
CSV	Comma Separated Value
DB	Database
DNS	Domain Name System
EUC	Extended Unix Code
FD	Floppy Disk
FQDN	Fully Qualified Domain Name
FTP	File Transfer Protocol
GUI	Graphical User Interface
HTML	Hyper Text Markup Language
IP	Internet Protocol
IPF	Itanium(R) Processor Family
ISAM	Indexed Sequential Access Method
JIS	Japanese Industrial Standards
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
NAT	Network Address Translator
NIC	Network Interface Card
NTP	Network Time Protocol
OS	Operating System
OU	Organization Unit
POSIX	Portable Operating System Interface for UNIX
RFC	Request For Comments
SNMP	Simple Network Management Protocol
SSL	Secure Socket Layer
TCP/IP	Transmission Control Protocol/Internet Protocol
UAC	User Account Control

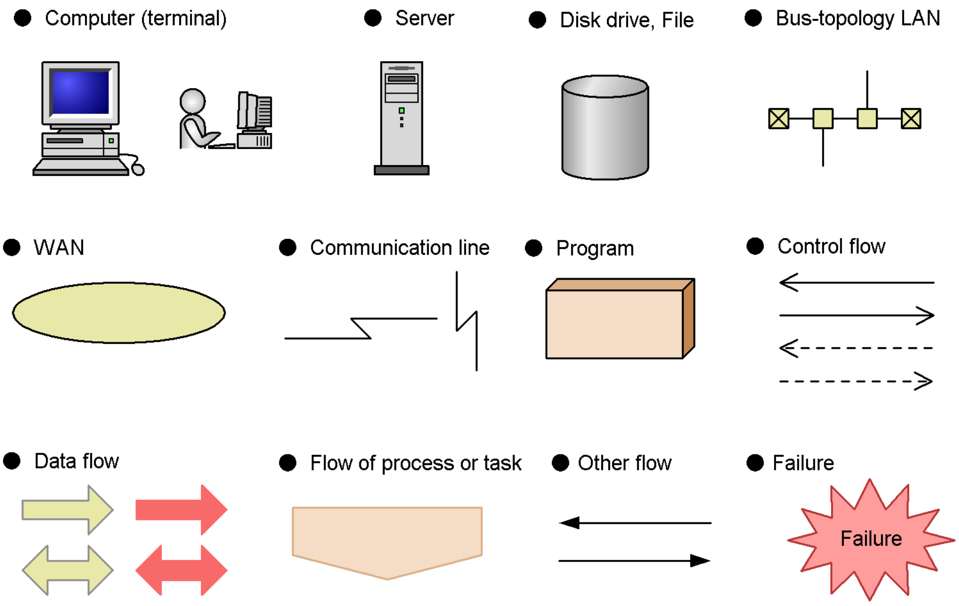
Abbreviation	Full name or meaning
UTC	Universal Time Coordinated
UTF	UCS Transformation Format
WWW	World Wide Web

Conventions: "Administrators permissions" as used in this manual

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

Conventions: Diagrams

This manual uses the following conventions in diagrams:



Conventions: Directory names

HP-UX directory names are used in this manual as a general rule. The directory names have symbolic links, so that users of UNIX OSs other than HP-UX can use the same directory names.

When HP-UX uses a different directory name from another flavor of UNIX, both directory names are given.

Conventions: Fonts and symbols

Font and symbol conventions are classified as:

- General font conventions
- Conventions in syntax explanations
- Conventions for mathematical expressions

These conventions are described below.

General font conventions

The following table lists the general font conventions:

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

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

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

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

Conventions in syntax explanations

Syntax definitions appear as follows:

Store**D**atabase [temp|perm] (*database-name* ...)

The following table lists the conventions used in syntax explanations:

Example font or symbol	Convention
`StoreDatabase`	Code-font characters must be entered exactly as shown.
database-name	This font style marks a placeholder that indicates where appropriate characters are to be entered in an actual command.
`SD`	Bold code-font characters indicate the abbreviation for a command.
`perm`	Underlined characters indicate the default value.
`[ ]`	Square brackets enclose an item or set of items whose specification is optional.
|	Only one of the options separated by a vertical bar can be specified at the same time.
`...`	An ellipsis (...) indicates that the item or items enclosed in ( ) or [ ] immediately preceding the ellipsis may be specified as many times as necessary.
`()`	Parentheses indicate the range of items to which the vertical bar (|) or ellipsis (...) is applicable.
{ }	One of the items enclosed in curly brackets must be specified.
△	This symbol is used to explicitly indicate a space. $\triangle_0$: Enter one or more spaces, or none (a space is optional). $\triangle_1$: Enter one or more spaces (a space is mandatory).

Conventions for mathematical expressions

This manual uses the following symbols in mathematical expressions:

Symbol	Meaning
x	Multiplication sign
/	Division sign
Σ	Total sign

Conventions: JP1/Base installation folder

This manual uses the following expressions for JP1/Base installation folder:

Product name	Installation folder	Default installation folder#
JP1/Base	*installation-folder*	*system-drive*`:\Program Files\HITACHI\JP1Base`

#: Shows the installation folder when each product is installed as default.

For Windows Server 2008 and Windows Vista, the manual uses the expression *system-drive*`:\ProgramData`. The actual value is determined by the OS environment variable when the program is installed. The installation destination may differ depending on the environment.

Conventions: KB, MB, GB, and TB

This manual uses the following conventions:

- 1 KB (kilobyte) is 1,024 bytes.
- 1 MB (megabyte) is $1{,}024^2$ bytes.
- 1 GB (gigabyte) is $1{,}024^3$ bytes.
- 1 TB (terabyte) is $1{,}024^4$ bytes.

Conventions: Version numbers

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

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

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

Contents

Preface i

PART 1: Overview

1. Overview of JP1/Base 1

PART 2: Installation and Setup

PART 3: Installation and Operation

PART 4: Reference

PART 5: Troubleshooting

Appendixes 757

Chapter

1. Overview of JP1/Base

This chapter provides an overview and explains the features of JP1/Base.

1.1 Overview of JP1/Base functionality

JP1/Base is the core of the JP1/IM job management system and the JP1/AJS integrated management system. JP1/Base enables you to manage events and JP1 users in a system, and also enables you to control the startup of services.

JP1/Base provides functionality for the following tasks:

- Managing users

  This functionality allows you to manage the user permissions for accessing a host on which JP1/IM - Manager or JP1/AJS - Manager is installed, and also for working with JP1 resources (jobs, jobnets, events, and so on) on that host. The JP1 users are managed independently of the OS accounts, and permissions for operations on other hosts can be managed for individual users, so that you can strengthen security.

- Controlling startup of services (Windows only)

  This functionality enables you to define the sequence for starting and stopping services. JP1/Power Monitor must be installed to define the sequence for stopping services.

- Handling events

  This functionality enables you to manage JP1 events reported to JP1/Base when an event occurs in the system, and to send and receive JP1 events between the local host and a remote host. You can also use an event filter to forward only the important JP1 events to the manager host.

- Converting events

  This functionality enables log messages and event log data to be converted into JP1 events. The converted JP1 events are stored in the JP1/Base event database provided by the event service, and can be managed in the same way as for JP1 events issued by JP1 series programs. This functionality can be used for the following:

  Performing log file trapping

  > This functionality converts the logs that application programs output into JP1 events.

  Performing event log trapping (Windows only)

  > This functionality converts the Windows event log data into JP1 events.

  Converting SNMP traps into JP1 events

  > This functionality converts the SNMP traps into JP1 events. For details on

the versions of NNM supported by the SNMP trap converter, see *I. Converting SNMP traps*.

- Collecting and distributing definitions (for JP1/IM)

  This functionality enables you to collect or distribute information defined in JP1/Base or JP1 products. This functionality can be used for the following:

  Managing definitions by using IM configuration management

  > If you are using the IM configuration management functionality, you can manage JP1/Base definition information by operating IM configuration management viewer. IM configuration management is a functionality introduced in JP1/IM - Manager 09-00.

  Checking information on the operation of services by using IM configuration management

  > If you are using the IM configuration management functionality, you can check information on the operation of JP1/Base services by operating IM configuration management viewer.

  Collecting and distributing definitions for the event service by using commands

  > If you are not using the IM configuration management functionality, you can collect or distribute information used for the forwarding settings file (`forward`) or event conversion.

  Collecting definitions of JP1 programs

  > You can collect definitions managed by JP1 programs, such as JP1/AJS jobnet definitions and JP1/PFM/SSO definitions. The collected definition information is managed as monitored objects within JP1/IM. For details, see the manual *Job Management Partner 1/Integrated Management - Manager Administration Guide*.

- Managing processes

  This functionality controls the operation of JP1/Base, including starting and stopping it. This functionality controls the following:

  - User management
  - Collecting and distributing definitions
  - Health check
  - Local action
  - Configuration management

    Configuration management manages the configuration of JP1/IM.

  - Command execution

Command execution executes commands requested by JP1/IM.

- Service management control

  Service management control controls agents of JP1/IM configuration management.

- Inter-process communication

  Inter-process communication is a communication base to be used for communicating with JP1/IM configuration management and service management control.

- Health check

  This functionality monitors JP1/Base processes and reports any hangups or other problems via a message or JP1 event. Use of this functionality enables early detection of process errors. As the process in which an error occurred can be easily identified, the user can take action to minimize its effects.

- Local action

  This functionality automatically executes a command when a specific JP1 event occurs. If a failure occurs, a command for notifying the system administrator via email or telephone, or for restarting JP1/Base, can be executed.

- ISAM-related utility commands

  JP1/Base provides utility commands as an aid when using ISAM. For details on these commands, see *13. Commands*.

- Tracing with Hitachi Network Objectplaza Trace Library (HNTRLib2)

  This functionality provides tracing of operation processing, including operations in the programs JP1/IM and JP1/AJS) for which JP1/Base is a prerequisite. The trace results are stored as log information, and can be used for investigating the cause of any problems in the program.

Some of the above JP1/Base functionality might not be supported by a particular OS. The following table shows the functionality that each OS supports.

Table 1-1: JP1/Base functionality and OS support (for Windows)

Functionality		OS	
		Win	**Win(V)**
User management	User authentication	Yes	Yes
	User authentication by a directory server[#1]	Yes	Yes

Functionality		OS	
		Win	Win(V)
	User mapping	Yes	Yes
Startup control	Start sequence control	Yes	Yes
	Stop sequence control[#2]	Yes	Yes
Event service		Yes	Part
Event conversion	Log file trapping	Yes	Yes
	Event log trapping	Yes	Part[#3]
	SNMP trap converter	Part[#4]	No
Collecting and distributing definitions	Checking information on the operation of services and managing definitions by using IM configuration management	Yes	Yes
	Collecting and distributing definitions for the event service by using commands	Yes	Yes
	Collecting definitions of JP1 programs	Yes	Yes
Process management		Yes	Yes
Health check		Yes	Yes
Local action		Yes	Yes
ISAM-related utility commands		Yes	Yes
Hitachi Network Objectplaza Trace Library (HNTRLib2)		Yes	Yes

Legend:

Win refers to Windows XP Professional, Windows Server 2003, and Windows Server 2003 (x64).

Win(V) refers to Windows Vista, Windows Server 2008 Enterprise, and Windows Server 2008 Standard.

Yes: Supported

Part: Partly supported only.

No: Not supported

#1: An Active Directory server is used for the directory server.

#2: JP1/Power Monitor is required for stop sequence control.

#3: This functionality does not support the event types introduced in Windows Vista and Windows Server 2008.

#4: Only JP1/Base running on Windows XP Professional or Windows Server 2003 is supported.

Table 1-2: JP1/Base functionality and OS support (for UNIX)

Functionality		OS			
		HP (IPF)	Sol(G)	Sol(N)	AIX
User management	User authentication	Yes	Yes	Yes	Yes
	User authentication by a directory server#1	No	No	No	No
	User mapping	Yes	Yes	Yes	Yes
Startup control#1	Start sequence control	No	No	No	No
	Stop sequence control	No	No	No	No
Event service		Part#2	Yes	Part#3	Yes
Event conversion	Log file trapping	Yes	Yes	Yes	Yes
	Event log trapping#1	No	No	No	No
	SNMP trap converter	Yes	Part#4	No	No
Collecting and distributing definitions	Checking information on the operation of services and managing definitions by using IM configuration management	Yes	Yes	Yes	Yes
	Collecting and distributing definitions for the event service by using commands	Yes	Yes	Yes	Yes
	Collecting definitions of JP1 programs	Yes	Yes	Yes	Yes
Process management		Yes	Yes	Yes	Yes
Health check		Yes	Yes	Yes	Yes
Local action		Yes	Yes	Yes	Yes

Functionality	OS			
	HP (IPF)	Sol(G)	Sol(N)	AIX
ISAM-related utility commands	Yes	Yes	Yes	Yes
Hitachi Network Objectplaza Trace Library (HNTRLib2)	Yes	Yes	Yes	Yes

Legend:

HP(IPF) refers to HP-UX (IPF).

Sol(G) refers to Solaris global zone.

Sol(N) refers to Solaris non-global zone.

AIX refers to AIX.

Yes: Supported

Part: Partly supported only.

No: Not supported

#1: This functionality is not supported in UNIX.

#2: The IPF version of JP1/Base does not support the tools (`jevmkcompat` and `jevconfcopy` commands) for importing environment definitions and commands from JP1/SES Version 5.

#3: You must recompile the user application. The version 5 compatibility events cannot be used.

#4: Only Solaris (SPARC) is supported.

1.2 Managing users

The JP1 products such as JP1/IM and JP1/AJS use the dedicated account *JP1 user* to operate safely in a distributed system where different OSs exist. JP1/Base manages JP1 users.

You can use JP1/Base user management functionality for:

- User authentication
- User mapping

For details on user authentication, see sections *1.2.1* to *1.2.4*. For details on user mapping, see *1.2.5*.

1.2.1 Authenticating users

User authentication functionality enables you to verify login requests from a viewer (such as JP1/IM - View or JP1/AJS - View) to a manager (such as JP1/IM Manager or JP1/AJS - Manager), and configure and manage what types of operation each JP1 user can perform for *JP1 resources*, that is, jobs, jobnets, and other resources handled by JP1. You can use the JP1/Base *authentication server* for centralized management of access and operating permissions for JP1 resources.

User authentication functionality is used for the following:

Login authentication

> Login authentication prevents unauthorized access when users log in from a viewer such as JP1/IM - View or JP1/AJS - View. JP1/Base checks whether the login user matches a registered JP1 user name and password. Usually, JP1 user names and passwords are registered on the authentication server, and login authentication is performed on the authentication server.
>
> In Windows, by linking with a directory server, the directory server can be used to authenticate logins. For details on login authentication by linking with a directory server, see *1.2.4 Login authentication by linking with a directory server (Windows only)*.

Managing operating permissions for JP1 resources

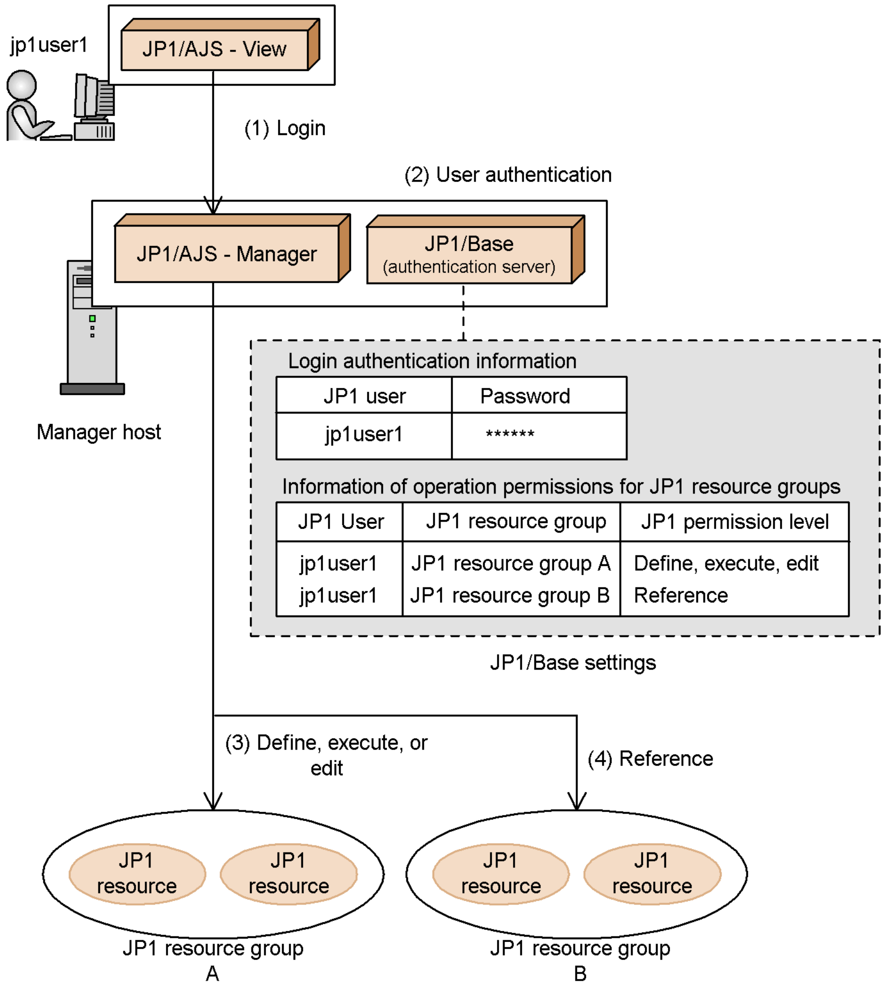
> There would be a security problem if all JP1 login users could perform all types of operations on JP1 resources in the system. Therefore, JP1 user access permissions and operating permissions for JP1 resources must be controlled for each user.
>
> The JP1 resources each JP1 user can access is specified for a *JP1 resource group*.
>
> For example, JP1/AJS classifies jobs, jobnets, and other JP1 resources into

several groups, called *JP1 resource groups*. JP1/IM handles settings for JP1/IM as JP1 resource groups.

The types of operation granted to JP1 users permitted to access JP1 resource groups are specified as a *JP1 permission level*.

The following figure shows an example of user authentication where the JP1 user `jp1user1` logs in to JP1/AJS - Manager:

Figure 1-1: Example of user authentication



Login authentication information

JP1 user	Password
jp1user1	******

Information of operation permissions for JP1 resource groups

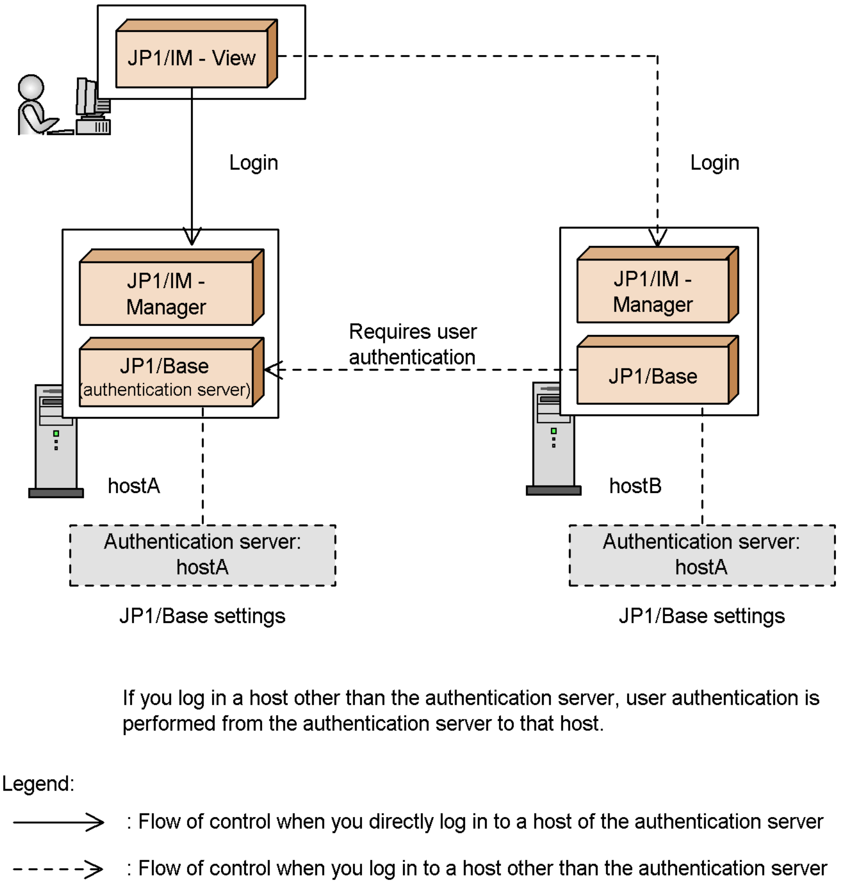
JP1 User	JP1 resource group	JP1 permission level
jp1user1	JP1 resource group A	Define, execute, edit
jp1user1	JP1 resource group B	Reference

(1) "jp1user1" logs in to JP1/AJS - Manager from JP1/AJS - View.
(2) The authentication server performs user authentication for the logged-in "jp1user1". Based on the registered login authentication information, the authentication server checks if "jp1user1" is registered. If there is no problem, the authentication server returns the operation permission information of "jp1user1" to JP1/AJS - Manager.
(3) "jp1user1" can define, execute, or edit JP1 resources within the "JP1 resource group A".
(4) "jp1user1" can reference JP1 resources within the "JP1 resource group B".

On the manager host, specify which of the hosts running JP1/Base is to be the authentication server beforehand. The authentication server can be any host that runs JP1/Base. If you specified a different host as the authentication server, the other host will be requested to authenticate users.

The following figure shows an example of user authentication when a user logs in to both the host that is the authentication server and a host that is not the authentication server.

Figure 1-2: Example of user authentication when a user logs in to both the host that is the authentication server and a host that is not the authentication server.


JP1/IM - View
Login
Login
JP1/IM - Manager
JP1/Base
(authentication server)
Requires user authentication
JP1/IM - Manager
JP1/Base
hostA
hostB
Authentication server: hostA
JP1/Base settings
Authentication server: hostA
JP1/Base settings
If you log in a host other than the authentication server, user authentication is performed from the authentication server to that host.
Legend:
: Flow of control when you directly log in to a host of the authentication server
: Flow of control when you log in to a host other than the authentication server

1.2.2 User authentication block

A group of hosts that references the same authentication server when authenticating users is called a *user authentication block*. A user authentication block indicates a range of hosts managed by the same authentication server. To build a user authentication block, specify the same authentication server on each host where a manager product (such as JP1/IM - Manager or JP1/AJS - Manager) has been installed.

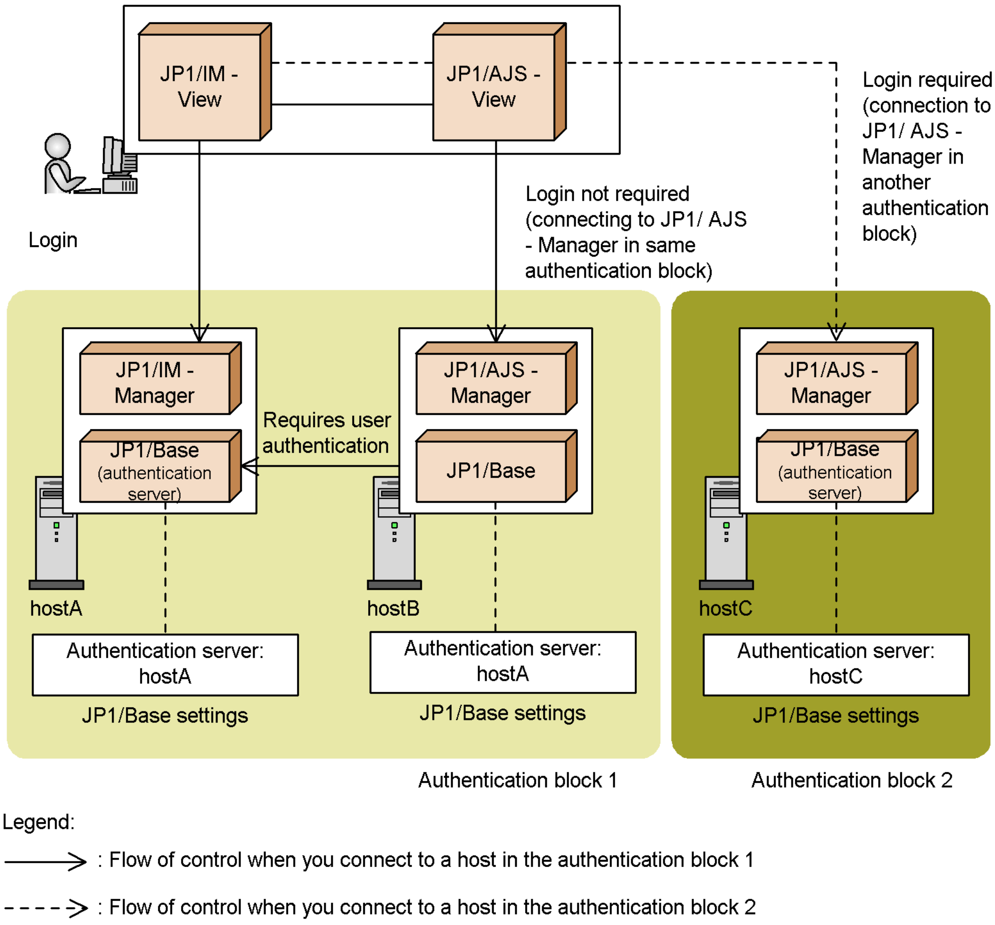
The following are examples in both JP1/IM and JP1/AJS:

Usually, login authentication is required when you connect from JP1/IM - View to JP1/

IM - Manager or from JP1/AJS - View to JP1/AJS - Manager. However, suppose you log in from JP1/IM - View to JP1/IM - Manager and call the JP1/AJS - View monitor window from JP1/IM - View to connect to JP1/AJS - Manager on another host. In this case, login is not required if the following hosts belong to the same authentication block: the host to which JP1/AJS - View connects, and the host where you have logged in with JP1/IM - View. If the host to which JP1/AJS - View connects is not located in the same authentication block as the host where you have logged in with JP1/IM - View, you must log in using a JP1 user name registered with the authentication server that manages the host.

The following figure shows an example of user authentication where you define two user authentication blocks:

Figure 1-3: Example of user authentication with two user authentication blocks


JP1/IM - View
JP1/AJS - View
Login
Login not required (connecting to JP1/ AJS - Manager in same authentication block)
Login required (connection to JP1/ AJS - Manager in another authentication block)
JP1/IM - Manager
JP1/Base (authentication server)
Requires user authentication
JP1/AJS - Manager
JP1/Base
JP1/AJS - Manager
JP1/Base (authentication server)
hostA
hostB
hostC
Authentication server: hostA
Authentication server: hostA
Authentication server: hostC
JP1/Base settings
JP1/Base settings
JP1/Base settings
Authentication block 1
Authentication block 2
Legend:
: Flow of control when you connect to a host in the authentication block 1
: Flow of control when you connect to a host in the authentication block 2

Notes on operating authentication servers

Authentication servers are important hosts that manage users in the entire system. You should take appropriate measures to prevent operations from being disrupted if the system cannot connect to an authentication server for any reason. The following shows some example measures you can take to enhance the reliability of authentication servers:

Install a secondary authentication server.

> You can install a secondary authentication server. If the primary authentication server fails, you can switch to the secondary authentication server to continue operation. For details on a secondary authentication server, see *1.2.3 Secondary authentication server*.

Use authentication servers in a cluster system.

> JP1/Base supports cluster systems. If you operate an authentication server in a cluster system and the authentication server on the primary node fails, you can switch to the authentication server on the secondary node to continue operation. For details on how to operate an authentication server in a cluster system, see *3. Setting Up JP1/Base for Use in a Cluster System*.

Monitor the status of the connections to the authentication servers.

> You can monitor the status of the connection to an authentication server. If the system cannot connect to the authentication server due to its failure or a network error, you can detect the status immediately and take corrective action. If JP1/Base cannot connect to an authentication server, it outputs a message to the integrated trace log. Therefore, the log helps you monitor the status of the connection to the authentication server.
>
> When you use a secondary authentication server, JP1/Base can also output a message to the integrated trace log if the status of authentication server connection is changed automatically and issue the message as a JP1 event. For details on how to issue a JP1 event indicating the blocked status of the authentication server, see *2.4.2 Setup for handling possible errors in JP1/Base*.

1.2.3 Secondary authentication server

Two authentication servers can be set up in one user authentication block. One authentication server is for normal use; the other is in reserve. These two JP1/Base programs are referred to as the *primary authentication server* and *secondary authentication server*, respectively. If the primary authentication server is disabled for any reason, the system automatically switches to the secondary authentication server to prevent operations from being disrupted.

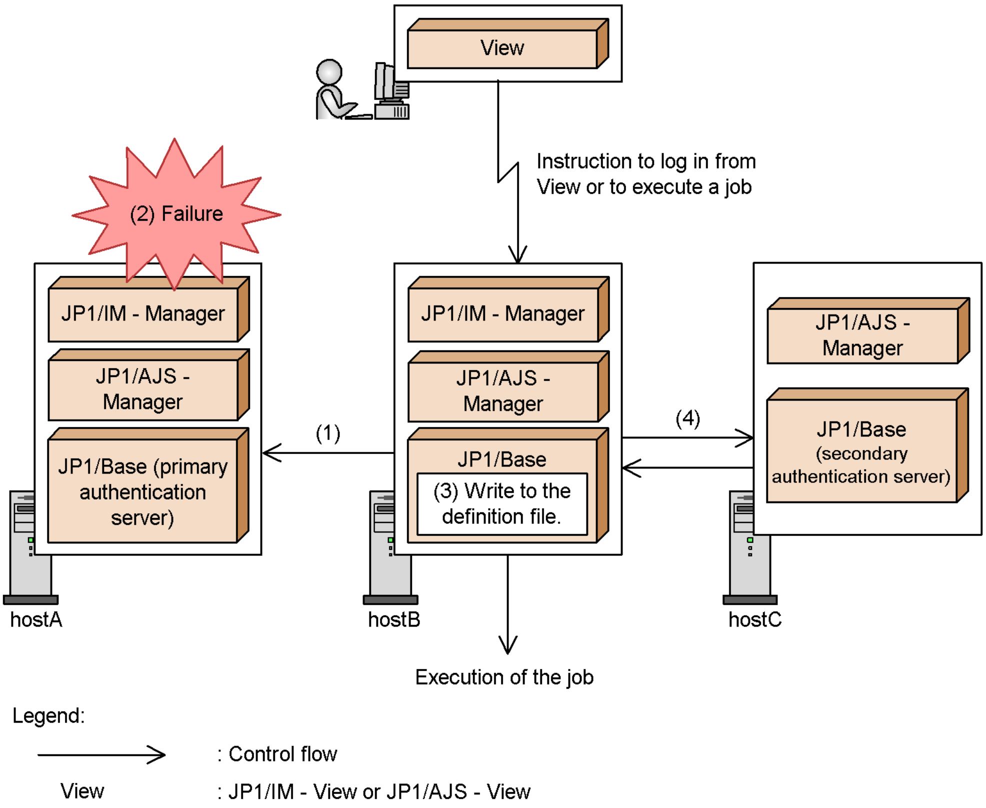
(1) Setting up a secondary authentication server

To set up a secondary authentication server, specify on each host which host is to serve as the secondary authentication server. If the JP1/Base version, JP1 user settings, or operating permission settings are different between the primary authentication server and the secondary authentication server, an authentication error could occur when JP1/Base switches the authentication servers. To make those settings identical, copy the settings from the primary authentication server to the secondary authentication server.

(2) Connection processing

The following figure shows the flow of processing to connect the user to the secondary authentication server if connection to the primary authentication server fails.

Figure 1-4: Connecting to the secondary authentication server if the connection with the primary authentication server fails


View
Instruction to log in from View or to execute a job
(2) Failure
JP1/IM - Manager
JP1/AJS - Manager
JP1/Base (primary authentication server)
(1)
JP1/IM - Manager
JP1/AJS - Manager
JP1/Base
(3) Write to the definition file.
(4)
JP1/AJS - Manager
JP1/Base (secondary authentication server)
hostA
hostB
hostC
Execution of the job
Legend:
: Control flow
View
: JP1/IM - View or JP1/AJS - View

(1) The user authentication function for hostB tries to connect to hostA, which is the primary authentication server.
(2) Connection to hostA fails for some reason.
(3) Notification of the connection failure is written to the definition file on hostB.
Once this failure is written to the file, hostB makes no further attempts to connect to that authentication server.
(4) hostC, which is set as the secondary authentication server, switches in as the target authentication server. hostB tries to connect to hostC and succeeds.
If a connection succeeds, you can log in JP1/IM - View or JP1/AJS - View and execute JP1/AJS jobs.

As shown in Figure 1-4, the status changes to the *blocked* status if the system does not attempt to reconnect to the authentication server after a connection failure. You can check the connection status via the GUI (Windows only) or by a command. The authentication server is shown as *Blocked* when the status of the connection is blocked.

The table below shows the status of the target authentication server and how to select the target authentication server.

Authentication server status	How the target authentication server is selected
Primary authentication server: Available Secondary authentication server: Available	Host tries to connect to the primary authentication server.
Primary authentication server: Blocked Secondary authentication server: Available	Host tries to connect to the secondary authentication server.
Primary authentication server: Available Secondary authentication server: Blocked	Host tries to connect to the primary authentication server. If connection to the primary authentication server fails, the host does not connect to the secondary authentication server.
Primary authentication server: Blocked Secondary authentication server: Blocked	Host tries to connect to the primary authentication server. If connection succeeds, the blocked status on the primary authentication server is released. If connection to the primary authentication server fails, the host tries to connect to the secondary authentication server. If connection succeeds, the blocked status on the secondary authentication server is released. If connection to the secondary authentication server fails, a connection error occurs.

Even if a user intentionally places both authentication servers in the blocked status, if there is an attempt to log in from JP1/IM - View or JP1/AJS - View or an attempt to execute a JP1/AJS job, the system will attempt to connect to an authentication server. If connection succeeds, the system will release the blocked status of one of the authentication servers.

Note that system operation stops if both authentication servers are blocked. You should detect the blocked status as early as possible and eliminate the cause.

To detect the blocked status, JP1/Base can automatically issue a JP1 event if the status of the connection to an authentication server changes. Issuing JP1 events enables JP1/IM - View and other programs to monitor connections to authentication servers. By default, JP/Base does not issue a JP1 event. For details on how to issue a JP1 event, see *2.4.2 Setup for handling possible errors in JP1/Base*.

If an error on the primary authentication server is resolved while you are connected to the secondary authentication server, manually release the blocked status of the primary authentication server. For details on how to release the blocked status, see *6.4 Setup for handling the blocked status (using a secondary authentication server)*.

Note

The target authentication server is switched only in the event of a communication error or if the authentication server has not started. Switching is not performed in response to a typing mistake or incorrect password entered by the executing user.

1.2.4 Login authentication by linking with a directory server (Windows only)

Within the user authentication functionality, only login authentication can be performed on a directory server. Login authentication linking with a directory server is called *directory server linkage*. An Active Directory server is used for the directory server.

A directory server manages JP1 user passwords for login authentication. JP1 users who use a directory server regularly update their passwords themselves, so the system administrator of JP1/Base does not need to update the users' passwords for them. The authentication server manages JP1 user names and operating permissions for JP1 resources. After a user has been authenticated, the authentication server grants the user permissions for accessing or operating the JP1 products.

A JP1 user whose password is managed by a directory server is called a *linkage user*. A JP1 user, whose information (including their password) is managed by an authentication server, is called a *standard user*. On an authentication server, you can specify which JP1 users are linkage users and which are standard users.

(1) Setting up linkage with a directory server

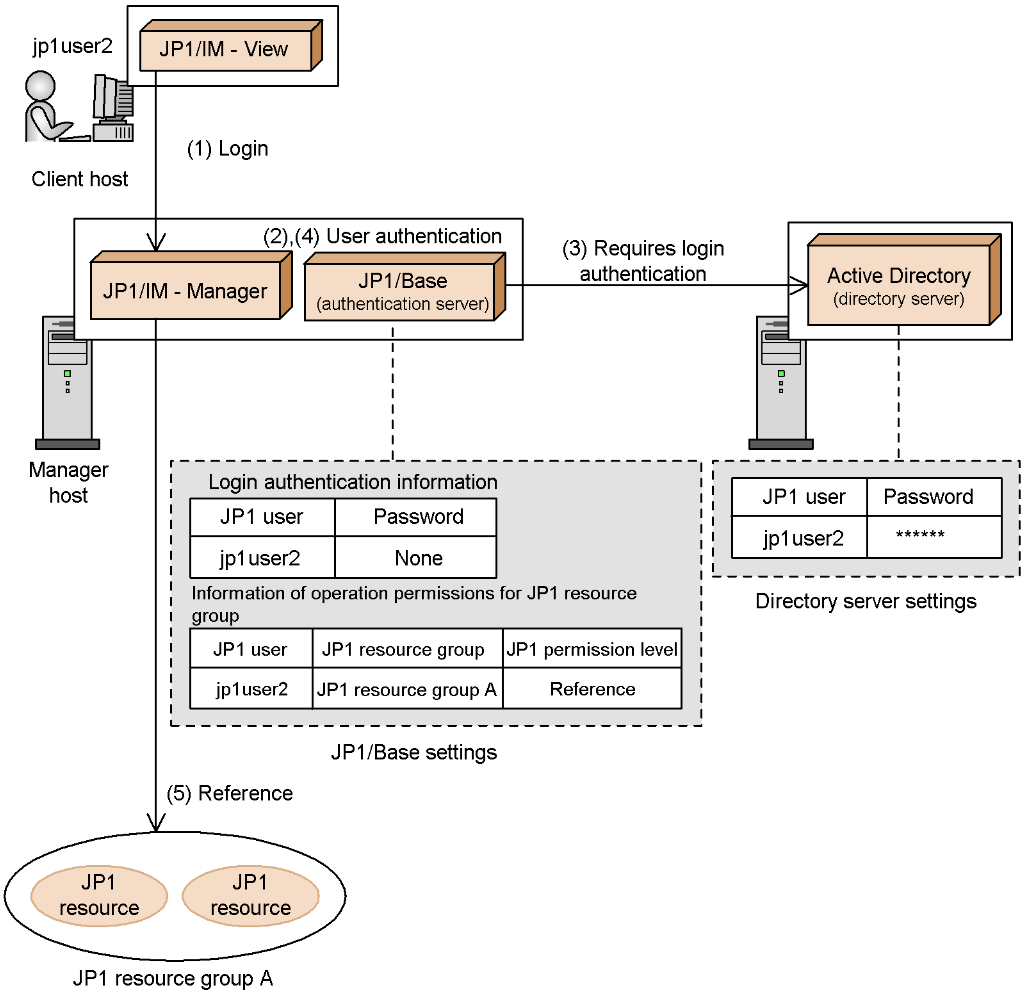
By default, directory server linkage is disabled. To link with a directory server, you will need to modify the default common definitions. For details on the settings, see *6.2 Setup for login authentication linking with the directory server (in Windows)*.

After modifying the common definitions, you can check the status of the connection to the directory server and the modified common definitions by using commands. If the directory server is temporarily disabled due to a failure, you can switch the target server by using commands.

(2) Processing flow of user authentication

The following figure shows the flow of authenticating login users linking with a directory server.

Figure 1-5: Example of user authentication when linking with a directory server



Login authentication information

JP1 user	Password
jp1user2	None

Information of operation permissions for JP1 resource group

JP1 user	JP1 resource group	JP1 permission level
jp1user2	JP1 resource group A	Reference

JP1 user	Password
jp1user2	******

(1) "jp1user2" logs in to JP1/IM - Manager from JP1/IM - View.

(2) The authentication server performs user authentication for the logged-in "jp1user2". Based on the registered information, the authentication server checks if "jp1user2" is registered and determines the type of the user.

(3) If "jp1user2" is a linkage user, the authentication server links with the directory server to perform login authentication.
The directory server compares the password of "jp1user2" with the passwords on the directory server, and then returns the result to the authentication server.

(4) If "jp1user2" is authenticated at login, the operation permission of "jp1user2" is returned to JP1/IM - Manager.

(5) "jp1user2" can reference JP1 resources within "JP1 resource group A".

(3) Notes on linking with a directory server

Sometimes login authentication takes a while from a JP1/Base authentication server because the following are also performed from the authentication server:

- Communicating between the authentication server and a directory server
- Authenticating login users on a directory server

The LDAP protocol is used for communicating between an authentication server and a directory server.

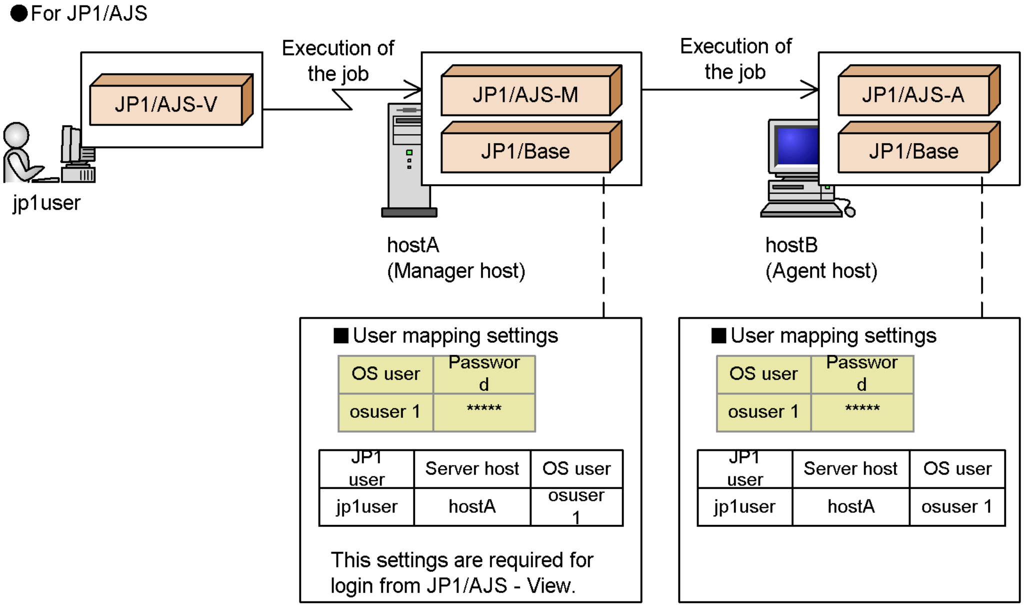
1.2.5 Mapping users

A JP1 user who wants to execute a job or command for another host requires the OS user permissions for that host. This means that you must associate JP1 users with OS users on the host where you want to execute a job or command. This is called *user mapping*. User mapping associates the following:

- The JP1 user who can execute instructions
- The server host from which the users can execute instructions
- The OS user permissions required for executing a job or command

The following is an example of user mapping in JP1/AJS and JP1/IM.

Figure 1-6: Example of user mapping



OS user	Password
osuser 1	*****

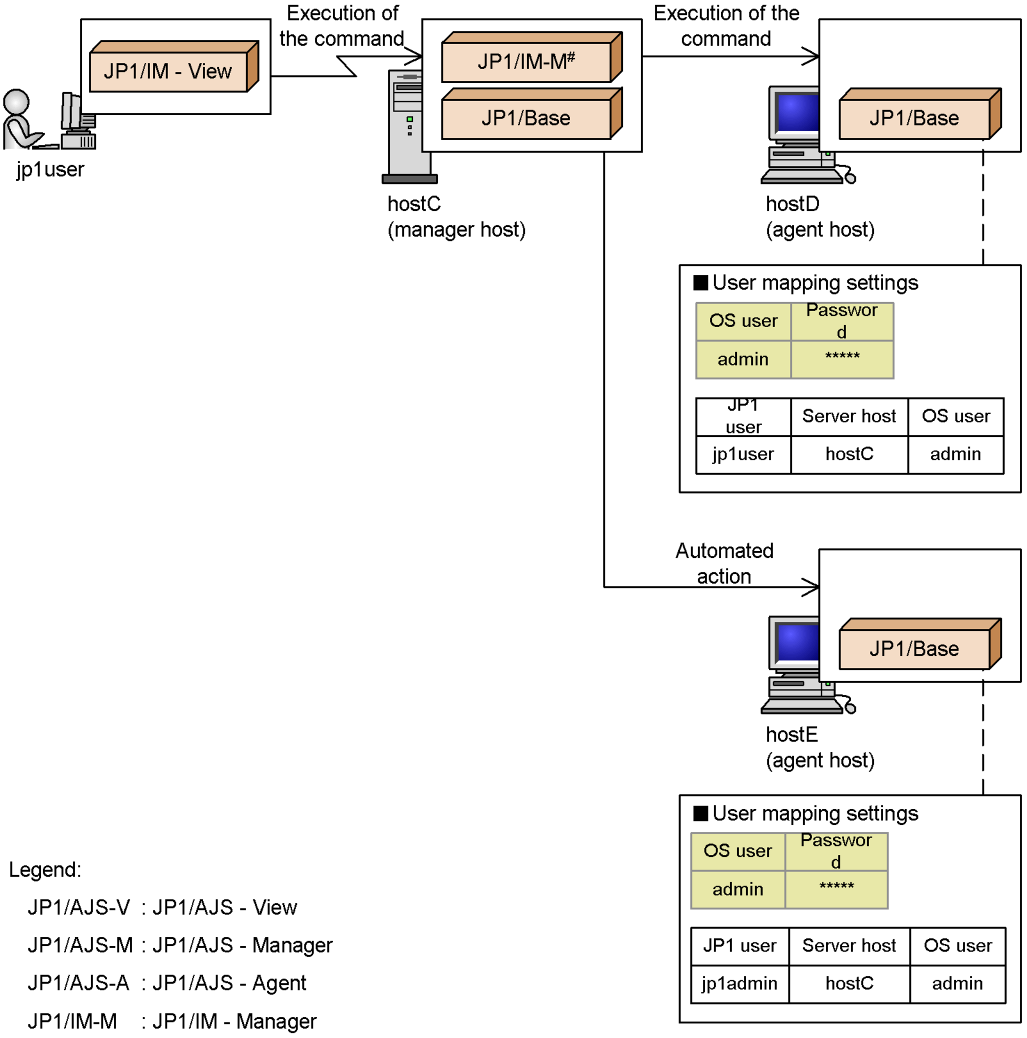
JP1 user	Server host	OS user
jp1user	hostA	osuser 1

This settings are required for login from JP1/AJS - View.

OS user	Password
osuser 1	*****

JP1 user	Server host	OS user
jp1user	hostA	osuser 1

● For JP1/IM



■ User mapping settings

OS user	Password
admin	*****

JP1 user	Server host	OS user
jp1user	hostC	admin

■ User mapping settings

OS user	Password
admin	*****

JP1 user	Server host	OS user
jp1admin	hostC	admin

Legend:

JP1/AJS-V : JP1/AJS - View

JP1/AJS-M : JP1/AJS - Manager

JP1/AJS-A : JP1/AJS - Agent

JP1/IM-M : JP1/IM - Manager

🟨 : Settings required when the OS of the target host is Windows (These settings are not required for UNIX).

Define automated action to be executed with the user name `jp1admin`.

JP1/AJS

If you log in from JP1/AJS - View to JP1/AJS - Manager, mapping of JP1 users to OS users is also required on the host running JP1/AJS - Manager. Therefore, you must set up user mapping on HostA (the manager host) and HostB (an agent host that executes jobs). For details, see the manuals *Job Management Partner 1/*

Automatic Job Management System 2 Setup Guide, *Job Management Partner 1/Automatic Job Management System 3 Configuration Guide 1*, and *Job Management Partner 1/Automatic Job Management System 3 Configuration Guide 2*.

JP1/IM

You must set up user mapping on HostD (an agent host), because commands are executed from HostD for operations from JP1/IM - View. Also, you must set up user mapping on HostE, because automated actions are executed from HostE.

The users that can execute automated actions are defined in JP1/IM - Manager.

Note the following points for user mapping:

- JP1 users mapped to OS users having the administrator privilege can operate all JP1 resources regardless of the operating permissions. If you want to control the operating permissions JP1 users have for JP1 resources, you should map the JP1 users to OS users who do not have the administrator privileges.
- In UNIX, only the OS user name is required for job or command execution by an OS user. In Windows, however, since both an OS user name and a password are required to execute a job or command, JP1/Base also manages OS passwords. If you need to change the password of an OS user in Windows, you must also change the JP1/Base password information.

1.3 Controlling the service start and stop sequences (Windows only)

Services for JP1/IM, JP1/AJS, and other products that require JP1/Base must be started after the JP1/Base service. Services for products that issue JP1 events must also be started after the JP1/Base service. This is because the services cannot be registered with JP1/Base if JP1 events are issued before the JP1/Base service starts.

JP1/Base enables you to control the sequence in which services provided by JP1 products and non-JP1 products start and stop.

To stop services, JP1/Power Monitor must be installed on the same machine. For details on JP1/Power Monitor, see the manual *Job Management Partner 1/Power Monitor Description, User's Guide and Reference*.

At startup, the JP1/Base Control Service starts first. The JP1/Base Control Service then launches each service in turn, according to the order in which the services are written in the start sequence definition file (`JP1SVPRM.DAT`). If any service fails to start within the time specified in the start sequence definition files (`JP1SVPRM.DAT`), JP1/Base Control Service launches the next service. Again, you can specify a command to be executed when each service has stopped.

At shutdown from JP1/Power Monitor, the services end in reverse order from the start sequence, and finally the JP1/Base Control Service ends. Again, you can specify a command to be executed when all services have stopped.

By default, the JP1/Base, JP1/IM, and JP1/AJS services start in that order. If you do not use JP1/IM or JP1/AJS, the system will output an error message to the Windows event log. In that case, you must edit the start sequence definition files (`JP1SVPRM.DAT`).

1.4 Sending and receiving events with the event service

Each host in a system might encounter various events, such as *Not enough disk space* or *Communication error occurred*. These events are reported to JP1/Base, where they can be managed. These events are referred to as *JP1 events*.

The JP1/Base event service can be used for the following:

- Storing JP1 events in the event database

  When JP1/Base receives JP1 events, it stores them in a file called the *event database*. Each host with JP1/Base has its own event database.

- Forwarding JP1 events to other hosts

  The JP1 events generated at each host can be forwarded to a management server at a higher level in the hierarchy. You can choose which JP1 events you want to forward to higher-level management servers. Forwarding events helps the management server monitor the status of each host and promptly detect any problems that might exist, dealing with them immediately.

  JP1/Base can also automatically re-forward JP1 events that were not sent the first time due to a transmission error caused by a network error or by the event server not running.

- Maintaining partial upward compatibility with the event services provided by the pre-Version 6 programs, JP1/SES and JP1/AJS

  Events issued by JP1/SES (a program in version 5 and earlier) running under UNIX, and events issued via commands executed in JP1/AJS (another program in version 5 and earlier) running under Windows NT, can also be acquired.

A program called the *event server* manages the above features. When the event server is active, JP1 events can be sent and received.

1.4.1 JP1 events acquired by JP1/Base

JP1/Base acquires the following JP1 events:

JP1 events issued by JP1 programs

> JP1/Base can acquire JP1 events issued by any JP1 program. JP1/Base can also recognize JP1 events that have the extended event attributes that were recognized by the pre-Version 6 program JP1/SES. JP1/Base can also acquire events handled by version 5 or earlier versions of JP1/IM. For details on these events, see the appropriate program manual.

Events handled by the pre-Version 6 programs, JP1/SES and JP1/AJS (events in the JP1/SES format)

On a UNIX system, JP1/Base can acquire events issued by JP1 programs and user applications, as well as log-file events, Console message events, and syslog message events. JP1/Base can also acquire events issued by JP1/SES (pre-Version 6 program) running under UNIX, and events issued via commands executed in JP1/AJS (pre-Version 6 program) running under Windows NT.

Note

Whereas JP1 events have basic attributes and extended attributes, events in the JP1/SES format have basic attributes only. To enable events in the JP1/SES format to appear in the Event Console window of JP1/IM, you must have given them extended attributes or modify settings in JP1/IM. For details, see *J.4 Converting JP1/SES events into JP1 events*.

JP1 events registered in an event server by the `jevsend` and `jevsendd` commands

JP1 events can be registered on an event server by executing the `jevsend` and `jevsendd` commands. (The `jevsendd` command was added in version 06-71. It allows you to confirm that a JP1 event is registered on an event server.) JP1 events registered by these commands must be given a *severity* extended attribute to enable display in the Event Console window of JP1/IM - View. For details on these commands, see the sections for *jevsend* and *jevsendd* in *13. Commands*.

JP1 events can be issued directly from a user application by using functions for issuing JP1 events. Also, JP1 events can be acquired directly from a user application by using functions for acquiring JP1 events. For details, see the manual *Job Management Partner 1/Base Function Reference*.

Log files of application programs

JP1/Base can acquire JP1 events that are converted from information output to a log file of an application program. For details on how to convert information, see *9.1 Converting application program log files*.

Windows event logs

JP1/Base can acquire JP1 events that are converted from information output to a Windows log file. For details on how to convert information, see *9.2 Converting Windows event logs*.

SNMP trap managed by NNM

JP1/Base can acquire JP1 events that are converted from SNMP traps managed by NNM version 7.5 or earlier. For details on how to convert traps, see *I. Converting SNMP traps*.

1.4.2 Event database

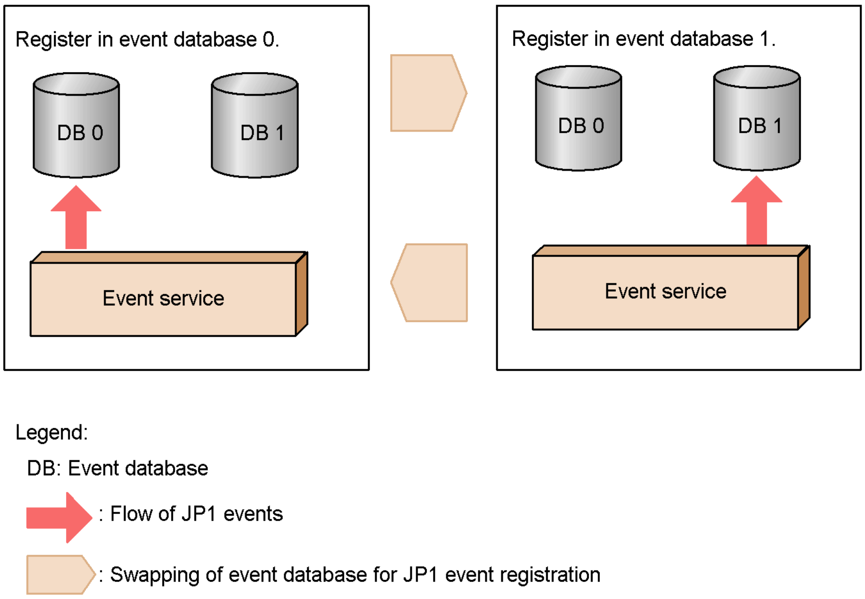
An event database consists of files that accumulate JP1 events occurring on hosts running JP1/Base. An event database consists of the following files:

- Data (IMEvent0.dat and IMEvent1.dat)
- Indexes (IMEvent0.idx and IMEvent1.idx)
- Transfer information (IMEvent0.fwd and IMEvent1.fwd)
- Duplication prevention table (IMEvent.rep)

The files above are generated automatically when an event service starts. Two data files, two index files, and two transfer information files are generated. When the first file reaches the size specified by the db-size parameter in the event server settings file (conf), the second file is swapped in. When the second file reaches the maximum size, the contents of the first file are cleared and new JP1 events are accumulated in the first file.

The following figure shows how the event databases are swapped over.

Figure 1-7: Swapping of event databases


Register in event database 0.
DB 0
DB 1
Event service
Register in event database 1.
DB 0
DB 1
Event service
Legend:
DB: Event database
: Flow of JP1 events
: Swapping of event database for JP1 event registration

The event database is swapped over when the data in the current database reaches the size specified in the event server settings file, or when the time limit for keeping JP1 events specified in the event server settings file has expired. You can also use a command to manually swap the databases.

You can view the contents of the event database by browsing them in the Event Console window or by outputting them to a CSV file. For information on JP1/IM - View, see the manual *Job Management Partner 1/Integrated Management - Manager Administration Guide*. For details on how to output the contents of the event database to a CSV file, see *8.3 Outputting the event database to a CSV file*.

(1) When event databases are checked for possible corruption

Note that the event database might become corrupted if you edit it directly, or if you use an OS command or backup software to back up or restore the event database while the event service is active.

JP1/Base checks whether the event database is corrupted at the following times:

- When the event service starts up
- When JP1 events are transferred
- When JP1 events are acquired by the event acquisition function#
- When an event search is performed from JP1/IM - View#

#

A message reporting that the database is corrupted is output only once for both the active and standby event databases. If an active event database is corrupted, this message appears only once when you attempt to acquire or retrieve a JP1 event from that database. The same is also true for a standby event database corruption.

To check messages in JP1/IM - View, convert the messages to JP1 events and send them to the manager host. For details on event conversion, see *9. Setting Up the Event Converters*.

(2) Checking duplicate registrations

The event service enables you to check whether any duplicate JP1 events exist in the event database when registering a JP1 event. Unless duplicate registration is checked, a duplicate JP1 event might be registered when the following situation occurs:

- When a communication error occurs between hosts sending and receiving the forwarded JP1 events
- The JP1 events being forwarded to multiple hosts are aggregated to a re-forwarding host
- The transfer route of JP1 events circulates.

(3) Duplication prevention table

The duplication prevention table enables you to check whether any duplicate JP1 event exists. The transfer records of JP1 events for each sending host are written in the duplication prevention table. When the event server receives a JP1 event, the transfer record of the JP1 event will be added to the duplication prevention table or updated the appropriate record.

If the `save-rep` flag has been specified in the `options` parameter in the event server settings file (`conf`), the duplication prevention table is kept in a file. If the `save-rep` flag has not been specified, the duplication prevention table is kept in memory. The behavior of the JP1 event server that receives JP1 events depends on whether the JP1 event is kept in a file or in memory. We recommend that the duplication prevention table be kept in a file.

The differences in the behavior of the JP1 event server are as follows:

When kept in a file

> The duplication prevention table is kept in a non-volatile state. Therefore, the data in the duplication prevention table is not erased even if the event server is restarted. When the event server receives a JP1 event from a host that has never been recorded in the duplication prevention table, the JP1 event is considered unknown and recorded in the duplication prevention table. The time necessary for recording a forwarded JP1 event is always the same, regardless of whether the JP1 event has already been forwarded or not.

When kept in memory

> The duplication prevention table is kept in a volatile state. Therefore, the data in the duplication prevention table is erased when the event server is restarted. When the event server receives a JP1 event from a host that has never been recorded in the duplication prevention table, the JP1 event is searched for in the event database, and then recorded in the duplication prevention table. The time necessary for recording a forwarded JP1 event depends on the fact that the JP1 event has already been forwarded or not.
>
> Also, if the event server receives a JP1 event forwarded from a new agent, the JP1 event is searched for among all of the JP1 events registered in the event database. This means that delays might occur when operating on JP1 events. The delay becomes greater in proportion to the size of the event database.

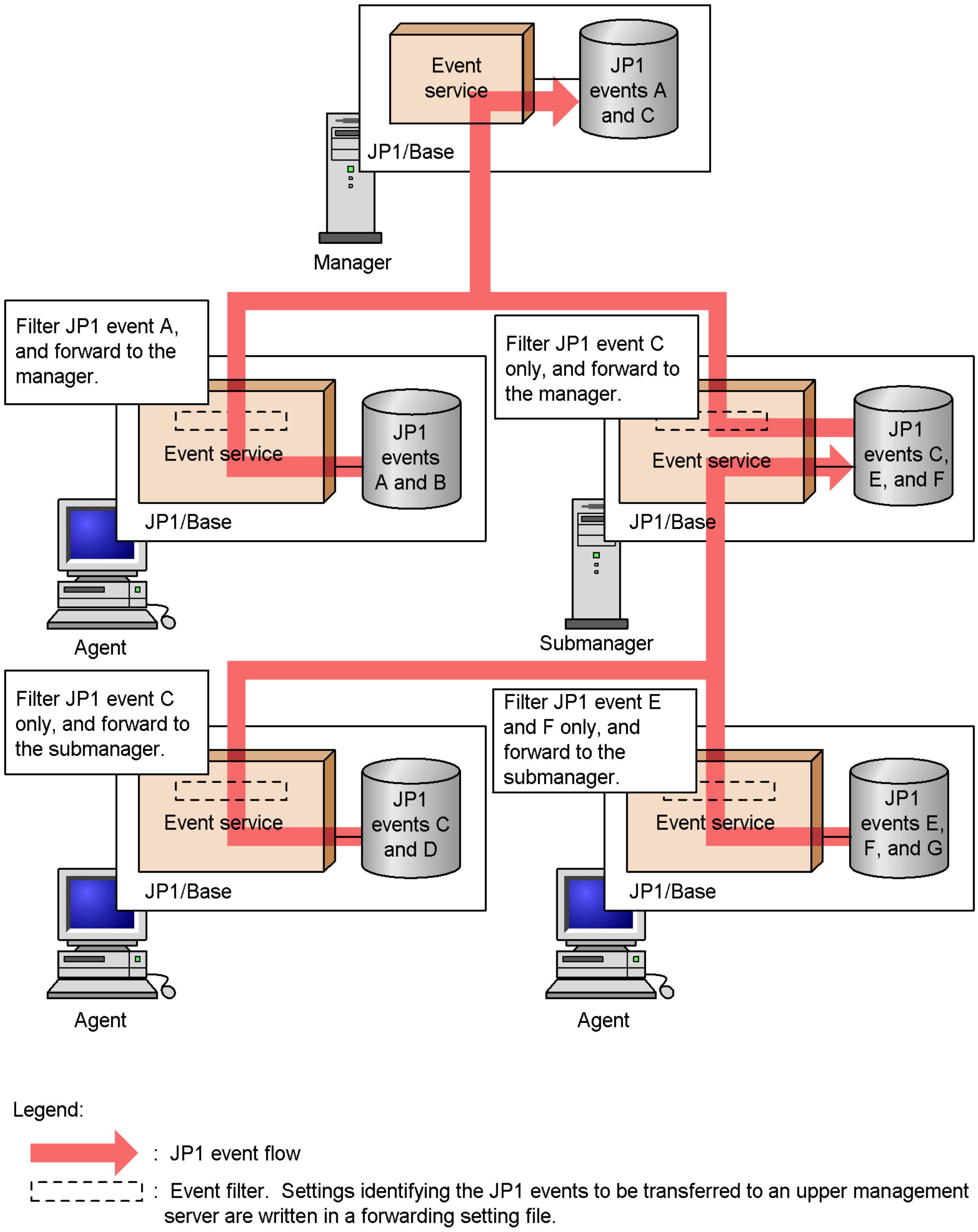
1.4.3 Forwarding JP1 events

JP1/Base can forward the JP1 events generated at each host to another host at a higher level in the system configuration as defined in JP1/IM - Manager. You can also specify that only the important JP1 events, such as failure notification and warning information, be forwarded.

You use a forwarding settings file (`forward`) to define the conditions (event filter) for JP1 events to be forwarded to a higher-level host. By default, the forwarding settings file transfers all important JP1 events to an upper management server, according to the server hierarchy defined in JP1/IM - Manager.

The following figure shows an example of forwarding JP1 events from agents to submanagers, and from submanagers to the manager host.

Figure 1-8: Example of forwarding JP1 events using an event filter


Event service
JP1 events A and C
JP1/Base
Manager
Filter JP1 event A, and forward to the manager.
Event service
JP1 events A and B
JP1/Base
Agent
Filter JP1 event C only, and forward to the manager.
Event service
JP1 events C, E, and F
JP1/Base
Submanager
Filter JP1 event C only, and forward to the submanager.
Event service
JP1 events C and D
JP1/Base
Agent
Filter JP1 event E and F only, and forward to the submanager.
Event service
JP1 events E, F, and G
JP1/Base
Agent
Legend:
: JP1 event flow
: Event filter. Settings identifying the JP1 events to be transferred to an upper management server are written in a forwarding setting file.

JP1/IM - View enables you to view the JP1 events forwarded to the manager host. You can log in from JP1/IM - View to the manager host and view the forwarded JP1 events to monitor the status of the entire system. You can also perform an automated action for recovery in response to a JP1 event indicating a failure.

Resending JP1 events

If forwarding of a JP1 event fails due to a temporary network error or shutdown of the event service at the higher-level host, JP1/Base will retry forwarding by default. You can specify the retry interval and time limit in the event server settings file (`conf`).

1.5 Converting log messages and event log data into JP1 events

Using the JP1/Base event service, you can convert log messages and event logs, and manage them as JP1 events. JP1/Base enables the following event conversion:

Log file trapping

> Converts information output to a log file of an application program into JP1 events.

Event log trapping (Windows only)

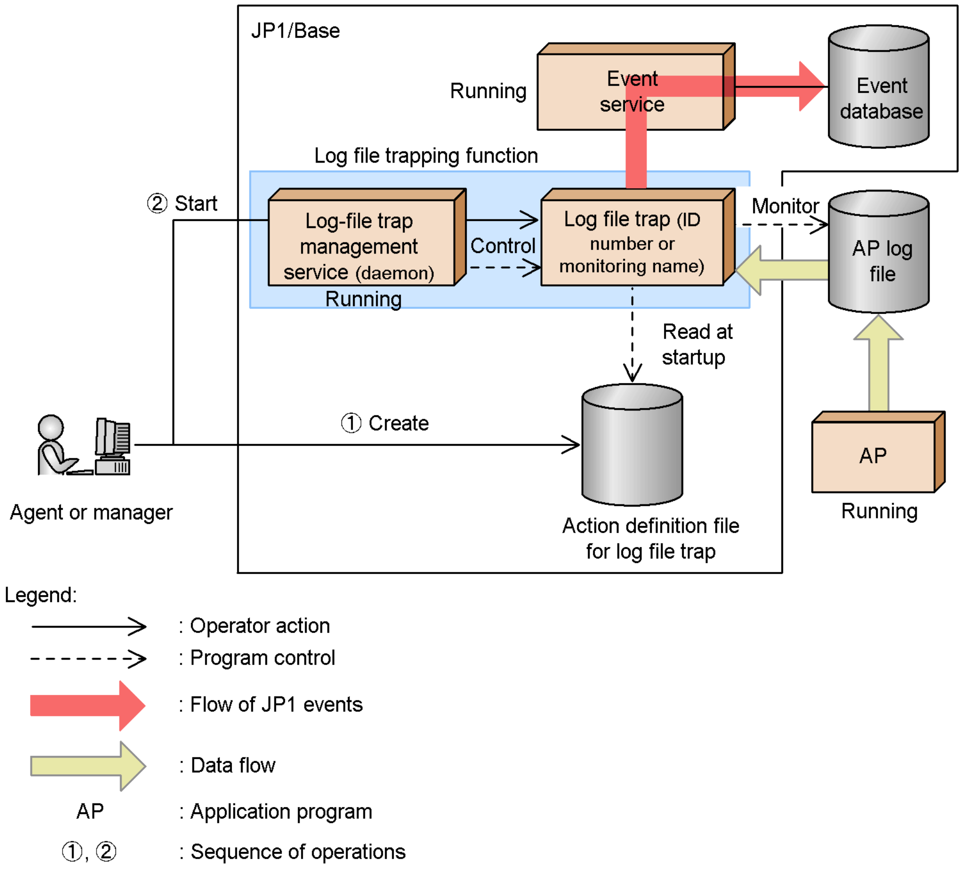
> Converts information output to Windows event logs into JP1 events.

For details on how to convert SNMP traps managed by NNM version 7.5 or earlier into JP1 events, see *I. Converting SNMP traps*.

1.5.1 Converting application program log files

The following figure shows how the log file trapping function converts the contents of application program log files into JP1 events and registers them in an event database.

Figure 1-9: Overview of application log conversion to JP1 event registration



To perform log file trapping, create an action definition file for log file trapping, and then specify the output format of the log file you want to monitor and the conditions for converting log data into JP1 events. After that, execute the command to generate log file traps from the Windows log-file trap management service (or UNIX log-file trap management daemon), and to monitor the log files. All log entries that match the monitoring conditions are converted into JP1 events, which are then registered in the event database. Because multiple log file traps can run simultaneously, you can monitor a variety of log files using different monitoring conditions. You can also monitor multiple log files with one log file trap.

By default, messages up to 511 bytes can be registered as JP1 events. If a message exceeds this limit, the message is truncated from the 512th byte when it is converted into a JP1 event. If you want to extend the length of the message, specify the number of bytes (up to `1023`) in the `-m` option of the `jevlogstart` command.

If you use a log file trap, the following conditions must be satisfied:

- The character codes of the following files or locale information (such as LANG) used when executing the following command must be unified:
    - Log file to be trapped
    - Action definition file for log file trapping
    - `jevlogstart` command

  If the character codes or locale information (such as LANG) are not unified, the characters might become garbled or log file traps might be generated.

- Both the event service and Windows log-file trap management service (or UNIX log-file trap management daemon) must be active.

  In Windows, the event service and log-file trap management service are set by default to start automatically when the system is started up.

  In UNIX, you must execute the appropriate commands to start the event service and log-file trap management daemon. For details on starting services, see *5.2 Starting and stopping JP1/Base (in UNIX)*.

Starting and stopping log file traps:

Use the `jevlogstart` and `jevlogstop` commands to start and stop log file traps. Even if a log file has not been created yet, by specifying the `-r` option in the `jevlogstart` command, you can set up a trap to wait for that log file.

You can also stop log file traps individually, or reload a specific action definition file while a trap is active. To do this, specify an ID number that is output to the standard output when the log file trap is activated, or specify a monitoring target name that you have specified in the `jevlogstart` command when the log file trap is activated.

For details on the attributes of JP1 events converted and registered to the JP1 event database by the log file trapping, see *15.3(10) Details about event IDs specified in the ACTDEF parameter in the action definition file*.

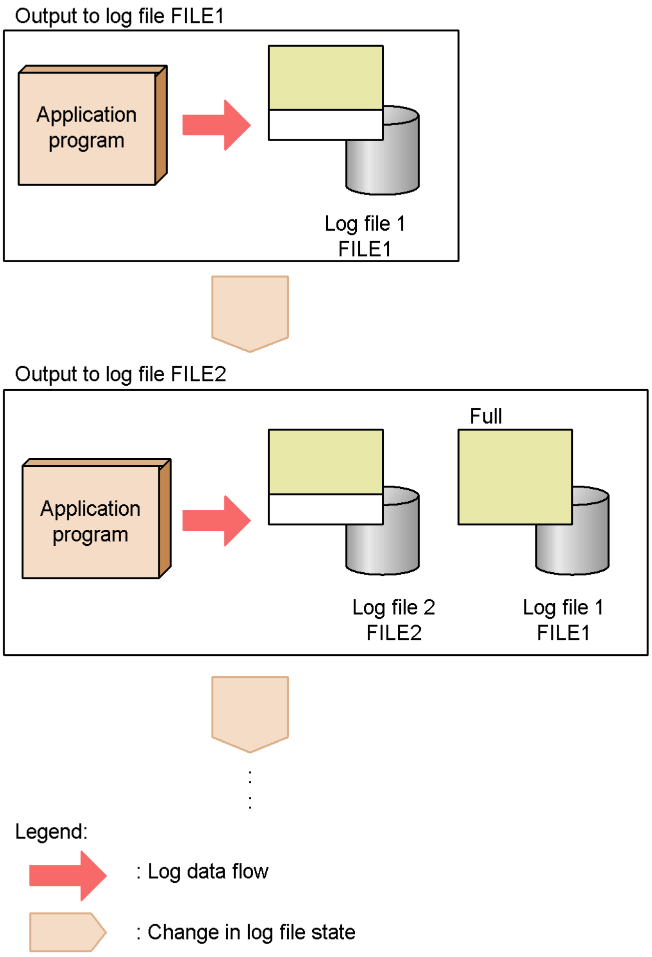
(1) Types of log files that can be monitored

Using the log file trapping, you can monitor log files up to 2 gigabytes in size. Also, you can monitor log files in a variety of formats. Check which file formats are supported, and specify the appropriate log file format in the action definition file for log file trapping. The supported log file formats are shown below.

- Sequential file (SEQ)

  A log file that is written to continuously or, when it reaches a certain size, is replaced with a new log file with a different file name. In the action definition file for log file trapping, specify `SEQ`. The following figure illustrates the behavior of a sequential file (SEQ).

Figure 1-10: Behavior of a sequential file (SEQ)



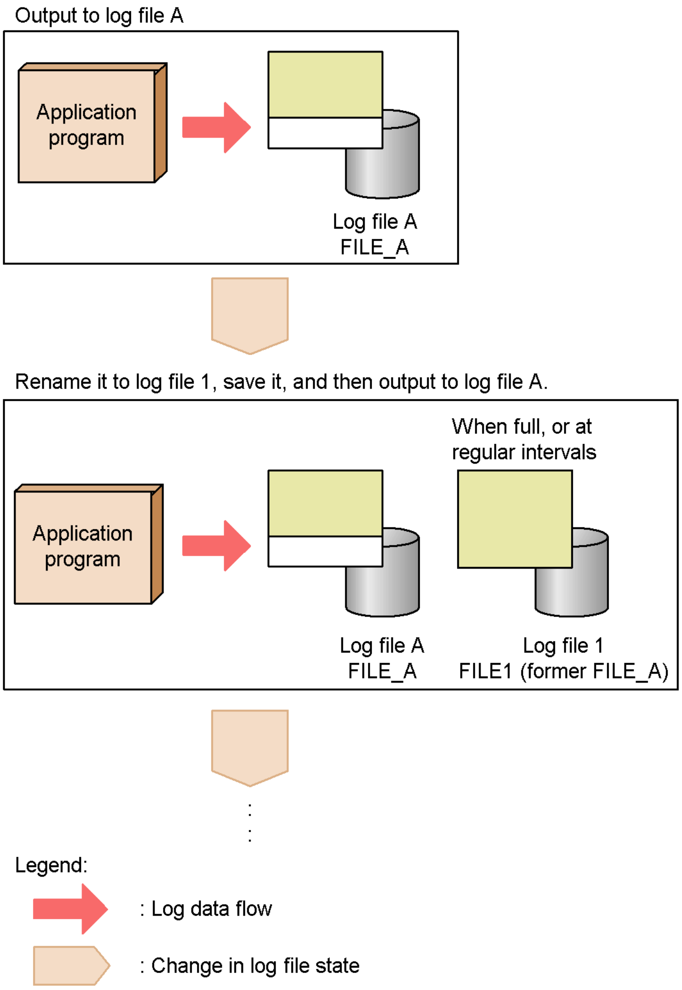
- ■ Sequential file (SEQ2)
    - In Windows:

      A log file that is renamed, and then replaced by a new log file created with the same name as the original file.
    - In UNIX:

      A log file that is renamed or deleted, and then replaced by a new log file created with the same name as the original file.

In the action definition file for log file trapping, specify SEQ2. The following figure illustrates the behavior of a sequential file (SEQ2).

Figure 1-11: Behavior of a sequential file (SEQ2)

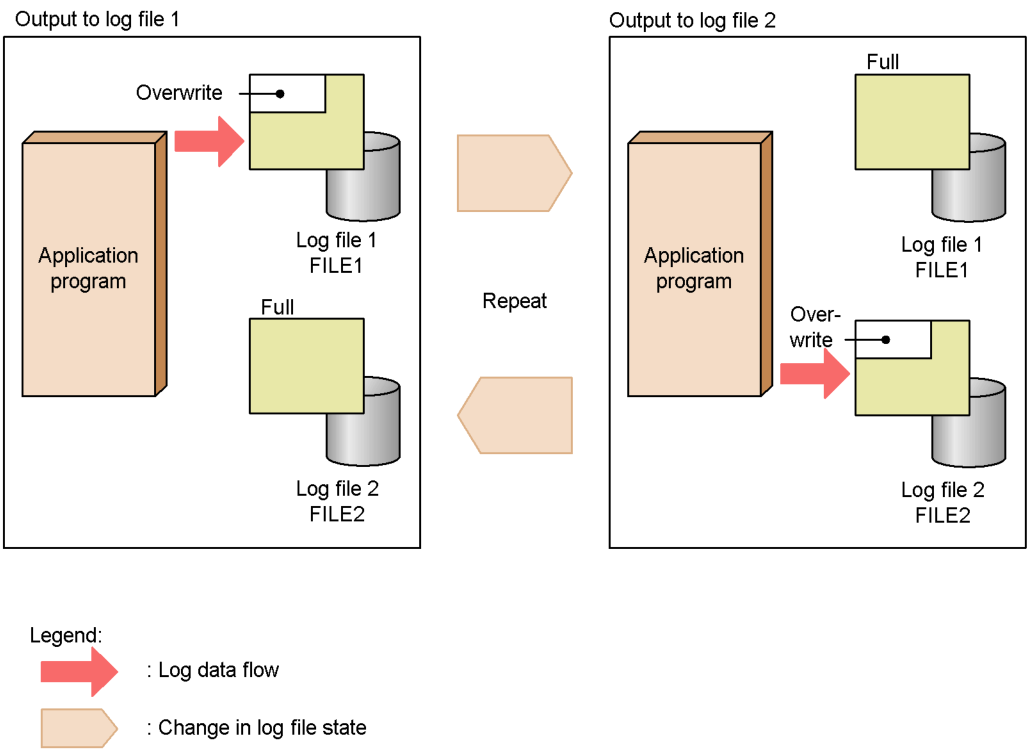


- Wrap-around file (WRAP1)

When the file reaches a certain size, data is wrapped around from the end, overwriting the existing data from the top of the file. In the action definition file for log file trapping, specify WRAP1.

To monitor a log file in WRAP1 format, disk space equal to or greater than the size of the file is required. The following figure illustrates the behavior of a wrap-around file (WRAP1).

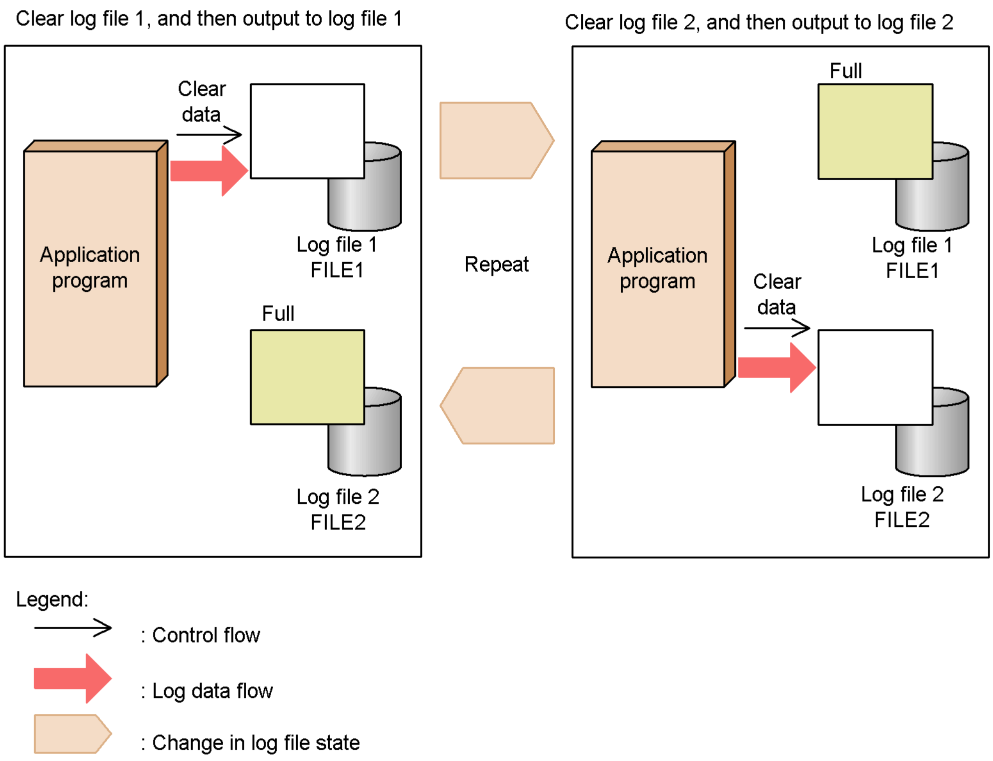
Figure 1-12: Behavior of a wrap-around file (WRAP1)



- ■ Wrap-around file (WRAP2)

When the file reaches a certain size, data is wrapped around from the end, all the data is deleted and the new log data is again written from the top of the file. In the action definition file for log file trapping, specify `WRAP2`. The following figure illustrates the behavior of a wrap-around file (WRAP2).

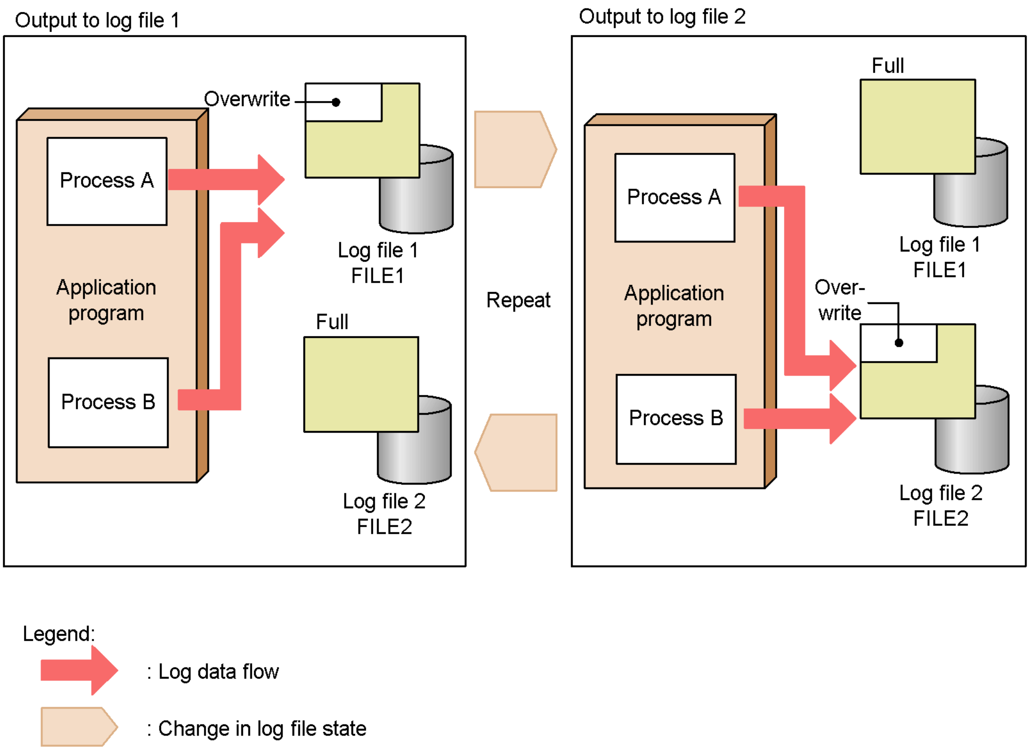
Figure 1-13: Behavior of a wrap-around file (WRAP2)



- Multi-process trace file (HTRACE)

Hitachi middleware-products, such as Cosminexus, use this log file format. The log file format is a group of fixed-size trace files that are shared by multiple processes as memory-mapped files. In the action definition file for log file trapping, specify `HTRACE`. The write method is the same as `WRAP1`. When the file reaches a certain size, data is wrapped around from the end, overwriting the existing data from the top of the file. The file modification time is not updated when data is written to the file. To determine whether the log file to be monitored is a multi-process trace file, see the relevant program manual. The following figure illustrates the behavior of a multi-process trace file (HTRACE).

Figure 1-14: Behavior of a multi-process trace file (HTRACE)



You can also monitor files with symbolic links using the log file trapping. However, you can change the file destination only for log files in SEQ2 format.

The following log files cannot be monitored:

- Wrap-around files (WRAP1) whose modification time is not updated when new data is added, or whose modification time is updated even when new data has not been added

  When a log file trap reads a wrap-around file (WRAP1), it references the date and time at which the file was last modified. Monitoring this type of file might cause the log file traps to operate incorrectly.
- Special file or device file

  A log file that contains records with binary data other than the end-of-line character.
- File without an identifiable file name

  A file whose file name contains values (such as process IDs) that change from time to time.

- Network file

  Operation cannot be guaranteed if a network error or delay occurs when a file on a remote computer is accessed by a file share or other method.

- Log file containing only one line of data

  A log file that always has only one line of data.

- File accessed in lock mode

  Log file traps open log files in read mode. In Windows, therefore, the program that outputs the monitored log might not be able to lock a target log file, so messages might not be logged.

- File output in a language not supported in JP1/Base

  In Windows, JP1/Base supports both MS932 and C.

(2) Estimating the number of log files that can be monitored

In Windows or UNIX, estimate the number of log files that can be monitored as follows.

In Windows:

The maximum number of log files that can be monitored is given by the following equation:

$$(a + m) + (b + n) \leqq 508$$

Legend:

a: Total number of log files monitored (including files monitored by multiple traps)

b: Total number of log files monitored by a log file monitoring job executed in JP1/AJS (including files monitored by multiple traps)

m: Number of `jevlogstart` command executions

n: Number of log file monitoring jobs executed in JP1/AJS

In UNIX:

A maximum of 100 files can be monitored by one log file trap. However, the maximum number that can be monitored on a specific UNIX system depends on a setting in the kernel parameters (maximum number of open files).

(3) Start and end of monitoring

Log file monitoring begins when you activate the log file trapping function via the `jevlogstart` command. The activated log file traps monitor the log files at set intervals. The default is 10 seconds. You can change the monitoring interval by specifying the `-t` option in the `jevlogstart` command. The time at which log file monitoring stops depends on whether you specify the `-w` option in the `jevlogstop` command. For details on the commands, see *13. Commands*.

If you restart a log file trap, log entries output between the time the trap stopped and the time it restarts are not monitored.

(4) Reattempting to monitor a log file when a trap fails

When the time at which a log file is being monitored conflicts with an update time, the log file might become locked by the updating program, which prevents the log file trap from opening and reading the log file. If this happens, you can still reattempt to monitor the log files.

If the log file trap is monitoring multiple log files and one of the files cannot be opened, the log file trap will reattempt to monitor the log file where the error occurred, and will also continue monitoring the other log files.

If a retry fails, the log file will no longer be monitored. Check the error message and determine whether there is an error in the log file. To restart the monitoring of a log file where an error occurred, restart the log file trap using the `jevlogstart` command.

The following describes the retry action when the log file trapping function is unable to open a log file at the start of monitoring or fails to read a log file during monitoring.

(a) When a log file cannot be opened for monitoring

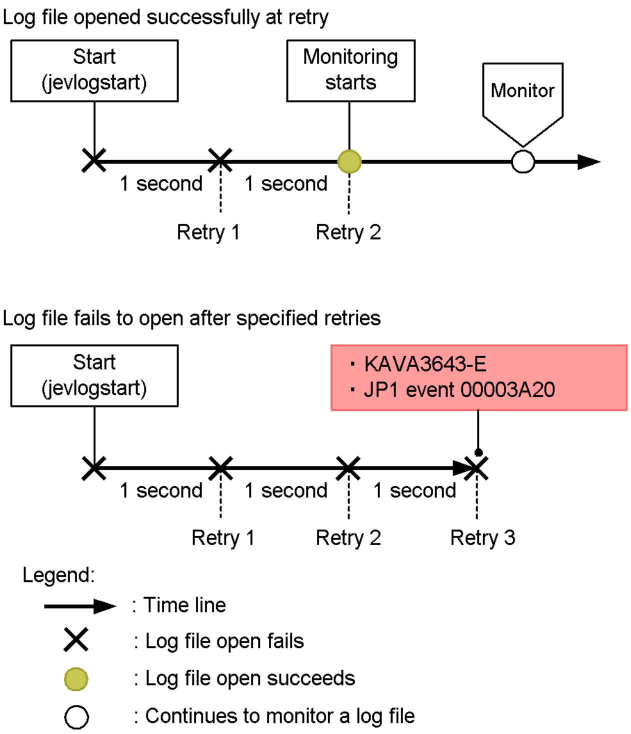
The log file that will be monitored opens when you start a log file trap using the `jevlogstart` command. If the file has been locked by the updating program, it cannot be opened and monitoring will not start. In this case, by default, the log file trap will retry one second later, and only once. You can reconfigure the retry interval and retry count in the action definition file for log file trapping.

If the log file opens successfully upon the retry, monitoring resumes from the point at which the file was opened.

If the log file fails to open after the specified number of retries, or if the monitoring process has not opened after 3,600 seconds have elapsed since the retries began, the error is reported by an error message and JP1 event 00003A20. For details on this JP1 event, see *15.3(4) Details about event ID 00003A20*.

The figure below shows an example of the retry process when the log file trap is temporarily unable to open a log file for monitoring. In this example, the retry interval is `1` second and the retry count is `3`.

Figure 1-15: Example of the retry process when a log file cannot be opened for monitoring



(b) When a log file cannot be read during monitoring

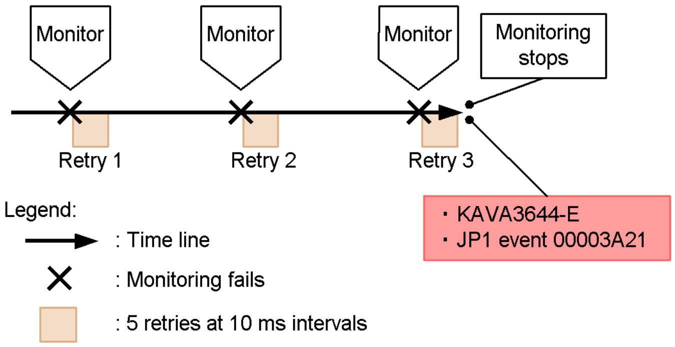
The log file trapping function retries five times at 10-millisecond intervals when it fails to read a log file during monitoring. If monitoring has not recovered after five retries, the trap is suspended until the next monitoring time. If the trap is still unable to open the file the next time it attempts to monitor the file, it retries another five times at 10-millisecond intervals. The retry interval and retry count are fixed.

By default, 100 sets of five retries at 10 ms intervals are performed. You can specify a threshold value for how many retry sets to perform in the action definition file for log file trapping.

If monitoring cannot be recovered after the specified number of retries, monitoring of the log file where the error occurred stops and JP1 event 00003A21 is issued. For details on this JP1 event, see *15.3(5) Details about event ID 00003A21*.

The figure below shows an example of the retry process when the log file trap is unable to read a log file during monitoring. In this example, a threshold of 3 is set for the number of retry sets.

Figure 1-16: Example of the retry process when a log file cannot be read during monitoring



(5) Reattempting to connect to the event service

By default, if a connection to the event service cannot be established, connection retry processing is not performed and the event log trapping fails to start, or stops if it is already active. To attempt a connection to the event service, set the parameter separately for specific log file traps in the action definition file for log file trapping. If the log file trapping function cannot connect to the event service after retrying for the specified number of times, it fails to start, or stops if already active.

The JP1 events converted during a retry are saved in the system up to a specified maximum number. When this maximum is reached, all subsequent JP1 events are deleted.

When successfully connected, the trap starts sending the retained JP1 events to the event service in the order in which they were held. Notification that a connection has been established is also sent as a JP1 event. For details on JP1 events, see *15.3(3) Details about event ID 00003A10*.

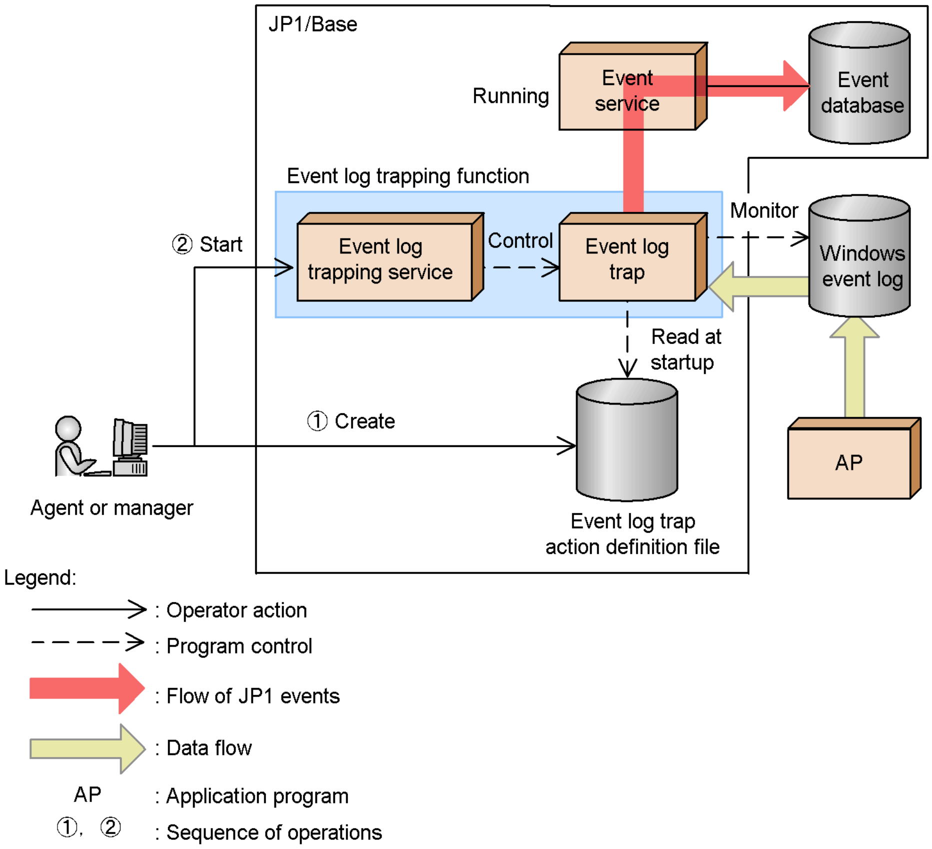
1.5.2 Converting Windows event logs

The following figure shows how the event log trapping function converts Windows event log entries into JP1 events and registers them in an event database.

Note

This functionality does not support the event types introduced in Windows Vista and Windows Server 2008.

Figure 1-17: Overview of Windows event log conversion to JP1 event registration



To use an event log trap, create an action definition file for event log trapping (`ntevent.conf`) and then specify the conditions for the log data you want to convert into JP1 events. If the event service is started first, and then the event log trapping service is started, an event log trap is generated and the event log is monitored. All event logs that match the monitoring conditions are converted into JP1 events, which are then registered in the event database. All JP1 events converted from the Windows event log are assigned an event ID of 00003A71. The severity corresponds to the type of event log data before they are converted to JP1 events.

By default, the event service is set to start automatically when the system is started, but the event log trapping service does not restart automatically. To start and end the event log trapping service automatically, set it up so that the event log trapping service starts after the event service starts. Use the startup control to do this.

By using the action definition file for event log trapping (`ntevent.conf`), you can set an event log trap so that it reattempts to connect to the event service if a connection cannot be established when the event log trapping starts or when event log data is trapped.

Trapped event log messages can be registered as JP1 events up to 1,023 bytes. If a message exceeds this limit, the message is truncated from the 1,024th byte when the message is converted into a JP1 event. For details on the JP1 event attributes, see *15.3(7) Details about event ID 00003A71*.

(1) Start and end of monitoring

Event log entries generated between the start and end of the event log trapping service are immediately converted into JP1 events if they match the monitoring conditions. The event log is monitored at set intervals to catch any event log that might be missed if a temporary error occurs. The default is 10 seconds. You can change this interval in the action definition file for event log trapping (`ntevent.conf`).

1.6 Collecting and distributing definitions (JP1/IM only)

A system configured with JP1/Base and JP1/IM has functionality for collecting and distributing definitions. This functionality can be used for the following:

- Managing definitions by using IM configuration management
- Checking information on the operation of services by using IM configuration management
- Collecting and distributing definitions for the event service by using commands
- Collecting definitions of JP1 programs

1.6.1 Managing definitions by using IM configuration management

If you are using the IM configuration management functionality, you can manage JP1/Base definition information by operating IM configuration management viewer. IM configuration management is functionality introduced in JP1/IM - Manager 09-00. IM configuration management - View enables you to do the following:

- Collect and check the contents of the JP1/Base definition file or definitions currently enabled (the contents of the definition file used when starting each service).
- Edit the JP1/Base definition file, and then distribute it to each host.

If JP1/Base is managed from a host not defined in the JP1/IM configuration definition file, you must define the manager host for controlling access to the host access control definition file in JP1/Base. For details on the definition file, see *Host access control definition file* in *14. Definition Files*.

For details on managing definitions by using IM configuration management, see the *Job Management Partner 1/Integrated Management - Manager Overview and System Design Guide*.

1.6.2 Checking information on the operation of services by using IM configuration management

If you are using the IM configuration management functionality, you can check information on the operation of JP1/Base services by operating IM configuration management viewer.

For details on checking information on the operation of services by using IM configuration management, see the *Job Management Partner 1/Integrated Management - Manager Overview and System Design Guide*.

If you are not using the IM configuration management functionality, you can check information on the operation of JP1/Base services on the local host by using the `jbsgetopinfo` command.

For details on the `jbsgetopinfo` command, see *jbsgetopinfo* in *13. Commands*.

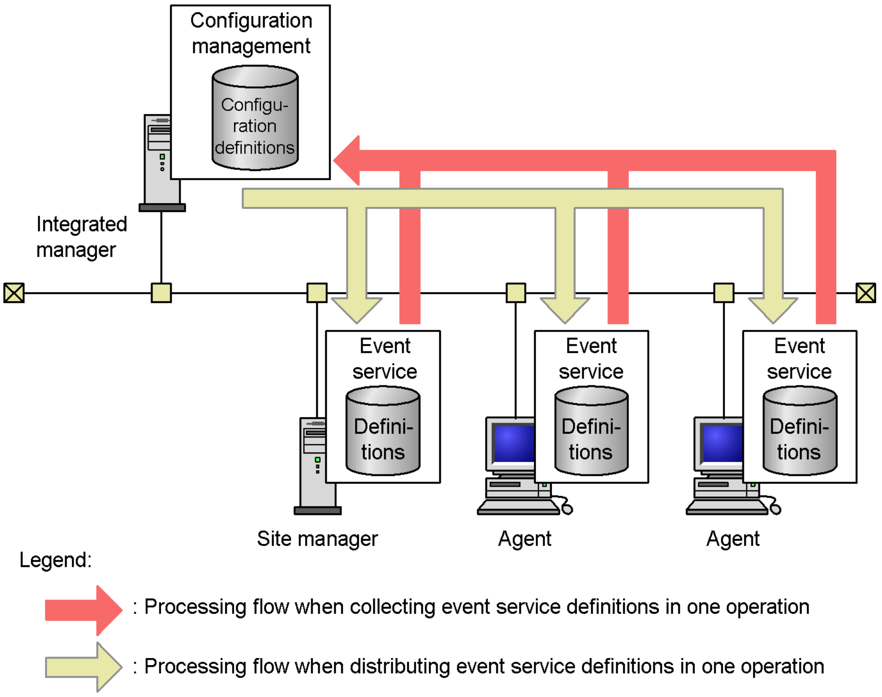
1.6.3 Collecting and distributing definitions for the event service by using commands

This section describes how to collect and distribute event service definitions by using commands. This type of operation is used when you are not using the IM configuration management functionality. To monitor the system using JP1/IM, you must decide and define what sorts of JP1/Base events occurring on the hosts are to be managed as JP1 events, and which JP1 events are to be forwarded to a higher-level host. One way of doing this is to check and change the individual JP1/Base definitions entered on each host. But this is an inefficient method which is prone to error.

Using the JP1/Base functionality for collecting and distributing definitions on the manager host, you can check all the JP1/Base information defined on every host in a single operation. You can also update JP1/Base definitions on each host by editing the definitions on the manager host, and then distributing them to all the hosts. This allows definitions relating to the event service to be managed in an efficient manner.

The following figure shows the processing flow when collecting and distributing definitions for the event service.

Figure 1-18: Processing flow when collecting and distributing event service definitions


Configuration management
Configu-ration definitions
Integrated manager
Event service
Defini-tions
Event service
Defini-tions
Event service
Defini-tions
Site manager
Agent
Agent
Legend:
: Processing flow when collecting event service definitions in one operation
: Processing flow when distributing event service definitions in one operation

(1) Requirements for collecting and distributing event service definitions

This section describes the requirements for collecting and distributing definitions.

- Install JP1/Base and JP1/IM - Manager.

  The following table lists the products you must install on each host in the system as well as their versions.

Host	Required products
Host that collects and distributes definitions	JP1/Base (Version 7 or later)
	JP1/IM - Central Console (Version 7) or JP1/IM - Manager (Version 8)
Host from which definitions are collected from or distributed to	JP1/Base (Version 7 or later)

- Define a system configuration in JP1/IM - Manager on the host that will collect and distribute the definitions.

  When JP1/Base collects or distributes definitions, it uses the configuration definition information in JP1/IM - Manager. JP1/Base collects definitions from or distributes definitions to the managed hosts defined in the system configuration. For details on how to define the system configuration, see the manual *Job Management Partner 1/Integrated Management - Manager Configuration Guide*.

Note:

When the manager host collects definitions from or distributes definitions to managed hosts, it communicates with the managed hosts directly, without using a submanager host. If a firewall exists between the manager host and submanager host, reconfigure the firewall so that port 20306 can pass data from the manager host to all managed hosts. Also ensure that names can be resolved between the manager host and managed hosts.

(2) Collectable and Distributable definitions

You can collect and distribute the following definitions:

In Windows:

Definition files	File names
Forwarding settings file	*installation-folder*`\conf\event\servers\default\forward`
	shared-folder`\jp1base\event\forward`
Action definition file for log file trapping	*installation-folder*`\conf\`*any-file*
Action definition file for event log trapping	*installation-folder*`\conf\event\ntevent.conf`

In UNIX:

Definition files	File names
Forwarding settings file	`/etc/opt/jp1base/conf/event/servers/default/forward`
	shared-folder`/event/forward`
Action definition file for log file trapping	`/etc/opt/jp1base/conf/`*any-file*

1.6.4 Collecting definitions of JP1 programs

Using the integrated scope feature of JP1/IM - Manager, the definitions managed by JP1 programs, such as work tasks (jobnets) defined in JP1/AJS and information monitored by JP1/PFM/SSO, can be viewed in a tree structure in a monitoring window. The display is generated automatically according to the system configuration defined in JP1/IM - Manager. The configuration definitions needed to automatically generate this display are acquired by the JP1/Base functionality for collecting and distributing definitions.

JP1/Base collects the following definition information:

- Information about operations being executed automatically by JP1/AJS
- Category information and application information being monitored by JP1/PFM/SSO
- Performance data being monitored by JP1/PFM

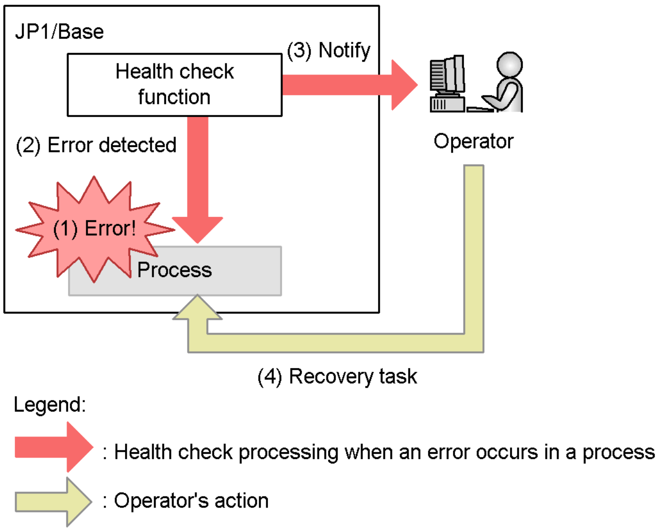
For details, see the manual *Job Management Partner 1/Integrated Management - Manager Administration Guide*.

1.7 Health check

When a JP1/Base process goes into an infinite loop or deadlock, the JP1/Base health check function issues a message or JP1 event prompting the operator to take recovery action. This is called the health check function.

The following figure shows how to use the health check function to troubleshoot problems.

Figure 1-19: Troubleshooting by using the health check function



(1) A hang-up or other problem occurs in a JP1/Base process.
(2) The health check function detects the process error.
(3) The health check function notifies the operator via a message or JP1 event.
(4) The operator checks the error notification and takes recovery action. For the action to taken when an error is detected by the health check function, see *16. Troubleshooting*.

The health check function is disabled by default. To enable the function, you must register the health check function information in the common definition information, and define the host to be monitored and the process-monitoring interval. For details, see *2.4.2 Setup for handling possible errors in JP1/Base*.

The process management service is activated and process monitoring begins.

Errors that can be detected by the health check function

The health check function can detect the following errors:

- Process hangups

If a process hangs, the health check function detects the error and notifies the operator. Hangups are caused by an infinite loop or deadlock, and mean that the process can no longer accept processing requests.

- Abnormal termination of a process

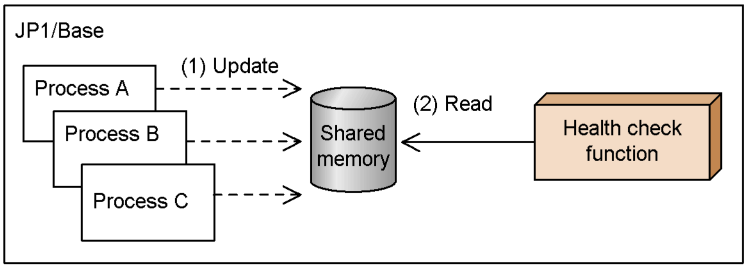
  If a process terminates abnormally of its own accord, the health check function detects the error and notifies the operator. However, if the operator forcibly terminates a process by the OS `kill` command or other means, this is not detected as abnormal termination. Rather, the function detects that there is no response from the process.

1.7.1 Process monitoring with the health check function

When a process aborts or hangs, the health check function detects this as an error. The function determines whether a process is hung by comparing the length of time a process takes with the threshold set for that process. The time taken for the processing performed by a specific process is monitored via the shared memory.

The following figure provides an overview of the health check function.

Figure 1-20: Overview of the health check function



(1) Each JP1/Base process accesses and updates the shared memory when it starts and ends processing.
(2) The health check function monitors the shared memory update time at 5-second intervals. If the shared memory update interval reaches the warning or abnormal threshold value because a process did not end in a timely manner, the health check function issues a message or JP1 event.

The health check function actually monitors the internal processes of the process being monitored to minimize the effects on the user environment. For this reason, the abnormal and warning thresholds are already set and no customization is required by the user.

(1) Monitored processes

The following table lists the processes monitored by the health check function.

Table 1-3: Processes monitored by the health check function

No.	Process	Process name
1	Process management	`jbsspmd`
2	Authentication server	`jbssessionmgr`
3	Configuration management	`jbsroute`
4	Command execution	`jcocmd`
5	Plugin service	`jbsplugin`
6	Event service	`jevservice`
7	Log file trapping	`jevtraplog`
8	Event log trapping (Windows only)	`jevtrapevt`
9	SNMP trap converter	`imevtgw`
10	Health check	`jbshcd` and `jbshchostd`
11	Service management control	`jbssrvmgr`
12	Local action	`jbslcact`
13	Inter-process communication	`jbscomd`

The process for starting JP1/Base process management (`jbs_service`) and the startup control (`jbapmsrvcecon`) simply start or stop a service and are not monitored by the health check function. Because other programs use the Hitachi Network Objectplaza Trace Library (HNTRLib2) (`hntr2mon`), it is not monitored either.

1.7.2 Remote host monitoring with the health check function

The health check function is meant to detect problems in JP1/Base, but this is not possible if a hangup or other error occurs in the function itself. Also, in a system that uses JP1/IM - Manager, if an error occurs in the event service, JP1 events cannot be issued or forwarded, so the higher-level host cannot be notified even if an error is detected.

In case something happens and there is no way of detecting or notifying a process error on the local host, the JP1/Base health check function and the event service can be monitored from a remote host. A maximum of 1,024 remote hosts can be monitored from one host.

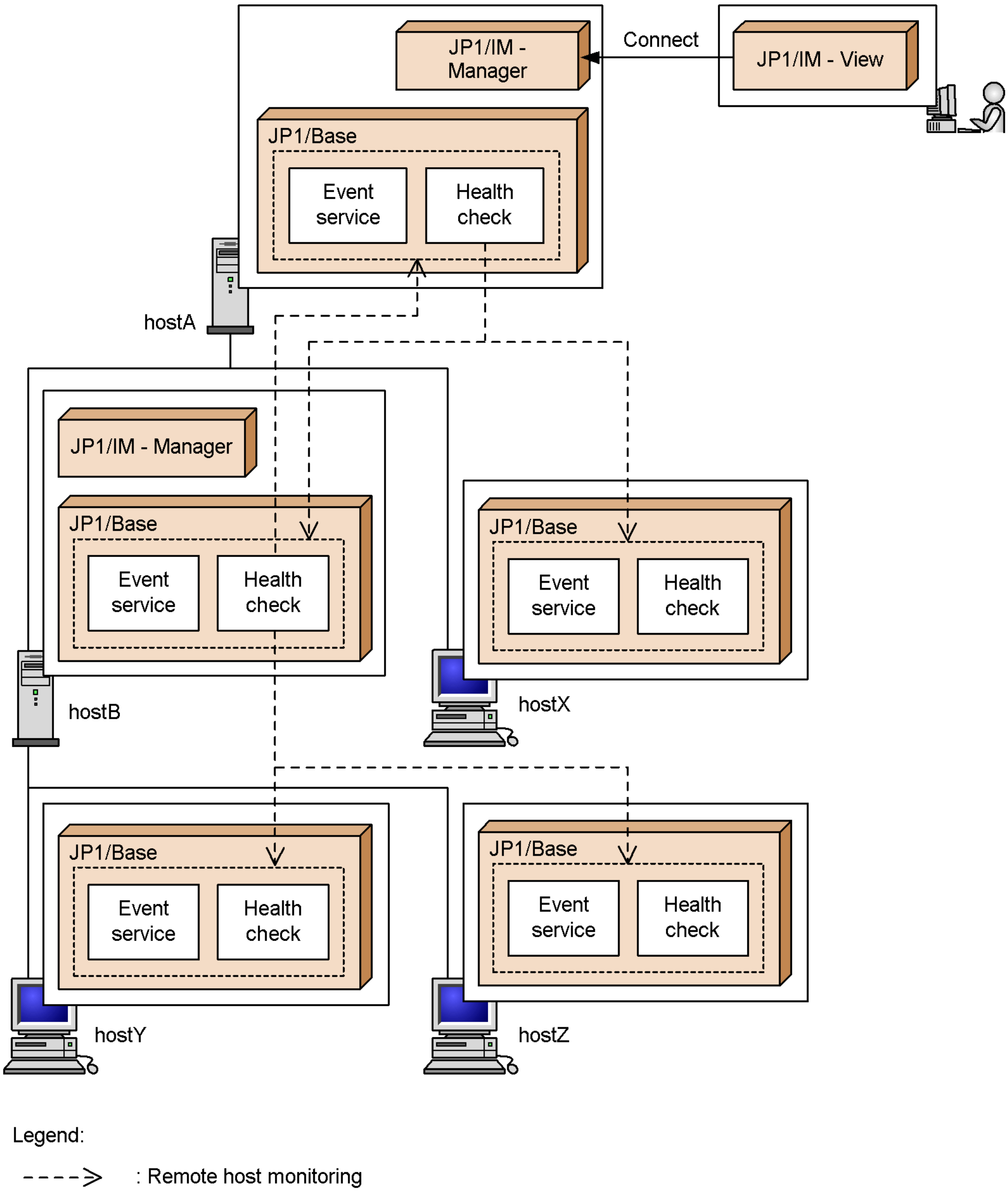
The following describes remote host monitoring and system operation with JP1/IM - Manager or JP1/AJS.

(1) Remote host monitoring in a system that uses JP1/IM - Manager

You can monitor whether the JP1/Base health check function and event service are operating normally on the remote hosts.

The following describes remote host monitoring in a system that uses JP1/IM - Manager, based on the following configuration example.

Figure 1-21: Example of remote host monitoring in a system that uses JP1/IM - Manager



The hosts in this example have the following settings.

Host	Purpose	Setting for remote host monitoring
hostA	Manager host	Monitor hostB and hostX.
hostB	Submanager host	Monitor hostA, hostY, and hostZ.
hostX	Agent host	None
hostY	Agent host	None
hostZ	Agent host	None

The following processing is performed if an error occurs in the health check function or event service at agent hostY or manager hostA.

Error in the health check function at hostY

The health check function at hostB detects the error and issues a JP1 event. The JP1 event is forwarded to hostA. At hostA, a message about the problem at hostY appears in JP1/IM - View.

Error in the event service at hostY

The health check function on hostY detects an error, but cannot issue a JP1 event. Therefore, the health check function at hostB detects the error and issues a JP1 event. The JP1 event issued by hostB is forwarded to hostA. At hostA, a message about the problem at hostY appears in JP1/IM - View.

Error in the health check function at hostA

The health check function at hostB detects the error and issues a JP1 event. The JP1 event is forwarded to hostA. At hostA, a message about the problem on the local host appears in JP1/IM - View.

Error in the event service at hostA

If the health check function is enabled at JP1/IM - Manager on hostA, the health check function at JP1/IM - Manager detects the error in the event service on the local host and a message appears in JP1/IM - View.

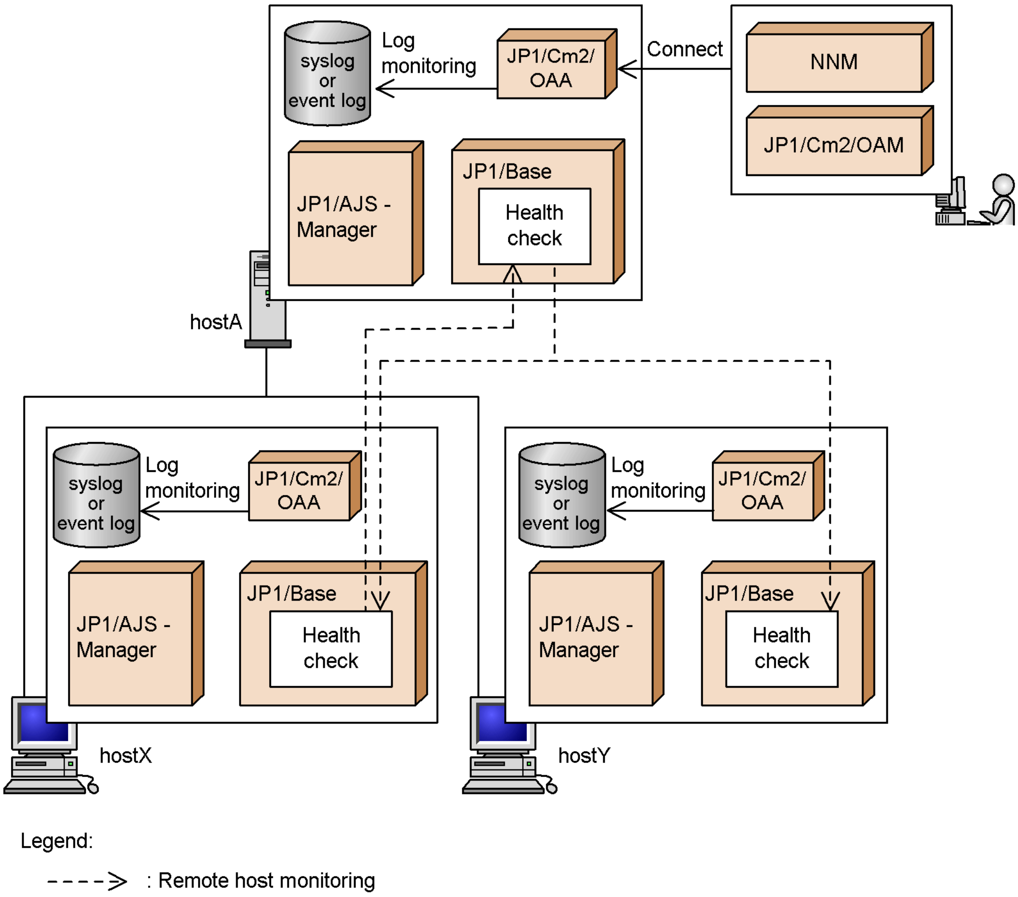
(2) Remote host monitoring in a system that uses JP1/AJS

By specifying the target remote hosts, you can monitor whether the JP1/Base health check function is operating normally on those hosts.

To report JP1/Base process errors to the manager host in a system that uses JP1/AJS, monitor the messages output to the syslog or event log by the health check function, and notify the manager host using JP1/Cm2/OAA and NNM.

The following describes remote host monitoring in a system that uses JP1/AJS, based on the following configuration example.

Figure 1-22: Example of remote host monitoring in a system that uses JP1/AJS



The hosts in this example have the following settings.

Host	Purpose	Setting for remote host monitoring
hostA	Manager host	Monitor hostX and hostY.
hostX	Agent host	Monitor hostA.
hostY	Agent host	None

The following processing is performed if an error occurs in the health check function at agent hostX or manager hostA.

Error in the health check function at hostX

The health check function at hostA detects the error and outputs a message to the syslog or event log. JP1/Cm2/OAA on hostA detects the output message and notifies NNM. A message about the problem at hostX appears in NNM.

Error in the health check function at hostA

The health check function at hostX detects the error and outputs a message to the syslog or event log. JP1/Cm2/OAA on hostX detects the output message and notifies NNM. A message about the problem at hostA appears in NNM.

(3) System operation with remote host monitoring

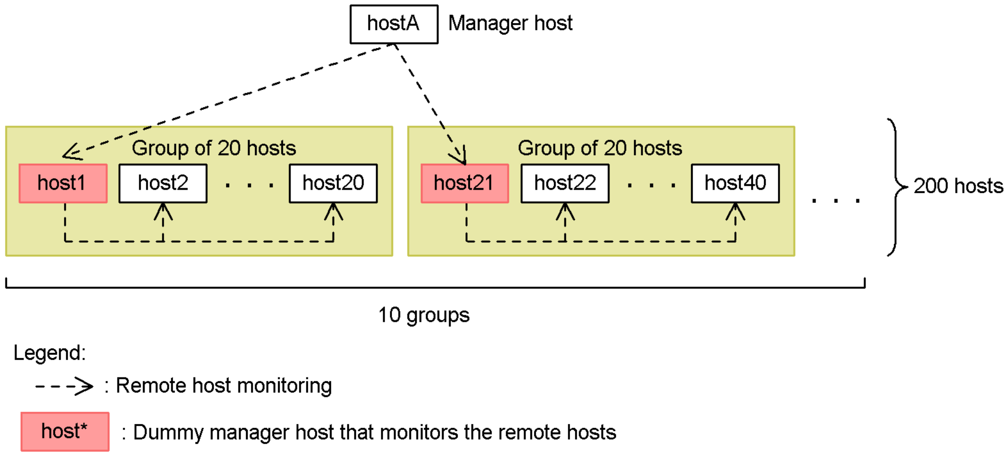
The following describes the system operation when monitoring remote hosts.

(a) Operation with a large number of monitored hosts

When two or more remote hosts are monitored from a single host, the health check function checks the status of the JP1/Base processes at each host in turn. It takes about 3 seconds at each host. This can take a long time if there are a large number of hosts to monitor.

For example, it would take 600 seconds for one host to check 200 remote hosts. You can reduce the monitoring time by splitting the target hosts into groups, and setting a dummy manager host for each group.

Figure 1-23: Example of monitoring 200 hosts

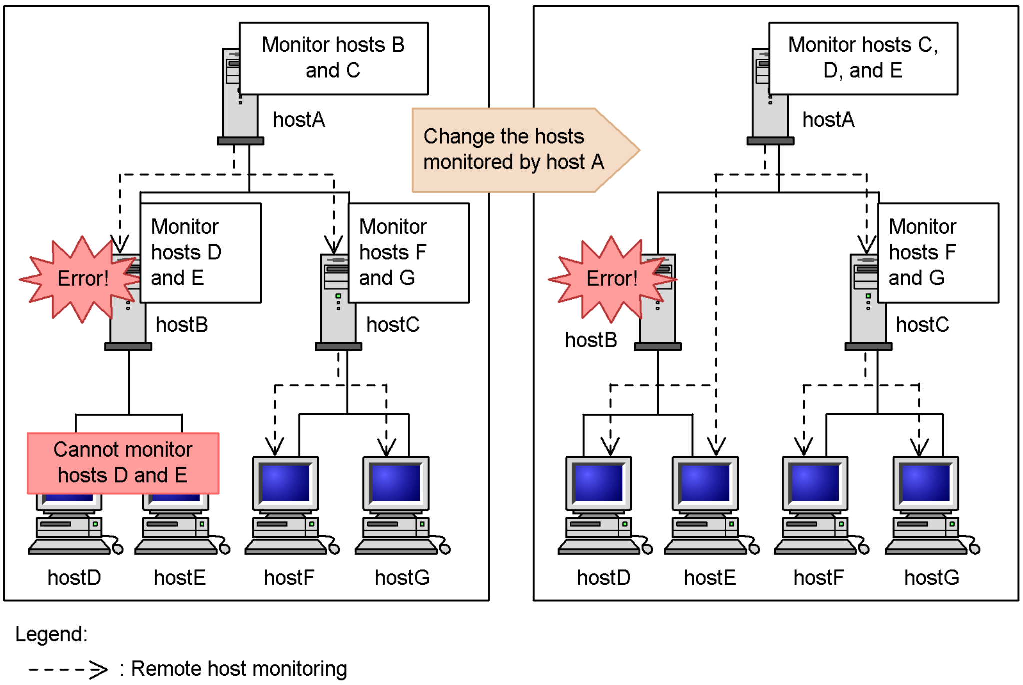


In this example, the target hosts are split into groups of 20 hosts each. Manager hostA monitors the dummy manager hosts (host1, host21, and so on). As monitoring is by group rather than by individual host, the monitoring time can be cut to about 60 seconds.

(b) Operation when errors occur in a hierarchical configuration

The following describes error handling when the target hosts are arranged in a hierarchy, as in the figure below.

Figure 1-24: Example of error handling in a hierarchical configuration



If an error occurs in the health check function or event service at hostB, errors at hostD and hostE being monitored by hostB cannot be detected or reported.

If hostB is restored quickly, any JP1 event issued because of an error at hostD or hostE while hostB was stopped will be forwarded when hostB retries the send operation at recovery. If hostB recovery takes a long time, you must change the settings in the health check definition file (`jbshc.conf`) so that hostD and hostE will be monitored directly by hostA until hostB is restored.

As illustrated in this example, in a hierarchical configuration, it is a good idea to prepare a health check definition file (`jbshc.conf`), specifying that the agent hosts are to be monitored directly from the manager host in the event of an error on the submanager host.

(c) Reviewing the monitoring interval

In the health check definition file (`jbshc.conf`), you can specify an interval for monitoring remote hosts. Perform a trial run before you start operations, and check whether the specified monitoring interval is appropriate. If message KAVA7219-W is output to the integrated trace log, the monitoring interval might be too short. Change the interval, referring to the estimate equation given in *Health check definition file* in

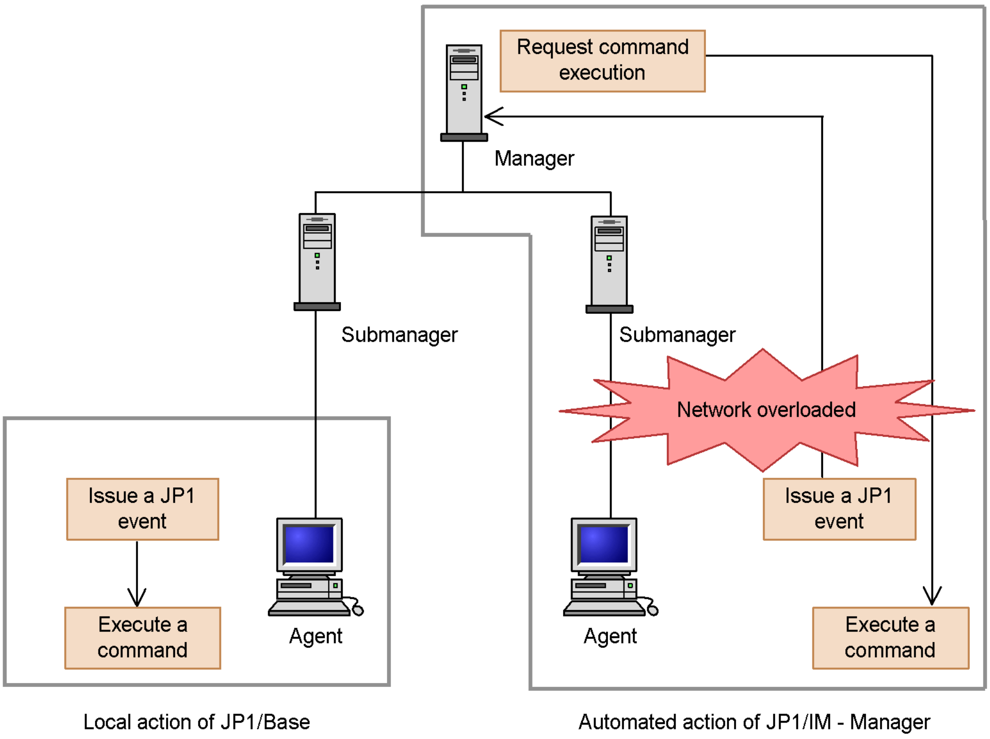
14. Definition Files.

1.8 Local action

If a JP1 event such as a failure notification is issued from an agent host, registered commands can be automatically executed from the agent host. This is called a *local action*. This functionality enables you to reduce the network load between managers and agents, and also enables you to execute commands even if an error occurs on the network between the managers and agents.

The following figure shows a comparison of JP1/Base local actions with JP1/IM - Manager automated actions.

Figure 1-25: Comparison of JP1/Base local actions with JP1/IM - Manager automated actions



To execute a local action, you must create a local action execution definition file and specify which commands to execute when a JP1 event is generated. If a JP1 event specified in the local action execution definition file is generated, JP1/Base executes the command or commands corresponding to the JP1 event.

The local action functionality also enables you to issue an action start event and action end event. Therefore, by forwarding those events to the manager host, you can check the execution or result of the local action at the manager host. The action execution log is also output to the local action execution log file.

The following subsections describe the local actions in detail.

1.8.1 Conditions for executing local actions

The conditions necessary for executing local actions are as follows:

- The version of JP1/Base running on the agent is 09-00.
- The system configuration has been defined in the JP1/IM configuration definition file and distributed to the hosts on which a local action is executed.

If the version of JP1/IM - Manager or JP1/Base running on a manager or submanager host is 09-00 and the IM configuration management functionality is used, you can define a local action execution definition file on the manager host and batch distribute it to each agent host. For details on managing definitions by using IM configuration management, see the *Job Management Partner 1/Integrated Management - Manager Overview and System Design Guide*.

1.8.2 Commands for local actions

The command formats that are available for local actions are listed below:

In Windows:

- Executable files (`.com` and `.exe`)
- Batch files (`.bat`)
- JP1/Script script files (`.spt`)

  (Note that the file association must be set to execute a `.spt` file.)

In UNIX:

- Commands for UNIX
- Shell scripts

Note that the following commands cannot be executed:

- Commands that require interactions with the user
- Commands that launch a window
- Commands that accompany an escape sequence or control code
- Commands that do not stop (such as a daemon)
- Commands that require the user to interact with the desktop (such as a Windows message mechanism or DDE)

- Commands that shut down the system (such as `shutdown` or `halt`)

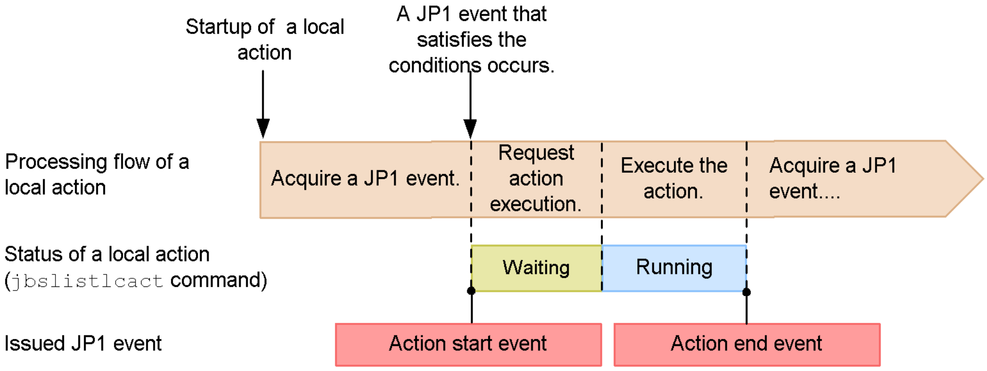
1.8.3 Execution status of local actions

A local action is set by default to start automatically when the system is started. If you start a local action, the JP1 events registered on the local host are acquired, and the JP1 event is compared to the conditions that have been specified in the local action execution definition file. If the acquired JP1 event matches the conditions, the corresponding command will be executed. Note that the JP1 event is compared to the conditions in the order in which they were defined in the local action execution definition file. In the local action execution definition file, you should define conditions in the order of priority.

You can check the execution status of local actions by using the `jbslistlcact` command. There are two types of execution statuses: "waiting" and "running". You can cancel the action in either of these statuses. The changes that the execution status goes through from the execution condition of the local action being satisfied to the completion of the executed action is notified by using JP1 events and the local action execution log file.

The following figure illustrates the execution status of local actions.

Figure 1-26: Changes to the execution status of local actions


Startup of a local action
A JP1 event that satisfies the conditions occurs.
Processing flow of a local action
Acquire a JP1 event.
Request action execution.
Execute the action.
Acquire a JP1 event....
Status of a local action (jbslistlcact command)
Waiting
Running
Issued JP1 event
Action start event
Action end event

You can control the number of local actions waiting or running by using the following functionalities.

(1) Preventing the same action from executing

Using this functionality, you can prevent the same action from executing multiple times over a set time period. This is useful for an action that is normally executed once only over a set time period (for example, when sending an email to the system administrator). While this functionality is enabled, the same action will not go to the waiting status, even if a condition is satisfied.

(2) Limiting the number of waiting actions

Using this functionality, you can specify a limit on the number of actions waiting. When the number of actions waiting exceeds the specified limit, any action goes to the waiting status, even if a condition is satisfied.

(3) Limiting the number of concurrently executing actions

Using this functionality, you can specify a limit on the number of actions that can be executed at the same time. The actions will be executed only when the number of actions being executing at the same time does not exceed the specified limit. When the limit is exceeded, the actions will go to the waiting status.

1.8.4 Pausing local actions

You can pause local actions, without stopping them. Even if you pause a local action, the execution of an action that was already waiting or running is not canceled. When local actions are paused, no JP1 events are acquired, and no more local actions go into the waiting status. When the local actions are unpaused, the system will acquire a JP1 event from the point at which the local actions were unpaused, and then execute the local actions.

1.9 Support for system configurations

The following describes JP1/Base support for various system configurations, such as a cluster system.

1.9.1 Using JP1/Base in a cluster system

JP1/Base supports cluster systems.

By using JP1/Base in a cluster system, a secondary server can take over job processing and continues operations, if the primary server fails.

For details, see *3. Setting Up JP1/Base for Use in a Cluster System*.

1.9.2 Using logical hosts in a non-cluster environment

Running JP1/Base on a logical host typically involves linking with cluster software in the cluster system. However, by allocating disk space and assigning an IP address to the logical host, you can set up and run JP1/Base in a logical host environment that is not linked to the cluster software and is not subject to failover.

For details, see *3.7 Setting up a logical host in a non-cluster environment*.

1.10 Communication protocols of JP1/Base

This section provides an overview of the communication protocols used by JP1/Base. The communication concepts described in this section and in *4. JP1/Base Communication Settings According to Network Configurations* also apply to products for which JP1/Base is a prerequisite.

JP1/Base supports two communication protocols: an appropriate protocol is automatically selected when you install JP1/Base or set up the logical host.

You might have to manually set up a communication protocol depending on the network configuration or operation method. For details on JP1/Base communication settings for different network configurations, see *4. JP1/Base Communication Settings According to Network Configurations*.

JP1/Base recognizes the host name when communicating with a host. When running on a physical host, JP1/Base recognizes, as the local host name, the host name returned by the `hostname` command. When running on a logical host, JP1/Base recognizes, as the local host name, the logical host name specified in the settings for the cluster system. Note, therefore, the following:

- Use one representative host name and avoid use of several alias names.
- JP1/Base does not operate properly if the IP address assigned to a host name cannot be resolved.
- You might not be able to start JP1/Base, log in from JP1/IM - View or JP1/AJS - View, or execute a job on JP1/AJS, if the `hosts` file or DNS settings are not correct.
- You must set up an environment that allows for both the conversion from a host name to an IP address and the conversion from an IP address to a host name. Setting the bi-directional conversion indicated above is necessary especially for resolving names on a DNS server (including Active Directory).

1.10.1 Recommended communication protocol

On JP1/Base, the following binding methods are recommended for communication:

When running JP1/Base on a physical host only: ANY binding method.

In the ANY binding method, JP1/Base performs communication using only the port number without recognizing an IP address. The communication wait process ensures that data sent to all IP addresses assigned to the host are received. When handling connections, you can send data to hosts on all subnets even if the host uses several subnets.

JP1/Base might not be able to communicate with hosts properly if it is activated using the ANY binding method in a cluster system. For example, a logical host might receive data addressed to a physical host, or vice versa.

When using a logical host (using a cluster):IP binding method

In the IP binding method, if the host uses several IP addresses when two or more IP addresses are assigned to one NIC (Network Interface Card) or one host has more than one NIC, JP1/Base receives only data addressed to a particular IP address. When handling connections, JP1/Base sends data via only an NIC that uses a particular IP address.

When JP1/Base runs in a cluster system, physical and logical hosts might coexist on a single host or two or more logical hosts might be started simultaneously. In such a case, the IP binding method ensures that physical hosts receive only data destined to their IP addresses, and logical hosts receive only data destined to their IP addresses.

By default, the ANY binding method is selected as the communication protocol. The IP-binding method is applied to both physical and logical hosts when you set up JP1/ Base for a cluster system as shown below:

In Windows, configure JP1/Base for the cluster system by using the GUI (`jp1bshasetup.exe`) or the command `jbs_setup_cluster`.

In UNIX, configure JP1/Base for the cluster system by using the command `jp1base_setup_cluster`.

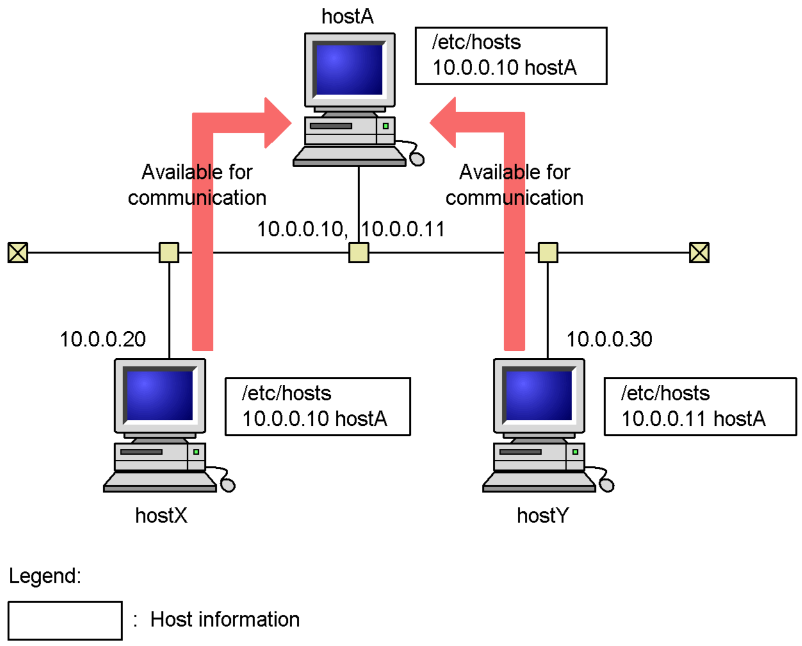
Note

Once a host is set up for a cluster system, the communication protocol of physical hosts does not return to the ANY binding method even when all logical hosts are removed. To restore operation using physical hosts only, modify the communication protocol back to the ANY binding method as described in *4.3.3 Changing communication settings*.

As an example, the illustrations below show how the communication waiting process changes when the JP1/Base communication protocol is the ANY or the IP binding method.

First, the following figure shows the communication waiting process when the communication protocol of JP1/Base is the ANY binding method.

Figure 1-27: Communication waiting process when JP1/Base is activated in the ANY binding method on hostA

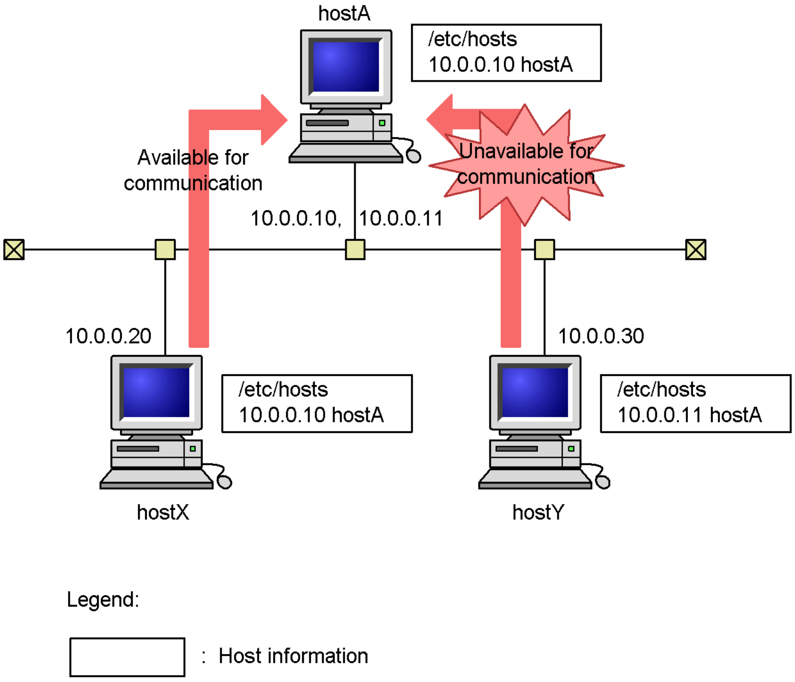


hostA has an NIC to which IP addresses `10.0.0.10` and `10.0.0.11` are assigned. This host is assumed to be able to resolve its own host name only into IP address `10.0.0.10`. (In fact, depending on the OS, the host might only be able to resolve one host name into one IP address.) hostX assumes that hostA is resolved by using IP address `10.0.0.10`, and hostY assumes that hostA is resolved by using IP address `10.0.0.11`.

When JP1/Base is activated in the ANY binding method on hostA, it can receive data from both hosts X and Y. In the ANY binding method, JP1/Base can receive data addressed to either 10.0.0.10 or 10.0.0.11 since it communicates with hosts by using only port numbers without considering IP addresses.

Next, the following figure shows the communication waiting process when the communication protocol of JP1/Base is the IP binding method.

Figure 1-28: Communication waiting process when JP1/Base is activated in the IP binding method on hostA



When JP1/Base is activated in the IP binding method on hostA, it receives only data addressed to `10.0.0.10`, and cannot recognize data addressed to `10.0.0.11`. This is because hostA does not accept data whose IP address is different from its own, even when the port numbers are the same.

1.10.2 Checking IP addresses corresponding to host names

You sometimes need to check which IP addresses can be used to resolve the host names that you want to use with JP1/Base. This is because the OS might not consider the IP address settings to be valid even when several IP addresses are assigned to one host name in the `hosts` file.

To check which IP addresses can be used to resolve the host names that you want to use with JP1/Base, use the following command:

`jp1ping` *host-name*

For details on this command, see the section for *jp1ping* in *13. Commands*.

1.11 JP1/Base compatibility

This section discusses the compatibility of JP1/Base Version 9 with the program products that can be linked with the JP1/Base event service functionality, and the compatibility between JP1/Base Version 9 and previous versions.

(1) Compatibility between JP1/Base and program products supported by event service functionality

JP1/Base Version 9 has upward compatibility and supports event transfer with the following program products that have event service functionality:

- JP1/AJS (Version 5 or earlier)
- JP1/SES (Version 5 or earlier)
- Program products that use JP1/SES protocol (JP1/OJE, for example)
- JP1/IM (Version 5 or earlier)

For details on the compatibility between JP1/Base Version 9 and these program products, see *J. Linking with Products That Use JP1/SES Events*.

(2) Compatibility with previous versions of JP1/Base

JP1/Base Version 9 is compatible with previous version of JP1/Base. However, note the following points.

(a) Using a secondary authentication server

Note the following if you are thinking of setting up a secondary authentication server and JP1/Base 06-00 exists in the same user authentication block.

If JP1/Base Version 6 is installed on a host that users log into from JP1/IM - View or JP1/AJS - View, or on a host in which users manage jobs (JP1/AJS - Manager):

> JP1/Base Version 6 supports only one destination authentication server. Therefore, if connection to the authentication server fails, the operation will fail. Any version of JP1/Base can be installed on the execution target host.

If JP1/Base version 06-51 or later is installed on a host that users log into from JP1/IM - View or JP1/AJS - View, or on a host in which users manage jobs (JP1/AJS - Manager):

> Any version of JP1/Base can be installed on the destination authentication server and execution target host.

(b) Changing the configuration definition from JP1/IM

If you change the configuration definition from JP1/IM, the forwarding settings file (`forward`) for the event service is reloaded dynamically in JP1/Base 06-51 or later, but not in JP1/Base 06-00. In JP1/Base 06-00, you must restart the event service manually.

(c) Migrating the command execution log when using JP1/IM

The storage format of the command execution log (ISAM) files has changed in Version 8. If you are using JP1/IM and want to preserve the command execution log (ISAM) after upgrading JP1/Base, make sure that you execute the `jcocmdconv` command before you recommence JP1/IM operation.

The `jcocmdconv` command migrates the command execution log (ISAM) files accumulated in a previous version of JP1/Base to the file format used in Version 8 or later. If you do not execute this command, you will not be able to access the command execution logs accumulated in Version 7 or earlier. During cluster operation, while the shared disk can be accessed, execute the `jcocmdconv` command once only (specifying the logical host) on either the primary or secondary node. For details on the `jcocmdconv` command, see *jcocmdconv* in *13. Commands*.

A command execution log is created only in JP1/Base on the manager host (on which JP1/IM is also installed).

(d) Setting up operating permissions granted to JP1 users for JP1/IM and JP1/AJS

JP1/IM 08-00 and JP1/AJS 08-00 now support operating permissions for JP1 users. You cannot use version 07-51 or earlier authentication servers to set up operating permissions for JP1 users.

(e) Collecting and distributing definitions for JP1/IM

To collect and distribute event service definitions, you must install JP1/Base Version 7 or later on both the source and destination hosts for collecting and distributing definitions.

(f) Using a shell script that references the return values of commands

In JP1/Base 06-71, return values of the following commands are altered:

- `jbsacllint`
- `jbsaclreload`
- `jbsadduser`
- `jbschgpasswd`
- `jbslistuser`
- `jbsrmuser`

If you use a shell script that references return values of the above commands in JP1/Base 06-51 or earlier, the shell script might not work properly in JP1/Base Version 7 or later. You must review how the command return values are used. For details on the command return values, see *13. Commands*.

Chapter

2. Installation and Setup

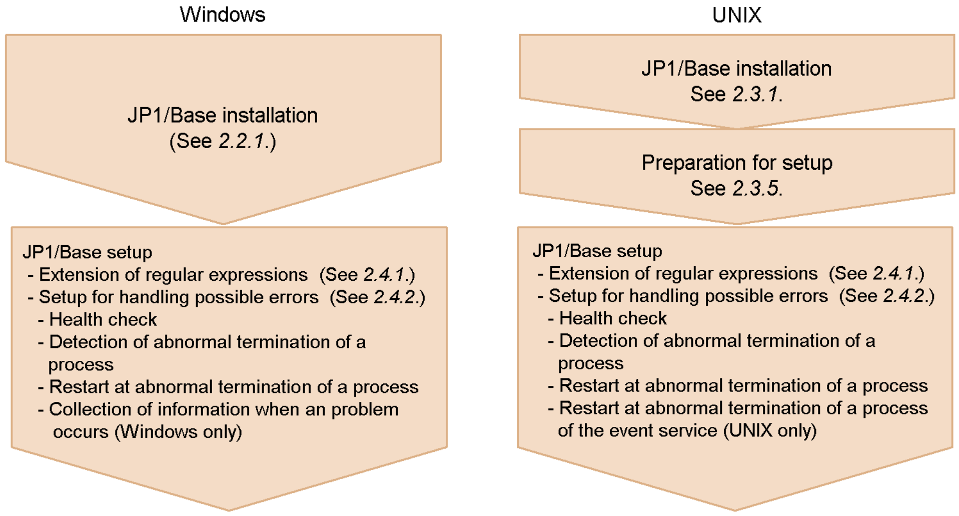
This chapter describes how to install, set up, back up, and recover JP1/Base.

2.1 Installation and setup overview

An overview of the process from installation to system operation is shown below.

Administrative permissions (in Windows) or superuser permissions (in UNIX) are required for installation and setup.

Figure 2-1: Installation and setup overview


Windows
JP1/Base installation
(See *2.2.1*.)
JP1/Base setup
- Extension of regular expressions (See *2.4.1*.)
- Setup for handling possible errors (See *2.4.2*.)
- Health check
- Detection of abnormal termination of a process
- Restart at abnormal termination of a process
- Collection of information when an problem occurs (Windows only)
UNIX
JP1/Base installation
See *2.3.1*.
Preparation for setup
See *2.3.5*.
JP1/Base setup
- Extension of regular expressions (See *2.4.1*.)
- Setup for handling possible errors (See *2.4.2*.)
- Health check
- Detection of abnormal termination of a process
- Restart at abnormal termination of a process
- Restart at abnormal termination of a process of the event service (UNIX only)

2.2 Installing JP1/Base (in Windows)

This section describes how to install and uninstall the Windows version of JP1/Base, and provides notes on these procedures.

2.2.1 Installing JP1/Base

To install JP1/Base:

1. Quit all programs.

   Be sure to quit all JP1 programs, and all programs that are currently accessing the JP1/Base event service, before you install JP1/Base.

2. Insert the supplied medium into the CD-ROM drive.

   Install JP1/Base as prompted by the Installer.

   During installation, set the following items:

   - User information
   - Installation folder
   - Automatic setup

     The Automatic Setup Selection window appears only when you perform a new installation of JP1/Base. If you select **Perform setup processing**, the installer automatically initializes JP1/Base so that it is ready for operation immediately after installation completes.

     The following items are set when you select automatic setup.

Table 2-1: User management defaults

Item		Contents
Authentication server settings	Authentication server name	Local host name
JP1 user settings	JP1 user name	jp1admin
	Password	jp1admin
	JP1 resource group	*
	Granted permissions	JP1_AJS_Admin, JP1_JPQ_Admin, JP1_AJSCF_Admin, JP1_PFM_Admin, JP1_Console_Admin, JP1_CF_Admin, JP1_CM_Admin, JP1_Rule_Admin, JP1_Audit_Admin, JP1_DM_Admin

Item		Contents
User mapping settings	OS user name and password	A window for entering the OS user name and password appears. Enter the OS user name and password.
	JP1 user name to be mapped	`jp1admin`
	`Server host name`	*
	Mapping between the JP1 user and OS user	The JP1 user (`jp1admin`) is mapped to the registered OS user.

If you choose not to perform automatic setup, only the JP1 user settings need to be entered.

For details on each item, see *6.1 User management setup (in Windows)*.

- Selecting a program folder

At execution, the Installer automatically installs the Hitachi Network Objectplaza Trace Library (HNTRLib2). The installation folder is *system-drive*`\Program Files\Hitachi\HNTRLib2\`.

This installation folder is fixed in the system drive. You cannot change the location.

3. Restart the system.

You must restart the system if you are installing JP1/Base for the first time.

Remote installation of JP1/Base (software deployment) through JP1/Software Distribution

JP1/Base supports remote installation through JP1/Software Distribution. JP1/Base allows you to perform the following types of installation:

- Installation of a new program

  You can install a new JP1/Base program in the target host. Remote installation using JP1/Software Distribution does not support automatic setup.

- Upgrade to a newer version

  You can upgrade an existing JP1/Base program to a newer version on the target host through remote installation.

For details on how to perform remote installation of JP1/Base through JP1/Software Distribution, see the manual *Job Management Partner 1/Software Distribution Administrator's Guide Volume 1*, for Windows systems.

2.2.2 Uninstalling JP1/Base

To uninstall JP1/Base:

1. Quit all programs.

   Before you uninstall JP1/Base, start the Control Panel and click **Services**, then shut down all services beginning with the words **JP1/Base**.

2. If you are using the SNMP trap converter, clear the SNMP trap converter setting.

   For details, see *I.2(5) Clearing the SNMP trap converter*.

3. Remove JP1/Base.

   In the Control Panel, click **Add/Remove Programs** and remove **JP1/Base**.

4. Restart the system.

   You must restart the system to disable the JP1/Base operating environment. Restart the system after completing steps 1 to 3.

5. Delete user files.#

   When you delete JP1/Base, the definition files and log files that were created after the installation are not deleted.

   To delete these files, delete the JP1/Base folder from Windows Explorer.

   #: Uninstalling JP1/Base causes HNTRLib2 to be uninstalled automatically. If the system contains other programs that use HNTRLib2, however, HNTRLib2 is not uninstalled until all of those programs are uninstalled.

2.2.3 Notes on installing and uninstalling JP1/Base

Note the following points when installing and uninstalling JP1/Base:

(1) Installation

- Do not install JP1/Base in a folder in which another program product is installed.
- If the JP1/Base installer displays a dialog box that asks you whether to replace the `msvcrt.dll` file, always choose **Restart** to replace the file and to restart the system after installing JP1/Base. If you choose **Ignore** to leave the old version of the `msvcrt.dll` file on the host, JP1/Base might not operate correctly (for example, the time of an event might be incorrect).

  If installation of another product causes JP1/Base to operate incorrectly, reinstall JP1/Base.
- After JP1/Base is installed, if you wish to install HNTRLib2 (provided by another program product) in a folder other than the default installation folder, you must first uninstall JP1/Base, delete the installation folder, and then reinstall JP1/Base.

(2) Re-installation

- If you are performing an overwrite installation of JP1/Base, be sure to shut down all services beginning with the words *JP1/Base*, and quit all programs currently accessing the JP1/Base event service.
- When uninstalling JP1/Base and then reinstalling it, you must first uninstall JP1/Base and all products that require it. Then, reinstall JP1/Base and then the products that require it.
  - JP1/IM - Manager

    Uninstall JP1/Base and then reinstall JP1/Base and JP1/IM - Manager. You do not need to uninstall JP1/IM - Manager.
  - JP1/AJS

    Uninstall both JP1/Base and JP1/AJS and then reinstall JP1/Base and JP1/AJS.
  - JP1/AJS2 for Mainframe

    Stop the services for JP1/AJS2 for Mainframe and then uninstall JP1/Base. Reinstall JP1/Base and then re-set up JP1/AJS2 for Mainframe.
  - JP1/Power Monitor

    Uninstall JP1/Power Monitor before uninstalling JP1/Base. Next, reinstall JP1/Base and JP1/Power Monitor.
- At a host running JP1/Base and JP1/IM - Manager, if you uninstall JP1/Base and then reinstall it in a folder that differs from the previous installation folder, JP1/IM - Manager will not operate correctly.

  If you want to reinstall JP1/Base in a different folder, first uninstall JP1/IM - Manager, delete its installation folder, and then reinstall JP1/IM - Manager.
- If you are using the SNMP trap converter, execute the `imevtgw_setup` command after reinstalling JP1/Base.

(3) Uninstallation

- Uninstalling JP1/Base deletes the definition files shared with other JP1 products, thereby disabling these programs.
- If you uninstall only JP1/AJS after JP1/AJS and JP1/Base are installed, the event service might not start up. In this case, you should remove the `include ajs-conf` parameter lines or change them to comments (add `#` to the beginning of the lines) in the event server settings file (`conf`).
- The following installer log file is created. Delete this log file after the installation ends normally.

Windows-installation-folder`\Temp\HITACHI_JP1_INST_LOG\jp1base_inst{1|2|3|4|5}.log`

(4) Setting the Windows environment

At JP1/Base installation, the path of the JP1/Base `bin` folder and the path of Hitachi Network Objectplaza Trace Library (HNTRLib2) are set as system environment variables (`Path`). The path of HNTRLib2 is the Hitachi common folder (*system-drive*`\Program files\Common Files\HITACHI`). In addition, the port numbers listed in *C. List of Port Numbers* are set in the `services` file. The path of the JP1/Base `bin` folder set in the system environment variable (`Path` variable) and the port number set in the `services` file are deleted when you uninstall JP1/Base. The service name `jp1imcmda` is not deleted if JP1/IM - View is installed. Manually delete any settings that remain in the system if no longer needed. However, take care not to delete the service name `jp1imcmda` if JP1/IM-View is installed. Note also that the path of the Hitachi common folder is used for products other than Hitachi Network Objectplaza Trace Library (HNTRLib2).

(5) Overwrite installation

Note the following points if you are installing JP1/Base in an environment running an earlier version of a JP1 program:

- If you wish to install JP1/Base on a host that runs either JP1/IM or JP1/IM - Agent (pre-Version 6 programs), you must set the following services to manual mode before you install JP1/Base:
  - JP1/IM Agent
  - JP1/IM Control Service
  - JP1/IM Event
  - JP1/IM Rmiregistry
- Installing JP1/Base disables the event service supported by the pre-Version 6 programs JP1/IM -Agent and JP1/IM. To launch the Version 5 event service, execute the following command:
  `jevmkcompat -u`

  After executing the above command, execute the following command to restart the JP1/Base event service. Some programs cannot send events to the JP1/Base event service unless this command is executed:
  `jevmkcompat -i`

  After installing or uninstalling JP1/IM - Agent or JP1/IM Version 5 on a host running JP1/Base, you must also execute the following command:
  `jevmkcompat -i`
- To start the JP1/Base event service and use the pre-Version 6 JP1/SES

functionality after installing JP1/Base, execute the following command:
`jevmkcompat -r`

To start the JP1/SES event service and return to the JP1/SES environment, execute the following command:
`jevmkcompat -u`

- You cannot install JP1/Base Version 7 or later on a host running Version 6 of JP1/IM - Central Console or JP1/AJS.
- If you install JP1/Base Version 7 or later by overwriting an earlier version of JP1/Base, HNTRLib2 will be installed without removing HNTRLib. If HNTRLib is no longer needed, uninstall it after making sure that it is not being accessed by any programs.
- If JP1/Base version 07-00 or earlier is being used in a cluster system and you perform an overwrite installation of 07-51 or later, you must complete the following tasks to upgrade the logical host environment.

1. Modify the settings to enable startup of the processes added with version 07-00 or a later version.

Modify the settings file as follows:

1-1 Back up the following files:

shared-folder`\jp1base\conf\jp1bs_spmd.conf`

shared-folder`\jp1base\conf\jp1bs_spmd.conf.session`

shared-folder`\jp1base\conf\jp1bs_spmd.conf.original`

shared-folder`\jp1base\conf\jp1bs_service_0700.conf`

1-2 Modify the following files so that the processes added in Version 7 or a later version will start.

shared-folder`\jp1base\conf\jp1bs_spmd.conf`

shared-folder`\jp1base\conf\jp1bs_spmd.conf.session`

shared-folder`\jp1base\conf\jp1bs_spmd.conf.original`

Open these files in a text editor or other program, and add the following lines to the end of each file.

If you are using JP1/Base version 07-00, add only `jbshcd` and `jbshchostd`.

`jbsplugin|`*C:\Program Files\HITACHI*`\JP1Base\bin\jbsplugind.exe|||60|`

`jbshcd|`*C:\Program*

Files\HITACHI\JP1Base\bin\jbshcd.exe|||60|

jbshchostd|*C:\Program Files\HITACHI*\JP1Base\bin\jbshchostd.exe|||60|

The part in italics is the installation folder. The lines to be added are written in the file \conf\jp1bs_spmd.conf.original in the installation folder. Copy the required lines from this file to the files you are modifying.

1-3 Modify the following file so that the processes added in version 07-51 or later will start.

If this file does not exist, it will be created automatically when the JP1/Base service starts. You do not need to create it manually.

shared-folder\jp1base\conf\jp1bs_service_0700.conf

Open this file in a text editor or other program, and add the following lines to the end of the file:

jbshcd|*C:\Program Files\HITACHI*\JP1Base\bin\jbshcd.exe||0|3|3|21600|

jbshchostd|*C:\Program Files\HITACHI*\JP1Base\bin\jbshchostd.exe||0|3|3|21600|

The part in italics is the installation folder. The line to be added is written in the file \conf\jp1bs_service_0700.conf in the installation folder. Copy the required lines from this file to the files you are modifying.

2. Copy the definition files added in Version 7 or later.

Copy the definition files as follows:

2-1 Create a folder named plugin in *shared-folder*\jp1base\conf\.

2-2 Copy the *installation-folder*\conf\plugin\reqforward.conf file to *shared-folder*\jp1base\conf\plugin.

2-3 Copy the *installation-folder*\conf\user_acl\JP1_AccessLevel file to *shared-folder*\jp1base\conf\user_acl\.

2-4 Create a folder named jbshc in *shared-folder*\jp1base\conf\.

2-5 Copy the files in *installation-folder*\conf\jbshc\ to *shared-folder*\jp1base\conf\jbshc\.

2-6 Create a folder named jbslcact in *shared-folder*\jp1base\conf\.

2-7 Copy the files in *installation-folder*\conf\jbslcact\ to *shared-folder*\jp1base\conf\jbslcact\.

2-8 Create a folder named jbsdfts in *shared-folder*\jp1base\conf\.

2-9 Copy the files in *installation-folder*`\conf\jbsdfts\` to *shared-folder*`\jp1base\conf\jbsdfts\`.

3. Add the common definition information added in Version 7 or later.

Modify the settings file as follows:

3-1 Back up the common definition information.

Execute the following command:

`jbsgetcnf -h` *logical-host-name* `>` *backup-file-name*

3-2 Prepare common definition information to be added to the logical host.

Copy the following files to the temporary directory.

If you are using JP1/Base version 07-00, copy `jcocmd0710.conf` and `jbshc_com.conf`.

installation-folder`\default\base_plugin.conf`

installation-folder`\default\jcocmd0700.conf`

installation-folder`\default\jcocmd0710.conf`

installation-folder`\default\jbsspm070.conf`

installation-folder`\conf\jp1bs_param_V7.conf`

installation-folder`\default\jbshc_com.conf`

installation-folder`\conf\jbscom_default.conf`

installation-folder`\conf\jbslcact_default.conf`

installation-folder`\conf\jbssrvmgr.conf`

3-3 Create common definition information for the logical host by modifying the copied files using a text editor or other program.

Replace all the occurrences of `JP1_DEFAULT` in the files with *logical-host-name*. Re-name each file as *file-name*`.conf`.

3-4 Set up the modified files as common definition information for the logical host.

Execute the following command for each file to add common definition information:

`jbssetcnf` *file-name*

This completes the upgrading of the logical host.

- The storage format of the command execution log (ISAM) files has changed in Version 8. If you are using JP1/IM and you upgraded to JP1/Base Version 8 by overwriting JP1/Base 07-51 or earlier, make sure that you execute the `jcocmdconv` command before you recommence JP1/IM operation.

The `jcocmdconv` command migrates the command execution log (ISAM) files accumulated in a previous version of JP1/Base to the file format used in Version 8. If you do not execute this command, you will not be able to access the command execution logs accumulated in Version 7 or earlier. During cluster operation, while the shared disk can be accessed, execute the `jcocmdconv` command once only (specifying the logical host) on either the primary or secondary node.

For details on the `jcocmdconv` command, see *jcocmdconv* in *13. Commands*.

A command execution log is created only in JP1/Base on the manager host (on which JP1/IM is also installed).

- In Version 9, the `save-rep` flag has been added to the `options` parameter in the event server settings file (`conf`). Setting this flag saves the duplication prevention table of the event database into the file. If this flag is not set, the duplication prevention table is saved to memory. In this case, if the event server is restarted, the table is deleted, and then re-created, causing the database to take longer to receive JP1 events forwarded from other hosts. We recommend that you set the `save-rep` flag for the event server that receives JP1 events forwarded from other hosts.

  If you perform an overwrite installation from JP1/Base 08-00 or earlier, this flag will not be set. In this case, you must perform the following procedure to create the duplication prevention table in the file.

To create this table in the file:

1. Add the `save-rep` flag to the `options` parameter in the event server settings file.

   For details on the event server settings file, see *Event server settings file* in *14. Definition Files*.

2. Execute the `jevdbmkrep` command.

   For details on the `jevdbmkrep` command, see *jevdbmkrep* in *13. Commands*.

3. Start the event server.

2.3 Installing JP1/Base (in UNIX)

This section describes how to install and uninstall the UNIX version of JP1/Base. It provides notes on these procedures, and explains the pre-setup tasks you need to perform.

2.3.1 Installing JP1/Base

To install JP1/Base:

1. Quit all programs.

   Be sure to quit all JP1 programs, and all programs that are currently accessing the JP1/Base event service, before you install JP1/Base.

2. Run the Hitachi Program Product Installer.

   Install JP1/Base as prompted by the Hitachi Program Product Installer. For the operation steps, see *2.3.2 Using the Hitachi Program Product Installer*.

   For a new installation, the Installer sets up and initializes JP1/Base automatically so that JP1/Base is ready for operation immediately after installation completes.

   The following items are set when you select automatic setup:

   Table 2-2: User management defaults

Item		Contents
Authentication server settings	Authentication server name	Local host name
JP1 user settings	JP1 user name	jp1admin
	Password	jp1admin
	JP1 resource group	*
	Granted permissions	JP1_AJS_Admin, JP1_JPQ_Admin, JP1_AJSCF_Admin, JP1_PFM_Admin, JP1_Console_Admin, JP1_CM_Admin, JP1_Rule_Admin, JP1_Audit_Admin, JP1_DM_Admin
User mapping settings	JP1 user name to be mapped	jp1admin
	Name of the server host where the JP1 user issues operating instruction	*

Item		Contents
	Mapping between the JP1 user and OS user	The JP1 user (`jp1admin`) is mapped to an OS user (`root`) registered with each host.

For details on each item, see *6.3 User management setup (in UNIX)*.

At execution, the Hitachi Program Products Installer automatically installs the Hitachi Network Objectplaza Trace Library (HNTRLib2). The installation folder is `/opt/hitachi/HNTRLib2/`.

Remote installation of JP1/Base (software deployment) through JP1/Software Distribution:

JP1/Base supports remote installation through JP1/Software Distribution. JP1/Base allows you to perform the following types of installation:

- Installation of a new program

  You can install a new JP1/Base program in the target host. Remote installation using JP1/Software Distribution does not support automatic setup.

- Upgrade to a newer version

  You can upgrade an existing JP1/Base program to a newer version on the target host through remote installation.

For details on how to perform an actual remote installation by using JP1/Software Distribution, see the manual *Job Management Partner 1/Software Distribution Manager Description* and *Administrator's Guide*, *Job Management Partner 1/Software Distribution SubManager Description and Administrator's Guide (for UNIX systems)*, and *Job Management Partner 1/Software Distribution Client Description and User's Guide (for UNIX systems)*.

2.3.2 Using the Hitachi Program Product Installer

The Hitachi Program Product Installer is stored on the medium supplied with JP1/Base. This section describes the following operations:

- Starting the Hitachi Program Product Installer
- Installing JP1/Base with the Hitachi Program Product Installer
- Deleting JP1/Base with the Hitachi Program Product Installer
- Checking the version of installed Hitachi program products with the Hitachi Program Product Installer

Notes on using the Hitachi Program Product Installer

Superuser permissions are required to use the Hitachi Program Product Installer.

Log in as the superuser, or execute the `su` command to change your user account to the superuser.

(1) Starting the Hitachi Program Product Installer

To install JP1/Base from the supplied magnetic tape:

1. Mount the JP1/Base tape in the tape unit.
2. Execute the following command to extract the Hitachi Program Product Installer:

   `tar xf` *device-file-name*

3. Execute the following command to start the Hitachi Program Product Installer:

   `/etc/hitachi_setup -i` *device-file-name*

To install JP1/Base from the supplied CD-ROM:

1. Insert the JP1/Base CD-ROM into the drive.
2. Mount the CD-ROM drive.

   Execute the command as follows: The command that you can use differs according to your OS. This step is unnecessary for a Solaris system.

   Command for HP-UX: `/usr/sbin/mount -F cdfs -r` *device-special-file-name*`/cdrom`

   Command for AIX: `/usr/sbin/mount -r -v cdrfs /dev/cd0 /cdrom`

   Note: The words in italics differ depending on your operating environment.

3. Execute the following command to install and start the Hitachi Program Product Installer:

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

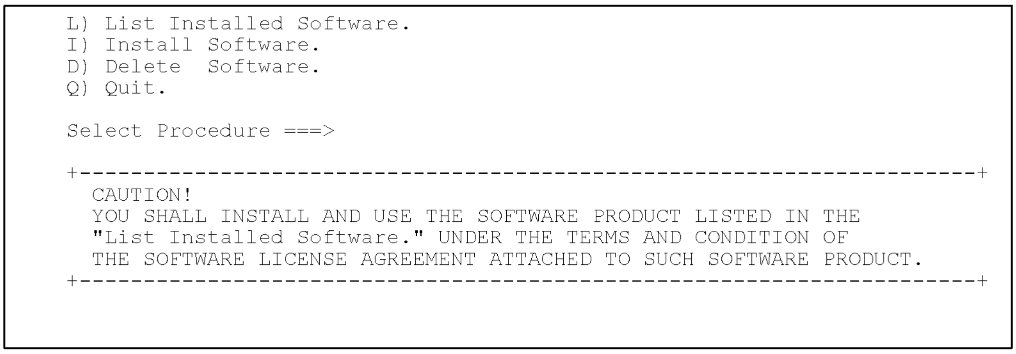
   XXXX differs depending on your operating environment.

   For an HP-UX system, change `setup` to upper-case `SETUP`. For Solaris, the CD-ROM drive is mounted automatically. Specify the device special file name for the automatically mounted drive for *device-special-file-name*`/cdrom`.

(2) Installing JP1/Base

The following explains how to install JP1/Base with the Hitachi Program Product Installer. The initial window appears when you start the Installer. An example is shown in the following figure.

Figure 2-2: Example of the Hitachi Program Product Installer initial window



```
L) List Installed Software.
I) Install Software.
D) Delete  Software.
Q) Quit.

Select Procedure ===>

+----------------------------------------------------------------------+
  CAUTION!
  YOU SHALL INSTALL AND USE THE SOFTWARE PRODUCT LISTED IN THE
  "List Installed Software." UNDER THE TERMS AND CONDITION OF
  THE SOFTWARE LICENSE AGREEMENT ATTACHED TO SUCH SOFTWARE PRODUCT.
+----------------------------------------------------------------------+
```

Enter `I` in this window to see a list of the software that you can install. Move the cursor to **JP1/Base**, then press the space bar to select that item. Enter `I` again to install JP1/Base. When you finish the installation, enter `Q` to return to the initial window.

(3) Deleting JP1/Base

Execute the following command to start the Hitachi Program Product Installer:
`/etc/hitachi_setup`

The initial Installer window appears. For an example, see Figure 2-2.

Enter `D` in this window to see a list of the installed software that can be deleted. Move the cursor to **JP1/Base**, then press the space bar to select that item. Enter `D` again to delete JP1/Base. When you finish deleting software, enter `Q` to return to the initial window.

(4) Displaying version information

Execute the following command to start the Hitachi Program Product Installer:
`/etc/hitachi_setup`

The initial Installer window appears. For an example, see Figure 2-2.

Enter `L` in this window to see a list of the installed Hitachi program products.

2.3.3 Uninstalling JP1/Base

To uninstall JP1/Base:

1. Quit all programs.

   Be sure to quit all JP1 programs. Also, quit all programs that are currently accessing the event service.

   If you are using JP1/AJS - Manager, stop the JP1/AJS - Monitor service.

2. If you are using the SNMP trap converter, clear the SNMP trap converter setting.

For details, see *I.2(5) Clearing the SNMP trap converter*.

3. Run the Hitachi Program Product Installer.

   Uninstall JP1/Base as prompted by the Hitachi Program Product Installer. All user files in the JP1/Base installation directory will be deleted at uninstallation. Therefore, be sure to back up required files first.

Note

Uninstalling JP1/Base causes HNTRLib2 to be uninstalled automatically. If the system contains other programs that use HNTRLib2, however, HNTRLib2 is not uninstalled until all of those programs are uninstalled.

2.3.4 Notes on installing and uninstalling JP1/Base

Note the following points when installing and uninstalling JP1/Base:

(1) Installation

- If you see a message stating that installation failed while using the Hitachi Program Product Installer, check the `/etc/.hitachi/.hitachi.log` file. We recommend that you back up this file as required because this file is overwritten every time you start the Hitachi Program Product Installer.

  The installation log is output to the `/var/opt/jp1base/log/JBS_SETUP` directory. Check the installation log.

- If you are installing JP1/Base in a Solaris non-global zone, use a version that supports the non-global zone (09-00 or later) for all JP1/Base instances on the same device.

(2) Re-installation

- If you are reinstalling JP1/Base over the existing JP1/Base program, be sure to quit JP1/Base and all JP1 programs, and quit all programs currently accessing the JP1/Base event service.

  If you are using JP1/AJS - Manager, stop the JP1/AJS - Monitor service.

- When you overwrite an existing JP1/Base program with a newer version, the Hitachi Network Objectplaza Trace Library (HNTRLib2) is disabled. You cannot collect information with the integrated trace log even when you run JP1/Base. When JP1/Base is overwritten, you should use the `ps` command to check that the Hitachi Network Objectplaza Trace Library (HNTRLib2) is activated (it is activated if the `hntr2mon` process is running). If not, use the `hntr2mon` command to run it. For details on the `hntr2mon` command, see *hntr2mon (UNIX only)* in *13. Commands*.

- When uninstalling JP1/Base and then reinstalling it, you must first uninstall JP1/Base and all products that require it. Then, reinstall JP1/Base and then the products that require it.

- JP1/IM - Manager

  Reinstall JP1/Base and then re-set up JP1/Base and JP1/IM - Manager.

- JP1/AJS

  Reinstall JP1/Base and then re-set up JP1/Base and JP1/AJS.

- JP1/AJS2 for Mainframe

  Uninstall both JP1/Base and JP1/AJS2 for Mainframe and then reinstall JP1/Base and JP1/AJS2 for Mainframe. Next, re-set up JP1/Base and JP1/AJS2 for Mainframe.

- JP1/Power Monitor

  Reinstall JP1/Base and then re-set up JP1/Base and JP1/Power Monitor. However, you do not need to set up JP1/Power Monitor again, if you have not set up a logical host or linkage with JP1/AJS.

- If you are using the SNMP trap converter, execute the `imevtgw_setup` command after reinstalling JP1/Base.

(3) Uninstallation

After uninstalling JP1/Base, check whether the following directories still exist and delete them if so:

- `/etc/opt/jp1base`
- `/opt/jp1base`
- `/var/opt/jp1base`

The following installer log file is created. Delete this log file after the installation ends normally.

`/tmp/HITACHI_JP1_INST_LOG/jp1base_inst{1|2|3|4|5}.log`

(4) Setting the OS environment

At JP1/Base installation, the port numbers listed in *C. List of Port Numbers* are set in the `/etc/services` file. This setting information is deleted when JP1/Base is uninstalled. However, the service name `jesrd` is not deleted. You must delete these settings manually when they are no longer needed.

(5) Overwrite installation

Note the following points if you are installing JP1/Base in an environment running an earlier version of a JP1 program:

- Installing JP1/Base disables the Version 5 event service. To launch the Version 5 event service, execute the following command:

```
jevmkcompat -r
```

After executing the above command, execute the following command to restart the JP1/Base event service. Some programs cannot send events to the JP1/Base event service unless this command is executed:

```
jevmkcompat -u
```

- To install or uninstall the JP1/IM Version 5 on a host running JP1/Base, execute the following command after installing or uninstalling JP1/IM:
  ```
  jevmkcompat -u
  ```
- You cannot install JP1/Base Version 7 or later on a host running Version 6 of JP1/IM - Central Console or JP1/AJS.
- If JP1/Base version 07-00 or earlier is being used in a cluster system and you perform an overwrite installation of 07-51 or later, you must complete the following tasks to upgrade the logical host environment.

1. Modify the settings to enable startup of the processes added with version 07-00 or a later version.

Modify the settings file as follows:

When starting the authentication server on the logical host:

```
cp -p /etc/opt/jp1base/conf/
jp1bs_spmd.conf.session.model shared-directory/jp1base/
conf/jp1bs_spmd.conf
```

```
cp -p /etc/opt/jp1base/conf/
jp1bs_service_0700.conf.model shared-directory/jp1base/
conf/jp1bs_service_0700.conf
```

When not starting the authentication server on the logical host:

```
cp -p /etc/opt/jp1base/conf/jp1bs_spmd.conf.model
shared-directory/jp1base/conf/jp1bs_spmd.conf
```

```
cp -p /etc/opt/jp1base/conf/
jp1bs_service_0700.conf.model shared-directory/jp1base/
conf/jp1bs_service_0700.conf
```

2. Copy the definition files added in Version 7 or later.

Copy the definition files as follows:

2-1 Create a directory named `plugin` in *shared-directory*`/jp1base/conf/`.

2-2 Copy `/etc/opt/jp1base/conf/plugin/reqforward.conf` to *shared-directory*`/jp1base/conf/plugin`.

2-3 Copy `/etc/opt/jp1base/conf/user_acl/JP1_AccessLevel` to *shared-directory*`/jp1base/conf/user_acl/`.

2-4 Create a directory named `jbshc` in *shared-directory*`/jp1base/conf/`.

2-5 Copy the files in `/etc/opt/jp1base/conf/jbshc/` to *shared-directory*`/jp1base/conf/jbshc/`.

2-6 Copy the files in `/etc/opt/jp1base/conf/jbslcact/` to *shared-directory*`/jp1base/conf/jbslcact/`.

2-7 Copy the files in `/etc/opt/jp1base/conf/jbsdfts/` to *shared-directory*`/jp1base/conf/jbsdfts/`.

3. Add the common definition information added with Version 7 or later.

Modify the settings file as follows:

3-1 Back up the common definition information.

Execute the following command:

`jbsgetcnf -h` *logical-host-name* `>` *backup-file-name*

3-2 Prepare common definition information to be added to the logical host.

Copy the following files to the temporary directory.

If you are using JP1/Base Version 7, copy `jcocmd0710.conf.model` and `jbshc_com.conf.model`.

```
/etc/opt/jp1base/default/base_plugin.conf.model

/etc/opt/jp1base/default/jcocmd0700.conf.model

/etc/opt/jp1base/default/jcocmd0710.conf.model

/etc/opt/jp1base/default/jbsspm070.conf.model

/etc/opt/jp1base/conf/jp1bs_param_V7.conf.model

/etc/opt/jp1base/default/jbshc_com.conf.model

/etc/opt/jp1base/default/jbscom_default.conf.model

/etc/opt/jp1base/default/jbslcact_default.conf.model

/etc/opt/jp1base/default/jbssrvmgr.conf.model
```

3-3 Create common definition information for the logical host by modifying the copied files using a text editor or other program.

Replace all the occurrences of `JP1_DEFAULT` in the files with *logical-host-name*. Re-name each file as *file-name*`.conf`.

3-4 Set up the modified files as common definition information for the logical host.

Execute the following command for each file to add common definition information:

```
jbssetcnf file-name
```

This completes the upgrading of the logical host.

- The storage format of the command execution log (ISAM) files has changed in Version 8. If you are using JP1/IM and you upgraded to JP1/Base Version 8 by overwriting JP1/Base 07-51 or earlier, make sure that you execute the `jcocmdconv` command before you recommence JP1/IM operation.

  The `jcocmdconv` command migrates the command execution log (ISAM) files accumulated in a previous version of JP1/Base to the file format used in Version 8. If you do not execute this command, you will not be able to access the command execution logs accumulated in Version 7 or earlier. During cluster operation, while the shared disk can be accessed, execute the `jcocmdconv` command once only (specifying the logical host) on either the primary or secondary node.

  For details on the `jcocmdconv` command, see *jcocmdconv* in *13. Commands*.

  A command execution log is created only in JP1/Base on the manager host (on which JP1/IM is also installed).

- In Version 9, the `save-rep` flag has been added to the `options` parameter in the event server settings file (`conf`). Setting this flag saves the duplication prevention table of the event database into the file. If this flag is not set, the duplication prevention table is saved to memory. In this case, if the event server is restarted, the table is deleted, and then re-created, causing the database to take longer to receive JP1 events forwarded from other hosts. We recommend that you set the `save-rep` flag for the event server that receives JP1 events forwarded from other hosts.

  If you perform an overwrite installation from JP1/Base 08-00 and earlier, this flag will not be set. In this case, you must perform the following procedure to create the duplication prevention table in the file.

To create this table in the file:

1. Add the `save-rep` flag to the `options` parameter in the event server settings file.

   For details on the event server settings file, see *Event server settings file* in *14. Definition Files*.

2. Execute the `jevdbmkrep` command.

   For details on the `jevdbmkrep` command, see *jevdbmkrep* in *13. Commands*.

3. Start the event server.

2.3.5 Pre-setup tasks

On a UNIX system, you must complete the following pre-setup task after installing JP1/Base:

- ■ Adjust the kernel parameters

(1) Adjusting the kernel parameters

Adjust the kernel parameters and allocate the resources required to run JP1/Base. The kernel parameters to be adjusted differ according to the OS. For details, see *G. List of Kernel Parameters*.

A kernel parameter is a setting for adjusting and optimizing a resource used by the UNIX system. Adjust the following values on your system:

- File system: Maximum number of files that can be opened, and maximum number of files that can be locked
- Shared memory: Maximum size of a shared memory segment, and maximum number of shared memory segments
- Semaphores: Maximum number of semaphores, and maximum number of undo structures

For further information about kernel parameters, see your OS and UNIX documentation.

2.4 JP1/Base setup

This section describes how to set the operating environment for JP1/Base.

2.4.1 Extending regular expressions to be used

JP1/Base supports regular expressions in filter conditions for forwarding JP1 events to higher-level hosts or converting Windows event logs and application logs to JP1 events.

By default, you can use the following regular expressions:

Table 2-3: Regular expressions supported by default

OS	Supported regular expressions
Windows	JP1-specific regular expressions
UNIX	Basic regular expressions provided by each OS

The following programs and definition files for JP1/Base support regular expressions:

- Event filters specified in the forwarding settings file (`forward`)
- Filters specified in the action definition file for event log traps (`ntevent.conf`) and the action definition file for log file trapping
- Filter file used for the `jevexport` command
- Event filters specified in the local action execution definition file
- Search for JP1 events from JP1/IM - View[#1]
- Event filters for the function for acquiring JP1 events from the JP1/Base event server (`JevGetOpen`)[#2]
- Event filters for the extended attributes mapping settings file

#1: When you search for JP1 events from JP1/IM - View, the settings of regular expressions for JP1/Base on the searched host apply.

#2: For details, see the manual *Job Management Partner 1/Base Function Reference*.

JP1/Base Version 7 and later versions allow you to extend the default regular expressions. By extending regular expressions, you can use common regular expressions for Windows and UNIX. The following table lists available regular expressions:

Table 2-4: Regular expressions available when extended

OS	Supported regular expressions
Windows	Complies with the syntax for XPG4 extended regular expressions.
UNIX	Complies with the syntax for XPG4 extended regular expressions. The syntax differs depending on the OS. For details, see the syntax of each regular expression (regexp or regex).

For the syntax and examples for frequently used regular expressions, see *F. Syntax of Regular Expressions*. Use them as reference for using regular expressions.

(1) Setup

The following describes the procedure for extending regular expressions. If you are using a cluster system, perform the following for both primary and secondary nodes.

To extend regular expressions:

1. Create a definition file with any name.

   Enter the following lines in the definition file:

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

   When using JP1/Base in a cluster system, specify the logical host name for `JP1_DEFAULT` in `[JP1_DEFAULT\JP1BASE\]`.

2. Execute the `jbssetcnf` command.

   `jbssetcnf` *definition-file-name*

   The settings are reflected in the common definition information.

To restore the default regular expressions, you can use the same procedure. In that case, enter the following in the definition file:

```
[JP1_DEFAULT\JP1BASE\]
"REGEXP"=""
```

(2) When the setting takes effect

The following table shows when the setting of regular expressions takes effect for JP1/Base facilities that support them:

Function	When the setting takes effect
Forwarding JP1 events	When the event service is started.

Function	When the setting takes effect
`jevexport` command	When the `jevexport` command is executed.
Local action	When the local action function is started.
Search for events from JP1/IM - View	When the event service is started on the target event server.
Function for acquiring JP1 events from the JP1/Base event server (`JevGetOpen`)	When the event service is started on the target event server.
Event log trapping	When the event-log trapping service is started. Complies with the setting on the physical host.
Log file trapping	When the log-file trap management service is started. The same as the setting on the physical host.
Converting JP1/SES events	When the event service is started.

2.4.2 Setup for handling possible errors in JP1/Base

JP1/Base provides the following features to minimize the effects of a failure in JP1/Base on system operations based on JP1/IM or JP1/AJS:

- Health check

  The function can detect hangups (infinite loops or deadlocks) or abnormal termination (other than forced termination) of processes such as process management, the event service, and event conversion.

- Detection of errors by the process management function

  The service can detect abnormal termination of a process managed by the process management service and switching of the authentication server.

- Restart when a process abnormally terminates

  JP1/Base restarts automatically if an error occurs in a process managed by the process management service.

- Restart the event service when a process abnormally terminates (UNIX only)

  JP1/Base restarts automatically if an error occurs in an event service process on the physical host.

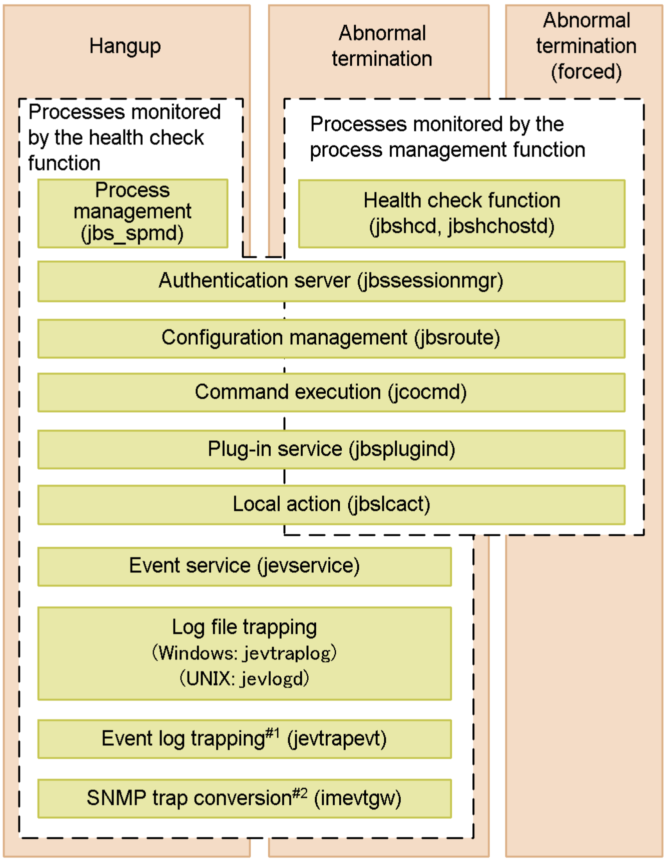
- Data collection when a failure occurs

  Troubleshooting information can be collected when a problem occurs in JP1/Base.

A process might terminate abnormally due to an error or it might be forcibly terminated by the OS `kill` command or other means. In the latter case, the health check function detects the process as having stalled, not as having terminated abnormally. To make sure that all process terminations are detected, use the process management function in conjunction with the health check function.

The following figure shows the range of process errors that can be detected by the health check and process management functions.

Figure 2-3: Range of process errors that can be detected by the health check and process management functions


Hangup
Abnormal termination
Abnormal termination (forced)
Processes monitored by the health check function
Process management (jbs_spmd)
Processes monitored by the process management function
Health check function (jbshcd, jbshchostd)
Authentication server (jbssessionmgr)
Configuration management (jbsroute)
Command execution (jcocmd)
Plug-in service (jbsplugind)
Local action (jbslcact)
Event service (jevservice)
Log file trapping (Windows: jevtraplog) (UNIX: jevlogd)
Event log trapping#1 (jevtrapevt)
SNMP trap conversion#2 (imevtgw)

#1: Supported in Windows only.
#2: Linked with NNM version 8 or earlier.

How to set each function is described below.

(1) Detecting process errors using the health check function

Use of the health check function enables early detection of process errors. Message notification enables the operator to identify the process in which the error occurred and take action to minimize the effects. To use the health check function, JP1/Base 07-51 or a later version must be installed on the monitoring host and target hosts.

(a) Enabling the health check function

The health check function is disabled by default. How to enable the health check function is described below. In a cluster system, enable the health check function on both the physical hosts and logical hosts after you complete the setup of the logical hosts.

To enable the health check function:

1. Register information to enable the health check function in the common definition information.

   1-1 Copy the model file (`jbshc_setup.conf.model`) for the common definition settings file (health check function) using any file name.

   1-2 Edit the copied file.

   1-3 Execute the following commands:

   `jbssetcnf` *file-name-of-copied-file*

   The health check function information is registered in the common definition information.

   For details on the `jbssetcnf` command, see *jbssetcnf* in *13. Commands*.

   For details on the common definition settings file (health check function), see *Common definition settings file (health check function)* in *14. Definition Files*.

2. Edit the health check definition file (`jbshc.conf`).

   Define the monitoring target host and monitoring interval. For details on the health check definition file, see *Health check definition file* in *14. Definition Files*.

3. Change the settings for forwarding JP1 events.

   Add the following condition to the forwarding settings file (`forward`) to send JP1 events issued by the health check function to the higher-level management server.

   ```
   E.OBJECT_TYPE IN JBSHC
   ```

   For details on the forwarding settings file (`forward`), see *Forwarding settings file* in *14. Definition Files.*

4. Restart all JP1/Base services and NNM (if using the SNMP trap converters).

   The health check function starts and process monitoring begins.

   If the health check definition file contains an error, that line is ignored and the default, if any, applies.

(b) Checking the health check settings

To check the health check settings and whether failovers at error detection are enabled, execute the following command and refer to the common definition information: `jbsgetcnf`

In the output information, locate the section about the health check function and check the settings.

For details on the `jbsgetcnf` command, see *jbsgetcnf* in *13. Commands*. For details on the common definition information, see *Common definition settings file (health check function)* in *14. Definition Files*.

(c) Changing the health check settings

To add a target host or change the monitoring interval:

1. Edit the health check definition file (`jbshc.conf`).

   For details on the health check definition file, see *Health check definition file* in *14. Definition Files*.

2. Apply the new settings in the health check definition file (`jbshc.conf`).

   In Windows, restart the JP1/Base (process management) service.

   In UNIX, execute the `jbs_spmd_reload` command. For details on the `jbs_spmd_reload` command, see *jbs_spmd_reload* in *13. Commands*.

   The reloaded settings apply at the next monitoring round.

   If an error occurs at reload due to an error in the health check definition file (`jbshc.conf`), that line is ignored and the previous setting applies.

Note on reloading settings

> If the settings are reloaded after an error has been detected during remote host monitoring, the monitoring status at the target host will be reset. If the failed host has not been restored when next polled, the health check function issues an error message or JP1 event again. If the failed host has been restored, no recovery message or JP1 event is issued.

(d) Disabling the health check function

To disable the health check function:

1. Edit the common definition settings file (health check function).

   1-1 Copy the model file for the common definition settings file (health check function) using any file name.

   1-2 Edit the copied file.

   For details on the common definition settings file (health check function), see

Common definition settings file (health check function) in *14. Definition Files*.

2. Execute the following commands:

   `jbssetcnf` *file-name-of-copied-file*

   The health check function is disabled.

   For details on the `jbssetcnf` command, see *jbssetcnf* in *13. Commands*.

3. Restart all JP1/Base services and NNM (if using the SNMP trap converters).

(e) Upgrading from JP1/Base Version 7 or earlier in a clustering environment

If you are using a cluster system with JP1/Base version 07-00 or earlier, you must upgrade the logical host environment after performing an overwrite installation of JP1/Base version 07-51 or later. For details on the upgrade procedure, see *2.2.3(5) Overwrite installation* (for Windows) or *2.3.4(5) Overwrite installation* (for UNIX).

After upgrading the logical host environment, perform the steps described in *(a) Enabling the health check function*.

(f) Notes

Note the following points when using the health check function.

- A process that is forcibly terminated by the `kill` command or other means is not detected as having terminated abnormally. Instead, the health check function detects that there is no response from the process (error message KAVA7014-E). However, the elapsed time at error detection in this case differs from the time passed since execution of the `kill` command. Because the health check function determines the error status from the update time of the shared memory used internally by the process, the abnormal status can be detected very soon after the process is forcibly terminated.
- When a process is forcibly terminated by the `kill` command or other means and termination processing does not finish, a message reporting that an error was detected in the aborted process might be issued when you restart the affected service.
- When process restart is specified in the extended startup process definition file (`jp1bs_service_0700.conf`) for a process that ends abnormally, a message (KAVB3605-I or KAVB3616-I) will be output to report that the process has restarted. This might be followed by another message (KAVA7017-E) reporting abnormal termination of the process. Check the process status using the `jbs_spmd_status` command.

(2) Detecting process termination and authentication server switching

When a process ends abnormally or the authentication server is swapped over automatically in a system with two authentication servers, JP1/Base outputs an error message to the integrated trace log. Such a message can be issued as a JP1 event. For details on the JP1 events issued by JP1/Base, see *15. JP1 Events*.

(a) Monitored processes

JP1/Base detects abnormal termination of the following processes managed by the process management service (`jbs_spmd`):

- `jbssessionmgr` (authentication server)
- `jbsroute` (configuration management)
- `jcocmd` (command execution)
- `jbsplugind` (plugin service)
- `jbshcd` (health check: for monitoring the local host)
- `jbshchostd` (health check: for monitoring remote hosts)
- `jbssrvmgr` (service management control)
- `jbslcact` (local action)
- `jbscomd` (inter-process communication)

(b) Triggering of JP1 events

When JP1 event issuance is enabled, a JP1 event is issued in the following situations:

Process managed by the process management service

- When a timeout occurs at process startup
- When the process ends abnormally
- When no startup notification is received and a timeout occurs at process startup
- When restart of a managed process that ended abnormally is completed#

  #: Only if restart has been specified for the process.

Authentication server (in a system with a secondary authentication server)

- When connection to the authentication server fails and the connection is automatically blocked
- When a blocked status is automatically released
- When connection is blocked to both the primary and secondary authentication servers

(c) Setup

To set up this functionality:

1. Edit the JP1/Base parameter definition file (`jp1bs_param_V7.conf`).

The `Restart or not` parameter is the fourth value of the values separated by vertical bars (`|`). `0` (do not restart; the default) or `1` (restart) can be specified for this parameter. Note that the third of the values separated by vertical bars (`|`) must not be changed. For details on the JP1/Base parameter definition file, see *JP1/Base parameter definition file* in *14. Definition Files*.

2. Execute the `jbssetcnf` command.

   The settings in the JP1/Base parameter definition file (`jp1bs_param_V7.conf`) are reflected in the common definition information.

   For details on the `jbssetcnf` command, see *jbssetcnf* in *13. Commands*.

3. Restart JP1/Base and the programs that require JP1/Base.

   The settings are applied.

(3) Restarting processes managed by the abnormally terminated process management function

Starting JP1/Base causes multiple processes to be generated. JP1/Base Version 7 or a later version can automatically restart a process that ends abnormally.

The process restart functionality described here is intended to restart JP1/Base in a non-cluster system. If you want to restart a process in a cluster system, use the cluster software.

(a) Target processes

The following target processes are managed by the process management function (`jbs_spmd`):

- `jbssessionmgr` (authentication server)
- `jbsroute` (configuration management)
- `jcocmd` (command execution)
- `jbsplugind` (plugin service)
- `jbshcd` (health check: for monitoring the local host)
- `jbshchostd` (health check: for monitoring remote hosts)
- `jbssrvmgr` (service management control)
- `jbslcact` (local action)
- `jbscomd` (inter-process communication)

(b) Setup

To set up this functionality:

1. Edit the extended startup process definition file (`jp1bs_service_0700.conf`).

For details on the extended start process definition file, see *Extended startup process definition file* in *14. Definition Files*.

2. Enable the setting.

   To enable the automatic restart setting, restart JP1/Base or execute the reload command (`jbs_spmd_reload`).

3. Disable Dr. Watson error notification (Windows only).

   If an error occurs and the Dr. Watson message box is displayed, the process cannot be restarted, so you need to disable the message display.

   From the **Start** menu, choose **Run**, and then execute `drwtsn32`. In the Dr. Watson dialog box, clear the **Visual Notification** check box.

   Because the settings for Dr. Watson are common to the whole system, the settings here are applied to the settings of all programs in the system.

   From the command prompt, execute the following command to enable the settings for Dr. Watson:

   ```
   drwtsn32 -i
   ```

   This command installs Dr. Watson as the default application debugger.

4. Disable Microsoft error reporting (Windows only).

   When an error occurs, a dialog box for reporting the error to Microsoft appears. This prevents the process from restarting. You must therefore disable such error reporting.

   1. In the Control Panel, double-click **System**.

   2. Select the **Advanced** tab, and then click **Error Reporting**.

   3. Select the **Disable error reporting** radio button, and make sure that the **But notify me when critical errors occur** check box is cleared.

(4) Restarting an abnormally-terminated event service process (UNIX only)

The UNIX version of JP1/Base version 9 or later can automatically restart an event service process on the physical host when the process terminates abnormally. This setting is disabled by default.

For the Windows version of JP1/Base, perform the settings for restarting services in the Windows Service Control Manager.

The process restart functionality described here is intended to restart JP1/Base in a non-cluster system. If you want to restart a process in a cluster system, use the cluster software.

(a) Target processes

The target process is the child process `jevservice` (event service) managed by `jevservice` (event service).

The child process `jevservice` (event service) managed by `jevservice` (event service) has a parent process whose process ID can be viewed by using the `jevstat` command.

(b) Setup

To set up this functionality:

1. Define the `restart` parameter in the event server settings file (`conf`).
2. Start the event service.

For details on the event server settings file (`conf`), see *Event server settings file* in *14. Definition Files*.

(5) Hitachi Network Objectplaza Trace Library (HNTRLib2)

JP1/Base outputs log files using the Hitachi Network Objectplaza Trace Library (HNTRLib2). These log files trace the system processing invoked in JP1/Base and in program products for which JP1/Base is a pre-requisite program. The logged data can be used for investigating the cause of any errors that might occur in a JP1 program.

The following defaults are set for the HNTRLib2:

- Size of one log file:256 KB
- Maximum number of log files: 4
- Output directory:

  In Windows:

  system-drive`\Program Files\Hitachi\HNTRLib2\spool\hntr2*.log`

  In UNIX:

  ```
  /var/opt/hitachi/HNTRLib2/spool/hntr2*.log
  ```

Usually, there is no need to change the default settings, but you can view and change the default settings by executing the `hntr2util`, `hntr2conf`, or `hntr2getconf` command. For details on the commands, see *hntr2util (Windows only)*, *hntr2util (UNIX only)*, *hntr2conf*, and *hntr2getconf*.

Note:

From Version 7, the automatic uninstallation functionality has been added to the Hitachi Network Objectplaza Trace Library whose name has been changed from HNTRLib to HNTRLib2. If you have used Version 6 or earlier of JP1/Base, note that information related to the Network Objectplaza Trace Library such as the command names and output destinations differs between Version 7 and Version 6.

(6) Preparing to collect information when a problem occurs (Windows only)

Prepare the supplied tool for collecting data in the event of a problem. When you execute this tool, it will collect all the information for fixing the problem.

The data collection tool can collect memory dumps and crash dumps, among other information. To output these dumps, perform the following setup in advance. Completing this setup enables dump data to be collected by the data collection tool.

(a) Setting up the memory dump output

1. In the Control Panel, double-click **System**.
2. Select the **Advanced** tab, and then choose **Set** for **Startup and Recovery**.
3. For the **Write Debugging Information** options, select **Complete Memory Dump**, and then in the **Dump File** entry box, specify the file to which you want to output memory dumps.

Note

The size of a memory dump differs depending on the size of real memory. A larger physical memory enables larger memory dumps. Allocate enough disk space for collecting memory dumps. For details, see *STOP error* in the Windows Help.

(b) Setting up the crash dump output

To set up the crash dump output:

1. From the **Start** menu, choose **Run**.
2. Type `drwtsn32` in the text box and click the **OK** button.
3. The Dr. Watson dialog box appears.
4. Select **Create Crash Dump File**, and specify an output file in the **Crash Dump** text box.
5. Click the **OK** button.

Note

Crash dumps output not only information on JP1 but also error information on other application programs. When a crash dump is output, the available disk space decreases accordingly. When you set up the crash dump output, make sure that there is enough disk space for it.

2.5 Backup and recovery

This section describes JP1/Base backup and recovery. From the description given here, work out backup and recovery procedures for JP1/Base as part of a system-wide backup plan.

2.5.1 Backup and recovery considerations

Back up the JP1/Base setup information and the event databases so that you can rebuild the system and resume operations in the same environment, should the system become corrupted in any way.

Back up the JP1/Base setup information whenever you change the system, such as at JP1/Base setup, for example.

2.5.2 Backup and recovery (in Windows)

The following describes the backup and recovery of setup information and event databases in the Windows version of JP1/Base.

(1) Backing up JP1/Base setup information

JP1/Base setup information includes:

- Definition files
- Common definition information

For each environment in a cluster system, back up the physical hosts, and then the logical hosts.

(a) Definition files

The following table lists the definition files that users set in JP1/Base. Back up these files by copying them or by some other means.

Table 2-5: JP1/Base files to back up in Windows

File name	Contents
JP1/Base-folder#1`\boot\JP1SVPRM.DAT`	Start sequence definition file
JP1/Base-folder#1`\boot\jp1svprm_wait.dat`	Service starting delay time / timer monitoring period definition file#2
JP1/Base-folder#1`\jp1bs_env.conf`	JP1/Base environment settings file
JP1/Base-folder#1`\jp1bs_param.conf` *JP1/Base-folder*#1`\jp1bs_param_V7.conf`	JP1/Base parameter definition file

File name	Contents
JP1/Base-folder[#1]\jp1bs_spmd.conf	JP1/Base process management definition file
JP1/Base-folder[#1]\jp1bs_service_0700.conf	Extended startup process definition file
Files in *JP1/Base-folder*[#1]\route\	Configuration definition file (used by JP1/IM)
JP1/Base-folder[#1]\user_acl\JP1_Passwd	JP1 user definition file
JP1/Base-folder[#1]\user_acl\JP1_Group	JP1 group definition file
JP1/Base-folder[#1]\user_acl\JP1_UserLevel	JP1 permission levels definition file
JP1/Base-folder[#1]\user_acl\JP1_AccessLevel	JP1 resource group definition file
JP1/Base-folder[#1]\user_acl\JP1_Accountaccess	JP1 account access information file
JP1/Base-folder[#1]\user_acl\jp1BsUmap.conf	User mapping definition file
JP1/Base-folder[#1]\ds\jp1bs_ds_setup.conf	Directory server linkage definition file
JP1/Base-folder[#1]\evtgw\imevtgw.conf	Action definition file for converting SNMP traps
JP1/Base-folder[#1]\evtgw\snmpfilter.conf	Filter file for converting SNMP traps
JP1/Base-folder[#1]\event\index	Event server index file
event-folder[#3]\conf	Event server settings file
event-folder[#3]\forward	Forwarding settings file
JP1/Base-folder[#1]\event\api	API settings file
JP1/Base-folder[#1]\event\ntevent.conf	Action definition file for event log traps
Any-file[#3] or *JP1/Base-folder*[#1]\jevlog.conf[#4]	Action definition file for log file trapping
event-folder[#3]\[jev_forward.conf | *any-file*] [#5]	Distribution definition file (for forward setting file)

File name	Contents
JP1/Base-folder[#1]\[jev_logtrap.conf | *any-file*][#5]	Distribution definition file (for action definition file for log file trapping)
JP1/Base-folder[#1]\event\[jev_ntevent.conf | *any-file*][#5]	Distribution definition file (for action definition file for event log traps)
any-file	Password definition file (Windows only)
JP1/Base-folder[#1]\user_acl\JP1_UserLevel	User permission level file
any-file	Directory server modification file (Windows only)
installation-folder\plugin\conf\*.conf	Adapter command settings file
JP1/Base-folder[#1]\jbshc\jbshc.conf	Health check definition file
any-file	Common definition settings file (health check function)
JP1/Base-folder[#1]\jp1hosts	jp1hosts definition file
JP1/Base-folder[#1]\jbsdfts*.conf	Service management control definition file
any-file	Local action environment variable file
JP1/Base-folder[#1]\lcact\jbslcact.conf	Local action execution definition file
any-file	Common definition settings file (local action function)
JP1/Base-folder[#1]\physical_ipany.conf	Communication protocol settings file
JP1/Base-folder[#1]\logical_ipany.conf	
JP1/Base-folder[#1]\physical_recovery_0651.conf	
JP1/Base-folder[#1]\logical_recovery_0651.conf	
JP1/Base-folder[#1]\physical_anyany.conf	
JP1/Base-folder[#1]\physical_ipip.conf	

File name	Contents
JP1/Base-folder#1\logical_ipip.conf	
JP1/Base-folder#1\jp1bs_baselog_setup.conf	Operation log definition file

#1: Replace *JP1/Base-folder* with the following folder:

- Physical host: *installation-folder*\conf
- Logical host: *shared-folder*\jp1base\conf

#2: Back up these files if you have enabled settings for delaying or monitoring service startup.

#3: Replace *event-folder* with the following folder:

- Physical host: *installation-folder*\conf\event\servers\default
- Logical host: *shared-folder*\jp1base\event

#4: You can assign any name to the action definition file for log file trapping. Remember to back up all the log files you are using. If you are not using the log file trapping, no action definition file for log file trapping will exist.

#5: You can create a distribution definition file using either the default file name or any other name. Remember to back up all the log files you are using. If you are not using the function for collecting and distributing definitions, no distribution definition file will exist.

Note

Backup and recovery do not apply to integrated trace log settings. If you have modified integrated trace log settings, you must reconfigure them when setting up JP1/Base.

(b) Common definition information

In JP1/Base, you must back up common definition information as well as the definition files. This information includes common definition information for JP1/Base, JP1/IM, and JP1/AJS. It is not possible to collect definition information separately for each of these program products.

To back up the common definition file, execute the following command:

```
jbsgetcnf > backup-file
```

When you run JP1/Base in a cluster system, execute the following command:

```
jbsgetcnf -h logical-host-name > backup-file
```

(2) Event database

There are two modes of backing up event database files:

- Backup for data recovery
- Backup for error reporting

(a) Backup for data recovery

To back up the event database files:

1. Stop all services that use JP1/Base.
2. Stop JP1/Base.
3. Copy or otherwise back up the event database files.

   Back up the following files:

   installation-folder`\sys\event\servers\default\IMEvent*.*`#

   or

   shared-folder`\jp1base\event\IMEvent*.*`#

   #: If a different path is specified in the event server index file (`index`) as the folder to be used by the event server, back up the files in that path.
4. Start JP1/Base.
5. Restart the services that use JP1/Base.

(b) Backup for error reporting

To back up an event database for error reporting purposes, use the `jevexport` command to output the database contents to a CSV-format file.

Each event server has two event databases. When one database is full (maximum 10 MB by default), the other event database is swapped in. The existing contents of the swapped-in database are erased. You should regularly check how large the event database has become, and execute the `jevexport` command before the event databases are swapped over.

(3) Recovering JP1/Base setup information

The following describes recovery for JP1/Base. In a cluster system, recover the physical hosts, and then the logical hosts for each environment.

(a) Recovering definition files

To recover the definition files, restore the backup files in the original locations. Make sure that the following conditions are satisfied before you start:

- JP1/Base is successfully installed.
- JP1/Base is stopped.
- JP1/Base in the logical host environment is set up (for a logical host).

- The shared disk is online (for a logical host).

(b) Recovering the common definition information

To recover common definition information, you also need to restore the backup of common definition information in addition to the definition files described above.

Execute the following command:
`jbssetcnf` *name-of-backup-file-backed-up-in-(1)(b)*

(4) Recovering the event database

The following conditions apply for successful recovery of backed-up event database files:

- Only a brief time elapsed between backup and recovery. It is also possible very few JP1 events were registered in the interval between backup and recovery.
- You switched to a different machine but did not change the host name.

To recover the event database files:

1. Stop all services that use JP1/Base.
2. Stop JP1/Base.
3. Move the backed-up files.

   Place the files in this folder:

   installation-folder`\sys\event\servers\default\`#

   or

   shared-folder`\jp1base\event\`#

   #: If a different path is specified in the event server index file (`index`) as the folder to be used by the event server, place the files in that path.
4. Start JP1/Base.
5. Restart the services that use JP1/Base.

2.5.3 Backup and recovery (in UNIX)

The following describes the backup and recovery of setup information and event databases in the UNIX version of JP1/Base.

(1) Backing up JP1/Base setup information

JP1/Base setup information includes:

- Definition files
- Common definition information

In a cluster system, back up physical hosts, and then logical hosts, for each environment.

(a) Definition files

The following table lists the definition files that users set in JP1/Base. You need to back up these files. You can use the `tar` or `cpi` command, or a more advanced backup command to back up these files. Choose any backup method.

Table 2-6: JP1/Base files to back up in UNIX

File names	Contents
JP1/Base-directory#1`/jp1bs_env.conf`	JP1/Base environment settings file
JP1/Base-directory#1`/jp1bs_param.conf` *JP1/Base-directory*#1`/jp1bs_param_V7.conf`	JP1/Base parameter definition file
JP1/Base-directory#1`/jp1bs_spmd.conf`	JP1/Base process management definition file
JP1/Base-directory#1`/jp1bs_service_0700.conf`	Extended startup process definition file
Files in *JP1/Base-directory*#1`/route/`	Configuration definition file (used by JP1/IM)
JP1/Base-directory#1`/user_acl/JP1_Passwd`	JP1 user definition file
JP1/Base-directory#1`/user_acl/JP1_Group`	JP1 group definition file
JP1/Base-directory#1`/user_acl/JP1_UserLevel`	JP1 permission levels definition file
JP1/Base-directory#1`/user_acl/JP1_AccessLevel`	JP1 resource group definition file
JP1/Base-directory#1`/user_acl/JP1_Accountaccess`	JP1 account access information file
JP1/Base-directory#1`/user_acl/jp1BsUmap.conf`	User mapping definition file
JP1/Base-directory#1`/evtgw/imevtgw.conf`	Action definition file for converting SNMP traps
JP1/Base-directory#1`/evtgw/snmpfilter.conf`	Filter file for converting SNMP traps
JP1/Base-directory#1`/event/index`	Event server index file
event-directory#4`/conf`	Event server settings file
event-directory#4`/forward`	Forwarding settings file
JP1/Base-directory#1`/event/API`	API settings file

File names	Contents
Any-file#2 or *JP1/Base-directory*#1/jevlog.conf	Action definition file for log file trapping
event-directory#4/[jev_forward.conf | *any-file*] #3	Distribution definition file (for forward setting file)
JP1/Base-directory#1/[jev_logtrap.conf | *any-file*] #3	Distribution definition file (for action definition file for log file trapping)
JP1/Base-directory#1/event/[jev_ntevent.conf | *any-file*] #3	Distribution definition file (for action definition file for event log traps)
/etc/opt/jp1base/conf/user_acl/JP1_UserLevel	User permission level file
/opt/jp1base/plugin/conf/*.conf	Adapter command settings file
JP1/Base-directory#1/jbshc/jbshc.conf	Health check definition file
any-file	Common definition settings file (health check function)
JP1/Base-directory#1/jp1hosts	jp1hosts definition file
JP1/Base-directory#1/jbsdfts/*.conf	Service management control definition file
any-file	Local action environment variable file
JP1/Base-directory#1/lcact/jbslcact.conf	Local action execution definition file
any-file	Common definition settings file (local action function)
JP1/Base-directory#1/physical_ipany.conf	Communication protocol settings file
JP1/Base-directory#1/logical_ipany.conf	
JP1/Base-directory#1/physical_recovery_0651.conf	
JP1/Base-directory#1/logical_recovery_0651.conf	
JP1/Base-directory#1/physical_anyany.conf	
JP1/Base-directory#1/physical_ipip.conf	

File names	Contents
JP1/Base-directory#1/`logical_ipip.conf`	
JP1/Base-directory#1/`jp1bs_baselog_setup.conf`	Operation log definition file

#1: Replace *JP1/Base-directory* with the following directory:

- Physical host: `/etc/opt/jp1base/conf`
- Logical host: *shared-directory*`/jp1base/conf`

#2: You can assign any name to the action definition file for log file trapping. Remember to back up all the log files you are using. If you are not using the log file trapping function, no action definition file for log file trapping exists.

#3: You can create a distribution definition file using either the default file name or any other name. Remember to back up all the log files you are using. If you are not using the function for collecting and distributing definitions, no distribution definition file will exist.

#4: Replace *event-directory* with the following directory:

- Physical host: `/etc/opt/jp1base/conf/event/servers/default`
- Logical host: *shared-directory*`/event`

When you run JP1/Base in a cluster system, back up the relevant definition files stored in a directory you specified when setting up JP1/Base for the cluster system.

Note

> Backup and recovery do not apply to integrated trace log settings. If you have modified integrated trace log settings, you must reconfigure them when setting up JP1/Base.

(b) Common definition information

In JP1/Base, you must back up common definition information as well as the definition files. This information includes common definition information for JP1/Base, JP1/IM, and JP1/AJS. It is not possible to collect definition information separately for each of these program products.

To back up the common definition file, execute the following command:
`jbsgetcnf >` *backup-file*

When you run JP1/Base in a cluster system, execute the following command:
`jbsgetcnf -h` *logical-host-name* `>` *backup-file*

(2) Backing up an event database

There are two modes of backing up event database files:

- Backup for data recovery
- Backup for error reporting

(a) Backup for data recovery

To back up the event database files:

1. Stop all services that use JP1/Base.
2. Stop JP1/Base.
3. Copy or otherwise back up the event database files.

   Back up the following files:

   `/var/opt/jp1base/sys/event/servers/default/IMEvent*.*`#

   or

   shared-directory`/event/IMEvent*.*`#

   #: If a different path is specified in the event server index file (`index`) as the directory to be used by the event server, back up the files in that path.
4. Start JP1/Base.
5. Restart the services that use JP1/Base.

(b) Backup for error reporting

To back up an event database for error reporting purposes, use the `jevexport` command to output the database contents to a CSV-format file.

Each event server has two event databases. When one database is full (maximum 10 MB by default), the other event database is swapped in. The existing contents of the swapped-in database are erased. You should regularly check how large the event database has become, and execute the `jevexport` command before the event databases are swapped over.

(3) Recovering JP1/Base setup information

The following describes recovery for JP1/Base. In a cluster system, recover the physical hosts, and then the logical hosts for each environment.

(a) Recovering definition files

To recover the definition files, restore the backup files in the original locations. Make sure that the following conditions are satisfied before you start:

- JP1/Base is successfully installed, and the setup command has been executed.
- JP1/Base is stopped.
- JP1/Base in the logical host environment is set up (for a logical host).

- The shared disk is online (for a logical host).

(b) Recovering the common definition information

To recover common definition information, you also need to restore the backup of common definition information in addition to the definition files described above.

Execute the following command:
`jbssetcnf` *backup-file-name*

For *backup-file-name*, specify the backup file generated by the `jbsgetcnf` command.

(4) Recovering an event database

The following conditions apply for successful recovery of backed-up event database files:

- Only a brief time elapsed between backup and recovery. It is also possible very few JP1 events were registered in the interval between backup and recovery.
- You switched to a different machine but did not change the host name.

To recover the event database files:

1. Stop all services that use JP1/Base.
2. Stop JP1/Base.
3. Move the backed-up files.

   Place the files in this directory:

   `/var/opt/jp1base/sys/event/servers/default/`#

   or

   shared-directory`/event/`#

   #: If a different path is specified in the event server index file (`index`) as the directory to be used by the event server, place the files in that path.
4. Start JP1/Base.
5. Restart the services that use JP1/Base.

Chapter

3. Setting Up JP1/Base for Use in a Cluster System

JP1/Base supports Microsoft Cluster Server and other cluster software. Linking with clustering software can improve the availability of JP1/Base. This chapter describes how to set up and use JP1/Base in a cluster system.

If you want to use the JP1/Base in a cluster system, check in advance whether JP1/Base supports the clustering software you are planning to use.

3.1 Overview of using JP1/Base in a cluster system

This section gives an overview of cluster systems and an overview of using JP1/Base in a cluster system.

3.1.1 Overview of a cluster system

A cluster system contains multiple server systems, which work together as a single system. If a failure occurs on one server, job processing can continue on another server.

A cluster system consists of a host that performs processing and a host that is on standby to take over processing if a failure occurs. Servers that execute jobs are called *primary servers*. Servers that are ready to take over a job if a failure occurs on a primary server are called *secondary servers*. If a failure occurs, the secondary server takes over for the primary server to prevent operations from being disrupted. This is called a *failover*.

Failovers are performed in units of logical servers, called *logical hosts*. Any applications running in a cluster system must operate in a logical host environment to enable failovers for continuous operations. Applications running on a logical host are independent of physical servers and can operate on any server.

A logical host consists of three elements: an application running as a service, a shared disk, and a logical IP address. An application running as a service, such as JP1, stores data on a shared disk and uses a logical IP address for communication.

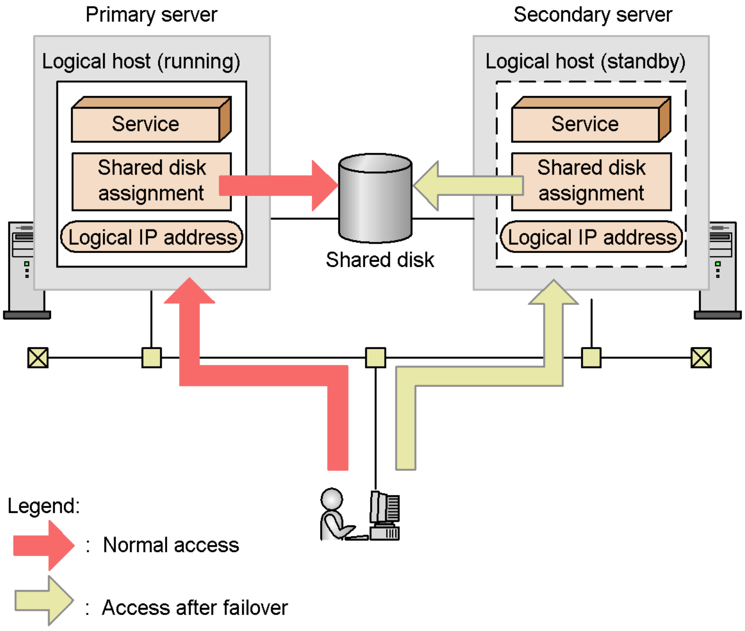
The following table shows the components of a logical host.

Table 3-1: Components of a logical host

Logical host component	Description
Service	An application, such as JP1, that runs in a cluster system. If the logical host for the primary node fails, the logical host for the secondary node starts the service using the same name, in order to take over.
Shared disk	A disk device connected to both the primary and secondary nodes. Information that will be inherited if a failover occurs (definitions, execution states, and so on) is stored on the shared disk. If a failure occurs on the primary logical host, the secondary server takes over the connection to the shared disk.
Logical IP address	An IP address assigned while a logical host is operating. If the primary server fails, the secondary server takes over the same logical IP address. This allows clients to access the same IP address as if a single server is always running.

The following figure shows access during normal operations and after a failover.

Figure 3-1: Access during normal operations and after a failover



While the primary server is running, on that server the shared disk and logical IP address are assigned and the services operate. If a problem occurs on the server, the secondary server takes over the shared disk and logical IP address, and restarts the same services that were on the primary server. Thus, although the physical server changes during a failover, since the secondary server takes over the shared disk and logical IP address, the change is transparent to clients.

3.1.2 Overview of using JP1/Base in a cluster system

This subsection gives an overview of using JP1/Base in a cluster system.

To operate JP1/Base in a logical host environment, you must provide a logical IP address and a shared disk for storing data necessary for failovers. You must also register JP1/Base with the clustering software so that the software can control the start and stop of JP1/Base and monitor the operations of JP1/Base. Setting up a logical host results in settings that specify which servers store necessary data on the shared disk and use a logical IP address for communication. When running in a logical host environment, JP1/Base uses data stored on the shared disk so that the secondary server can take over processing from the primary server if the primary server fails.

The following sections describe prerequisites for using JP1/Base in a cluster system, and explain how to set up an environment as such.

3.2 Prerequisites for using JP1/Base in a cluster system and the support range

In a cluster system, JP1 runs in a logical host environment to enable failovers. The prerequisites for executing JP1 in a logical host environment are that clustering software can normally control the assignment and deletion of a shared disk or logical IP address and the monitoring of operations.

Note

> Even the clustering software supported by JP1 might not satisfy the prerequisites described below depending on the system configuration and environment settings. You should determine the system configuration and environment settings so that the prerequisites are satisfied.

(1) Prerequisites for a logical host environment

When operating JP1 in a logical host environment, you must satisfy the following prerequisites for a logical IP address and shared disk:

Table 3-2: Prerequisites for a logical host environment

Logical host component	Prerequisites
Shared disk	• A shared disk must be used that can be taken over from the primary server to the secondary server. • The shared disk must be assigned before JP1 is started. • The assignment of the shared disk must not be canceled while JP1 is running. • The assignment of the shared disk must be canceled after JP1 is stopped. • The shared disk must be locked so that multiple servers do not inadvertently use it. • Files must be protected using a file system with the journal functionality or other measures so that the files will not be lost due to a system failure. • Failovers must guarantee that the contents of all files are taken over correctly. • Failovers must be forced to occur even when a process is using the shared disk during failover. • Clustering software must be responsible for recovery upon the detection of any failure on the shared disk so that JP1 does not need to perform recovery. Clustering software must issue a start or stop request to JP1 if it is necessary to start or stop JP1 as part of recovery.

Logical host component	Prerequisites
Logical IP address	• Communication must be performed using a logical IP address that can be taken over. • The logical IP address must be uniquely determined from the logical host name. • The logical IP address must be assigned before JP1 is started. • The logical IP address must not be deleted while JP1 is running. • The correspondence between the logical host name and logical IP address must not be modified while JP1 is running. • The logical IP address must be deleted after JP1 is stopped. • Clustering software must be responsible for recovery upon the detection of a network failure so that JP1 does not need to perform a recovery. Clustering software must issue a start or stop request to JP1 if it is necessary to start or stop JP1 as part of recovery.

If any of the above requirements are not satisfied, JP1 might malfunction. For example:

- If data written from the primary server corrupts upon a failover

  JP1 might encounter a problem, such as an error, lost data, or a failure in starting up.

- If no recovery is performed when a LAN board fails

  A communication error occurs, preventing JP1 from operating normally until clustering software switches the LAN board or failover to another server occurs.

(2) Prerequisites for a physical host environment

The following conditions are the prerequisites for operating JP1 in a physical host environment. If you only execute JP1 in a logical host environment, the following prerequisites must also be satisfied as the system environment.

Table 3-3: Prerequisites for a physical host environment

Physical host component	Prerequisites
Server	• A cluster must consist of two or more servers. • The CPU performance must be sufficient for the processing to be performed. (For example, the CPU must be able to handle the startup of multiple logical hosts.) • The real memory capacity must be sufficient for the processing to be performed. (For example, the servers must have sufficient memory capacity to handle the startup of multiple logical hosts.)
Disk	• Files must be protected using a file system with a journal functionality or other measures so that the files will not be lost due to a system failure.

Physical host component	Prerequisites
Network	• Communication must be enabled using an IP address corresponding to the host name (result of the `hostname` command). (Clustering software or other programs must not modify the state to prevent communication.) • The correspondence between the host name and IP address must not be modified while JP1 is running. (The correspondence must not be modified by clustering software or a name server.) • In Windows, the LAN board corresponding to the host name must have the highest priority in the network binding settings. (Any other LAN board, such as that for heartbeat, must not have higher priority.)
OS and clustering software	• The clustering software and its version must be supported by JP1. • All patches and service packs required by JP1 and the clustering software must have been applied. • The same environment must be set up for all of the servers so that the same processing can be continued after a failover occurs.

(3) Range supported by JP1

When you are using JP1 in a cluster system, JP1 only supports its own operations. Control over the logical host environment (shared disk and logical IP address) depends the clustering software.

If the above prerequisites for a logical or physical host environment are not satisfied or if there is a problem in controlling the logical host environment, JP1 does not support the problems that might occur with JP1 operations. In such a case, the clustering software or OS controlling the logical host environment must address the problem.

(4) Specifying a logical host

When executing a command, you must specify the logical host name so that the command will be executed on the logical host. If you do not specify the logical host name, the command will be executed on the physical host. You can specify the logical host name either by setting the name in the `JP1_HOSTNAME` environment variable or by specifying a command option. The following table describes each method.

Method	Description
`JP1_HOSTNAME` environment variable	Specify the logical host name in the `JP1_HOSTNAME` environment variable. If you specify a logical host name in both the command option and environment variable, the setting with the command option takes precedence.

Method	Description
Command option	Specify the command option in the following format: *command* `-h` *logical-host-name*. For details, see the description of each command.

Note

In Windows, do not set the `JP1_HOSTNAME` environment variable as a system environment variable or as a user environment variable. If so, this could disable services or otherwise disrupt program operation. Set the `JP1_HOSTNAME` environment variable at the command prompt or in a batch file.

(5) Rules for specifying logical host names

Comply with the following rules when specifying logical host names:

- Number of characters:1 to 196 bytes in Windows (63 bytes or less recommended)#1; 1 to 255 bytes in UNIX (63 bytes or less recommended)#1, #2
- Usable characters: Alphanumeric characters and hyphens.

#1: These are the numbers of characters supported in JP1/Base. Your clustering software might not support these characters. Be sure to specify logical host names within the limitation of both JP1/Base and the cluster system you use. In actual operations, we recommend a host name of 63 bytes or less.

#2: For the UNIX-only forced termination command (`jbs_killall.cluster`), you must specify a logical host name of 15 bytes or less. You cannot specify a logical host name that exceeds 15 bytes.

Notes

- Note the following if you specify the same name for both the logical host name and the physical host name (as output by the `hostname` command). We strongly recommend that the logical host name you specify in a cluster system be different from the physical host name.
    - Start JP1 on the logical host only.

      Start JP1 on the logical host only and do not start JP1 on the physical host.
    - Modify the settings for the event service environment.

      Comment out the line `server * default`, which is coded in the event server index file (`index`) by default. If this line remains in the file, the event database for the logical host is created on the local disk so that it cannot be taken over during a failover. You must complete the setup on both the primary and secondary server.
    - Modify the settings for the environment setting directory.

To share the environment setting directory on the physical host, modify the settings as follows. You must complete the setup on both the primary and secondary server.

In Windows:

1. Create a definition file with the following contents.

You can choose any name for the definition file.

```
[JP1_DEFAULT\JP1BASE\]
"JP1BASE_CONFDIR"="shared-folder\jp1base\conf\"
```

2. Execute the following command to reflect the settings in the created definition file in the common definition information:

```
jbssetcnf definition-file-name
```

In UNIX:

1. Create a definition file with the following contents.

You can choose any name for the definition file.

```
[JP1_DEFAULT\JP1BASE\]
"JP1BASE_CONFDIR"="/shared-directory/jp1base/conf/"
```

2. Execute the following command to reflect the settings in the created definition file in the common definition information:

```
/opt/jp1base/bin/jbssetcnf  definition-file-name
```

- Restart the Hitachi Network Objectplaza Trace Library (HNTRLib2).

To modify the host name while the system is running, you must restart the Hitachi Network Objectplaza Trace Library (HNTRLib2). To restart HNTRLib2, perform the following procedure:

In Windows:

1. Manually stop HNTRLib2 in the Services dialog box in the Control Panel.

2. Change the host name.

3. Manually start HNTRLib2 in the Services dialog box in the Control Panel.

In UNIX:

1. Use the `hntr2kill` command to stop HNTRLib2.

2. Change the host name.

3. Execute the following command to start HNTRLib2.

```
hntr2mon -d &
```

Trace information is not logged until you restart HNTRLib2. Stop all applications that are using HNTRLib2 before stopping HNTRLib2. Conversely, start HNTRLib2 before starting any application that uses HNTRLib2. For details on the `hntr2kill` command, see *hntr2kill (UNIX only)* in *13. Commands*.

- If you are using DNS, use a host name that is not in FQDN format as the logical host name. For example, specify `jp1v7` as the logical host name from `jp1v7.soft.hitachi.co.jp`. Make sure that names can be resolved by using this host name.
- In Windows, do not set the `JP1_HOSTNAME` environment variable as a system environment variable or as a user environment variable. If so, this could disable services or otherwise disrupt program operation. Set `JP1_HOSTNAME` at the command prompt or in a batch file.
- When using the UNIX forced termination command (`jbs_killall.cluster`), make sure the first 15 bytes of the logical host name uniquely identifies the host within the cluster system. The `jbs_killall.cluster` command determines the host by using the first 15 bytes and forcibly terminates the associated process. You cannot kill a process for a logical host name that exceeds 15 bytes.

3.3 Functions of JP/Base in a cluster system

This section describes the JP1/Base functions that are necessary to understand when using JP1/Base in a cluster system.

3.3.1 Cluster operation with the log file trapping function

In a cluster system, you must start the log file trapping function separately on each physical host. You cannot start the function by specifying a logical host. However, you can specify whether JP1 events will be forwarded to the event service on a logical host where they can be centrally managed. Configure a forwarding destination that works well with how your system is run.

By default, JP1 events are registered in the event service on the physical host. To register them in the event service of a logical host, execute the `jevlogstart` command, specifying the event server name of the logical host in the `-s` option.

The following describes how to monitor log files on shared and local disks.

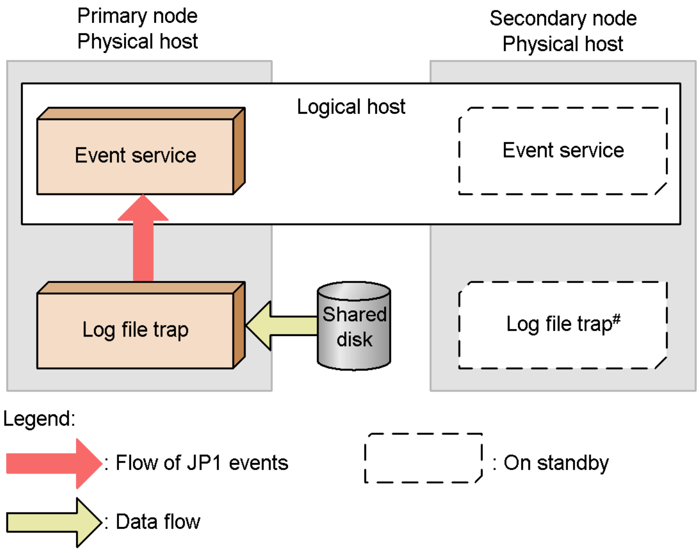
(1) Monitoring log files on a shared disk

To monitor log files on a shared disk, you must coordinate the start and end of the log file trapping function with the startup and shutdown of the logical host. In the event of a failover on the primary node, stop the log file trapping function on the failed server, and then restart the function on the server that has taken over as the active system.

Leave the shared disk allocated so that it can be accessed while log files are being monitored. If you change the shared disk allocation during file monitoring, problems such as errors in the monitoring process and control failure in disk space allocation and deallocation could occur.

An example of a configuration for monitoring log files on a shared disk is shown in the following figure.

Figure 3-2: Configuration example for monitoring log files on a shared disk



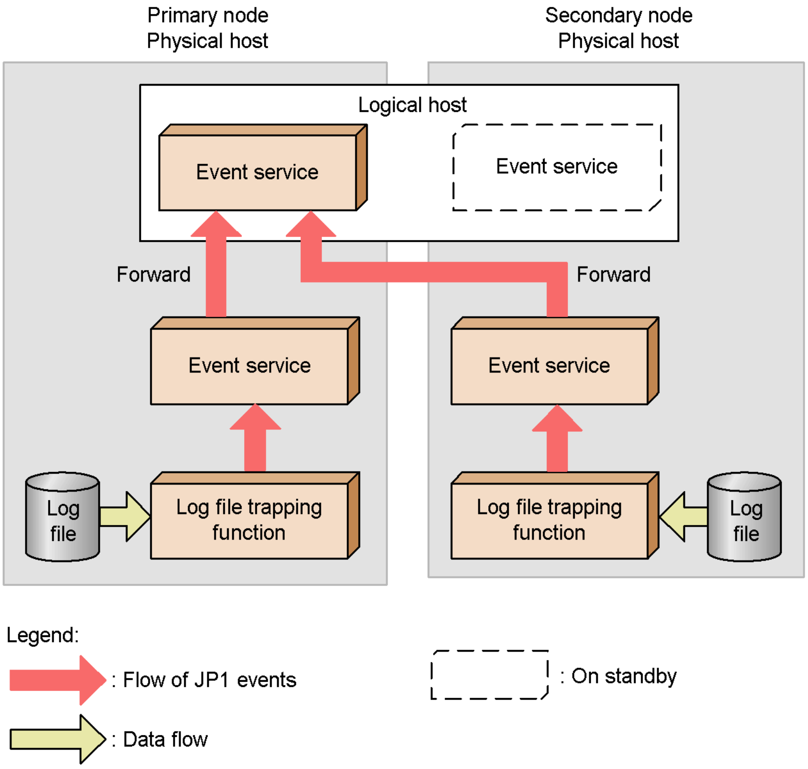
When a failover occurs, stop the log file trap on the failed server, and then restart it on the server that has taken over as the active system.

(2) Monitoring log files on local disks

To monitor log files on the local disk of both the primary and secondary nodes, the JP1 events converted from log data must first be registered in the event service of the physical host. After that, configure a forwarding settings file (`forward`) so that the JP1 events are forwarded to the event service on the logical host. For details on the forwarding settings file, see *Forwarding settings file* in *14. Definition Files*.

An example of a system configuration for monitoring, on a logical host, log files on local disks is shown in the following figure.

Figure 3-3: Configuration example for monitoring, on a logical host, log files on local disks



3.3.2 Cluster operation with the event log trapping function

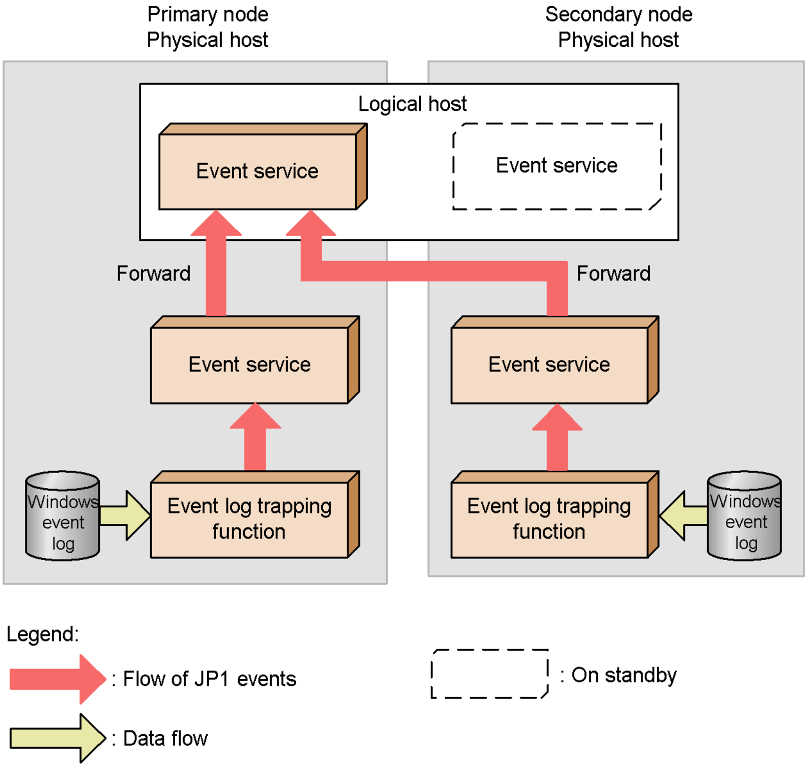
In a cluster system, you must start the event log trapping function separately on each physical host. You cannot start the function by specifying a logical host. However, you can specify whether JP1 events will be forwarded to the event service on a logical host where they can be centrally managed. Configure a forwarding destination that works well with how your system is run.

By default, JP1 events are registered in the event service on the physical host. To register them in the event service of a logical host, specify the event server name of the logical host in the `server` parameter in the action definition file. Note that if your system is configured so that JP1 events converted from event log data are registered directly on a logical host, the event log on the secondary node cannot be monitored.

To monitor the event log on both the primary and secondary nodes, first register the converted JP1 events in the event service on the physical host. Then forward the registered JP1 events to the event service on the logical host, using a forwarding settings file (`forward`). For details on the forwarding settings file, see *Forwarding* *settings file* in *14. Definition Files*.

A configuration example for monitoring event logs on both the primary and secondary nodes is shown in the following figure.

Figure 3-4: Configuration example for monitoring event logs on both primary and secondary nodes of the logical host



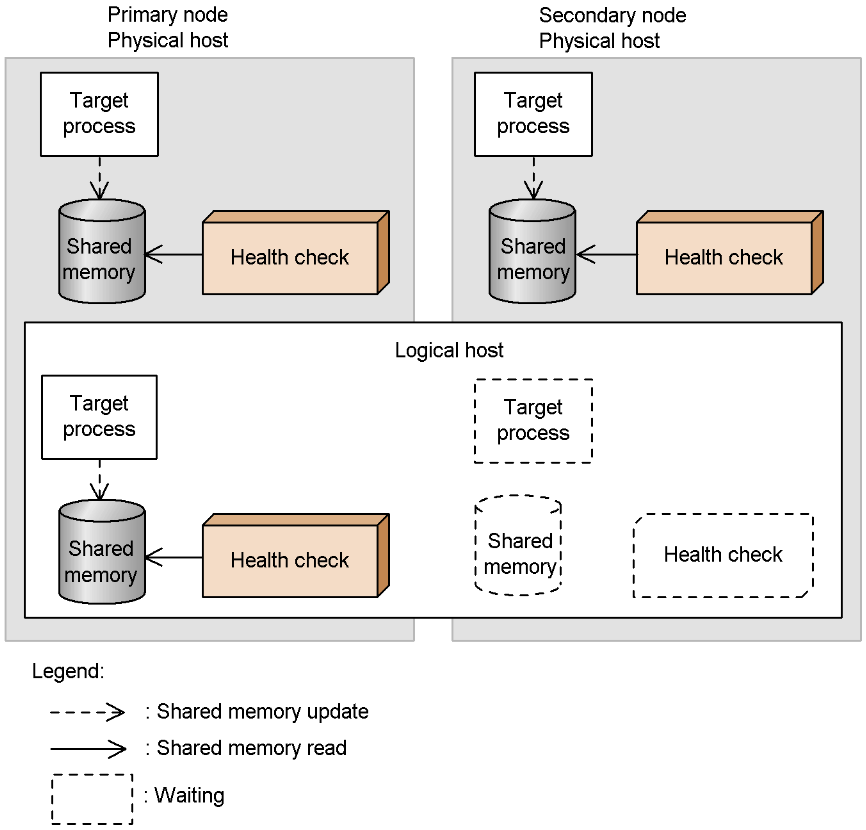
3.3.3 Cluster operation with the health check function

The health check function runs on a physical host or logical host and monitors the processes running on each host. By using this function, process halts and hangups can be identified as errors and a failover initiated.

To initiate a failover when the health check function detects a process error, enable failover in the health check setup file. For details on the forwarding settings file, see *Forwarding settings file* in *14. Definition Files*.

The following figure shows a configuration example using the health check function in a clustering environment.

Figure 3-5: Configuration example using the health check function in a clustering environment



In this example, the health check function is used on the physical hosts (primary and secondary servers) and on the logical host. If the health-check function detects an abnormal process on a logical host when monitoring the local host, in Windows, the JP1/Base service will stop; and in Unix, the health check process (`jbshcd`) will stop. If the system detects such a stop, the system will try to initiate a failover by using the cluster software.

Note

The monitoring status at the target host is reset when a failover occurs at detection of an error during remote host monitoring. If the failed remote host has not been restored when next polled, the health check function issues an error message or JP1 event again. If the failed remote host has been restored, no recovery message or JP1 event is issued.

3.4 Setting up the environment for a cluster system (in Windows)

This section describes how to set up the JP1/Base environment to support a cluster system.

3.4.1 Required environment settings

The following describes the required environment settings for using JP1/Base in a cluster system. For the setting procedure, see *3.4.3 Setup*.

(1) Specifying a shared folder

When setting up a logical host, specify a shared folder for sharing information between the primary and secondary servers. In the shared folder, the following files and folders are created.

Shared file type	Folder for the shared files
Definition files	*shared-folder*`\jp1base\conf\`
Log file	*shared-folder*`\jp1base\log\`
Event server settings file	*shared-folder*`\jp1base\event\`

Assign a shared folder to each logical host. You must not assign the same folder to different logical hosts. The following shows an example of folder creation on a shared disk.

Example: Specify `\shdsk\node0` as a shared folder for logical host `node0`.

```
\shdsk\node0\jp1base\conf\
\shdsk\node0\jp1base\log\
```

The event service can be set up to independently run in cluster mode. However, if you set up the environment according to *3.4.3 Setup*, JP1/Base automatically specifies the logical host names in the event server index file (`index`) and creates the event server settings file (`conf`) in a shared folder.

(2) Communication protocol

When you set up the JP1/Base environment to support a cluster system, the socket binding method used in TCP/IP communication is automatically changed to IP addressing. This change affects settings for the logical hosts to be created and their constituent physical hosts. For details on the JP1/Base communication protocol, see *1.10 Communication protocols of JP1/Base*.

To configure both physical and logical host environments on the same host, you need to set up the network control. For details, see *3.4.7 Settings to configure both physical and logical host environments on the same logical host*.

(3) Common definition information

In JP1/Base and the programs that require JP1/Base (JP1/IM, JP1/AJS, or JP1/Power Monitor), information about the logical hosts is set as common definition information in the local disk. You must therefore set identical information about each logical host.

The common definition information is updated when you:

- Change the common definition information for JP1/Base and the programs that require JP1/Base (JP1/IM, JP1/AJS, or JP1/Power Monitor).
- Change the user mapping information.
- Change the authentication server.
- Delete the common definition information on the logical host.
- Change the password management information for an OS user.
- Change the `jp1hosts` information.

If you change the common definition information, match the information on each server, referring to *3.4.5 Modifying common definition information*.

(4) Registering with clustering software

To enable the cluster software to control the JP1/Base on the logical host, you must register the JP1/Base service corresponding to the logical host to the cluster software. Logical host services are created when the logical host is set up.

3.4.2 Installing JP1/Base

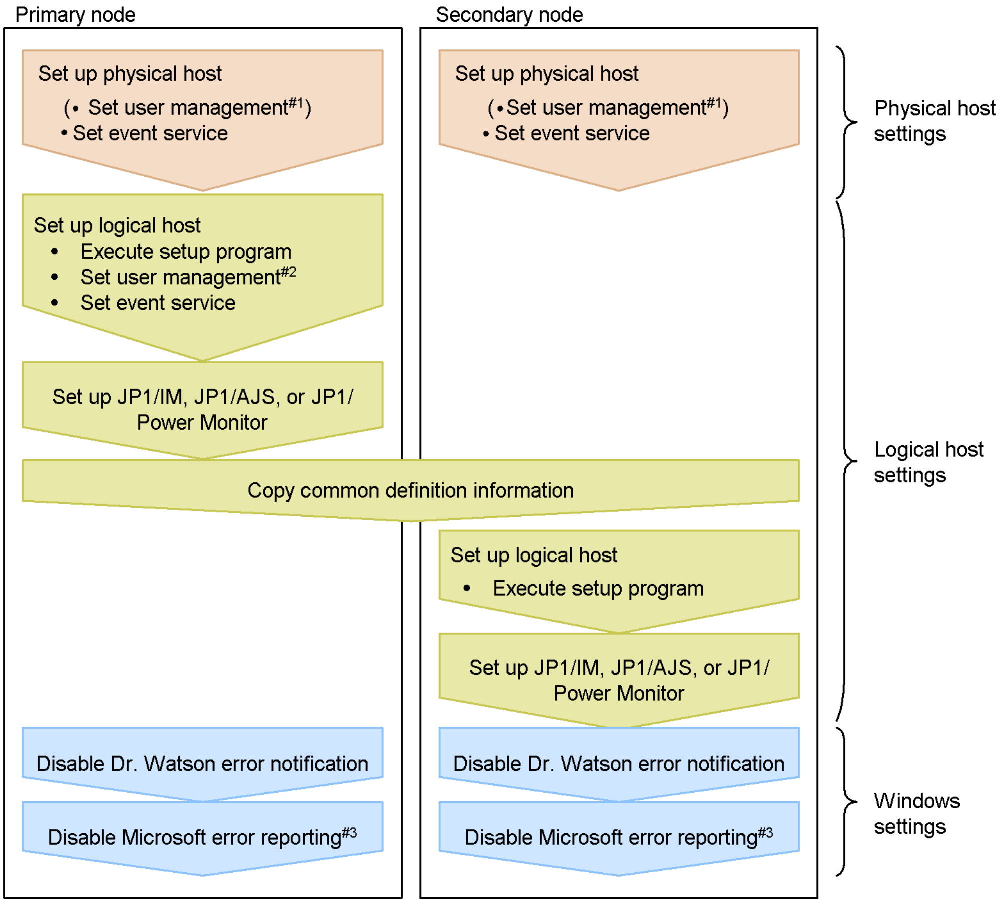
Install JP1/Base on both the primary and secondary node local disks. The installation drive and folder must be the same on both nodes. Do not install JP1/Base on a shared disk.

If you are using JP1/Base 07-00 or an earlier version in a cluster system, you must upgrade the logical host environment after an overwrite installation. For details on the upgrade procedure, see *2.2.3(5) Overwrite installation*.

3.4.3 Setup

To operate JP1/Base in a cluster system, you must set up a physical host environment (for primary and secondary nodes) and a logical host environment (for primary and secondary nodes). The setup procedure is shown in the following figure.

Figure 3-6: Setup procedure for a cluster system (In Windows)



#1: Required when using the authentication server on a physical host.

#2: Required when using the authentication server on a logical host.

#3: Required only on Windows Server 2003.

(1) Setup on the primary node

To set up the physical and logical hosts on the primary node:

1. Set user management function for the physical host.

   Specify this option if you want to run an authentication server on the physical host. For details on the user management function, see *6.1 User management setup (in Windows)*.

2. Modify the event server settings (`conf`) for the physical host.

Modify the settings for the event service communication protocol (`ports` parameter) and retry limit for forwarding JP1 events (`forward-limit` parameter).

For the `ports` parameter, specify the IP address used for the physical host or the name of the physical host.

The event service stops during failovers. Use the `forward-limit` parameter to specify the maximum period to retry forwarding the JP1 events that could not be sent during a failover. By default, the system continues to retry for 3,600 seconds.

The event server settings file (`conf`) resides in the following location:
installation-folder`\conf\event\servers\default\`

The following shows an example of the parameter settings:

```
ports IP-address-of-physical-host jp1imevt jp1imevtapi
forward-limit 3600
```

For details on the event server settings file, see *Event server settings file* in *14. Definition Files*.

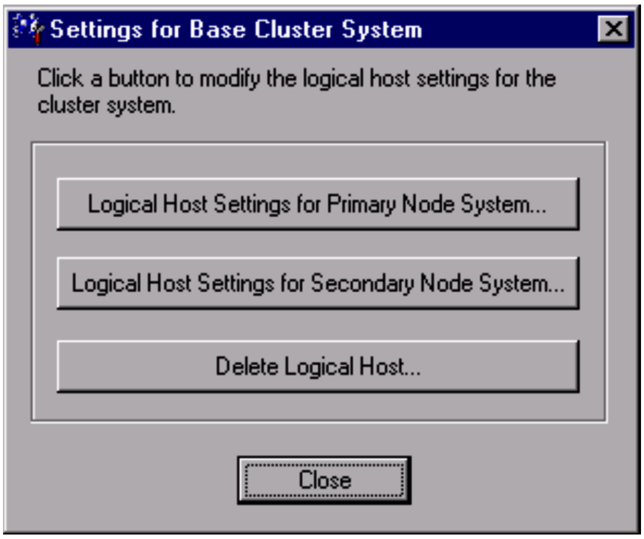
3. Set the logical host.

Setting up through GUI

1. Execute *installation-folder*`\bin\jp1bshasetup.exe`.

The Settings for Base Cluster System dialog box appears.

Figure 3-7: Settings for Base Cluster System dialog box

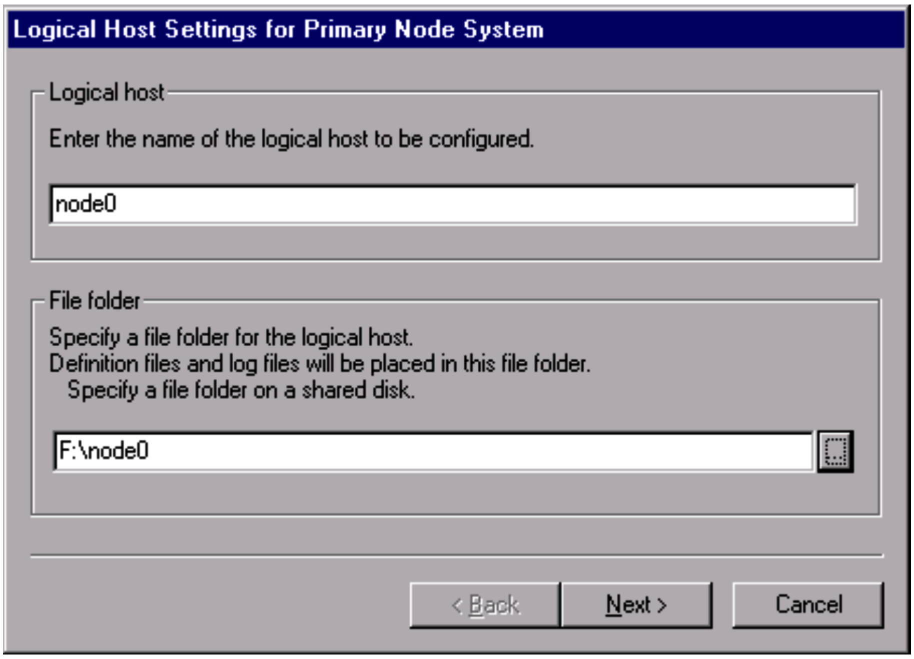

Settings for Base Cluster System
Logical Host Settings for Primary Node System...
Logical Host Settings for Secondary Node System...
Delete Logical Host...
Close

Click a button to modify the logical host settings for the cluster system.

2. Click the **Logical Host Settings for Primary Node System** button.

The Logical Host Settings for Primary Node System dialog box appears.

Figure 3-8: Logical Host Settings for Primary Node System dialog box



Enter the name of the logical host to be configured.

node0

Specify a file folder for the logical host.
Definition files and log files will be placed in this file folder.
Specify a file folder on a shared disk.

F:\node0

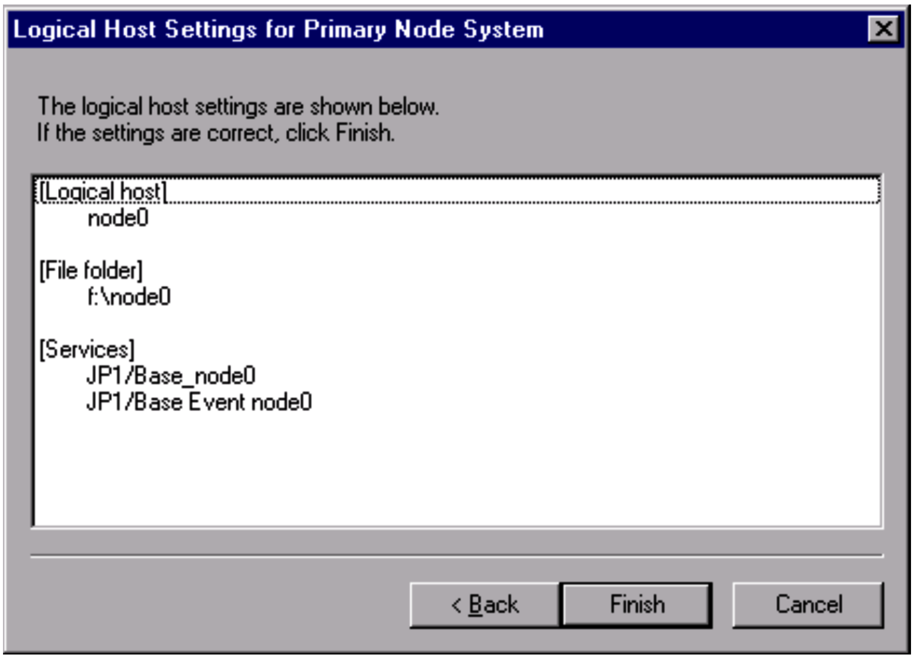
In this dialog box, specify the name of the logical host for which information will be created and a folder on a shared disk for creating shared folders and shared files.

The shared folders and shared files are created in the *specified-folder*`\jp1base\` folder. Before you specify these items, be sure to mount the shared disk.

3. Click the **Next** button.

The following dialog box appears.

Figure 3-9: Logical Host Settings for Primary Node System dialog box (confirmation window)



Logical Host Settings for Primary Node System

The logical host settings are shown below.
If the settings are correct, click Finish.

```
[Logical host]
      node0

[File folder]
      f:\node0

[Services]
      JP1/Base_node0
      JP1/Base Event node0
```

You can use this dialog box to check the settings. If the settings are correct, click the **Finish** button.

This completes all the settings except the communication protocol for the event service.

4. Set up the authentication server on the logical host.

The authentication servers that have been set on the physical host are set for the logical host. Use the GUI to set an authentication server that has a different physical host. For details, see *6.1.1 Specifying the authentication servers to use*.

Set up by using commands

Execute the command as follows: Create a shared folder and shared files on a shared disk to set up the authentication server.

```
jbs_setup_cluster -h node0 -d d:\node0 -a node0
```

For details on the `jbs_setup_cluster` command, see *jbs_setup_cluster (Windows only)* in *13. Commands*.

4. Set up user management for the logical host.

Specify this option if you want to run an authentication server on the logical host.

Set up by using the GUI

1. From the Windows **Start** menu, choose **Programs**, **JP1_Base**, and then **Environment Settings**.

2. In the Select Logical Host dialog box, select the logical host for which you want to set up user management.

Set up by using commands

1. Register the JP1 user in the common definition information (only when using the logical host as the authentication server).

Make sure that the authentication server is active, and then execute the following command to register a JP1 user:

`jbsadduser -h` *logical-host-name JP1-user-name*

To check the registered JP1 user, execute the following command:

`jbslistuser -h` *logical-host-name*

2. Register the user mapping information in the common definition information.

The user mapping definition file (`jp1BsUmap.conf`) resides in the following location:

shared-folder`\jp1base\conf\user_acl\jp1BsUmap.conf`

After editing the file (`jp1BsUmap.conf`), execute the following command to register the user mapping definition information:

`jbsmkumap -h` *logical-host-name*

To check the registered user mapping information, execute the following command:

`jbsgetumap -h` *logical-host-name*

3. Match the common definition information on the physical hosts.

When you finish these operations, match the information on all the physical hosts, as described in *3.4.5 Modifying common definition information*.

4. Set JP1 user operating permissions (only when using the logical host as the authentication server).

The user permission level file (`JP1_UserLevel`) is located in the following directory:

shared-folder`\conf\user_acl\JP1_UserLevel`

After editing this file (`JP1_UserLevel`), execute the `jbsaclreload` command to apply the settings.

For details on the user management function, see *6.1 User management setup (in Windows)*.

Notes on operating authentication servers in a cluster system:

The settings files for authentication servers are stored in the following folder:

shared-folder`\jp1base\conf\user_acl\`

If you are using a secondary authentication server, you must copy the settings files from the primary authentication server to the secondary authentication server. Note that the copy destination varies depending on whether you use the secondary authentication server in a cluster system:

When using a cluster system:

shared-folder`\jp1base\conf\user_acl\`

When not using a cluster system:

installation-folder`\conf\user_acl\`

After copying the settings files, execute the following command to apply the settings. You need to specify the `-h` option only if you use the secondary authentication server in a cluster system.

`jbs_spmd_reload -h` *logical-host-name*

5. Modify the event server settings (`conf`) for the logical host.

   Modify the settings for the event service communication protocol (`ports` parameter) and retry limit for forwarding JP1 events (`forward-limit` parameter).

   For the `ports` parameter, specify the IP address used for the logical host or the name of the logical host.

   The event service stops during failovers. Use the `forward-limit` parameter to specify the maximum period to retry forwarding the JP1 events that could not be sent during a failover. By default, the system continues to retry for 3,600 seconds.

The event server settings file (`conf`) resides in the following location:

shared-folder`\jp1base\event\`

The following shows an example of the parameter settings:

```
ports IP-address-of-logical-host jp1imevt jp1imevtapi
forward-limit 3600
```

For details on the event server settings file, see *Event server settings file* in *14. Definition Files*.

This completes JP1/Base setup on the primary node.

If any of the programs that require JP1/Base (JP1/IM, JP1/AJS, or JP1/Power Monitor) are installed, you must complete the failover settings for these programs. For details, see the *Job Management Partner 1/Integrated Management - Manager Configuration Guide*, *Job Management Partner 1/Integrated Management - Manager Administration Guide*, *Job Management Partner 1/Automatic Job Management System 2 Planning and Administration Guide*, *Job Management Partner 1/Automatic Job Management System 3 System Design (Configuration) Guide*, *Job Management Partner 1/Automatic Job Management System 3 System Design (Work Tasks) Guide*, *Job Management Partner 1/Automatic Job Management System 3 Administration Guide*, and the *Job Management Partner 1/Power Monitor Description, User's Guide and Reference*.

(2) Setup on the secondary node

Before you start setup on the secondary node, make sure that you complete the setup tasks for JP1/Base and the programs that require JP1/Base (JP1/IM, JP1/AJS, or JP1/Power Monitor) on the primary node.

To set up the physical and logical hosts on the secondary node:

1. Set user management function for the physical host.

   Specify this option if you want to run an authentication server on the physical host. For details on the user management function, see *6.1 User management setup (in Windows)*.

2. Modify the event server settings (`conf`) for the physical host.

   Modify the settings for the event service communication protocol (`ports` parameter) and retry limit for forwarding JP1 events (`forward-limit` parameter).

   For the `ports` parameter, specify the IP address used for the physical host or the name of the physical host.

The event service stops during failovers. Use the `forward-limit` parameter to specify the maximum period to retry forwarding the JP1 events that could not be sent during a failover. By default, the system continues to retry for 3,600 seconds.

The event server settings file (`conf`) resides in the following location:

installation-folder`\conf\event\servers\default\`

The following shows an example of the parameter settings:

```
ports IP-address-of-physical-host jp1imevt jp1imevtapi
forward-limit 3600
```

For details on the event server settings file, see *Event server settings file* in *14. Definition Files*.

3. On the primary node, execute the `jbsgetcnf` command.

   Execute the following command on the primary node: This command saves the common definition information to the backup file.
   `jbsgetcnf -h` *logical-host-name* `>` *backup-file-name*

4. Copy the backup file to the secondary node.

5. On the secondary node, execute the `jbssetcnf` command:

   Execute the following command on the secondary node: In *backup-file-name*, specify the backup file created by the `jbsgetcnf` command.
   `jbssetcnf` *backup-file-name*

6. Set the logical host.

   Setting up through GUI

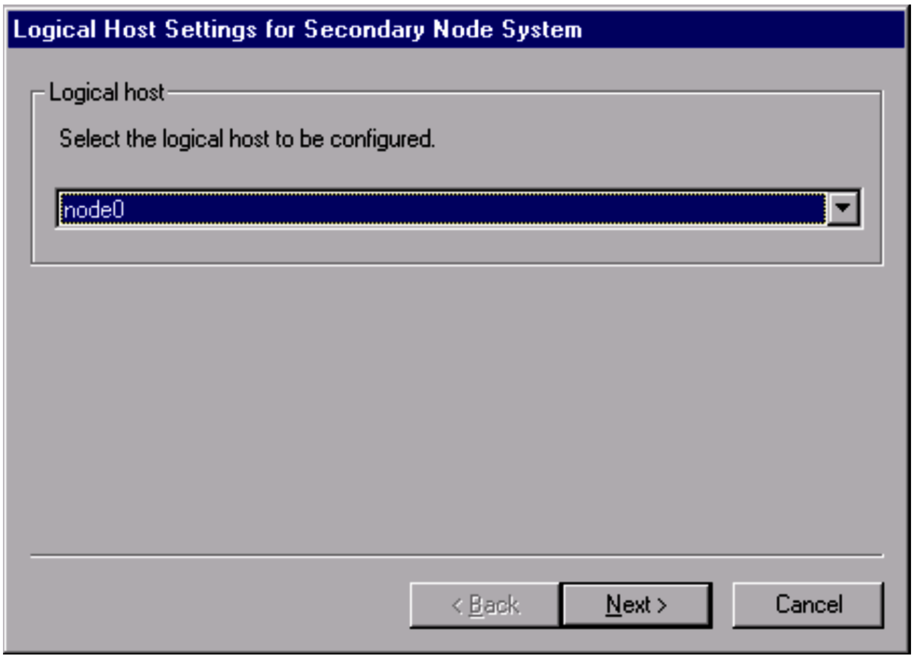
   1. Execute *installation-folder*`\bin\jp1bshasetup.exe`.

      The Settings for Base Cluster System dialog box appears.

   2. Click the **Logical Host Settings for Secondary Node System** button.

      The Logical Host Settings for Secondary Node System dialog box appears. In this dialog box, select the logical host name that you specified on the primary node.

Figure 3-10: Logical Host Settings for Secondary Node System dialog box



Logical Host Settings for Secondary Node System

Logical host

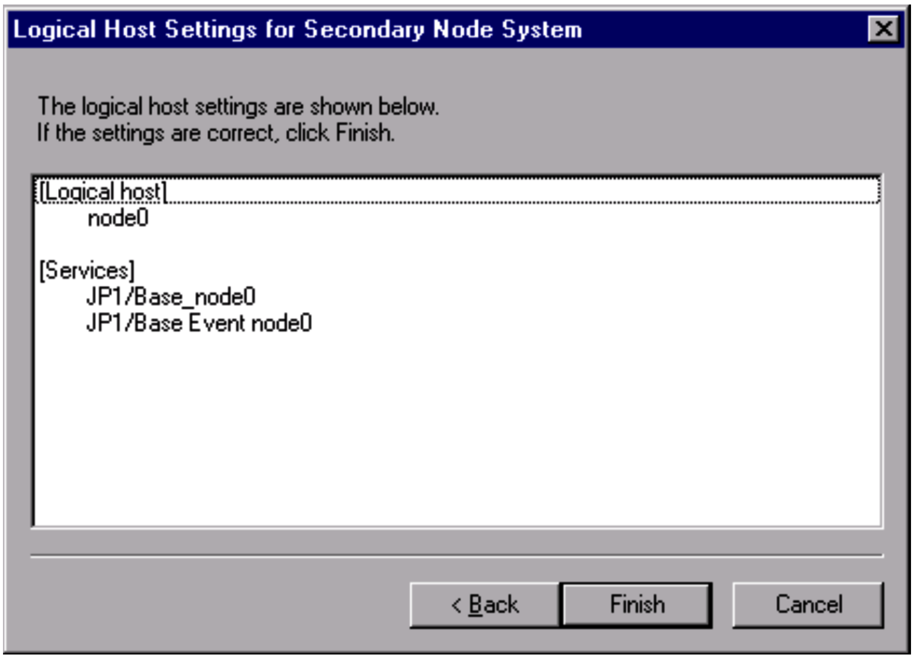
Select the logical host to be configured.

node0

3. Click the **Next** button.

The settings for the selected logical host are displayed.

Figure 3-11: Logical Host Settings for Secondary Node System dialog box (confirmation window)



Logical Host Settings for Secondary Node System

The logical host settings are shown below.
If the settings are correct, click Finish.

```
[Logical host]
    node0

[Services]
    JP1/Base_node0
    JP1/Base Event node0
```

You can use this dialog box to check the settings. If the settings are correct, click the **Finish** button.

Set up by using commands

Execute the command as follows:

```
jbs_setup_cluster -h node0
```

For details on the `jbs_setup_cluster` command, see *jbs_setup_cluster (Windows only)* in *13. Commands*.

This completes JP1/Base setup on the secondary node.

(3) Disabling Dr. Watson error notification (primary and secondary nodes)

The display of the Dr. Watson message box for reporting an application error might prevent failovers from occurring. As this might prevent JP1/Base from failing over successfully, you must disable the box display.

Note that disabling error notification might affect information acquisition when an application error occurs.

To disable Dr. Watson error notification:

1. From the command prompt, enter `drwtsn32 -i` to enable settings for Dr. Watson.

   This command installs Dr. Watson as the default application debugger.
2. From the **Start** menu, choose **Run**.
3. Type `drwtsn32` in the text box and click the **OK** button.

   The Dr. Watson dialog box appears.
4. Clear the **Visual Notification** check box.
5. Click the **OK** button.

(4) Disabling Microsoft error reporting (primary and secondary nodes)

In Windows Server 2003, when an application error occurs, a dialog box appears for reporting the error to Microsoft. The display of this dialog box might prevent failovers from occurring. You must therefore disable such error reporting.

To disable Microsoft error reporting:

1. In the **Control Panel**, double-click **System**.

   The System Properties dialog box appears.
2. Select the **Advanced** tab, and then click the **Error Reporting** button.

   The Error Reporting dialog box appears.
3. Select the **Disable error reporting** radio button and clear the **But notify me when critical errors occur** check box.
4. Click the **OK** button.

3.4.4 Registering services in the cluster software

In the cluster software used in your system, register the JP1/Base services for the logical host. In Windows, you must register the following services to the cluster software:

Name	Service name
`JP1/Base_`*logical-host-name*	`JP1_Base_`*logical-host-name*
`JP1/Base Event` *logical-host-name*	`JP1_Base_Event` *logical-host-name*

Note

> The *logical-host-name* specified after `JP1_Base_Event` corresponds to the *event server name* appearing in the description of the event service in this manual.

For details on the registration procedure, see the documentation for your cluster software. Remember the following points when registering services:

- Ensure that the secondary node can take over the services, together with the IP address and shared disk, from the primary node. Also, if the failover of an application program leads to the failover of a service, ensure that the secondary node can also take over the application program.
- After the logical IP address and shared disk have become available, start JP1/Base first, and then start JP1/IM and JP1/AJS. When stopping the products, stop them in the reverse order.

3.4.5 Modifying common definition information

To use JP1/Base in a cluster system, the common definition information pertaining to JP1/Base and the programs that require JP1/Base (such as JP1/IM, JP1/AJS, or JP1/Power Monitor) must be identical on each of the servers. After you complete the setup of JP1/Base and the programs based on JP1/Base on the physical hosts of the primary node, or if you modify the common definition information, perform the following operations to ensure that the information is consistent on all the physical hosts.

Note that this procedure affects JP1/Base and the programs that require JP1/Base.

To match the common definition information on all physical hosts:

1. At the primary node, execute the `jbsgetcnf` command to back up the common definition information:

   Execute the following:
   `jbsgetcnf -h` *logical-host-name* `>` *backup-file-name*

2. Copy the backup file to the secondary node.
3. At the secondary node, execute the `jbssetcnf` command, specifying the backup file for the argument.

   Execute the following:
   `jbssetcnf` *backup-file-name*

If you delete part of the user mapping information, you must also perform the following:

1. At the primary node, execute the `jbsgetumap` command to back up user mapping information.

   Execute the following:
   `jbsgetumap -h` *logical-host-name* `>` *backup-file-name*

2. Copy the backup file to the secondary node.
3. At the secondary node, execute the `jbsmkumap` command, specifying the backup file for the argument.

Execute the following:

```
jbsmkumap -h logical-host-name -f backup-file-name
```

3.4.6 Deleting logical hosts

The following describes how to delete a logical host. You can delete a logical host in Windows by using either the GUI or commands. You must delete the logical host on both the primary and secondary nodes. To delete a logical host:

Using the GUI

1. Execute the `jp1bshasetup.exe` command.
2. In the Settings for Base Cluster System dialog box, click the **Delete Logical Host** button.
3. Select the logical host name that you want to delete.

Using commands

Execute the command as follows:

```
jbs_setup_cluster -h node0 -r
```

For details on the `jbs_setup_cluster` command, see *jbs_setup_cluster (Windows only)* in *13. Commands*.

This procedure deletes the logical host information for JP1/Base, JP1/IM, and JP1/AJS, and deletes those services. This procedure also deletes the logical host information for JP1/Power Monitor. However, shared files and shared directories remain on the shared disk. Manually delete these files and directories.

Notes

Note the following if you specify the same name for both the logical host name and the physical host name (as output by the `hostname` command).

- Modify the settings for the event service environment.

  Enable the line `server * default`, which is coded in the event server index file (`index`) by default.

- Modify the settings for the environment setting directory.

  To specify the environment setting directory on the physical host to be the installation folder, modify the settings as follows:

  1. Create a definition file with the following contents.

  You can choose any name for the definition file.

  ```
  [JP1_DEFAULT\JP1BASE\]
  "JP1BASE_CONFDIR"="installation-folder\conf\"
  ```

2. Execute the following command to reflect the settings in the created definition file in the common definition information:

`jbssetcnf` *definition-file-name*

3.4.7 Settings to configure both physical and logical host environments on the same logical host

To configure both physical and logical host environments on the same host, you need to set up the network control. To set up network control, perform the procedure below.

1. Create a definition file that contains the following information using a text editor (such as Notepad):

   physical-host-name *physical-IP-address* `#node1`

   physical-host-name *physical-IP-address* `#node2`

   You can use any name for the definition file. Define the physical host names and the physical IP addresses to match the host environment. As a physical host name, specify a host name displayed by the `hostname` command. Physical host names and physical IP addresses must be separated by one or more spaces or tab characters. The characters following the hash and up to the next linefeed constitute a comment. End the final line of the file with a linefeed character.

   Example: When you build a 2-node cluster with `jp1-node1` (IP address is `100.100.100.1`) and `jp1-node2` (IP address is `100.100.100.2`) on the logical host `jp1-cluster`, create a definition file as stated below:

   ```
   jp1-node1  100.100.100.1

   jp1-node2  100.100.100.2
   ```

2. Apply the settings to the common definition information.

   Execute the `jbshostsimport` command to apply the contents of the definition file to the common definition information for the physical and logical hosts. For details on the `jbshostsimport` command, see *jbshostsimport* in *13. Commands*.

   Example: Execute the `jbshostsimport` command in the following formats:

   Stop JP1/Base services on physical and logical hosts.

   `c:\>`*installation-folder*`\bin\jbshostsimport -o` *definition-file-name*

   `c:\>`*installation-folder*`\bin\jbshostsimport -o` *definition-file-name* `-h jp1-cluster`

   Start JP1/Base services on physical and logical hosts.

3. Check if the settings are correctly applied to the common definition information.

Execute the following command to check the applied settings:

Example:

To check the setting of the physical host `jp1-node1`, execute:

```
c:\>installation-folder\bin\jp1ping jp1-node1
LogicalHostnameKey : no define. use JP1_DEFAULT
jp1hosts           : Use jp1hosts entry in JP1_DEFAULT
Search jp1hosts    : jp1-node1 is found.
Resolved Host List : jp1-node1 -> jp1-node1(100.100.100.1)
      ...
```

To check the setting of the physical host `jp1-node2`, execute:

```
c:\>installation-folder\bin\jp1ping jp1-node2
LogicalHostnameKey : no define. use JP1_DEFAULT
jp1hosts           : Use jp1hosts entry in JP1_DEFAULT
Search jp1hosts    : jp1-node2 is found.
Resolved Host List : jp1-node2 -> jp1-node2(100.100.100.2)
      ...
```

To check the setting of the logical host `jp1-cluster`, execute:

```
c:\>installation-folder\bin\jp1ping -h jp1-cluster jp1-node1
LogicalHostnameKey : jp1-cluster
jp1hosts           : Use jp1hosts entry in jp1-cluster
Search jp1hosts    : jp1-node1 is found.
Resolved Host List : jp1-node1 ->
100.100.100.1(100.100.100.1)
    ...
c:\>installation-folder\bin\jp1ping -h jp1-cluster jp1-node2
LogicalHostnameKey : jp1-cluster
jp1hosts           : Use jp1hosts entry in jp1-cluster
Search jp1hosts    : jp1-node2 is found.
Resolved Host List : jp1-node2 ->
100.100.100.2(100.100.100.2)
```

```
. . .
```

The settings are correctly applied if the Resolved Host List line indicates the *physical IP address* you specified, as shown in the above example. When the indicated physical IP address is different from what you have specified, review the definition file and retry the application.

3.5 Setting up the environment for a cluster system (in UNIX)

This section describes how to set up the JP1/Base environment to support a cluster system.

3.5.1 Required environment settings

The following describes the required environment settings for using JP1/Base in a cluster system. For the setting procedure, see *3.5.3 Setup*.

(1) Shared directory and files

To ensure that the primary and secondary nodes access the same information at node switching, create the following directory and files on a shared disk:

Shared file type	Directory for the shared files
Definition files	*shared-directory*`/jp1base/conf/`
Log file	*shared-directory*`/jp1base/log/`
Event server settings file	*shared-directory*`/event/`

Assign a shared directory to each logical host. You must not assign the same directory to different logical hosts. In each shared directory assigned to the logical host, create the shared files and directories.

An example of creating a directory on a shared disk is shown below.

Example: Specify `/shdsk/node0` as a shared directory for logical host `node0`.

```
    /shdsk/node0/jp1base/conf/
    /shdsk/node0/jp1base/log/
```

The event service can be set independently to run in cluster mode. However, if you set up the environment according to *3.5.3 Setup*, JP1/Base automatically specifies the logical host names in the event server index file (`index`) and creates the event server settings file (`conf`) in a shared directory.

(2) Communication protocol

When you set up the JP1/Base environment to support a cluster system, the socket binding method used in TCP/IP communication is automatically changed to IP addressing. This change affects settings for the logical hosts to be created and their constituent physical hosts. For details on the JP1/Base communication protocol, see *1.10 Communication protocols of JP1/Base*.

(3) Common definition information

In JP1/Base and the programs that require JP1/Base (JP1/IM, JP1/AJS, or JP1/Power Monitor), information about the logical hosts is set as common definition information in the local disk. You must therefore set identical information about each logical host.

The common definition information is updated when you:

- Change the common definition information for JP1/Base and the programs that require JP1/Base (JP1/IM, JP1/AJS, or JP1/Power Monitor).
- Change the user mapping information.
- Change the authentication server.
- Delete the common definition information on the logical host.
- Change the `jp1hosts` information.

If you change the common definition information, match the information on each server, referring to *3.5.5 Modifying common definition information*.

(4) Registering with clustering software

When starting or stopping the logical host, the clustering software controls the starting, stopping, assigning, and releasing of the services, shared disks, and logical IP addresses. The clustering software initially has functionality for controlling the shared disks and logical IP addresses. It does not, however, have functionality for controlling the services, therefore, you must register the service control functionality with the clustering software.

The following table shows the functionality you register with the clustering software and the command used for each function:

Functionality	Description	Command
Start	Start JP1/Base.	`jbs_start.cluster` *logical-host-name*
Stop	Stop JP1/Base.	`jbs_stop.cluster` *logical-host-name*
Operation monitoring	Monitor whether JP1/Base is operating normally. Or, check whether JP1/Base is currently operating normally. Some clustering software does not support this functionality. Register this functionality only when a failover is required upon a failure in JP1/Base.	`jbs_spmd_status -h` *logical-host-name*
Kill	Kill JP1/Base and release the resources it has been using.	`jbs_killall.cluster` *logical-host-name*

Within the `jbs_start.cluster` and `jbs_stop.cluster` commands, the following commands are executed:

Commands executed in the `jbs_start.cluster` command:

- `jevstart` *logical-host-name* (command for starting the event service)
- `jbs_spmd -h` *logical-host-name* (command for starting JP1/Base processes other than the event service)

Commands executed in the `jbs_stop.cluster` command:

- `jevstop` *logical-host-name* (command for stopping the event service)
- `jbs_spmd_stop -h` *logical-host-name* (command for stopping JP1/Base processes other than the event service)

Note

The *logical-host-name* argument in the `jevstart` and `jevstop` commands corresponds to the *event server name* in descriptions of the event service in this manual.

3.5.2 Installing JP1/Base

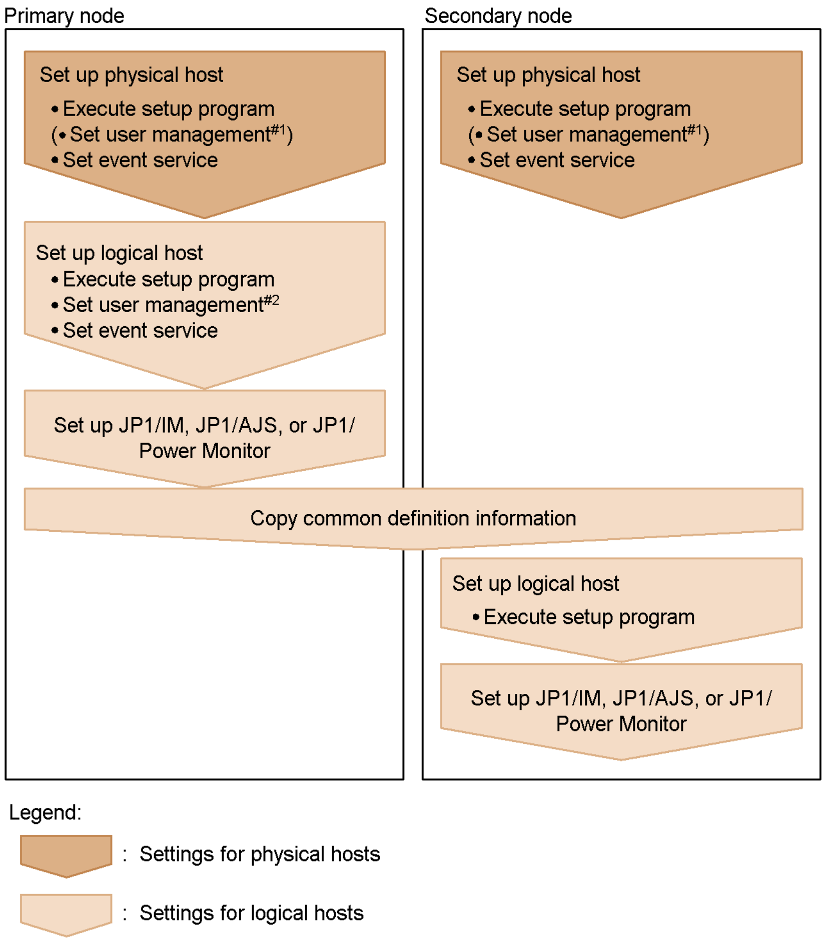
Install JP1/Base on the local disks of both the primary node and secondary node. Do not install JP1/Base on a shared disk.

If you are using JP1/Base 07-00 or an earlier version in a cluster system, you must upgrade the logical host environment after an overwrite installation. For details on the upgrade procedure, see *2.3.4(5) Overwrite installation*.

3.5.3 Setup

To operate JP1/Base in a cluster system, you must set up a physical host environment (for primary and secondary nodes) and a logical host environment (for primary and secondary nodes). The setup procedure is shown in the following figure.

Figure 3-12: Setup procedure for a cluster system (in UNIX)



#1: Required when using the authentication server on a physical host.

#2: Required when using the authentication server on a logical host.

(1) Setup on the primary node

To define the environment on the primary node:

1. Set user management for the physical host (when running an authentication server on the physical host).

   Specify this option if you want to run an authentication server on the physical host. For details on user management, see *6.3 User management setup (in UNIX)*.

2. Modify the event server settings (`conf`) for the physical host.

   Modify the settings for the event service communication protocol (`ports` parameter) and retry limit for forwarding JP1 events (`forward-limit` parameter).

For the `ports` parameter, specify the IP address used for the physical host or the name of the physical host.

The event service stops during failovers. Use the `forward-limit` parameter to specify the maximum period to retry forwarding the JP1 events that could not be sent during a failover. By default, the system continues to retry for 3,600 seconds.

The event server settings file (`conf`) resides in the following location:

```
/etc/opt/jp1base/conf/event/servers/default/
```

The following shows an example of the parameter settings:

```
ports IP-address-of-physical-host jp1imevt jp1imevtapi
forward-limit 3600
```

For details on the event server settings file, see *Event server settings file* in *14. Definition Files*.

3. Set the logical host.

   Execute the command as follows: Create a shared directory and shared file on a shared disk to set up the authentication server.

   ```
   jp1base_setup_cluster -h node0 -d /shdsk/node0 -a node0 -s
   ```

   For details on the `jp1base_setup_cluster` command, see *jp1base_setup_cluster (UNIX only)* in *13. Commands*.

4. Set user management function for the logical host.

   If you have specified a logical host as an authentication server, register the JP1 users, set up user mapping, and set up the operating permissions of the JP1 users as follows:

   - Register the JP1 user in the common definition information (only when using the logical host as the authentication server).

     Make sure that the authentication server is active, and then execute the following command to register a JP1 user:

     `jbsadduser -h` *logical-host-name JP1-user-name*

     To check the registered JP1 user, execute the following command:

     `jbslistuser -h` *logical-host-name*

   - Register the user mapping information in the common definition information.

The user mapping definition file (`jp1BsUmap.conf`) resides in the following location:

shared-directory/`jp1base/conf/user_acl/jp1BsUmap.conf`

After editing the file (`jp1BsUmap.conf`), execute the following command to register the user mapping definition information:

`jbsmkumap -h` *logical-host-name*

To check the registered user mapping information, execute the following command:

`jbsgetumap -h` *logical-host-name*

- Match the common definition information on the physical hosts.

  When you finish these operations, match the information on all the physical hosts, as described in *3.5.5 Modifying common definition information*.

- Set JP1 user operating permissions (only when using the logical host as the authentication server).

  The user permission level file (`JP1_UserLevel`) is located in the following directory:

  shared-directory`/jp1base/conf/user_acl/JP1_UserLevel`

  After editing this file (`JP1_UserLevel`), execute the `jbsaclreload` command to apply the settings.

For details on setting user management, see *6.3 User management setup (in UNIX)*.

Notes on operating authentication servers in a cluster system:

The settings files for authentication servers are stored in the following directory.

shared-directory`/jp1base/conf/user_acl/`

If you are using a secondary authentication server, you must copy the settings files from the primary authentication server to the secondary authentication server. Note that the copy destination varies depending on whether you use the secondary authentication server in a cluster system:

When using a cluster system:

shared-directory`/jp1base/conf/user_acl/`

When not using a cluster system:

`/etc/opt/jp1base/conf/user_acl/`

After copying the settings files, execute the following command to apply the settings. You need to specify the `-h` option only if you use the secondary authentication server in a cluster system.

`jbs_spmd_reload -h` *logical-host-name*

Notes when not operating authentication servers in a cluster system:

If you omit the `-s` option when executing the `jp1base_setup_cluster` command, the authentication server process will not start for the JP1/Base instance running on that logical host.

By changing the configuration settings, you can start the authentication server process after executing the `jp1base_setup_cluster` command.

Follow these steps:

1. Stop JP1/Base.

Stop the logical host whose configuration you are changing and all programs dependent on JP1/Base on that logical host.

2. Modify the definition file.

Execute the following command to change the JP1/Base process definition file:

```
cd /shared-directory/jp1base/conf
```

```
cp -p jp1bs_spmd.conf.session.model jp1bs_spmd.conf
```

3. Restart JP1/Base.

Restart the logical host whose configuration you changed and the programs dependent on JP1/Base on that logical host.

The changed definition takes effect when you restart JP1/Base.

5. Modify the event server settings (`conf`) for the logical host.

Modify the settings for the event service communication protocol (`ports` parameter) and retry limit for forwarding JP1 events (`forward-limit` parameter).

For the `ports` parameter, specify the IP address used for the logical host or the name of the logical host.

The event service stops during failovers. Use the `forward-limit` parameter to specify the maximum period to retry forwarding the JP1 events that could not be sent during a failover. By default, the system continues to retry for 3,600 seconds.

The event server settings file (`conf`) resides in the following location: *shared-directory*`/event/`

The following shows an example of the parameter settings:

```
ports IP-address-of-logical-host jp1imevt jp1imevtapi
forward-limit 3600
```

For details on the event server settings file, see *Event server settings file* in *14. Definition Files*.

This completes JP1/Base setup on the primary node.

If any of the programs that require JP1/Base (JP1/IM, JP1/AJS, or JP1/Power Monitor) is installed, you must complete the failover settings for these programs. For details, see the *Job Management Partner 1/Integrated Management - Manager Configuration Guide*, *Job Management Partner 1/Integrated Management - Manager Administration Guide*, *Job Management Partner 1/Automatic Job Management System 2 Planning and Administration Guide*, *Job Management Partner 1/Automatic Job Management System 3 System Design (Configuration) Guide*, *Job Management Partner 1/Automatic Job Management System 3 System Design (Work Tasks) Guide*, *Job Management Partner 1/Automatic Job Management System 3 Administration Guide*, and the *Job Management Partner 1/Power Monitor Description, User's Guide and Reference*.

(2) Setup on the secondary node

Before you start to set up on the secondary node, make sure that you complete the setup tasks for JP1/Base, JP1/IM, JP1/AJS, and JP1/Power Monitor on the primary node. To set up on the secondary node, perform the following procedure:

1. Set user management for the physical host (when running an authentication server on the physical host).

   Specify this option if you want to run an authentication server on the physical host. For details on user management, see *6.3 User management setup (in UNIX)*.

2. Modify the event server settings (`conf`) for the physical host.

   Modify the settings for the event service communication protocol (`ports` parameter) and retry limit for forwarding JP1 events (`forward-limit` parameter).

   For the `ports` parameter, specify the IP address used for the physical host or the name of the physical host.

   The event service stops during failovers. Use the `forward-limit` parameter to specify the maximum period to retry forwarding the JP1 events that could not be sent during a failover. By default, the system continues to retry for 3,600 seconds.

   The event server settings file (`conf`) resides in the following location:
   `/etc/opt/jp1base/conf/event/servers/default/`

The following shows an example of the parameter settings:

```
ports IP-address-of-physical-host jp1imevt jp1imevtapi
forward-limit 3600
```

For details on the event server settings file, see *Event server settings file* in *14. Definition Files*.

3. On the primary node, execute the `jbsgetcnf` command.

   Execute the following command on the primary node. This command saves the common definition information to the backup file:

   ```
   jbsgetcnf -h logical-host-name > backup-file-name
   ```

4. Copy the backup file to the secondary node.

5. On the secondary node, execute the `jbssetcnf` command:

   Execute the following command on the secondary node. In *backup-file-name*, specify the backup file created by the `jbsgetcnf` command:

   ```
   jbssetcnf backup-file-name
   ```

6. Set the logical host.

   Execute the command as follows:

   ```
   jp1base_setup_cluster -h node0
   ```

   For details on the `jp1base_setup_cluster` command, see *jp1base_setup_cluster (UNIX only)* in *13. Commands*.

This completes JP1/Base setup on the secondary node.

3.5.4 Registering daemons in the cluster software

In the cluster software used in your system, register the JP1/Base daemons for failovers. For details on the registration procedure, see the documentation for your cluster software. Remember the following points when registering services:

- Ensure that the secondary node can take over the daemons from the primary node, together with the IP address and shared disk. Also, if the failover of an application program leads to the failover of a service, ensure that the secondary node can also take over the application program.
- After the logical IP address and shared disk have become available, start JP1/Base first, and then start JP1/IM and JP1/AJS. When stopping the products, stop them in the reverse order.

The information needed when registering JP1/Base into cluster software is shown below:

Functionality	Description
Start	Start JP1/Base. • Command `jbs_start.cluster` *logical-host-name* • End timing of the start command The start command ends after JP1/Base is started. If starting JP1/Base does not complete for any reason after the timeout period (typically 60 seconds) elapsed the command ends before JP1/Base is started. In such a case, an attempt to start JP1/Base is not suspended; the command ends but an attempt to start JP1/Base continues. • Result start judgment for the start command The result of starting JP1/Base should be determined by the operation monitor method described below. Usually, the operation monitor functionality of the clustering software is used. The return value of the start command cannot be used for judgment because it is either `0` (normal end) or `1` (abnormal argument).
Stop	Stop JP1/Base. • Command `jbs_stop.cluster` *logical-host-name* • End timing of the stop command The stop command ends after JP1/Base is stopped. If stopping JP1/Base does not complete for any reason after the timeout period (typically 60 seconds) elapsed, the command ends before JP1/Base is stopped. In such a case, the attempt to stop JP1/Base is not suspended; the command ends but the attempt to stop JP1/Base continues. • Result judgment for the stop command The result of stopping JP1/Base should be determined by the operation monitor method described below. The return value of the stop command cannot be used for judgment because it is either `0` (normal end) or `1` (abnormal argument). Remarks: We recommend that you execute the kill command, described below, after the stop command ends. This ensures that the process terminates regardless of any problem, thus preventing failovers from failing.

Functionality	Description
Operation monitoring	Use the return values from the `jbs_spmd_status` and `jevstat` commands to monitor whether JP1/Base is operating normally. These commands judge the operating status based on whether each process is running or not. Some clustering software does not support this functionality. Register this functionality only when a failover is required upon a failure in JP1/Base. • Command `jbs_spmd_status -h` *logical-host-name* `jevstat` *logical-host-name* • Result judgment for operation monitoring The return values have the following meanings: Return value = `0` (all operating) JP1/Base is operating normally. Return value = `1` (error) An unrecoverable error has occurred. Judge this as a failure. Note If you execute the `jbs_spmd_status` command on the secondary node with the shared disk offline, it returns `1` because the shared disk is not found. Return value = `4` (partial stop) Some of the JP1/Base processes have stopped for some reason. Judge this as a failure (for UNIX).# Return value = `8` (all stopped) All processes of JP1/Base have stopped for some reason. Judge this as a failure. Return value = 12 (error but retry possible) While the `jbs_spmd_status` command is checking the operating status, an error has occurred which can be recovered by retry. Retry checking the operating status up to a specified number of times. For the `jevstat` command, this return value indicates an error for which retry is not possible.
Kill	Kill JP1/Base and release the resources it has been using. • Command `jbs_killall.cluster` *logical-host-name* When you execute the `jbs_killall.cluster` command, each process is forcibly stopped without performing any processing for stopping JP1/Base. Note Stop JP1/Base using the stop command before executing the kill command. Use the kill command only when a problem has occurred, for example, when executing the stop command cannot terminate processing.

# In Windows, operation differs from that in UNIX due to the relationship with service control by Windows. If some processes have stopped in Windows, the JP1 process management automatically stops all the processes, placing the service into the stopped state. You can determine a failure by detecting the stop of the service or when the `jbs_spmd_status` command returns a value of 8.

Remarks: Restarting JP1

If a JP1 failure is detected in a cluster system, the primary server might restart JP1 to attempt recovery before it performs a failover to the secondary server.

In such a case, we recommend that you use the clustering software control to restart JP1 rather than restarting by JP1 process management.

The clustering software attempts to restart JP1 after a failure is detected, so that it might prevent the normal operation of the JP1 restart functionality. To ensure a more reliable restart, restart JP1 under the control of the clustering software.

3.5.5 Modifying common definition information

If you are running JP1/Base or any of the programs that require JP1/Base (JP1/IM, JP1/AJS, or JP1/Power Monitor) in a cluster system, you must set the same common definition information on each physical host. After you complete the setup of JP1/Base and the programs based on JP1/Base on the physical hosts of the primary node, or if you modify the common definition information, perform the following operations to ensure that the information is consistent on all the physical hosts.

Note that this procedure affects JP1/Base and the programs that require JP1/Base.

To match the common definition information on all physical hosts:

1. At the primary node, execute the `jbsgetcnf` command to back up the common definition information:

   Execute the following:
   `jbsgetcnf -h` *logical-host-name* `>` *backup-file-name*

2. Copy the backup file to the secondary node.

3. At the secondary node, execute the `jbssetcnf` command, specifying the backup file for the argument.

   Execute the following:
   `jbssetcnf` *backup-file-name*

If you delete part of the user mapping information, you must also perform the following:

1. At the primary node, execute the `jbsgetumap` command to back up user mapping information.

   Execute the following:
   `jbsgetumap -h` *logical-host-name* `>` *backup-file-name*

2. Copy the backup file to the secondary node.

3. At the secondary node, execute the `jbsmkumap` command, specifying the backup file for the argument.

   Execute the following:

```
jbsmkumap -h logical-host-name -f backup-file-name
```

3.5.6 Deleting logical hosts

The following describes how to delete a logical host. In UNIX, use commands to delete a logical host. You must delete the logical host on both the primary and secondary nodes. Execute the following:

```
jbsunsetcnf -i -h logical-host-name
```

For details on the `jbsunsetcnf` command, see *jbsunsetcnf* in *13. Commands*.

This procedure deletes the logical host information for JP1/Base and the programs that require JP1/Base (JP1/IM, JP1/AJS, or JP1/Power Monitor). However, shared files and shared directories remain on the shared disk. Delete these files and directories manually.

Notes

Note the following if you specify the same name for both the logical host name and the physical host name (as output by the `hostname` command).

- Modify the settings for the event service environment.

  Enable the line `server * default`, which is coded in the event server index file (`index`) by default.

- Modify the settings for the environment setting directory.

  To specify the environment setting directory on the physical host to be the installation folder, modify the settings as follows:

  1. Create a definition file with the following contents.

  You can choose any name for the definition file.

  ```
  [JP1_DEFAULT\JP1BASE\]
  "JP1BASE_CONFDIR"="/etc/opt/jp1base/conf"
  ```

  2. Execute the following command to reflect the settings in the created definition file in the common definition information:

  ```
  /opt/jp1base/bin/jbssetcnf definition-file-name
  ```

3.6 Notes on using JP1/Base in a cluster system

This section provides some notes on using JP1/Base in a cluster system. These notes are divided into common guidelines for both Windows and UNIX, notes for Windows only, and notes for UNIX only.

(1) Guidelines common to both Windows and UNIX

- When setting up JP1/Base in a cluster system, make sure that you stop the JP1/Base services active on the physical host and existing logical hosts. If you do not stop the JP1/Base services before setting up JP1/Base, the services on the logical hosts will not operate properly. If this happens, recover by restarting the server.
- To issue events from a user application in a cluster system, use the `jevsend` command with the `-s` option specified. For the `-s` option, specify the event server name. This option allows issued events to be inherited from the primary node to the secondary node when a failover occurs.
- When node switching is enabled, JP1/Base does not support duplication of the event database and command execution log (ISAM) file. Use a mirror disk or RAID disk to ensure the reliability of the disk system.
- When using JP1/Base in a cluster system, specify `sync` for the `options` parameter in the event server settings file (`conf`). The OS normally stores data written from a program in buffer memory, and then writes it to the disk in order to improve performance. Therefore, if the system suddenly terminates because of a power failure or an error in the OS, any data not yet written to the disk will be lost. The event service suppresses this buffering to prevent data from disappearing. If you specify `no-sync` for the `option` parameter or specify neither `sync` nor `no-sync`, data might be lost.
- The more logical hosts you concurrently activate in a cluster system, the greater the system resources required.
- To run JP1/Base on both the logical and physical hosts in a cluster system, you must change the event service setting on the physical hosts to IP addressing. Edit the event server settings file (`conf`) on both the primary and secondary nodes, changing the address specified in the `ports` parameter to the local host name or to the IP address of the local host. The event service on the physical host is set by default to `0.0.0.0`, but the event service with this address cannot be activated concurrently with the event service on the logical host. For details on the event server settings file, see *Event server settings file* in *14. Definition Files*.
- When the authentication server is switched during a failover, the related programs behave as follows:

  JP1/IM

A communication error occurs. Operations are restored after the failover.

JP1/AJS

A communication error occurs. The user must log in again after the failover.

You can avoid potential problems due to this behavior of JP1/IM and JP1/AJS2 by placing the authentication server on a host outside the cluster system.

- If you want to monitor files on a shared disk using the JP1/Base log file trapping function, ensure that the shared disk remains accessible while the files are being monitored. If you change the shared disk allocation during file monitoring, problems such as errors in the monitoring process and control failure in disk space allocation and deallocation could occur.
- To prevent data from being lost from the command execution log file (ISAM), specify `ON` for the `-flush` option of the `jcocmddef` command, enabling the command execution log to be written line-by-line to the disk. For details on the `jcocmddef` command, see the manual *Job Management Partner 1/Integrated Management - Manager Command/Definition Reference*.

(2) Notes concerning Windows only

- Always perform the operations from the primary node when you are specifying an authentication server or registering JP1 users on a logical host. Be sure to start the JP1/Base service on the logical host before you start JP1 user registration.
- When backing up the definitions on the primary node in a cluster environment, make sure that all the letters in the logical host name that you specify in the `jbsgetcnf` command match the case of the logical host name in the definitions.

  If you make a mistake, delete the logical host and specify it again.
- Before you delete a logical host, first stop the services of JP1/Base and the programs that require JP1/Base (JP1/IM, JP1/AJS, or JP1/Power Monitor) running on that logical host. If you delete a logical host with a service still active, delete that service in either of the following ways:
  - Recreate a logical host with the same name, and then delete it.
  - Uninstall JP1/Base.
- If you create a logical host with the same host name as the local host, the `JP1/Base Event` service on the physical host will be deleted if you later delete that logical host. To restore the service, execute the following command:

  ```
  jevregsvc -r
  ```
- If you cannot start or stop the JP1/Base service, a JP1/Base process might not have completed. In this case, restart the system.
- Even if you are not using JP1/Base on a particular physical host, the JP1/Base

LogTrap service is still required for processing by the logical host. If you are not using the JP1/Base Control Service, set auto startup for the JP1/Base LogTrap service.

- The startup control function is not available for the services running on logical hosts. The startup control function is only available for the services running on physical hosts. Use cluster software to control startup of services on logical hosts.

(3) Notes concerning UNIX only

- If you stop JP1/Base services that support logical hosts, a JP1/Base process might fail to stop. In this case, execute the `jbs_killall.cluster` command to forcibly stop the process. Note that this command should be used only when JP1/Base processes cannot be stopped with the normal procedure. For details on the `jbs_killall.cluster` command, see *jbs_killall.cluster (UNIX only)* in *13. Commands*.
- In a cluster system that performs monitoring even during stop processing, modify the command that terminates JP1/Base (the event service and process management including user management), as follows:

```
cd /etc/opt/jp1base

cp -p jbs_stop.cluster.retry.model jbs_stop.cluster
```

3.7 Setting up a logical host in a non-cluster environment

This section describes how to configure and run logical hosts that will not fail over. The setup and operation of logical hosts in a non-failover environment are the same as for logical hosts used in an ordinary cluster system.

3.7.1 Considerations when using logical hosts in a non-cluster environment

When you run JP1 on multiple logical hosts, each instance of JP1 takes up system resources (including memory, disk space, CPU time, and semaphores). The system will not work properly if insufficient resources are available when multiple JP1 programs run concurrently. Estimate the system resources required according to the number of JP1 programs that will run concurrently. Alternatively, you can limit the number of concurrent JP1 programs to a number that the system can handle.

For information on estimating memory and disk space requirements, see the *Release Notes*.

3.7.2 Configuring a logical host in a non-cluster environment

The following describes how to run JP1 in an environment with logical hosts that are not linked with cluster software and do not fail over.

(1) Preparing the logical host environment

To create the logical host environment, prepare the disk area and IP address for each logical host.

- Disk area for the logical host

  Create a directory on the local disk, different from that used by JP1 programs on the physical host or any existing logical host, for sole use by JP1 on the logical host you are configuring.

- IP address for the logical host

  Have the OS allocate an IP address to the logical host.

  You can use a real IP or an alias. However, make sure that the IP address can be uniquely resolved from the logical host name.

  The prerequisites for the logical host environment are the same as for running JP1 in a cluster system. However, because the logical host does not fail over, some requirements do not apply, such as the ability to inherit data between servers.

Note that the descriptions in *3. Setting Up JP1/Base for Use in a Cluster System* about shared disks and logical IP addresses when setting up a cluster system should be understood as the disk area and IP address allocated in the steps above for a non-cluster environment.

- Performance estimation

  Take the following points into consideration when you estimate whether system resources are adequate:

  - Estimate whether sufficient resources can be allocated within the system to allow multiple instances of JP1 to start. If the system has insufficient resources, it might not operate correctly or performance might be degraded.
  - When you set the total number of JP1 events or JP1/AJS jobs that are permitted to start concurrently among all of the logical hosts, do not exceed the amount of application traffic that the physical host can handle. Keep in mind that starting multiple JP1 programs on separate logical hosts does not provide a proportionate increase in processing capacity.

(2) Setting up JP1 in the logical host environment

Set up JP1 in the logical host environment in the same way that a primary server is set up in a failover cluster system. For a failover cluster system, setup must be performed on both servers. For a non-failover environment, you only set up JP1 on the server where it will run.

(3) Setting up automatic startup and automatic termination in a logical host environment

The settings for automatic startup and automatic termination are not specified when you set up JP1 for a logical host environment. To specify these settings, see *3.7.3(2) Examples of setting up automatic startup and automatic termination*.

3.7.3 Logical host operation in a non-cluster environment

JP1 operations and backup and recovery procedures are the same on a logical host that does not fail over as on a logical host in a cluster system. However, this excludes the fact that the logical host does not fail over with the cluster software.

(1) Startup and termination

Start JP1 services on the logical host in the following order:

1. JP1/Base
2. JP1 programs for which JP1/Base is a prerequisite

Stop JP1 services on the logical host in the following order:

1. JP1 programs for which JP1/Base is a prerequisite
2. JP1/Base

(2) Examples of setting up automatic startup and automatic termination

To start and stop JP1 services on a logical host automatically at system startup and shutdown, you must set up JP1/Base as described below. The procedure differs for each OS. The following shows the procedure for each OS.

(a) In Windows

1. Using a text editor, add the following lines to the start sequence definition file (`JP1SVPRM.DAT`):

   File location: *JP1/Base-installation-folder*`\conf\boot\JP1SVPRM.DAT`

```
[Jp1BaseEvent_logical-host-name]
Name=JP1/BaseEvent_logical-host-name
ServiceName=JP1_Base_Event logical-host-name

[Jp1Base_logical-host-name]
Name=JP1/Base_logical-host-name
ServiceName=JP1_Base_logical-host-name
StopCommand=jbs_spmd_stop.exe -h logical-host-name

[Jp1AJS2_logical-host-name]
Name=JP1/AJS2_logical-host-name
ServiceName=JP1_AJS2_logical-host-name
StopCommand=jajs_spmd_stop.exe -h logical-host-name
```

   The command specified in `StopCommand` is executed when JP1/Power Monitor shuts down the host.

(b) HP-UX environment

1. Create the automatic startup and automatic termination scripts for the logical host.

   `Location:/sbin/init.d/jp1_service_cluster`

   Example automatic startup and automatic termination scripts

```
#!/bin/sh

## Set Environment-variables
PATH=/sbin:/bin:/usr/bin:/opt/jp1base/bin
export PATH
JP1_HOSTNAME=logical-host-name
export JP1_HOSTNAME

case $1 in
start_msg)
      echo "Start JP1 Service $JP1_HOSTNAME"
      ;;
```

```
stop_msg)
      echo "Stop JP1 Service $JP1_HOSTNAME"
      ;;

'start')
      if [ -x /etc/opt/jp1base/jbs_start.cluster ]
      then
              /etc/opt/jp1base/jbs_start.cluster
      fi
      if [ -x /etc/opt/jp1ajs2/jajs_start.cluster ]
      then
              /etc/opt/jp1ajs2/jajs_start.cluster
      fi
      ;;

'stop')
      if [ -x /etc/opt/jp1ajs2/jajs_stop.cluster ]
      then
              /etc/opt/jp1ajs2/jajs_stop.cluster
      fi
      if [ -x /etc/opt/jp1base/jbs_stop.cluster ]
      then
              /etc/opt/jp1base/jbs_stop.cluster
      fi
      ;;

esac

exit 0
```

2. Link to the scripts you created at step 1.

Startup script

Execute the following command to set up the link:

```
ln -s /sbin/init.d/jp1_service_cluster /sbin/rc2.d/
S***_JP1_SERVICE
```

The higher the value in ***, the later the startup script is executed.

Termination script

Execute the following command to set up the link:

```
ln -s /sbin/init.d/jp1_service_cluster /sbin/rc1.d/
K***_JP1_SERVICE
```

The higher the value in ***, the later the termination script is executed.

Typically, set the values so that a JP1 service that starts earlier stops later.

(c) Solaris environment

1. Create the automatic startup and automatic termination scripts for the logical host.

   Location: `/etc/init.d/jp1_service_cluster`

   Example automatic startup and automatic termination scripts

```
#!/bin/sh

## Set Environment-variables
PATH=/sbin:/bin:/usr/bin:/opt/jp1base/bin
export PATH
JP1_HOSTNAME=logical-host-name
export JP1_HOSTNAME

case $1 in
start_msg)
      echo "Start JP1 Service $JP1_HOSTNAME"
      ;;

stop_msg)
      echo "Stop JP1 Service $JP1_HOSTNAME"
      ;;

'start')
      if [ -x /etc/opt/jp1base/jbs_start.cluster ]
      then
              /etc/opt/jp1base/jbs_start.cluster
      fi
      if [ -x /etc/opt/jp1ajs2/jajs_start.cluster ]
      then
              /etc/opt/jp1ajs2/jajs_start.cluster
      fi
      ;;

'stop')
      if [ -x /etc/opt/jp1ajs2/jajs_stop.cluster ]
      then
              /etc/opt/jp1ajs2/jajs_stop.cluster
      fi
      if [ -x /etc/opt/jp1base/jbs_stop.cluster ]
      then
              /etc/opt/jp1base/jbs_stop.cluster
      fi
      ;;
```

```
esac

exit 0
```

2. Link to the scripts you created at step 1.

   Startup script

   Execute the following command to set up the link:

   ```
   ln -s /etc/init.d/jp1_service_cluster /etc/rc2.d/
   S**_JP1_SERVICE
   ```

   The higher the value in **, the later the startup script is executed.

   Termination script

   Execute the following command to set up the link:

   ```
   ln -s /etc/init.d/jp1_service_cluster /etc/rc0.d/
   K**_JP1_SERVICE
   ```

   The higher the value in **, the later the termination script is executed.

   Typically, set the values so that a JP1 service that starts earlier stops later.

(d) In AIX environment

1. Using the `mkitab` command, make the following entries in the `/etc/inittab` file:

   ```
   # mkitab -i hntr2mon "jp1base:2:wait:/etc/opt/jp1base/
   jbs_start.cluser logical-host-name"
   # mkitab -i jp1base "jp1ajs2:2:wait:/etc/opt/jp1ajs2/
   jajs_start.cluser logical-host-name"
   ```

   The added lines execute startup processing for JP1 services when the system starts.

2. Using a text editor, add the following lines to the `/etc/rc.shutdown` file, after the code that terminates programs for which JP1/Base is a prerequisite:

   ```
   test -x /etc/opt/jp1ajs2/jajs_stop.cluster && /etc/opt/
   jp1ajs2/jajs_stop.cluster logical-host-name
   test -x /etc/opt/jp1base/jbs_stop.cluster && /etc/opt/
   jp1base/jbs_stop.cluster logical-host-name
   test -x /opt/hitachi/HNTRLib2/etc/D002stop &&
   /opt/hitachi/HNTRLib2/etc/D002stop
   ```

   The added lines execute termination processing for JP1 services when the system stops.

(e) Setting to start and stop JP1 automatically on both logical host and physical host

To start and stop JP1 automatically on the logical host and physical host, you must perform the following setting in addition to the setup for automatic startup and termination of the logical host. Note that the setup procedure depends on the OS. The following shows the procedure for each OS.

In Windows:

The startup control executes start/stop processing in the order in which services are written in the start sequence definition file (JP1SVPRM.DAT), starting from the service written first. If you want to change the order in which the physical host and logical host start or stop, define their start/stop sequence in this file, in the order in which you want the hosts to start or stop.

In HP-UX or Solaris:

The order in which JP1 services start and stop automatically is determined by the value set in the numerical portion (S** and K**) in the automatic startup and automatic termination scripts. The higher the value, the later the service starts or stops. For a physical host, the symbolic links to these scripts are created at installation. If you want the logical host to start and stop automatically with the physical host, adjust the start/stop sequence by changing the names of the symbolic links created for the logical host.

JP1/Base describes automatic startup and automatic termination scripts for a physical host in advance. The table below describes the symbolic links to these scripts.

Table 3-4: Symbolic links to automatic startup and automatic termination scripts for a physical host

OS	Startup script	Termination script
HP-UX	/sbin/rc2.d/S900jp1_base	/sbin/rc1.d/K100jp1_base
Solaris	/etc/rc2.d/S99_JP1_10_BASE	/etc/rc0.d/K01_JP1_90_BASE

Adjust the order in which the physical host and logical host start and stop by changing the S** and K** (number) part of the symbolic links shown above so that its value is higher or lower relative to the S** and K** (number) part of the symbolic links in the automatic startup and termination scripts.

For example, if you want the logical host to start first, set the number part (S**) of the symbolic link to the automatic startup script you created for the logical host to a value lower than 900 (for HP-UX) or 99 (for Solaris).

In AIX:

To start and stop the physical host automatically, additional settings are required. For details on the additional settings, see *5.2.1 Setting services to start and stop automatically*.

(3) Operations on JP1 running on the logical host

When executing a command for JP1 configured on a logical host, specify the logical host name explicitly in the same way as for a logical host running in a cluster system.

(4) Inheritance of logical host information

A logical host in a non-cluster environment cannot be failed over because it does not inherit the management information on the shared disk. For this reason, do not use such a logical host in a multiple-host environment where a logical host IP is passed from one host to another.

Chapter

4. JP1/Base Communication Settings According to Network Configurations

This chapter describes JP1/Base communication settings according to network configurations. The issues discussed in this chapter regarding JP1/Base communication settings also apply to the JP1/Base prerequisite programs.

For an overview of the communication protocol of JP1/Base, see *1.10 Communication protocols of JP1/Base*.

4.1 Using JP1/Base on a single network

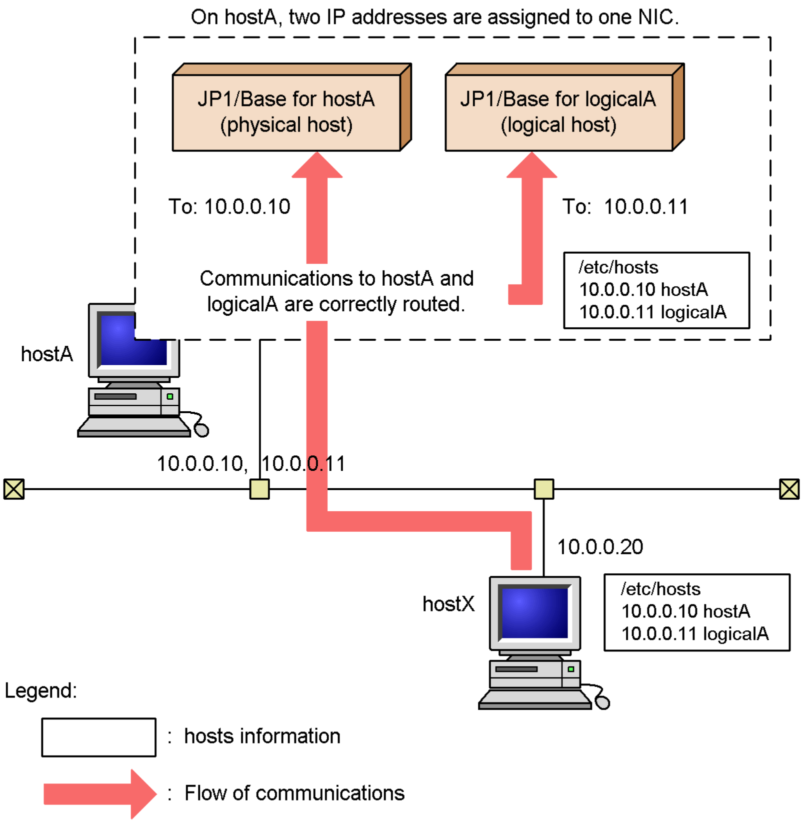
This section describes how to use JP1/Base on a single network and how you should configure the communication settings for this use.

When you use physical hosts only, JP1/Base can be used in the default setting (ANY binding method). There is no need to change the communication settings.

Even when you use JP1/Base in a cluster system, there is no need to change the communication settings if you configure JP1/Base for the cluster system by using either the GUI (`jp1bshasetup.exe`) or the `jbs_setup_cluster` command in Windows, or the `jp1base_setup_cluster` command in UNIX, which all automatically set JP1/Base to use the IP binding method. If you configure JP1/Base for a cluster system, the physical hosts receive the communications to the physical hosts and the logical hosts receive the communications to the logical hosts.

The following figure shows the communication procedure when you use JP1/Base in a cluster system on a single network.

Figure 4-1: Communication procedure of JP1/Base used in a cluster system on a single network



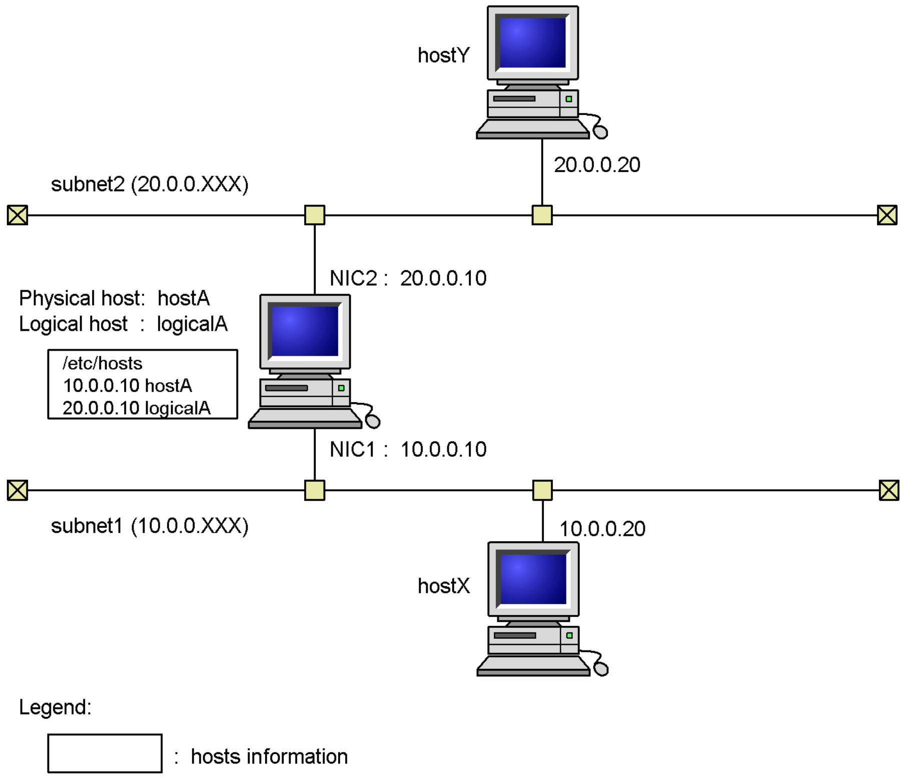
4.2 Using JP1/Base on multiple networks

This section describes how to use JP1/Base in multiple networks and how you should configure the communication settings for this use.

When you use only physical hosts on a host connected by multiple NICs to multiple networks, JP1/Base can be used in the default setting (ANY binding method). There is no need to change the communication settings.

When you use logical hosts on a host connected by multiple NICs to multiple networks (cluster operation), you need to change communication settings of JP1/Base. The following descriptions about communication settings are based on the system configuration example shown in the following figure.

Figure 4-2: A system configuration example to use JP1/Base in a cluster system on a host connected to multiple networks



(1) Conditions

The communication settings need to be changed if the following conditions are satisfied:

- hostA has 2 NICs and each of them is part of a separate subnet.
- The host name of hostA (physical host) resolves to the IP address `10.0.0.10` and the host name of logicalA (logical host) resolves to the IP address `20.0.0.10`.

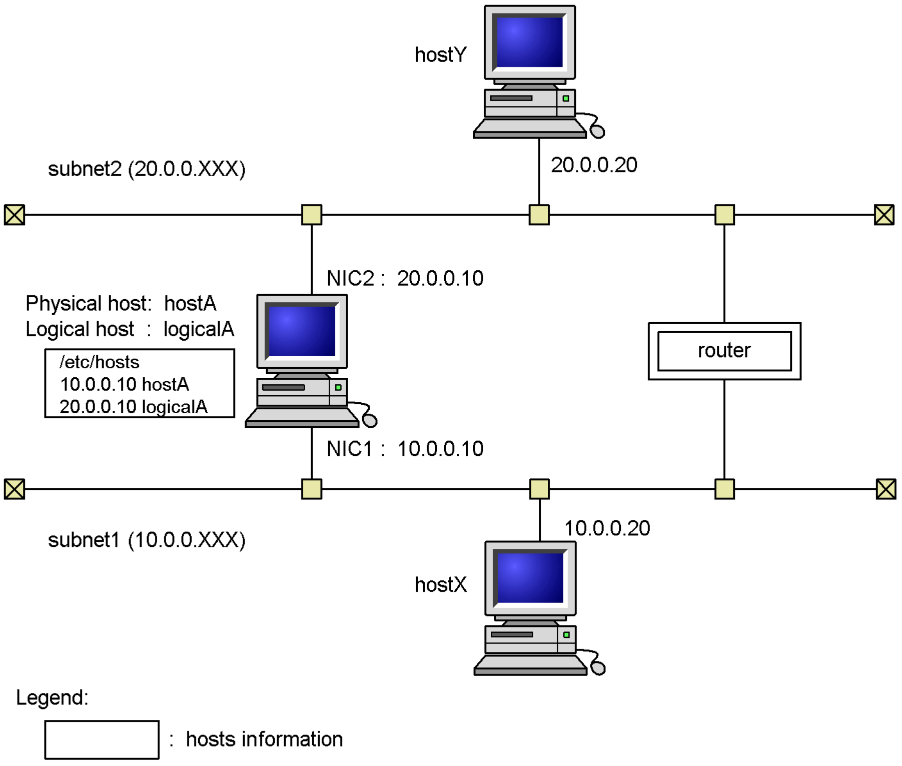
(2) Concept of communication

The physical host hostA is handled as a host within subnet1 and the logical host logicalA behaves as a host connected to subnet2 only. In this case, hostX in subnet1 can communicate with hostA, but not with logicalA. Similarly, hostY, which is in subnet2, can communicate with logicalA, but not with hostA. Therefore, you must change the communication settings to enable communications between hostX and logicalA and between hostY and hostA.

(3) Communication settings

To enable communication between all hosts, you need to configure the *routing* between subnets (there is no need to change the communication settings of JP1/Base). For information about the port numbers used in JP1/Base, see *C.1 Port numbers for JP1/Base*. By specifying routing settings, you can enable communications between hostX and logicalA, and between hostY and hostA.

Figure 4-3: A system configuration example of routing settings



You might not want to configure the routing settings for several reasons, such as your networks do not support routing, or you do not want to allow communications between subnets. If this is the case, you can change the communication settings to use JP1/Base in an environment of distinct networks. This functionality is called *multi-LAN connectivity*, and has been supported from JP1/Base 06-71. For details, see *4.3 Using JP1/Base in an environment of distinct networks*.

4.3 Using JP1/Base in an environment of distinct networks

Even when your networks do not support routing, or you do not want to allow communications between subnets, JP1/Base allows you to use JP1/Base in an environment of distinct networks. You can change JP1/Base communication settings independently from the system and other applications, which allows you to flexibly cope with various network configurations and operations. We call this functionality *multi-LAN connectivity*.

In this section, we discuss some issues when you use JP1/Base in an environment of distinct networks using multi-LAN connectivity. Then we describe how to configure the communication settings for this use.

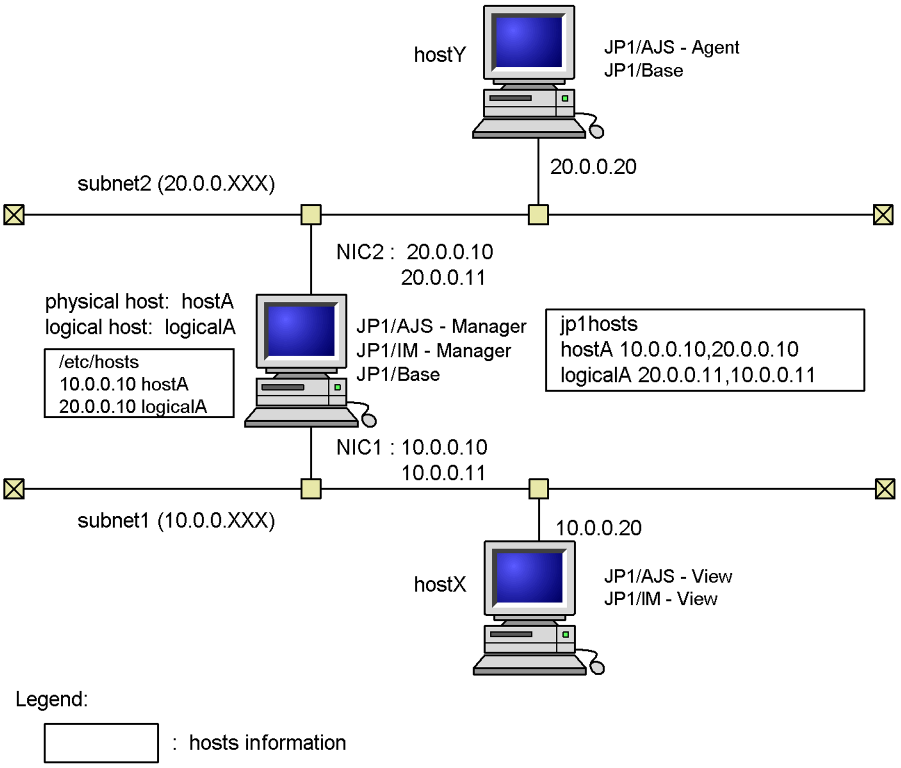
Note

When you change communication settings of a host, JP1/Base 06-71 or later must be installed on the host.

4.3.1 Issues on using JP1/Base in an environment of distinct networks

This subsection describes some issues on using JP1/Base in an environment of distinct networks, based on the system configuration example shown in the following figure. This configuration assumes that the physical host hostA and the logical host logicalA are used as manager hosts, and hostX and hostY are used as agent (or client) hosts. In this configuration, you can log in from JP1/AJS - View on hostX to JP1/AJS - Manager on hostA to execute jobs on hostY, or you can log in from JP1/IM - View on hostX to JP1/IM - Manager on hostA to monitor hostY and to execute automated actions on hostY.

Figure 4-4: A system configuration example to use JP1/Base in an environment of distinct networks



The following is a list of things to consider for the settings:

- Whether you will adopt the JP1/Base communication protocol.
- How you want to configure the communication settings of the main part of JP1/Base.

  The communication settings of the main part of JP1/Base are required to exchange data other than JP1 events between hosts. This includes the data for user authentication, distribution of the configuration definition information, or remote commands (for JP1/IM). When you consider the communication settings of the main part of JP1/Base, the following two points are important:

  - definition of `jp1hosts` information.
  - selection of the communication protocol to transmit/receive data.
- How you want to configure the communication settings of event services.

  The communication settings of event services are required to exchange JP1 events between hosts.

Note that you must restart JP1/Base after you change the communication settings.

(1) Whether you will adopt the JP1/Base communication protocol.

By default, JP1/Base 06-71 and later versions run using the communication settings of version 06-51 or earlier to maintain backward compatibility. You must first decide whether you will adopt the JP1/Base communication protocol.

(2) Definition of jp1hosts information (for the main part of JP1/Base)

Some OSs do not allow resolution of one host name into multiple IP addresses. If this is the case, JP1/Base can resolve IP addresses by defining its own hosts information. This hosts information dedicated for JP1/Base is called `jp1hosts` information. To enable both physical and logical hosts to use subnet1 and subnet2, assign IP addresses of physical and logical hosts to both NICs (use the `ipconfig` command in UNIX). Then, the assignments must be defined as the `jp1hosts` information.

When you execute `ping logicalA` on hostX, it might detect `20.0.0.11` of subnet2 and you might not be able to establish communication. This case can also be resolved by defining `jp1hosts` on hostX.

Note

Define the `jp1hosts` information only when host names cannot be resolved with `hosts` and DNS settings.

To apply the `jp1hosts` information written in a `jp1hosts` definition file, use the `jpshostsimport` command to register it with the common definition information. For details, see *4.3.2 Defining jp1hosts information*.

(3) Selection of communication protocol to transmit/receive data (for the main part of JP1/Base)

You need to change the communication protocol when you use a host connected to multiple networks in a cluster system. This subsection briefly describes the selection of the communication protocol based on Figure 4-4.

A host connected to multiple networks uses both physical and logical hosts. If you change the reception setting to the ANY binding method, the logical hosts might receive the data directed to the physical hosts and vice versa. Therefore, the reception setting must be the IP binding method.

On the other hand, the transmission setting must be the ANY binding method because the IP binding method might send data only to subnet1 or subnet2.

When you set JP1/Base for use in a cluster system, both transmission and reception settings are set to the IP binding method by default. Therefore, you need to change the transmission setting to the ANY binding method. To apply the changes of the communication protocol for the main part of JP1/Base, use the `jbssetcnf` command to register the communication protocol settings files with the common definition information. For details, see *4.3.3 Changing communication settings*.

(4) Communication settings of event services

In the case of event services, edit the event server settings file (`conf`) to change the communication settings described in *11.3.1(2) Definition of jp1hosts information (for the main part of JP1/Base)* and *11.3.1(3) Selection of communication protocol to transmit/receive data (for the main part of JP1/Base)*. For details, see *4.3.4 Changing communication settings of event services*.

(5) Restart JP1/Base

You must restart JP1/Base after you change the communication settings.

4.3.2 Defining jp1hosts information

JP1/Base can hold its own hosts information, which enables resolution of IP addresses independently of the OS. By registering this dedicated hosts information (`jp1hosts` information) with the common definition information, the main part of JP1/Base can communicate with IP addresses that do not correspond to physical or logical host names on the destination host. For example, if your OS cannot resolve one host name into multiple IP addresses, you can define `jp1hosts` information to enable JP1/Base to solve it. The `jp1hosts` information does not exist at the installation of JP1/Base. You need to register it with the common definition information when required. For information about which functionality of JP1/Base support the `jp1hosts` information, see *H. Handling Changes in Communication Settings*.

Note

> When you define `jp1hosts` information, the definitions in the `hosts` file and DNS are not referenced for the host names and IP addresses defined in the `jp1hosts` information.
>
> Example:
>
> `jp1hosts` information:
> ```
>   hostA 100.0.0.10, 200.0.0.10
> ```
>
> `hosts` file:
> ```
>   100.0.0.10 hostA hostB
>   200.0.0.10 hostC
> ```
>
> In these definitions, the `hosts` file is not referenced for hostA, `100.0.0.10`, and `200.0.0.10`.

The `jp1hosts` information must be registered with the common definition information when:

- using a host connected to multiple networks in a cluster system, or

- communication cannot be established with the IP address used in the connection with the destination host.

To register `jp1hosts` information with the common definition information:

1. Edit the `jp1hosts` definition file.

   A `jp1hosts` definition file is provided by default. It is stored as the `jp1hosts` file in *installation-folder*`\conf\` for Windows or `/etc/opt/jp1base/conf/` for UNIX. This default `jp1hosts` definition file cannot be used without editing it. When you use the default `jp1hosts` definition file, you must first edit it according to the use in JP1/Base. When you create your own `jp1hosts` definition file, store it in the same folder as the default `jp1hosts` file is stored. For details on the format of the `jp1hosts` definition file, see *jp1hosts definition file* in *14. Definition Files*.

2. Execute the `jbshostsimport` command in the following format to register the `jp1hosts` definition file with the common definition information.

   Execute the command as follows:
   `jbshostsimport {-o|-r}` *jp1hosts-definition-file-name* `[-h` *logical-host-name*`]`

Use the `jbshostsexport` command to check the `jp1hosts` information registered with the common definition information. For details on these commands, see *13. Commands*.

4.3.3 Changing communication settings

JP1/Base can be used in an environment of distinct networks by changing communication settings of JP1/Base itself. To change the communication settings of the main part of JP1/Base, edit the communication protocol settings files and register it with the common definition information. For information about which JP1/Base functionalities support the communication protocol settings files, see *H. Handling Changes in Communication Settings*.

The communication protocol for the main part of JP1/Base must be changed when:

- using a host connected to multiple networks in a cluster system.

You do not need to change the communication protocol when you use a host connected to multiple networks as a physical host only.

Use the `jbssetcnf` command to register the communication protocol settings files with the common definition information. The table below describes the seven kinds of communication protocol settings files, which are stored in *installation-folder*`\conf\` for Windows or in `/etc/opt/jp1base/conf/` for UNIX.

Communication protocol settings file	Purpose
physical_ipany.conf	This file sets the IP binding method for receiving and the ANY binding method for sending. It is mainly used for changing the communication protocol for the physical hosts used in a cluster system.
logical_ipany.conf	This file sets the IP binding method for receiving and the ANY binding method for sending. It is mainly used for changing the communication protocol for the logical hosts used in a cluster system. This file must be edited.
physical_recovery_0651.conf	This file resets the communication protocol registered with the common definition information back to the communication protocol used in version 06-51 or earlier. It is mainly used for changing the communication protocol set for the physical hosts back to the communication protocol used in version 06-51 or earlier.
logical_recovery_0651.conf	This file resets the communication protocol registered with the common definition information back to the communication protocol used in version 06-51 or earlier. It is mainly used for changing the communication protocol set for the logical hosts back to the communication protocol used in version 06-51 or earlier. This file must be edited.
physical_anyany.conf	This file sets the ANY binding methods for both sending and receiving. It is mainly used for resetting the hosts used in a cluster system back to be used on physical hosts. Using this file changes the communication protocol of the physical hosts to the ANY binding method. In this case, the physical hosts cannot be used together with logical hosts on the same host.
physical_ipip.conf	This file sets the IP binding method for both sending and receiving. It is mainly used to explicitly specify the IP address for sending through a firewall. If you apply this setting to the host connected to multiple networks, only one network will be available.
logical_ipip.conf	This file sets the IP binding method for both sending and receiving. It is mainly used to explicitly specify the IP address for sending through a firewall. This file must be edited. If you apply this setting to the host connected to multiple networks, only one network will be available.

To apply the contents of the communication protocol settings file to the physical hosts on a host connected to multiple networks, execute the `jbssetcnf` command in the following format:

```
jbssetcnf physical_ipany.conf
```

To apply the contents of the communication protocol settings file to the logical hosts on a host connected to multiple networks, open `logical_ipany.conf` using a text editor and change LOGICALHOSTNAME in [LOGICALHOSTNAME\JP1BASE] to the logical host name specified in the settings for the cluster system, and then execute the jbssetcnf command in the following format:

```
jbssetcnf logical_ipany.conf
```

4.3.4 Changing communication settings of event services

The communication settings of event services are managed using the event server settings file (conf). You can change the communication settings of event services by changing the contents of this file. The following parameters are required to use JP1/Base in an environment of distinct networks:

- ports parameter
- client-bind parameter

The ports parameter is used to receive JP1 events and the client-bind parameter is used to transmit JP1 events. For details on these parameters, see *Event server settings file* in *14. Definition Files*.

You need to set these parameters in the conf file when:

- communication cannot be established with the IP address used in the connection with the destination host, or
- using a host connected to multiple networks in a cluster system.

To change the communication settings of event services:

1. Open conf files using a text editor.

   The conf files are stored by default in *installation-folder*\conf\event\servers\default\ for Windows or /etc/opt/jp1base/conf/event/servers/default/ for UNIX.

   When you want to edit a conf file for logical hosts, edit the one created when you set JP1/Base for use in a cluster system.

2. Find the ports parameter and edit it to match the use of JP1/Base.

   Add the ports parameter if the conf file does not contain it. When the host is not used in a cluster system, you can retain the default setting of the ports parameter, which is:

   ```
   ports 0.0.0.0 jp1imevt jp1imevtapi
   ```

   When you use a host connected to multiple networks in a cluster system, and you assign multiple IP addresses for each physical and logical host, edit the port parameter as below:

   ```
   ports IP-address:IP-address jp1imevt jp1imevtapi
   ```

The *IP-addresses* are the IP addresses that the event server uses for reception of JP1 events. Use a colon (:) to delimit multiple names. You can specify up to four IP addresses.

3. Add the `client-bind` parameter.

   This parameter should be written in the following format:

   ```
   client-bind 0.0.0.0
   ```

This setting enables JP1/Base to use event services even in an environment of distinct networks.

Note

If you set the port settings and `client-bind` parameters, but JP1/Base is still not communicating properly, add the `remote-server` parameter to the `conf` file. The `remote-server` parameter allows you to specify a connection method to other event servers. Using this parameter, you can specify the address of a network explicitly with an IP address. This parameter should be written in the following format:

`remote-server` *event-server-name* `close` *IP-address*

For details, see *Event server settings file* in *14. Definition Files*.

4.3.5 Restarting JP1/Base

You must restart JP1/Base when you change the communication settings of the main part of JP1/Base or event services. When you have changed the communication settings of a host, stop and restart JP1/Base, JP1/Base prerequisite programs (JP1/IM, JP1/AJS etc.), and the programs that have dependency relationships with JP1/Base, which are running on that host.

4.3.6 Note on transmitting/receiving an event to/from earlier versions of event servers

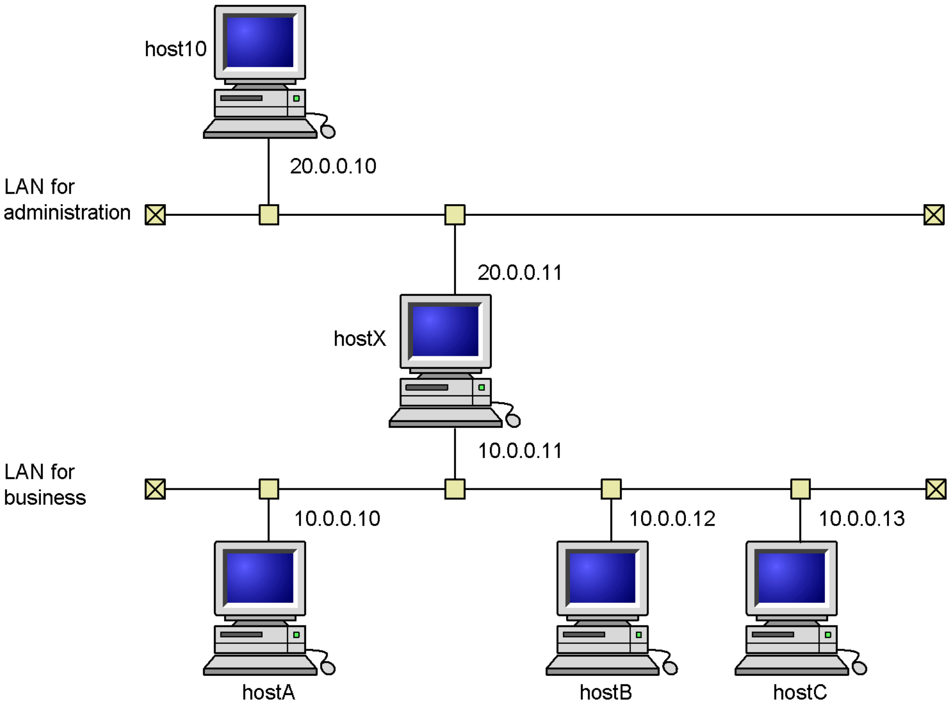
The earlier versions of event servers (pre-Version 6 programs JP1/SES or JP1/AJS, and programs that use the JP1/SES protocol) are only able to receive events from IP addresses that are calculated using the network functionality (`gethostbyname`), which is managed by the OS.

When you transmit/receive events between an earlier version of the event server and JP1/Base, implement the event server on the host on the network that uses the IP address calculated with `gethostbyname`. (If you implement the earlier version of event server on another host, it can transmit events but cannot receive events.)

4.4 An example of communication settings when JP1/Base is not used in a cluster system (in an environment of distinct networks)

This section describes the communication settings in an environment of distinct networks when JP1/Base is not used in a cluster system, based on the system configuration example shown in the following figure.

Figure 4-5: A system configuration example when JP1/Base is not used in a cluster system (in an environment of distinct networks)



This configuration assumes that only host10 connects to hostX with the IP address `20.0.0.11` which cannot be resolved against the host name, and the other hosts connect to hostX with the IP address `10.0.0.11` which can be resolved.

The table below indicates if the communication settings of each host must be changed or not in this configuration.

Host name	Communication settings of the main part of JP1/Base		Communication settings of event services (edit of `conf`)
	jp1hosts information	Communication protocol settings	
host10	Required	Not required	Required
hostX	Not required	Not required	Not required
hostA	Not required	Not required	Not required
hostB	Not required	Not required	Not required
hostC	Not required	Not required	Not required

4.4.1 Changing communication settings

This subsection describes how to change communication settings of each host.

(1) Changes required for host10

Unlike the other hosts, host10 connects to hostX with the IP address `20.0.0.11`, which does not correspond to the physical host name (which is hostX). You need to let JP1/Base and event servers recognize `20.0.0.11` as the IP address that corresponds to hostX. This can be done with the `jp1hosts` definition file and the event server settings file (`conf`).

To change the communication settings required for host10:

1. Edit the `jp1hosts` definition file.

   Edit the `jp1hosts` definition file with the following information:
   ```
   # Correspond the IP address 20.0.0.11 to hostX
   hostX 20.0.0.11
   ```

2. Execute the `jbshostsimport` command.
   `jbshostsimport {-o|-r}` *jp1hosts-definition-file-name*

3. Edit the event server settings file (`conf`).

   Add the following line to the event server settings file (`conf`):
   ```
   remote-server hostX close 20.0.0.11
   ```

4. Restart JP1/Base.

   Restart JP1/Base, JP1/Base prerequisite programs, and the programs that have dependency relationships with JP1/Base.

This completes the communication settings for host10.

(2) Changes required for hostX

You do not need to change the communication setting for hostX.

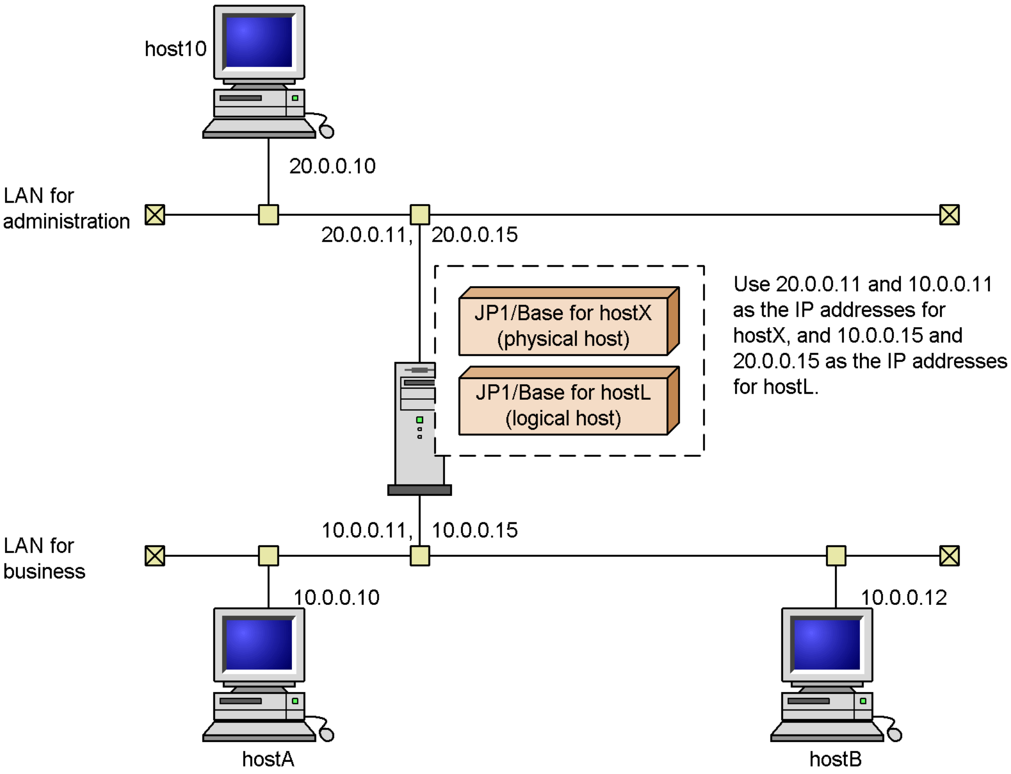
(3) Changes required for hostA, hostB, and hostC

You do not need to change the communication setting for hostA, hostB, and hostC since they are connected to hostX with the IP address `10.0.0.11`, which corresponds to the physical host name (which is hostX).

4.5 An example of communication settings when JP1/Base is used in a cluster system (in an environment of distinct networks)

This section describes the communication settings in an environment of distinct networks when a host connected to multiple networks is used in a cluster system, based on the system configuration example shown in the following figure.

Figure 4-6: A system configuration example when JP1/Base is used in a cluster system (in an environment of distinct networks)


host10
20.0.0.10
LAN for administration
20.0.0.11,
20.0.0.15
JP1/Base for hostX (physical host)
JP1/Base for hostL (logical host)
Use 20.0.0.11 and 10.0.0.11 as the IP addresses for hostX, and 10.0.0.15 and 20.0.0.15 as the IP addresses for hostL.
10.0.0.11,
10.0.0.15
LAN for business
10.0.0.10
10.0.0.12
hostA
hostB

This configuration assumes that only host10 connects to the physical host hostX and a logical host hostL with the IP addresses `20.0.0.11` (for the physical host) and `20.0.0.15` (for the logical host), both of which cannot be resolved against these host names. The other hosts are assumed to connect to hostX and hostL with the IP addresses `10.0.0.11` (for the physical host) and `10.0.0.15` (for the logical host), both of which can be resolved.

The table below indicates if the communication settings of each host must be changed or not in this configuration.

Host name	Communication settings of the main part of JP1/Base		Communication settings of event services
	jp1hosts information	Communication protocol settings	(edit of `conf`)
host10	Required	Not required	Required
hostX (physical host)	Required	Required	Required
hostL (logical host)	Required	Required	Required
hostA	Not required	Not required	Not required
hostB	Not required	Not required	Not required

4.5.1 Changing communication settings

This subsection describes how to change communication settings of each host.

(1) Changes required for host10

Host10 connects to hostX and hostL with the IP addresses `20.0.0.11` and `20.0.0.15`, which do not correspond to the physical host name (which is hostX) and the logical host name (which is hostL). You need to let JP1/Base and event servers recognize `20.0.0.11` and `20.0.0.15` as IP addresses that correspond to hostX and hostL. This can be done with the `jp1hosts` definition file and the event server settings file (`conf`).

To change the communication settings required for host10:

1. Stop all programs for which JP1/Base is a prerequisite or that depend on JP1/Base.
2. Stop JP1/Base.
3. Edit the `jp1hosts` definition file.

   Edit the `jp1hosts` definition file with the following information:
   ```
   # Correspond the IP addresses 20.0.0.11 and 20.0.0.15 to
   # the hosts that each IP address should correspond to.
   hostX 20.0.0.11
   hostL 20.0.0.15
   ```
4. Execute the `jbshostsimport` command.
   `jbshostsimport {-o|-r}` *jp1hosts-definition-file-name*
5. Edit the event server settings file (`conf`).

   Add the following line to the event server settings file (`conf`):

```
remote-server hostX close 20.0.0.11
remote-server hostL close 20.0.0.15
```

6. Restart JP1/Base.

   Restart JP1/Base, JP1/Base prerequisite programs, and the programs that have dependency relationships with JP1/Base.

This completes the communication settings for host10.

(2) Changes required for hostX

To change the communication settings required for hostX:

1. Stop all programs for which JP1/Base is a prerequisite or that depend on JP1/Base.

2. Stop JP1/Base.

3. Edit the `jp1hosts` definition file.

   Edit the `jp1hosts` definition file with the following information:
   ```
   # Correspond the IP address to the host name.
   hostX 10.0.0.11, 20.0.0.11
   ```

4. Execute the `jbshostsimport` command.
   `jbshostsimport {-o|-r}` *jp1hosts-definition-file-name*

5. Execute the `jbssetcnf` command.
   ```
   jbssetcnf physical_ipany.conf
   ```

6. Edit the event server settings file (`conf`).

   In the event server settings file (`conf`), change the ports and the `client-bind` parameters as below:
   ```
   ports 10.0.0.11:20.0.0.11 jp1imevt jp1imevtapi
   client-bind 0.0.0.0
   ```

7. Restart JP1/Base.

   Restart JP1/Base, JP1/Base prerequisite programs, and the programs that have dependency relationships with JP1/Base.

This completes the communication settings for hostX.

(3) Changes required for hostL (logical host)

To change the communication settings required for hostL:

1. Stop all programs for which JP1/Base is a prerequisite or that depend on JP1/Base.

2. Stop JP1/Base.

3. Edit the `jp1hosts` definition file.

   Edit the `jp1hosts` definition file with the following information:
   ```
   # Correspond the IP address to the host name.
   hostL 10.0.0.15, 20.0.0.15
   ```

4. Execute the `jbshostsimport` command.
   `jbshostsimport {-o|-r}` *jp1hosts-definition-file-name* `-h hostL`

5. Edit the `logical_ipany.conf`.

   Open the `logical_ipany.conf` using a text editor, look for `[LOGICALHOSTNAME\JP1BASE]`, and change it to `[hostL\JP1BASE]`.

6. Execute the `jbssetcnf` command.
   ```
   jbssetcnf logical_ipany.conf
   ```

7. Edit the event server settings file (`conf`).

   In the event server settings file (`conf`), change the ports and the `client-bind` parameters as below:
   ```
   ports 10.0.0.15:20.0.0.15 jp1imevt jp1imevtapi
   client-bind 0.0.0.0
   ```

8. Restart JP1/Base.

   Restart JP1/Base, JP1/Base prerequisite programs, and the programs that have dependency relationships with JP1/Base.

This completes the communication settings for hostL.

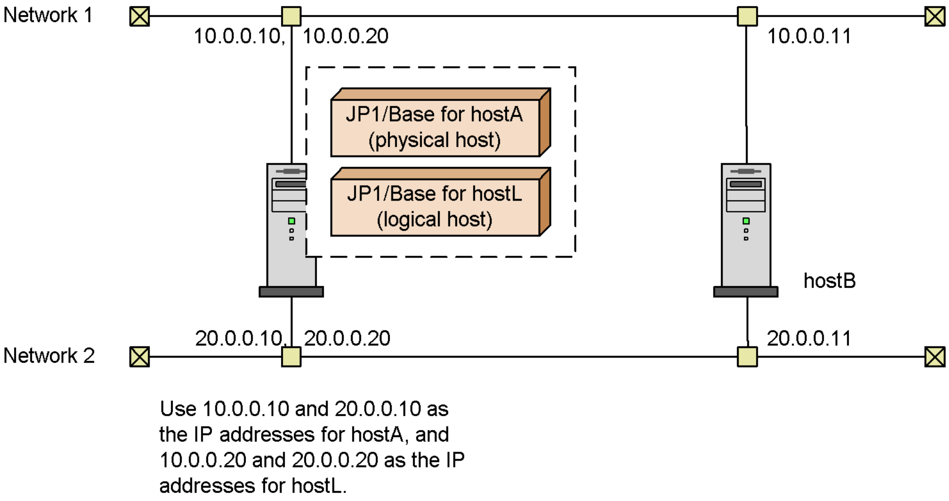
(4) Changes required for hostA and hostB

You do not need to change the communication setting for hostA and hostB since they are connected to hostX and hostL with IP addresses that correspond to the physical and the logical host names.

4.6 Communication settings example when JP1/Base is operating within a specific network in an environment with multiple networks

This section explains how to specify the communication settings when JP1/Base is operating within a specific network in an environment with multiple networks, based on the system configuration example shown in the following figure.

Figure 4-7: System configuration example when using JP1/Base (within a specific network in an environment with multiple networks)


Network 1
10.0.0.10, 10.0.0.20
10.0.0.11
JP1/Base for hostA (physical host)
JP1/Base for hostL (logical host)
hostB
Network 2
20.0.0.10, 20.0.0.20
20.0.0.11
Use 10.0.0.10 and 20.0.0.10 as the IP addresses for hostA, and 10.0.0.20 and 20.0.0.20 as the IP addresses for hostL.

The above figure assumes that hostL (a logical host) is a manager host, and that JP1/Base on each host is connected through network 2.

The table below indicates whether the communication settings for each host need to be changed in this configuration.

Host name	Communication settings of the main part of JP1/Base		Event service communication settings (edit of `conf`)
	jp1hosts information	Communication protocol settings	
hostA (physical host)	Required	Required	Required
hostL (logical host)	Required	Required	Required
hostB	Required	Required	Required

The procedure for changing the communication settings on each host is described below:

(1) Changes required for hostA

You need to set up the `jp1hosts` definition file and event server settings file (`conf`) so that JP1/Base on each host recognizes the IP address.

To specify communication settings:

1. Stop all programs for which JP1/Base is a prerequisite or that depend on JP1/Base.
2. Stop JP1/Base.
3. Edit the `jp1hosts` definition file.

   Edit the `jp1hosts` definition file with the following information:

   ```
   # Correspond the IP address 20.0.0.10 to hostA, and 20.0.0.20
   to hostL
   hostA 20.0.0.10
   hostL 20.0.0.20
   ```

4. Execute the `jbshostsimport` command.
   `jbshostsimport {-o|-r}` *jp1hosts-definition-file-name*

5. Execute the `jbssetcnf` command.
   `jbssetcnf physical_ipany.conf`

6. Edit the event server settings file (`conf`).

   In the event server settings file (`conf`), change the `ports` and the `remote-server` parameters shown below:

   ```
   ports 20.0.0.10 jp1imevt jp1imevtapi
   remote-server hostL close 20.0.0.20
   ```

7. Restart JP1/Base.

   Restart JP1/Base, JP1/Base prerequisite programs, and the programs that have dependency relationships with JP1/Base.

This completes the communication settings for hostA.

(2) Changes required for hostL (logical host)

To change the communication settings required for hostL (a logical host):

1. Stop all programs for which JP1/Base is a prerequisite or that depend on JP1/Base.
2. Stop JP1/Base.
3. Edit the `jp1hosts` definition file.

Edit the `jp1hosts` definition file with the following information:

```
# Correspond the IP address 20.0.0.10 to hostA, 20.0.0.11 to
hostB, and 20.0.0.20 to hostL
hostA 20.0.0.10
hostB 20.0.0.11
hostL 20.0.0.20
```

4. Execute the `jbshostsimport` command.
   `jbshostsimport {-o|-r}` *jp1hosts-definition-file-name* `-h hostL`

5. Edit the `logical_ipany.conf`.

   Open the `logical_ipany.conf` using a text editor, look for `[LOGICALHOSTNAME\JP1BASE]`, and change it to `[hostL\JP1BASE]`.

6. Execute the `jbssetcnf` command.

   ```
   jbssetcnf logical_ipany.conf
   ```

7. Edit the event server settings file (`conf`).

   In the event server settings file (`conf`), change the `ports` and the `remote-server` parameters shown below:

   ```
   ports 20.0.0.20 jp1imevt jp1imevtapi
   remote-server hostL close 20.0.0.20
   ```

8. Edit the API settings file (`api`).

   In the API settings file (`api`), add the `server` parameters shown below:

   ```
   server hostA keep-alive 20.0.0.10
   server hostL keep-alive 20.0.0.20
   server hostB keep-alive 20.0.0.11
   ```

9. Restart JP1/Base.

   Restart JP1/Base, JP1/Base prerequisite programs, and the programs that have dependency relationships with JP1/Base.

This completes the communication settings for hostL (a logical host).

(3) Changes required for hostB

To change the communication settings required for hostB:

1. Stop all programs for which JP1/Base is a prerequisite or that depend on JP1/Base.

2. Stop JP1/Base.

3. Edit the `jp1hosts` definition file.

   Edit the `jp1hosts` definition file with the following information:

   ```
   # Correspond the IP address 20.0.0.11 to hostB, and 20.0.0.20
   ```

```
to hostL
hostB 20.0.0.11
hostL 20.0.0.20
```

4. Execute the `jbshostsimport` command.
   `jbshostsimport {-o|-r}` *jp1hosts-definition-file-name*

5. Execute the `jbssetcnf` command.
   `jbssetcnf physical_ipany.conf`

6. Edit the event server settings file (`conf`).

   In the event server settings file (`conf`), add the `ports` and the `remote-server` parameters shown below:
   ```
   ports 20.0.0.11 jp1imevt jp1imevtapi
   remote-server hostL close 20.0.0.20
   ```

7. Restart JP1/Base.

   Restart JP1/Base, JP1/Base prerequisite programs, and the programs that have dependency relationships with JP1/Base.

This completes the communication settings for hostB.

4.7 Resetting JP1/Base to a single network after use on multiple networks

To reset the communication settings changed for an environment of distinct networks back to operation on a single network:

1. Delete `jp1hosts` information from the common definition information.

   If you have registered `jp1hosts` information with the common definition information, execute `jbshostsimport` command to delete it.
   `jbshostsimport -d [-h` *logical-host-name*`]`

2. Apply the communication protocol settings file to the common definition information.

   To do this, use the `jbssetcnf` command.

   For physical hosts, execute the `jbssetcnf` command in the following format:

   ```
   jbssetcnf physical_recovery_0651.conf
   ```

   For logical hosts, open the `logical_recovery_0651.conf` using a text editor, look for `[LOGICALHOSTNAME\JP1BASE]`, and replace the `LOGICAHOSTNAME` with the logical host name specified in the settings for the cluster system. Then execute the `jbssetcnf` command in the following format:

   ```
   jbssetcnf logical_recovery_0651.conf
   ```

3. Edit the event server settings file (`conf`).

   Delete the client-bind parameter; and then change the IP address of the ports parameter to `0.0.0.0` when you do not want to use it in a cluster system, or change it to IP addresses that correspond to the physical and logical host names when you want to use it in a cluster system.

4. Restart JP1/Base.

   Restart JP1/Base, JP1/Base prerequisite programs, and the programs that have dependency relationships with JP1/Base.

Chapter

5. Startup and Termination

This chapter describes how to start and stop JP1/Base.

5.1 Starting and stopping JP1/Base (in Windows)

This section describes how to start and stop JP1/Base. The following table lists the services provided in the Windows version of JP1/Base.

Table 5-1: JP1/Base services (in Windows)

Service	Name shown in the Services dialog box opened from the Control Panel
Hitachi Network Objectplaza Trace Library (HNTRLib2)	Hitachi Network Objectplaza Trace Monitor 2
Startup control	JP1/Base Control Service
Process management including user management	JP1/Base#1
Event service	JP1/Base Event#1
Log-file trap management service#2	JP1/Base LogTrap
Event-log trapping service	JP1/Base EventlogTrap

#1: Service names for logical hosts are represented as follows:

- `JP1_Base_`*logical-host-name*
- `JP1_Base_Event` *logical-host-name*

#2: The log-file trap management service is required to perform log file trapping.

Note

In the Service dialog box, leave the **Log On As** setting for each of the above services as the default system account. Do not select the **Allow Service to Interact with Desktop** option. If so, the service might not operate correctly.

The following describes the procedure for starting and stopping services.

5.1.1 Starting services

In the Windows version of JP1/Base, the following services are registered by default as **Automatic** and are set to start automatically at system startup:

- Hitachi Network Objectplaza Trace Monitor 2 (Hitachi Network Objectplaza Trace Library)
- JP1/Base Control Service (startup control)#

  #: In a system environment with JP1/Power Monitor installed, do not set the JP1/Base Control Service to **Manual**. If so, the Power Monitor service might not operate correctly.

The following services are set by default to start automatically when the JP1/Base Control Service (startup control) starts:

- JP1/Base (process management including user management)
- JP1/Base Event (event service)
- JP1/Base LogTrap (Log-file trap management service)

There is normally no need to change these settings. Using the JP1/Base Control Service (startup control), you can set the JP1/Base EventlogTrap (event log trapping service) and other application programs to start automatically in a predefined sequence. For details on using the startup control, see *7. Setting the Service Start and Stop Sequences (Windows Only)*.

When not using JP1/Base Control Service:

> To start a particular service without using the JP1/Base Control Service (startup control), add comment delimiters to the service definitions in the start sequence definition file (`JP1SVPRM.DAT`). Also, add comment delimiters to all the service definitions having dependencies with that service. That is, enter a # symbol at the beginning of every line of the definitions about the services.
>
> Having edited the start sequence definition file (`JP1SVPRM.DAT`) in this way, you can then work with that service in the Services dialog box that opens from the Control Panel in Windows. If you start the services automatically or manually without adding comment delimiters, the KAVA4003-E message might appear and the system might not operate correctly.

Notes

- When using the startup control, do not use the Services dialog box to work with any of the services defined in the start sequence definition file (`JP1SVPRM.DAT`). Starting or stopping these services in the Services dialog box could cause the KAVA4003-E message to appear, and could make automatic start and stop control by the JP1/Base Control Service fail to operate correctly.
- The event service must be running before the log-file trap management service and event-log trapping service can start. Always start **JP1/Base Event** before **JP1/Base LogTrap** and **JP1/Base EventlogTrap**.
- The performance of programs that use the event service can be affected if JP1/Base is installed but the event service is not running. To avoid such problems, prohibit events from being issued or acquired if you do not wish to use the event service. For details, see *API settings file* in *14. Definition Files*.

5.1.2 Confirming service startup

You can use the Services dialog box of the Control Panel to confirm that a JP1/Base service is activated. A service is activated if its state is **Started**.

If the Hitachi Network Objectplaza Trace Monitor 2 service (HNTRLib2) is not activated, you need to start it up manually with the Services dialog box of the Control Panel.

To start other JP1/Base services, we recommend that you use the JP1/Base Control Service (startup control) (by default, this functionality starts services other than the Hitachi Network Objectplaza Trace Monitor 2 and JP1/Base EventlogTrap services). For details on the startup control, see *7. Setting the Service Start and Stop Sequences (Windows Only)*. For details on how to start services without using the startup control, see *5.1.1 Starting services*.

5.1.3 Stopping services

Using the JP1/Base Control Service (startup control), you can stop services automatically at system shutdown. JP1/Power Monitor must be installed for this functionality. Install JP1/Power Monitor if you want to stop services automatically.

For details on using the JP1/Base Control Service (startup control), see *7. Setting the Service Start and Stop Sequences (Windows Only)*. For details on JP1/Power Monitor, see the *Job Management Partner 1/Power Monitor Description, User's Guide and Reference*.

To stop a service without using the JP1/Base Control Service (startup control) or JP1/Power Monitor, use the Services dialog box that opens from the Control Panel in Windows.

5.2 Starting and stopping JP1/Base (in UNIX)

On a UNIX system, you can start and stop services using commands.

The following table lists the services that you can start and stop by command.

Table 5-2: JP1/Base services that can be started and stopped by command (in UNIX)

Function	Start command	Stop command
Hitachi Network Objectplaza Trace Library (HNTRLib2)#1	`hntr2mon -d &`	`hntr2kill`
Event service	`jevstart`	`jevstop`
Process management including user management	`jbs_spmd`	`jbs_spmd_stop`
Log-file trap management daemon#2	`jevlogdstart`	`jevlogdstop`
JP1/Base	`jbs_start.model`#3	`jbs_stop.model`#4

#1: At JP1/Base installation, the Hitachi Network Objectplaza Trace Library (HNTRLib2) is set by default to start and end automatically.

#2: The log-file trap management daemon is required to perform log file trapping. You can shut down the JP1/Base system while the log-file trap management daemon is active.

#3: The `jbs_start.model` is stored in the `/etc/opt/jp1base` directory. Using the `jbs_start.model`, you can start all services other than the Hitachi Network Objectplaza Trace Library (HNTRLib2). Use this script to start JP1/Base in normal circumstances.

#4: The `jbs_stop.model` is stored in the `/etc/opt/jp1base` directory. Using the `jbs_stop.model`, you can stop all services other than the Hitachi Network Objectplaza Trace Library (HNTRLib2) and log-file trap management daemon. Use this script to stop JP1/Base in normal circumstances. In a system other than a cluster system, if you want to stop functionality other than HNTRLib2 without running JP1/Base on every logical host, execute the `jevlogdstop` command after you execute `jbs_stop.model`.

For details on the above commands, see *13. Commands*.

In UNIX, you can make process management (including user management), the event service, and the log-file trap management daemon all automatically start when the system starts up. You can also make process management and the event service automatically stop when the system shuts down.

The setup required for automatic start and stop control is explained below.

5.2.1 Setting services to start and stop automatically

The following describes how to set the UNIX version of JP1/Base to start and stop services automatically.

To automatically start process management (including user management), the event service, and the log-file trap management daemon when the system starts up, run the following script after completing the installation and setup:

```
cd /etc/opt/jp1base
cp -p jbs_start.model jbs_start
```

To automatically end process management (including user management) and the event service when the system shuts down, run the following script after completing the installation and setup:

```
cd /etc/opt/jp1base
cp -p jbs_stop.model jbs_stop
```

Notes

- To automatically start log file trapping, edit `jbs_start` as required. Edit the file so that log file trapping starts after the event service and the log-file trap management daemon have started.
- After services are set to automatically start and stop, the environment variable `LANG` is set to `C` by default. You can change the setting, as required.

In AIX environment

To automatically start and stop services in an AIX environment, perform the following procedure in addition to the above operations.

1. Clear the automatic start setting of the previous versions.

   If services in the previous versions have already been specified to start automatically, check the settings in the `/etc/rc.tcpip` file. If you find the following lines, delete them:

   For JP1/Base version 6 and the programs that require JP1/Base version 6:

   ```
   test -x /etc/opt/jp1base/jbs_start && /etc/opt/jp1base/
   jbs_start
   ```

   ```
   test -x /etc/opt/jp1cons/jco_start && /etc/opt/jp1cons/
   jco_start
   ```

   ```
   test -x /etc/opt/jp1cons/jajs_start && /etc/opt/jp1ajs2/
   jajs_start
   ```

   For JP1/IM - Agent version 5:

```
test -x /etc/opt/jp1_ima/ima_start && /etc/opt/jp1_ima/
ima_start
```

2. Specify the settings to automatically start services.

   Using the `mkitab` command, make the following entries in the `/etc/inittab` file:

   ```
   mkitab -i hntr2mon "jp1base:2:wait:/etc/opt/jp1base/
   jbs_start"
   ```

   To reset the programs that require JP1/Base to automatically start after the automatic startup setting has been cleared in step 1, use the `mkitab` command to add a product description after the `jp1base` line. For details on how to add a description, see the *Release Notes* of the program.

3. Check the settings.

   Use the `lsitab` command to check settings in the `/etc/inittab` file.

   ```
   lsitab -a
   ```

   The execution results are displayed.

   Confirm that the descriptions are in the same order as the order in which the processes start (first `hntr2mon` (Hitachi Network Objectplaza Trace Library), and then `jp1base`).

   ```
   init:2:initdefault:

   brc::sysinit:/sbin/rc.boot 3 >/dev/console 2>&1 # Phase
   3 of system boot

   ...

   ...

   hntr2mon:2:once:/opt/hitachi/HNTRLib2/etc/D002start

   jp1base:2:wait:/etc/opt/jp1base/jbs_start
   ```

4. Clear the automatic stop setting for the previous versions.

   If services in the previous versions have already been specified to automatically stop, check the settings in the `/usr/sbin/shutdown` file. If you find the following lines, delete them:

   For JP1/Base version 6 and the programs that require JP1/Base version 6:

   ```
   test -x /etc/opt/jp1ajs2/jajs_stop && /etc/opt/jp1ajs2/
   jajs_stop

   test -x /etc/opt/jp1cons/jco_stop && /etc/opt/jp1cons/
   ```

```
jco_stop
```

```
test -x /etc/opt/jp1base/jbs_stop && /etc/opt/jp1base/
jbs_stop
```

For JP1/IM - Agent version 5:

```
test -x /opt/jp1_ima/bin/ima_shutdown && /opt/jp1_ima/
bin/ima_shutdown
```

Also, the following lines are used to automatically stop Hitachi Network Objectplaza Trace Library versions 03-03-/B and earlier. If you find the following lines, delete them:

```
test -x /opt/hitachi/HNTRLib2/bin/hntr2kill && /opt/
hitachi/HNTRLib2/bin/hntr2kill
```

5. Specify the settings to automatically stop services.

   Using a text editor, add the following lines to the `/etc/rc.shutdown` file below the descriptions of the programs that require JP1/Base:

   ```
   test -x /etc/opt/jp1base/jbs_stop && /etc/opt/jp1base/
   jbs_stop
   ```

   ```
   test -x /opt/hitachi/HNTRLib2/etc/D002stop && /opt/
   hitachi/HNTRLib2/etc/D002stop
   ```

   To re-specify the automatic stop settings for the programs that require JP1/Base and whose automatic stop settings were deleted in step 4, add product descriptions before the `jp1base` line. For details on how to add descriptions, see the *Release Notes* for the specific programs.

6. Add the description for shutdown processing.

   Add the following line to the end of the `/etc/rc.shutdown` file.

   ```
   exit 0
   ```

   If the command that is executed last has a result code other than `0`, the `/etc/rc.shutdown` script will recognize it as an error and interrupt the shutdown processing.

Note

After services are set to automatically start and stop, the environment variable `LANG` is set to `C` by default. You can change the setting as required.

5.2.2 Confirming JP1/Base startup

To confirm that JP1/Base is running, use the `jbs_spmd_status` and `jevstat` commands to check the status of the JP1/Base process. For details on JP1/Base processes, see *B.2 UNIX processes*. If your desired JP1/Base functionality is not activated, use the relevant command to start it. For details on commands, see *13. Commands*.

Note

> When you install a JP1/Base program by overwriting the existing one, use the `hntr2mon` command to start the Hitachi Network Objectplaza Trace Library. This is because the Hitachi Network Objectplaza Trace Library is disabled when you overwrite an existing JP1/Base program, so that you cannot collect information with the trace log even when you run JP1/Base. To start the Hitachi Network Objectplaza Trace Library (HNTRLib2) manually, you need to execute the `hntr2mon` command from the C shell. For details on the `hntr2mon` command, see *hntr2mon (UNIX only)* in *13. Commands*.

Chapter

6. User Management Setup

This chapter describes how to set up user management in Windows and UNIX.

The descriptions in this chapter focus on JP1/IM and JP1/AJS, but some descriptions might apply to other JP1 programs. For details, see the manual for the specific JP1 program.

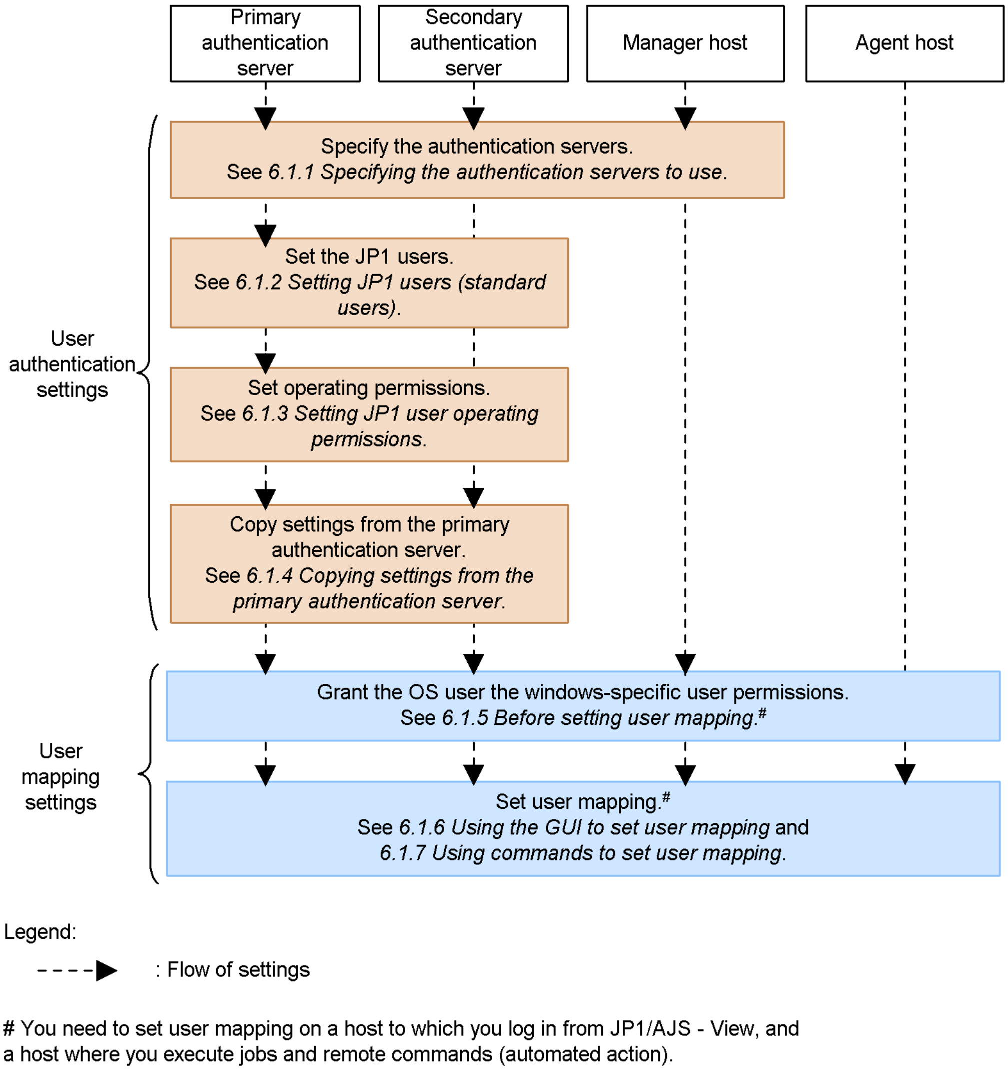
6.1 User management setup (in Windows)

This section describes the user management setup required in Windows. If you performed an automatic setup to install JP1/Base, the default value has been set. For details on the default of automatic setup, see *2.2.1 Installing JP1/Base*.

The setup method differs depending on whether the host will be used as an authentication server.

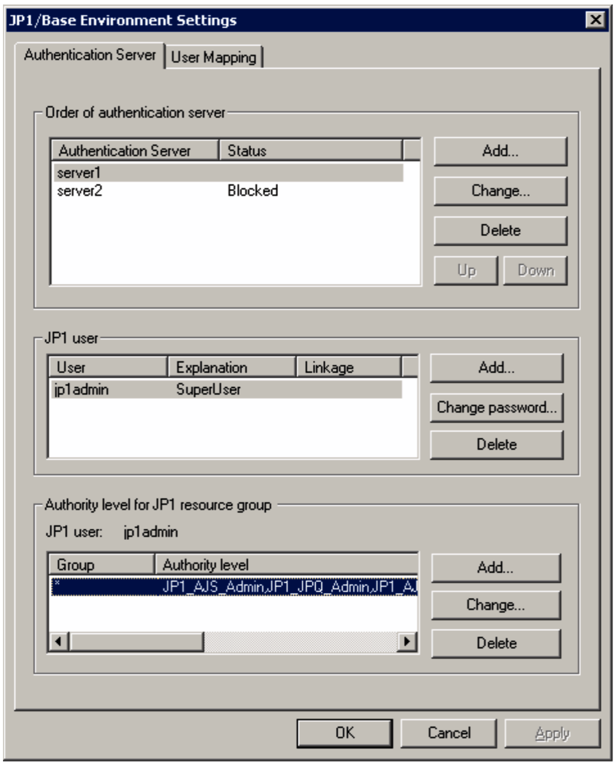
If you use the secondary authentication server, the setting information for both the primary authentication server and the secondary authentication server must be the same. The following figure shows the setup procedure required on each host and the corresponding sections in this manual.

Figure 6-1: User management setup procedure (in Windows)


Primary authentication server
Secondary authentication server
Manager host
Agent host
User authentication settings
Specify the authentication servers.
See *6.1.1 Specifying the authentication servers to use*.
Set the JP1 users.
See *6.1.2 Setting JP1 users (standard users)*.
Set operating permissions.
See *6.1.3 Setting JP1 user operating permissions*.
Copy settings from the primary authentication server.
See *6.1.4 Copying settings from the primary authentication server*.
User mapping settings
Grant the OS user the windows-specific user permissions.
See *6.1.5 Before setting user mapping*.#
Set user mapping.#
See *6.1.6 Using the GUI to set user mapping* and *6.1.7 Using commands to set user mapping*.
Legend:
: Flow of settings
# You need to set user mapping on a host to which you log in from JP1/AJS - View, and a host where you execute jobs and remote commands (automated action).

In Windows, you can use the GUI or commands to set up user management. To display the GUI, from the Windows **Start** menu, choose **Programs**, **JP1_Base**, and then **Environment Settings**. The JP1/Base Environment Settings dialog box appears. Note that administrative permissions are required to operate the GUI. The following figure shows the JP1/Base Environment Settings dialog box.

Figure 6-2: JP1/Base Environment Settings dialog box



Authentication Server	Status
server1	
server2	Blocked

User	Explanation	Linkage
jp1admin	SuperUser	

JP1 user: jp1admin

Group	Authority level
*	JP1_AJS_Admin,JP1_JPQ_Admin,JP1_A

6.1.1 Specifying the authentication servers to use

Specify the host running JP1/Base that will be used as the authentication server. The authentication server must be specified on the following hosts:

- Every host to be used as an authentication server (primary or secondary)
- Host on which JP1/IM - Manager or JP1/AJS - Manager is installed

A host specified as an authentication server manages JP1 users and the operating permissions for JP1 resource groups. If JP1/IM and JP1/AJS coexist in your system, and if you want to use just one user authentication block, specify the same authentication server on each of the hosts.

The setup procedure is shown below for an authentication server when performed both from the GUI and by using commands.

(1) Using the GUI to set up the authentication server

To specify an authentication server, from the **Authentication Server** page of the JP1/ Base Environment Settings dialog box, click **Order of authentication server**. In the

Order of authentication server area, you can add an authentication server, and then delete or change an entered authentication server. The following describes these procedures. If you want to set the local host as the authentication server (primary or secondary authentication server), stop the JP1/Base service before you complete this area.

Adding an authentication server:

You can use up to two hosts as authentication servers. The first host listed in the **Authentication Server** field will be the primary authentication server, and the one below will be the secondary authentication server.

You can add an authentication server, unless two authentication servers are already listed in the **Authentication Server** field.

To add an authentication server:

1. Click the **Add** button.

   The Authentication Server dialog box appears.

2. Type the authentication server name, then click **OK**.

   The **Authentication Server** page comes to the front. The authentication server name you specified in the **Authentication Server** dialog box appears in the **Authentication Server** field. You can specify both the local host and another host for the authentication server.

Note

For the authentication server name, enter a host name. You cannot specify an IP address.

Deleting an authentication server:

To delete an authentication server:

1. From the **Authentication Server** field, select the authentication server you want to delete.
2. Click the **Delete** button.

Changing an authentication server:

To change an authentication server:

1. From the **Authentication Server** field, select the authentication server you want to change.
2. Click the **Change** button.

   The Authentication Server dialog box appears. Change the authentication server in this dialog box.

3. Click the **OK** button.

   The **Authentication Server** page comes to the front. The authentication server name you changed in the **Authentication Server** dialog box appears in the **Authentication Server** field.

If you want to swap the primary and secondary authentication servers, select one of the host names listed in the **Authentication Server** field, and then click the **Up** or **Down** button.

Note

> When you add a second authentication server or change one of the two authentication servers, the **Set this authentication server in state of blockage** check box in the Authentication Server dialog box becomes available. If you select this check box, any hosts whose host names you type in cannot be used as an authentication server. Do not select this check box in normal circumstances.

When you finish the settings in the **Order of authentication server** area, click **Apply**. The settings take effect. If you specify the local host as an authentication server, and then select (highlight) the local host as the authentication server in the **Authentication Server** field, the **JP1 user** and **Authority level for JP1 resource group** areas become available.

(2) Using commands to set authentication server

Use the `jbssetupsrv` command to register and delete an authentication server. For details on the `jbssetupsrv` command, see *jbssetupsrv (Windows only)* in *13. Commands*.

Registering an authentication server

To register an authentication server, execute the following command:

```
jbssetupsrv [-h logical-host-name]
             primary-authentication-server-name
 [secondary-authentication-server-name]
```

Deleting an authentication server

To delete an authentication server, execute the following command:

```
jbssetupsrv [-h logical-host-name]
             -d [authentication-server-name]
```

If you omit the logical host name from the `-h` option, the logical host name set for the environment variable `JP1_HOSTNAME` is used by default. If the environment variable `JP1_HOSTNAME` is not set, the physical host name is assumed.

If you omit the secondary authentication server name, JP1/Base uses only one authentication server in the user authentication block.

If you only specify the `-d` option, all the authentication servers on the specified logical host are deleted.

(3) After setting authentication servers

To check which hosts are set as authentication servers, execute the following command:

```
jbslistsrv [-h logical-host-name]
```

For details on the `jbslistsrv` command, see *jbslistsrv* in *13. Commands*.

If you specified the local host as the primary authentication server, go to *6.1.2 Setting JP1 users (standard users)*.

If you specified the local host as the secondary authentication server, complete the settings of the authentication server for the host you specified as the primary authentication server, and then go to *6.1.4 Copying settings from the primary authentication server*.

If you did not specify the local host as an authentication server, the settings for user authentication are now finished.

6.1.2 Setting JP1 users (standard users)

In this section, you can set up JP1 users (standard users) for whom login authentication is performed from an authentication server. For details on how to set up JP1 users (linked users) for whom login authentication is performed from the directory server, see *6.2.2 Setting JP1 users (linked users)*. Unless otherwise specified, *JP1 user* means *JP1 user (standard user)* in this section.

JP1 users must be set only from a host that was specified as an authentication server (a primary authentication server). The JP1/Base service must also be running before you can set JP1 users. If the JP1/Base service is inactive, start the service before attempting to set JP1 users.

The setup procedure is shown below for JP1 users when performed both from the GUI and by using commands.

(1) Using the GUI to set up JP1 users

You can set JP1 users in the **JP1 user** area in the **Authentication Server** page of the JP1/Base Environment Settings dialog box.

To set information in the **JP1 user** area, you must activate it first. To do this, select (highlight) an authentication server in the **Authentication Server** field in the **Order of authentication server** area. Note, however, that the **JP1 user** area remains dimmed if:

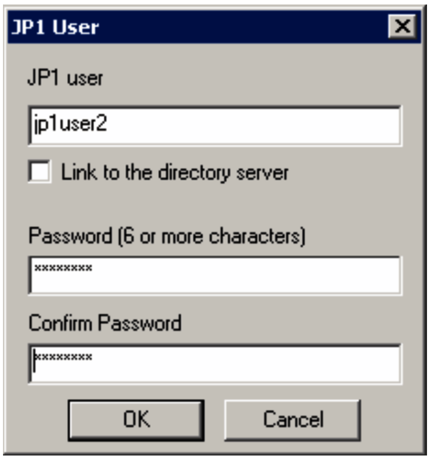
- You change an authentication server in the **Order of authentication server** area and the **Apply** button is active

- The selected (highlighted) authentication server is blocked

If the **Apply** button is active, click the button. If the selected authentication server is blocked, clear that status as described in *6.4 Setup for handling the blocked status (using a secondary authentication server)*.

Clicking the **Add** button displays the JP1 User dialog box.

Figure 6-3: JP1 User dialog box



JP1 User

JP1 user: jp1user2

☐ Link to the directory server

Password (6 or more characters): ********

Confirm Password: ********

In this dialog box, specify a JP1 user and password. Do not select the **Link to the directory server** check box. If you select this check box, the mode is changed to the linked-user mode, and you cannot enter a password.

JP1 user names must be specified in lower-case alphanumeric characters. If you use upper-case characters, they are automatically converted into lower-case characters. The password is case-sensitive. The following table lists the limits on the number of characters that can be used for JP1 user names and passwords.

Table 6-1: Character limits on JP1 user names and passwords

Item	Number of bytes	Prohibited characters
JP1 user name	1 to 31 bytes	`* / \ " ' ^ [ ] { } ( ) : ; | = , + ? < >` and spaces and tabs
Password	6 to 32 bytes	`\ " :` and spaces and tabs

When you click the **OK** or **Cancel** button, the **Authentication Server** page comes to the front.

The registered JP1 user name appears in the **User** field. If you want to change the password of a registered JP1 user, select the JP1 user in the **JP1 user** area, and then click the **Change Password** button.

To delete a JP1 user name listed in the **User** field, select the user name and click the **Delete** button. The selected JP1 user will be deleted.

(2) Using commands to set JP1 users

You can also use commands to register or delete JP1 users or change their passwords. JP1/Base also supports a command that lists the registered JP1 users. For details on the commands, see *13. Commands*.

Registering a JP1 user:

To register a JP1 user on the authentication server, execute the following command:

```
jbsadduser JP1-user-name
```

For *JP1-user-name*, use lower-case characters.

This command prompts you to enter the password. The password is case-sensitive. Table 6-1 lists the characters that can be specified for JP1 user names and passwords.

Changing the password of a JP1 user:

To change the password of a registered JP1 user, execute the following command:

```
jbschgpasswd JP1-user-name
```

Deleting a JP1 user:

To delete a registered JP1 user, execute the following command:

```
jbsrmuser JP1-user-name
```

Listing the JP1 users:

To list the registered JP1 users, execute the following command:

```
jbslistuser
```

6.1.3 Setting JP1 user operating permissions

You must set the JP1 user operating permissions from an authentication server (a primary authentication server). For this setting, you set what kind of operations are permitted to JP1 users (the JP1 permission level) when they operate JP1 resource groups, such as jobs and jobnets.

Note

You can only set operating permissions for jobs and jobnets for which you have specified JP1 resource group names with JP1/AJS. For other jobs and jobnets, all types of access by all JP1 users are permitted.

You can use either the GUI or commands to set operating permissions given to JP1 users. When using the GUI, you can set operating permissions for individual JP1 users. When using commands, you can set operating permissions for a group of JP1 users as well as for individual users.

The setup procedure is shown below for JP1 user operating permissions when performed both from the GUI and by using commands.

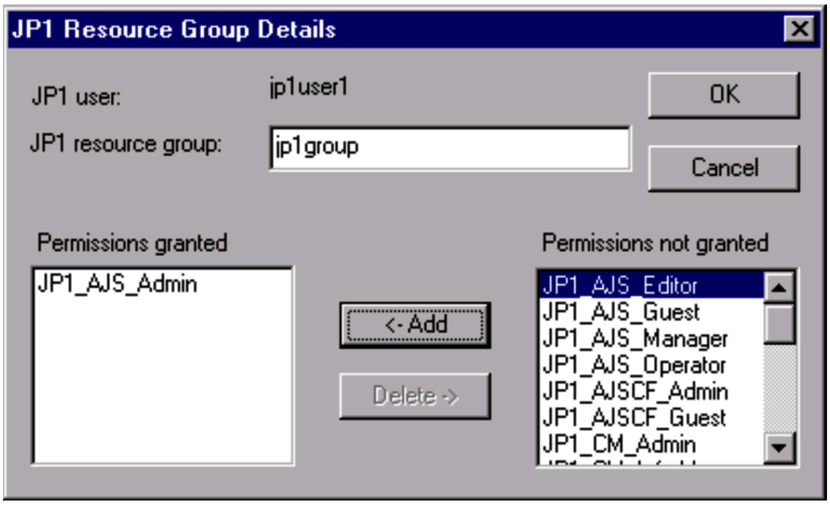
(1) Using the GUI to set JP1 user operating permissions

In the **Authentication Server** page of the JP1/Base Environment Settings dialog box, you can set the JP1 user operating permissions in the **Authority level for JP1 resource group** area.

In the **JP1 user** area of the JP1/Base Environment Settings dialog box, select a user in the **User** field to set permissions for that user. When you select a user name, the group (*JP1 resource group*) that the user is permitted to access, and the authority level (*JP1 permission level*) of that group, appear in the **Authority level for JP1 resource group** area.

If you click the **Add** button, or if you select a group in the **Group** field and then click the **Change** button, the JP1 Resource Group Details dialog box appears.

Figure 6-4: JP1 Resource Group Details dialog box



JP1 user: jp1user1

JP1 resource group: jp1group

Permissions granted

JP1_AJS_Admin

Permissions not granted

JP1_AJS_Editor
JP1_AJS_Guest
JP1_AJS_Manager
JP1_AJS_Operator
JP1_AJSCF_Admin
JP1_AJSCF_Guest
JP1_CM_Admin

In the JP1 Resource Group Details dialog box, set the JP1 resource group and JP1 permission level. If you specify an asterisk (*) as a JP1 resource group, you can access all the JP1 resource groups. For a JP1 user, if you specified an asterisk (*) for the JP1 resource groups, you cannot specify anything other than an asterisk (*).

For details on the JP1 resource groups and JP1 permission levels to be specified, see the manual for the JP1 program that uses JP1/Base user authentication.

(2) Using a command to set operating permissions for multiple JP1 users simultaneously

You can use a command to set operating permissions for multiple JP1 users simultaneously. To do this, define operating permissions in the user permission level file (`JP1_UserLevel`). After editing the file, execute the `jbsaclreload` command to apply the settings. For details on the `jbsaclreload` command, see *jbsaclreload* in *13. Commands*. For details on the user permission level file, see *User permission level file* in *14. Definition Files*.

Note

> The user permission level file (`JP1_UserLevel`) is also used for the GUI. Any information you enter in the GUI will be applied to this file. Likewise, if you edit the file in an editor and then execute the `jbsaclreload` command, the edited information will be reflected in the GUI.

(3) Using a command to register operating permissions for individual JP1 users

To use a command to add or modify operating permissions for JP1 users, you must create a definition file that describes operating permissions given to each JP1 user you want to register.

You can create the definition file in any location. The file format is the same as that of the user permission level file (`JP1_UserLevel`). For details on the user permission level file, see *User permission level file* in *14. Definition Files*.

After preparing the definition file, execute the following command to register the information in the definition file with the authentication server:

```
jbssetacl -f definition-file-name
```

For details on the `jbssetacl` command, see *jbssetacl* in *13. Commands*.

(4) Using a command to delete operating permissions for individual JP1 users

To delete operating permissions for a registered JP1 user, execute the following command:

```
jbsrmacl -u JP1-user-name
```

Note that this command deletes all operating permissions that have been given to the specified JP1 user.

For details on the `jbsrmacl` command, see *jbsrmacl* in *13. Commands*.

6.1.4 Copying settings from the primary authentication server

When using a secondary authentication server, you must set it up with the same information set on the primary authentication server. After completing the setup for the primary authentication server, therefore, you must copy the settings from the primary authentication server to the secondary authentication server.

To copy the settings from the primary authentication server to the secondary authentication server:

1. On the primary authentication server, complete the settings for JP1 users and operating permissions.

   For details on how to set up JP1 users, see *6.1.2 Setting JP1 users (standard users)* or *6.2.2 Setting JP1 users (linked users)*.

   For details on the settings of the JP1 user operating permissions, see *6.1.3 Setting JP1 user operating permissions*.

2. Start the secondary authentication server.

   Start the JP1/Base service to start the secondary authentication server. You can use the `jbs_spmd_status` command to verify that the secondary authentication server has started. The secondary authentication server is running if the information shown by the command contains `jbssessionmgr`.

3. Use FTP, a floppy disk, or other method to copy the settings files from the primary authentication server.

   Using FTP, a floppy disk, or other method, copy the settings file from the primary authentication server to the secondary authentication server. Copy the following files: `JP1_AccessLevel`, `JP1_Group`, `JP1_Passwd`, and `JP1_UserLevel`. These files are stored in the following folder:

   installation-folder`\conf\user_acl\`

   Copy the files to the same folder on the local host. For a logical host, the files are stored in the following folder:

   shared-folder`\jp1base\conf\user_acl\`

4. Use the `jbs_spmd_reload` command to apply the settings.

   Execute the `jbs_spmd_reload` command to apply the contents of the copied settings files. The settings take effect when the command terminates normally.

For details on the commands, see *13. Commands*.

Notes

- Ensure that the same version of JP1/Base is running on the primary and secondary authentication servers.

- If the secondary authentication server has not started, make sure that the local host is specified as the secondary authentication server. In the **Authentication Server** page of the JP1/Base Environment Settings dialog box, make sure that the local host is specified in the **Order of authentication**

server area, and that the **JP1 user** and **Authority level for JP1 resource group** areas are available. If these areas are available, starting the JP1/Base service also starts the secondary authentication server.

- The settings files are text files. When transferring the files between different platforms, be careful about the character set. If you transfer them by FTP, be sure to use the ASCII transfer mode.

6.1.5 Before setting user mapping

User mapping is functionality that associates JP1 users with OS users. In Windows, before setting user mapping, you need to assign certain Windows user rights to the OS users who set the mapping and those who are mapped.

You can use the OS functionality to assign these rights to OS users. In a domain environment using an Active Directory, the procedure differs for a host with a domain controller and for a host within a domain. The following describes the rights required by OS users, and how to set user rights in an Active Directory environment.

(1) Rights required by OS users who set the user mapping

OS users who set the user mapping include the following:

- Users who set the user mapping in the **User Mapping** page of the JP1/Base Environment Settings dialog box
- Users who execute the `jbsmkpass` command
- Users who execute the `jbsmkumap` command
- Users who execute the `jbspassmgr` command
- Users who execute the `jbssetumap` command
- Users who execute the `jbsumappass` command

Usually, you need to assign the user right **Act as a part of the operating system** to the OS users who perform the above operations. However, in the Windows versions that are supported in this manual, you do not have to assign this user right. Instead, you can set the user mapping without having that user right.

Notes

- If you assign the user right **Act as a part of the operating system** to the OS user who set the user mapping, log off from the OS one time. If you do not log off the OS, the new user right might not be applied, and the setting of user mapping might not be performed correctly.
- If the check box **The logon check is not done to Windows, when OS user is set** is selected in the **User Mapping** page, user mapping becomes available even if the user right is not assigned to the user. In this case, however, note that the mappings for the OS users below are also successful. If the mapped

JP1 user tries to execute a job or remote command, an insufficient rights error occurs:

- OS users who are not registered in the system (Windows)

- OS users who have invalid password

- OS users who do not have the right **Log on locally**

(2) User rights required by mapped OS users

Mapped OS users require the following user rights.

To execute remote commands or automated actions from JP1/IM - Manager:

Log on locally

Log on as a service

To execute jobs in JP1/AJS:

Log on locally

To assign a user right, use **Local Security Policy** in **Administrative Tools** on each local host. **Administrative Tools** are located in the Control Panel.

(3) Assigning a user right to an OS user in an Active Directory environment

This subsection describes how to assign a user right to an OS user in an Active Directory environment. While you just set user rights on a local host in a conventional environment, the procedure to set them differs between a host with a domain controller and a local host within a domain in an Active Directory environment. The following shows how to set user rights for each host.

- In Active Directory environments, all OS users default to have the right **Log on locally**. When you use the default user rights, do not specify a new set of **Log on locally** rights.
- The following setup procedure applies to an environment that deploys multiple local hosts immediately under a single host with a domain controller. If you use complex settings such as building a site or organization unit (OU) or stopping policy inheritance, you might not be able to assign user rights in this procedure. For details, contact your Active Directory administrator.

Setting a user right on a host with a domain controller

To set a user right on a host with a domain controller:

1. Select your desired right and add a domain user in the **Domain Controller Security Policy** dialog box on the host that is the domain controller.
2. Use commands to apply the security policy update.

   Execute the following command:

```
gpupdate /target:user
gpupdate /target:computer
```

You can use the event viewer to confirm that the settings are in effect.

3. Make sure that **Effective policy setting** is selected in the **Local Security Policy Setting** dialog box on the host that is the domain controller.

   The policy settings are inherited and overwritten in order of the local, site group, domain group, and organization unit (OU) group policies. You can also specify a setting to stop inheritance at some point in these levels. This setting might disable a user right given at a higher level, or might result in the disabling of a user right given during the inheritance. You must make sure that **Effective policy setting** is selected.

Setting a user right on a local host within a domain:

To set a user right on a local host within a domain:

1. Select your desired user right and add a domain user or group in the **Domain Security Policy Setting** dialog box on the host that is the domain controller.

   You cannot add a local user on the local host.

2. Select your desired user right and add a domain user or group in the **Local Security Policy Setting** dialog box on the local host (this step can be omitted).

3. Use the commands to reflect the policy update on the host that is the domain controller.

   Execute the following command:

   ```
   gpupdate /target:user
   gpupdate /target:computer
   ```

   You can use the event viewer to confirm that the settings are in effect.

   To ensure the update, you should also execute the commands on the local host.

4. Make sure that **Effective policy setting** is selected in the **Local Security Policy Setting** dialog box on the local host.

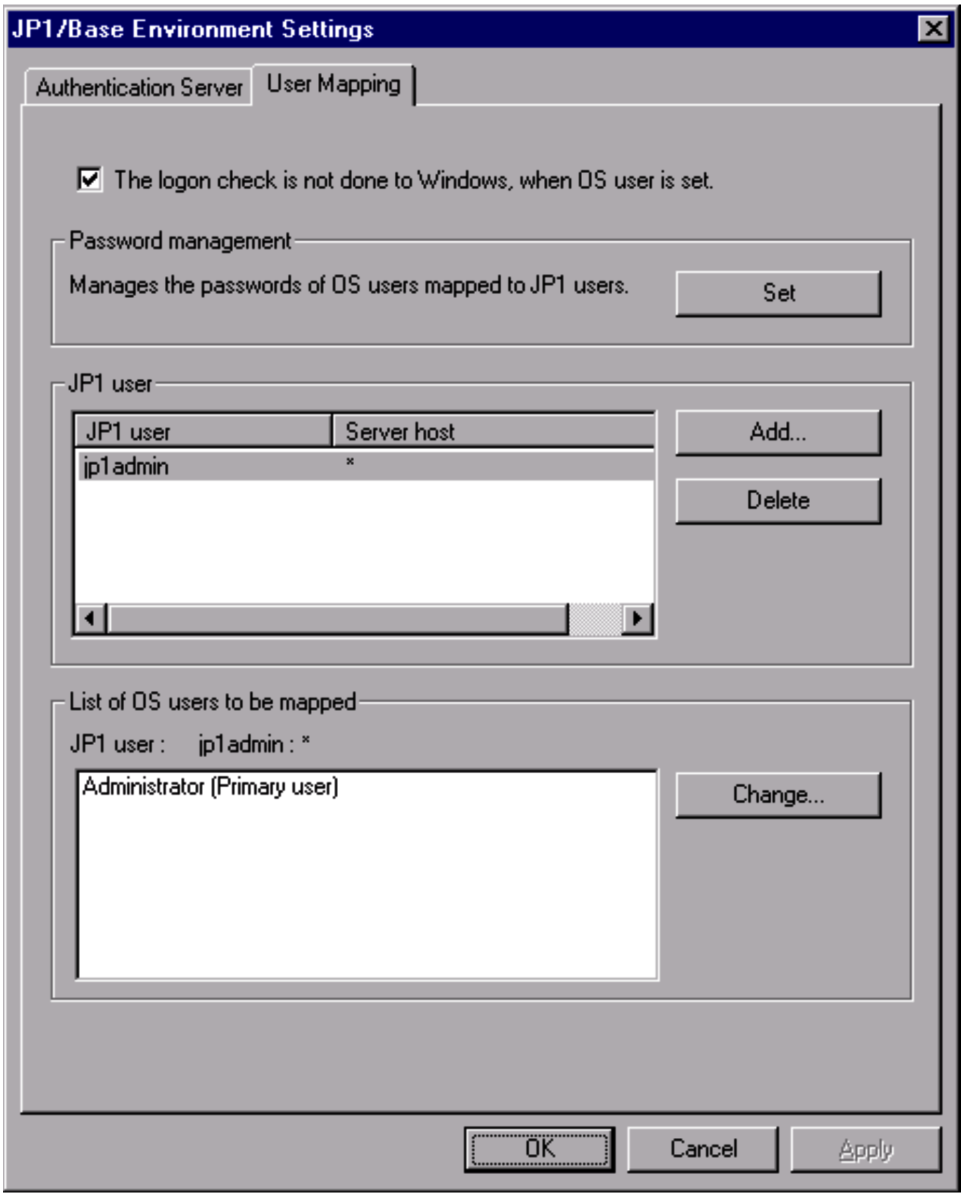
   The policy settings are inherited and overwritten in order of the local, site group, domain group, and organization unit (OU) group policies. You can also specify a setting to stop inheritance at some point in these levels. This setting might disable a user right given at a higher level, or might result in the disabling of a user right given during the inheritance. You must make sure that **Effective policy setting** is selected.

A user right might not be assigned even when **Effective policy setting** is selected in the **Local Security Policy Setting** dialog box. This sometimes occurs if a DNS or IP address setting is wrong. For details, see the online help or related documentation for your OS.

6.1.6 Using the GUI to set user mapping

To set user mapping through the GUI, in the JP1/Base Environment Settings dialog box, click the **User Mapping** page. The following figure shows the **User Mapping** page of the JP1/Base Environment Settings dialog box.

Figure 6-5: JP1/Base Environment Settings dialog box (User Mapping page)



☑ The logon check is not done to Windows, when OS user is set.

Password management

Manages the passwords of OS users mapped to JP1 users.

JP1 user

JP1 user	Server host
jp1admin	*

List of OS users to be mapped

JP1 user : jp1admin : *

Administrator (Primary user)

In the **User Mapping** page, you can associate the JP1 users registered on the authentication server with one or more users registered on the OS of the local host. Before setting user mapping, you need to assign certain Windows user rights to the OS users who set the mapping and those who are mapped. For details, see *6.1.5 Before setting user mapping*.

(1) Settings in the Password management area

In Windows, you must enter the OS users to be mapped to JP1 users, and the password information for those OS users, on every host where user mapping is required. This information is registered as password management information in JP1/Base. The **Password management** area is for registering OS users and their password information as password management information.

If you change the password of the system OS user after registering the password management information, make sure that you also change the password in the registered information.

The procedure for setting password management information is described below.

Notes

When **The logon check is not done to Windows, when OS user is set** is selected, the OS users can be successfully registered even if the following conditions are met:

- Registration of an OS user not registered in the system (in Windows)
- Registration of an OS user with an incorrect password
- Registration of an OS user, set in the **Password management** area, who does not have the right **Act as a part of the operating system**#
- Registration of an OS user who does not have the right **Log on locally**

If you do not select **The logon check is not done to Windows, when OS user is set**, any attempt to register an OS user under the above conditions will fail.

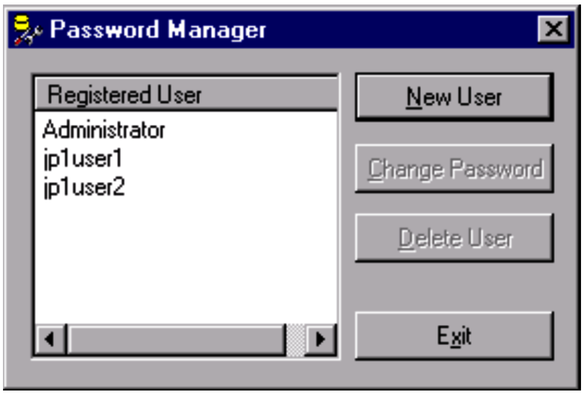
#: The user right required for the Windows versions that are not supported in this manual. For Windows versions supported in this manual, you can successfully register an OS user even if you did not assign this user right.

To set password management information:

1. In the **Password management** area, click the **Set** button.

   The Password Manager dialog boxis displayed.

Figure 6-6: Password Manager dialog box



2. Enter, change, or delete OS users and their password information.

   Click the **New User** button to register a new OS user and password. Click the **Change Password** button if any registered users have changed their passwords. Click the **Delete User** button to delete the password of a registered OS user.

   As the OS user name to be registered, you can specify not only a user name but also the name of the domain to which the local host belongs or the local host name. In this case, use a backslash (\) as a separator between the domain or local host name and user name (for example, `domain\user1` or `server\user1`). If you specify a domain name or local host name, JP1/Base checks if the specified OS user is a user who belongs to that domain or is a local user. If the specified OS user name is not a user of the domain or is not a local user, you cannot register the user under the OS user name.

   If you do not specify a domain name or local host name, JP1/Base checks whether the specified OS user is a local user. If the entered OS user is not a local user, JP1/Base checks whether it is a user in a domain containing a trusted domain. If the specified OS user name is not a local user or a user of the domain, you cannot register the user under the OS user name.

   To register an OS user name with the Windows domain controller, use the format *domain-name*\user-name. As the domain controller does not differentiate between a domain user and local user, the user name will be treated as a domain user.

   Note

   > Take care when selecting **The logon check is not done to Windows, when OS user is set** in the **User Mapping** page. When this check box is selected, the OS users can still be registered even if an OS user name or password is incorrect. However, if the mapped JP1 user tries to execute a job or remote command, an insufficient rights error occurs.

3. Click the **Exit** button.

   The Password Manager dialog box closes, and the **User Mapping** page of the JP1/Base Environment Settings dialog box appears again.

(2) Settings in the JP1 user area

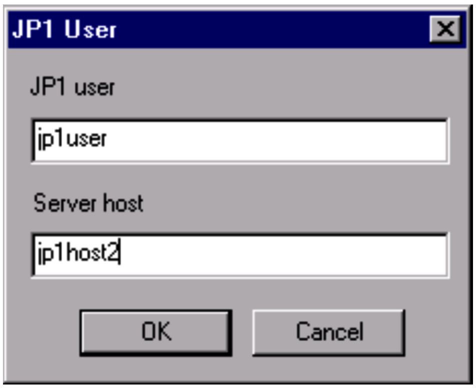
In the **JP1 user** area, set the OS users, the JP1 users mapped to OS users, and the server host from which the JP1 users issue operating instructions.

To set up this functionality:

1. Click the **Add** button.

   The JP1 User dialog box appears.

   Figure 6-7: JP1 User dialog box



JP1 User

JP1 user: jp1user

Server host: jp1host2

In this dialog box, you must define the JP1 users to be mapped to OS users, and the server hosts from which the JP1 users issue operating instructions such as jobs and remote commands (automated actions). Or enter an asterisk (`*`) as a server host name to validate operations from any server host.

Specifying a physical host in **Server host**

> Specify the host name displayed by the `hostname` command. If you are using domain names with the DNS service, specify the host name in FQDN format.

Specifying a logical host in **Server host**

> Specify the logical host name whether or not you are using the DNS service.

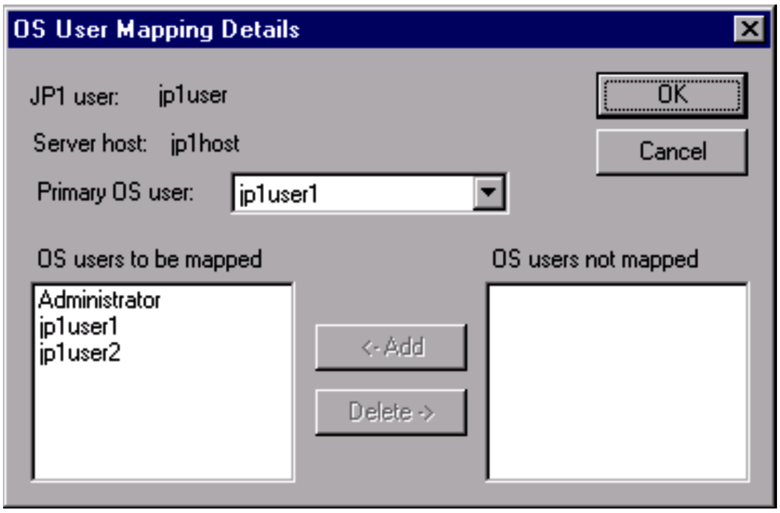
To enable users to log into the system from JP1/AJS - View or to execute JP1/AJS commands from the local host, you must specify the local host name as the server host name. For details see the manual *Job Management Partner 1/Automatic Job Management System 2 Planning and Administration Guide*, *Job Management Partner 1/Automatic Job Management System 3 System Design (Configuration)*

Guide, *Job Management Partner 1/Automatic Job Management System 3 System Design (Work Tasks) Guide*, and the *Job Management Partner 1/Automatic Job Management System 3 Administration Guide*.

2. Click the **OK** button.

   The JP1 User dialog box closes, and the OS User Mapping Details dialog box appears.

   Figure 6-8: OS User Mapping Details dialog box



OS User Mapping Details

JP1 user: jp1user

Server host: jp1host

Primary OS user: jp1user1

OS users to be mapped

Administrator
jp1user1
jp1user2

OS users not mapped

3. In the OS User Mapping Details dialog box, associate the entered JP1 user with one or more OS users.

   In this dialog box, set the OS users to be mapped to the JP1 user, and the OS users not mapped to that JP1 user. The OS users listed here are OS users registered in the Password Manager dialog box.

   In **Primary OS user**, select the name of a default OS user to be mapped when no OS user name is specified at job execution or command execution.

4. Click the **OK** button.

   This completes the mapping of the JP1 user to OS users.

(3) Settings in the List of OS users to be mapped area

The list box in the **List of OS users to be mapped** area lists the OS users who have been mapped. You can use this list to check which OS user is mapped to a specific JP1 user. You can also change the mapping relationships.

To change mapping relationships:

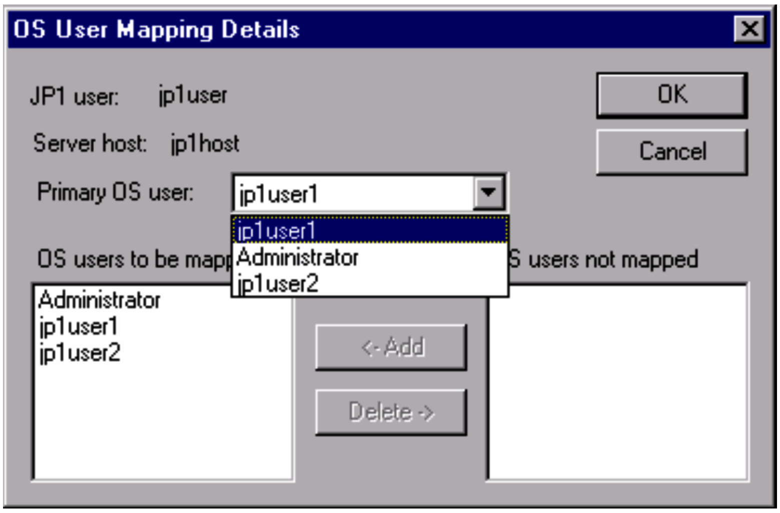
1. In the **JP1 user** area, select a user name listed in the **JP1 user** field to redefine the mapping relationships for that JP1 user.

   A list of the OS users mapped to the selected JP1 user appears in the **List of OS users to be mapped** area.

2. Click the **Change** button.

   The OS User Mapping Details dialog box appears.

   Figure 6-9: A list of the OS users mapped to the selected JP1 user



OS User Mapping Details

JP1 user: jp1user

Server host: jp1host

Primary OS user: jp1user1

3. In the OS User Mapping Details dialog box, move names between **OS users to be mapped** and **OS users not mapped**, and set the **Primary OS user**.

4. Click the **OK** button.

   This completes the mapping of the JP1 user to OS users.

6.1.7 Using commands to set user mapping

The procedure for setting user mapping by command execution is described below. Before setting user mapping, you need to assign certain Windows user rights to the OS users who set the mapping and those who are mapped. For details, see *6.1.5 Before setting user mapping*.

In Windows, you must enter the OS users to be mapped to JP1 users, and the password information for those OS users, on every host where user mapping is required. This information is registered as password management information in JP1/Base.

Note

When the check box **The logon check is not done to Windows, when OS user**

is set is selected in the **User Mapping** page of the JP1/Base Environment Settings dialog box, the OS users can be successfully registered even if the following conditions are met:

- Registration of an OS user not registered in the system (in Windows)
- Registration of an OS user with an incorrect password
- Registration of an OS user, set in the **Password management** area, who does not have the right **Act as a part of the operating system**#
- Registration of an OS user who does not have the right **Log on locally**

If you do not select **The logon check is not done to Windows, when OS user is set**, any attempt to register an OS user under the above conditions will fail.

#: The user right required for the Windows versions that are not supported in this manual. For Windows versions supported in this manual, you can successfully register an OS user even if you did not assign this user right.

JP1/Base provides a number of commands for setting password management information. The following table lists these commands and their purpose.

Table 6-2: Commands for setting password management information

Command name	Purpose	See:
`jbspassmgr`	Displays the Password Manager dialog box.	(1)
`jbsmkpass`	Sets password management information for multiple OS users in one operation from a definition file.	(2)
`jbsumappass`	Adds a specific OS user or changes the password of an OS user registered in the password management information.	(3)
`jbsrmumappass`	Deletes a specific OS user registered in the password management information.	(4)

After setting password management information for JP1/Base by using one of the above four commands, register user mapping information.

JP1/Base supports a command that sets user mapping information in the common definition information at one time, as well as commands that register, modify, or delete specific user mapping information. The following table lists these commands and their purpose.

Command name	Purpose	See:
`jbsmkumap`	Sets user mapping information in the common definition information at one time from a definition file.	(5)

Command name	Purpose	See:
`jbssetumap`	Adds or modifies user mapping information in the common definition information at one time from a definition file.	(6)
`jbsrmumap`	Deletes specific user mapping information from the common definition information.	(7)

(1) Displaying the Password Manager dialog box

The `jbspassmgr` command displays the Password Manager dialog box. This dialog box is for registering and managing the OS users registered at each host, and their password information. Enter the same password as the Windows account. For details on how to perform operations in the Password Manager dialog box, see *6.1.6(1) Settings in the Password management area*

For details on the `jbspassmgr` command, see *jbspassmgr (Windows only)* in *13. Commands*.

(2) Setting password management information for OS users in one operation

When you execute the `jbsmkpass` command, all the password information registered in the common definition information is deleted, and the password management information written in the password definition file is batch-registered in its place. For details on the `jbsmkpass` command, see *jbsmkpass (Windows only)* in *13. Commands*. To use the `jbsmkpass` command, you must first enter password management information in a password definition file. You can create the definition file in any location. Do not forget where you created it. For details on the password definition file, see *Password definition file (Windows only)* in *14. Definition Files*.

(3) Registering specific OS users

Using the `jbsumappass` command, you can register a new OS user in the JP1/Base password management information, or change the password of a registered OS user.

You can use this command in a shell script or other program to change the password information managed by the OS and simultaneously update the password management information managed by JP1/Base.

Execute the command as follows:

```
jbsumappass -u OS-user-name [-p password]
```

For details on the `jbsumappass` command, see *jbsumappass (Windows only)* in *13. Commands*.

(4) Deleting specific OS users

Using the `jbsrmumappass` command, you can delete a specified OS user from the JP1/Base password management information.

You can use this command in a shell script or other program to delete a user managed by the OS and simultaneously delete that OS user from the password management information managed by JP1/Base.

Execute the command as follows:

```
jbsrmumappass -u OS-user-name
```

For details on the `jbsrmumappass` command, see *jbsrmumappass (Windows only)* in *13. Commands*.

(5) Setting user mapping information in one operation

You can use a command to set user mapping information in one operation from the user mapping definition file (`jp1BsUmap.conf`). For details on the user mapping definition file, see *User mapping definition file* in *14. Definition Files*.

After editing the user mapping definition file (`jp1BsUmap.conf`), execute the `jbsmkumap` command, which deletes all the mapping information registered in the common definition information, and replaces it with the information written in a user mapping definition file (`jp1BsUmap.conf`). To check the defined mapping relationships, execute the `jbsgetumap` command.

For details on the `jbsmkumap` and `jbsgetumap` commands, see *jbsmkumap* and *jbsgetumap* in *13. Commands*.

Note

The user mapping definition file (`jp1BsUmap.conf`) is also used by the GUI. Any information you enter in the GUI will be applied to this file. Conversely, if you edit the user mapping definition file and then execute the `jbsmkumap` command, the edited information will be reflected in the GUI.

(6) Registering specific user mapping information

You can execute the jbssetumap command to add or modify specific user mapping information. You can either specify user mapping information directly with an option for the jbssetumap command or use a definition file containing user mapping information.

If you specify user-mapping information to register it in the common definition information, execute the following command:

```
jbssetumap {-u JP1-user-name| -ua}
           {-sh server-host-name| -sha}
            -o OS-user-name [,OS-user-name]
           [-no]
```

If you create a definition file and register user-mapping information in that file, execute the following command:

```
jbssetumap -f definition-file-name
```

You can store the definition file in any location. When you store the file, the file format must be the same as the user mapping definition file (`jp1BsUmap.conf`). For details on the format of the user mapping definition file, see *User mapping definition file* in *14. Definition Files*. For details on the `jbssetumap` command, see *jbssetumap* in *13. Commands*.

(7) Deleting specific user mapping information

To delete specific user mapping information from the common definition information, use the `jbsrmumap` command.

Execute the command as follows:

```
jbsrmumap -u JP1-user-name
```

For details on the `jbsrmumap` command, see *jbsrmumap* in *13. Commands*.

6.1.8 Notes on user management setup

Note the following when setting up user management:

- You might need to start or stop the JP1/Base service when setting an authentication server or registering a JP1 user in the JP1/Base Environment Settings dialog box. However, the JP1/Base service might fail to start or stop in the following cases:
  - If any of the services whose **Startup Type** is set to **Automatic** in the Windows Services dialog box has not completed startup
  - If the JP1/Base, JP1/IM, or JP1/AJS service is in the process of starting or stopping
  - If the JP1/Base, JP1/IM, or JP1/AJS service cannot start or stop

  If the JP1/Base service fails to start or stop, exit the JP1/Base Environment Settings dialog box. Open the Services dialog box from the Control Panel, and check whether it is possible to start or stop the service indicated in the error dialog box from this window. If it is possible, open the JP1/Base Environment Settings dialog box again and complete the settings. If you cannot start or stop the affected service from the Services dialog box, collect information about the service using the data collection tool and contact the system administrator.
- If you change the password information managed by the OS after setting user mapping, you also need to change the password management information for the OS user that was set in JP1/Base user mapping. If you do not change the information, execution of JP1/AJS jobs or JP1/IM - Manager remote commands (automated actions) might be unsuccessful.

To change the password management information in JP1/Base, use the `jbsumappass` command or `jbsrmumappass` command.

- When you set user management in a cluster system, you must first set up the environment for a cluster system as described in *3. Setting Up JP1/Base for Use in a Cluster System*. Then, do the following:

1. From the Windows **Start** menu, choose **Programs**, **JP1_Base**, and then **Environment Settings**.
2. In the Select Logical Host dialog box, select the logical host for which you want to set up user management.
3. Set up user management as described in *6.1 User management setup (in Windows)*.

When you operate an authentication server in a cluster system, the setting files for the authentication server are stored in the following folder:

shared-folder`\jp1base\conf\user_acl\`

If you are using a secondary authentication server, you must copy the settings files from the primary authentication server to the secondary authentication server. Note that the copy destination varies depending on whether you use the secondary authentication server in a cluster system:

When using a cluster system:

shared-folder`\jp1base\conf\user_acl\`

When not using a cluster system:

installation-folder`\conf\user_acl\`

After copying the settings files, execute the following command to apply the settings. You need to specify the `-h` option only if you use the secondary authentication server in a cluster system.

`jbs_spmd_reload -h` *logical-host-name*

6.2 Setup for login authentication linking with the directory server (in Windows)

If login authentication is performed by linking with the directory server, both the JP1 administrator and directory server administrator need to perform setup tasks. Perform the following setup tasks:

Setup tasks for the JP1 administrator

Setting up the authentication server linking with the directory server

- Specifying a directory server
- Setting up a JP1 user (linked user)

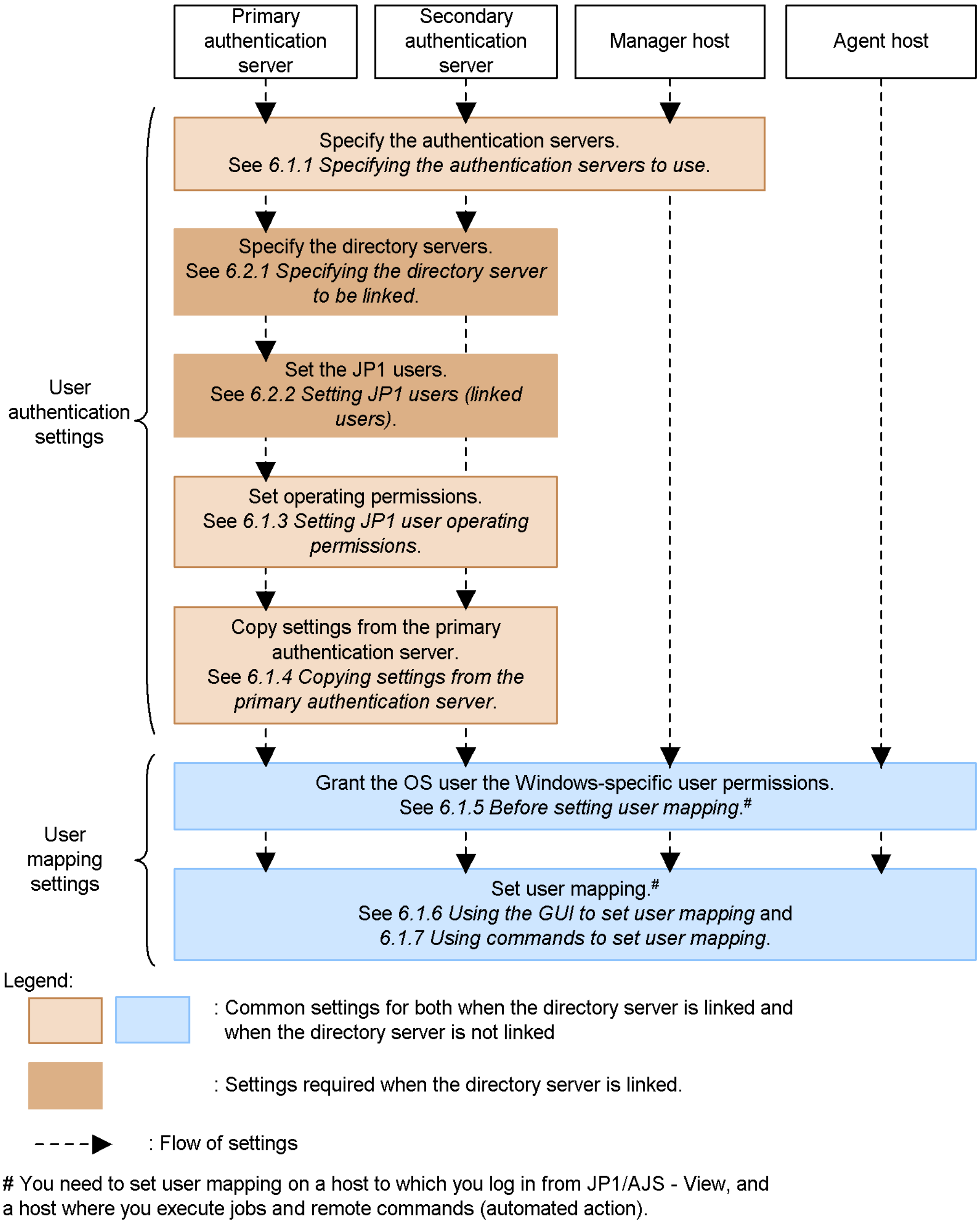
Setup tasks for the directory server administrator

Registering a JP1 user (linked user) in the directory server

This section describes the JP1 administrator's setup tasks.

The following figure shows the setup procedure required on each host and the corresponding subsections in this manual when performing login authentication by linking with the directory server.

Figure 6-10: User management setup procedure (when linking with the directory server)


Primary authentication server
Secondary authentication server
Manager host
Agent host
Specify the authentication servers.
See *6.1.1 Specifying the authentication servers to use*.
Specify the directory servers.
See *6.2.1 Specifying the directory server to be linked*.
Set the JP1 users.
See *6.2.2 Setting JP1 users (linked users)*.
Set operating permissions.
See *6.1.3 Setting JP1 user operating permissions*.
Copy settings from the primary authentication server.
See *6.1.4 Copying settings from the primary authentication server*.
Grant the OS user the Windows-specific user permissions.
See *6.1.5 Before setting user mapping*.#
Set user mapping.#
See *6.1.6 Using the GUI to set user mapping* and *6.1.7 Using commands to set user mapping*.
User authentication settings
User mapping settings
Legend:
: Common settings for both when the directory server is linked and when the directory server is not linked
: Settings required when the directory server is linked.
: Flow of settings

You need to set user mapping on a host to which you log in from JP1/AJS - View, and a host where you execute jobs and remote commands (automated action).

The settings required only when linking with the directory server as described in the subsections below. For details on other settings, see the location in this manual indicated in Figure 6-10. The settings are the same as the settings when using the authentication server only.

Notes when linking with the directory server

- A standard user can log into the authentication server even if directory server linkage is enabled.
- When the directory server administrator sets up the directory server, register JP1 users in the same container object. When linking with the directory server, CNs (common names) of a user in the directory server must be the same as the JP1 user name. For an example configuration, see *Directory server linkage definition file (Windows only)* in *14. Definition Files*.
- When SSL is used, check the following:

  Directory server

  - Whether the certification service has been installed

  Authentication server

  - Whether the certification exported from the directory server has been installed

6.2.1 Specifying the directory server to be linked

If you want to perform login authentication linking with the directory server, you must set up the common definition information from the authentication server. The directory server linkage function is disabled by default, so you must change the setting. If you use a secondary authentication server, set up the function on both the primary authentication server and secondary authentication server.

To change the directory server settings:

1. Edit the directory server linkage definition file (`jp1bs_ds_setup.conf`).

   For details on the directory server linkage definition file, see *Directory server linkage definition file (Windows only)* in *14. Definition Files*.

2. Execute the `jbssetcnf` command.

   The settings are reflected in the common definition information.

3. Execute the `jbschkds` command.

   You can check the settings of directory server linkage. You can check the following by executing the `jbschkds` command:

   - Whether the directory server linkage function is enabled

- Directory server name to be linked
- Destination port number of the directory server to be connected
- Whether SSL is to be used
- ID
- Whether the connection to the directory server was successful
- Whether the user authentication was successful

For details on the `jbschkds` command, see *jbschkds (Windows only)* in *13. Commands*.

6.2.2 Setting JP1 users (linked users)

This subsection describes how to set JP1 users (linked users) to whom login authentication is performed from the directory server. To set JP1 users, use the GUI or commands to register and delete JP1 users who use JP1/IM or JP1/AJS. The JP1 users you register will be used for login from JP1/IM - View or JP1/AJS - View. Unless otherwise specified, *JP1 user* means *JP1 user (linked user)* in this subsection.

JP1 users must be set only from a host that is an authentication server (a primary authentication server). For JP1/Base version 8 or earlier, you cannot set a linked user. Use JP1/Base 9 or later to set JP1 users.

The JP1/Base service must be running before you set JP1 users. If the JP1/Base service is inactive, start the service before attempting to set JP1 users.

The setup procedure is shown below for JP1 users when performed both from the GUI and by using commands.

(1) Using the GUI to set JP1 users

You can set JP1 users in the **JP1 user** area in the **Authentication Server** page of the JP1/Base Environment Settings dialog box.

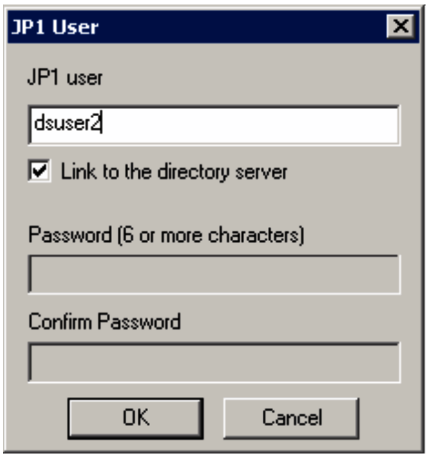
To set information in the **JP1 user** area, you must activate it first. To do this, select (highlight) an authentication server in the **Authentication Server** field in the **Order of authentication server** area. Note, however, that the **JP1 user** area remains dimmed if:

- You change an authentication server in the **Order of authentication server** area and the **Apply** button is active
- The selected (highlighted) authentication server is blocked

If the **Apply** button is active, click the button. If the selected authentication server is blocked, clear that status as described in *6.4 Setup for handling the blocked status (using a secondary authentication server)*.

Click the **Add** button to display the JP1 User dialog box.

Figure 6-11: JP1 User dialog box



JP1 User

JP1 user

dsuser2

☑ Link to the directory server

Password (6 or more characters)

Confirm Password

In this dialog box, specify a JP1 user. Enter the JP1 user name to be registered, and select the **Link to the directory server** check box. You do not need to enter a password. Make sure that the JP1 user name to be registered is different from the standard user name. You must use lower-case alphanumeric characters to specify a JP1 user name. If you use upper-case characters, they are automatically converted into lower-case characters.

The following table lists the limit on the number of characters that can be specified for the JP1 user name.

Table 6-3: Character limit for JP1 user names

Item	Number of bytes	Prohibited characters
JP1 user name	1 to 31 bytes	`* / \ " ' ^ [ ] { } ( ) : ; | = , + ? < >` spaces and tabs

When you click the **OK** or **Cancel** button, the **Authentication Server** page comes to the front.

The registered JP1 user name appears in the **User** field. For a linked user, `DS` is displayed in the **Linkage** field.

To delete a JP1 user name listed in the **User** field, select the user name and click the **Delete** button. The selected JP1 user is deleted.

(2) Using commands to set JP1 users

You can use commands to register and delete JP1 users. JP1/Base also supports a command that lists the registered JP1 users. For details on the commands, see *13. Commands*.

Registering a JP1 user:

To register a JP1 user on the authentication server, execute the following command:

```
jbsadduser -ds JP1-user-name
```

For *JP1-user-name*, use lower-case characters. Table 6-3 lists the specifiable characters for the JP1 user name.

Changing the password of a JP1 user:

You cannot change the password of a linked user in JP1/Base. Change the password from the directory server.

Deleting a JP1 user:

To delete a registered JP1 user, execute the following command:

```
jbsrmuser JP1-user-name
```

Listing registered JP1 users:

To list the registered JP1 users (standard users and linked users), execute the following command:

```
jbslistuser
```

To list only the registered linked users, execute the following command:

```
jbslistuser -ds
```

(3) Password for a linked user

Passwords for linked users are managed on the directory server, the specifiable characters are the same as those for standard users. The passwords are case-sensitive. The specifiable characters for a password are shown below:

- Byte string (6 to 32 bytes)
- Prohibited characters: \ `"` `:` and spaces and tabs

If the number of bytes of a password registered on the directory server in not within the predefined range, or a prohibited character is used in the password, user authentication will fail.

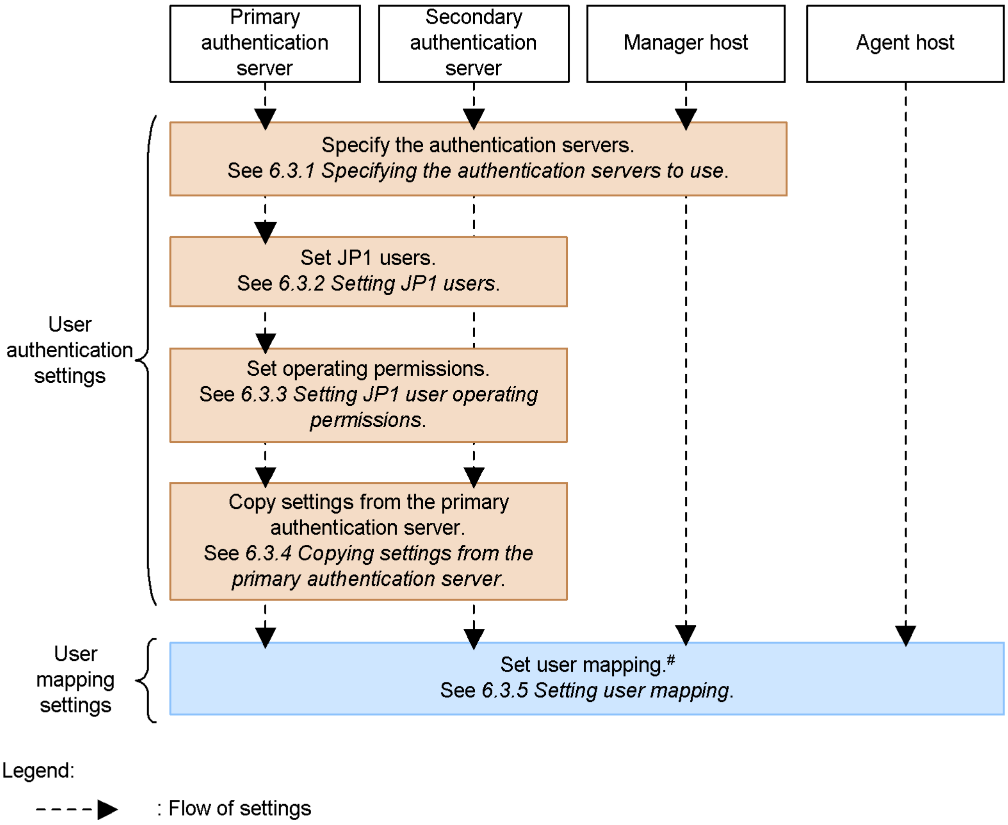
6.3 User management setup (in UNIX)

This section describes the user management setup required in UNIX. If you performed automatic setup when installing JP1/Base, the default value has been set. For details on the default of automatic setup, see *2.3.1 Installing JP1/Base*.

The setup method differs depending on whether the host is to be used as an authentication server.

If you use the secondary authentication server, setting information for both the primary authentication server and the secondary authentication server must be the same. The following figure shows the setup procedure required on each host and the corresponding sections in this manual.

Figure 6-12: User management setup procedure (in UNIX)


Primary authentication server
Secondary authentication server
Manager host
Agent host
User authentication settings
Specify the authentication servers.
See *6.3.1 Specifying the authentication servers to use*.
Set JP1 users.
See *6.3.2 Setting JP1 users*.
Set operating permissions.
See *6.3.3 Setting JP1 user operating permissions*.
Copy settings from the primary authentication server.
See *6.3.4 Copying settings from the primary authentication server*.
User mapping settings
Set user mapping.#
See *6.3.5 Setting user mapping*.
Legend:
: Flow of settings

You need to set user mapping on a host to which you log in from JP1/AJS - View, and a host where you execute jobs and remote commands (automated action).

6.3.1 Specifying the authentication servers to use

Specify the host running JP1/Base that will be used as the authentication server. The authentication server must be specified on the following hosts:

- Every host to be used as an authentication server (primary or secondary)
- Host on which JP1/IM - Manager or JP1/AJS - Manager is installed

A host specified as an authentication server manages JP1 users and the operating permissions for JP1 resource groups. If JP1/IM and JP1/AJS are both installed in your system, and if you want to use just one user authentication block, specify the same authentication server on each host.

(1) Setting the authentication servers

To specify an authentication server, execute the following command:
`jbssetusrsrv` *primary-authentication-server* [*secondary-authentication-server*]

For details on the `jbssetusrsrv` command, see *jbssetusrsrv (UNIX only)* in *13. Commands*.

Notes

- Before you start JP1/Base, in the `hosts` file or on the DNS server, enter the host name(s) set as the authentication server (or primary and secondary authentication servers). You can set the authentication servers (execute the `jbssetusrsrv` command) first, or enter the information in the `hosts` file or on the DNS server first. The order of these tasks does not matter, provided the system can resolve the IP address from the host name at JP1/Base startup.
- Specify the host names on both the primary and secondary authentication servers. You cannot specify an IP address.

(2) Checking the specified authentication servers

To check which hosts are set as authentication servers, execute the following command:
`jbslistsrv [-h` *logical-host-name*`]`

For details on the `jbslistsrv` command, see *jbslistsrv* in *13. Commands*.

(3) Disabling startup of the authentication server on the local host

When you install JP1/Base for the first time, the local host is set as the authentication server and this authentication server starts automatically. Even if you change the authentication server setting to a remote host, the authentication process on the local host will still be activated.

To disable the authentication process and prevent startup of the authentication server on the local host:

1. Make sure that disabling the local-host authentication server will not affect operations.
2. Execute the following commands:
```
cd /etc/opt/jp1base/conf
cp -p jp1bs_spmd.conf.model jp1bs_spmd.conf
```
3. Restart JP1/Base.

If you want to again specify the local host as an authentication server (primary or secondary) after disabling startup as above, take the following steps to enable startup:

1. Execute the following commands:

```
cd /etc/opt/jp1base/conf
cp -p jp1bs_spmd.conf.session.model jp1bs_spmd.conf
```

2. Restart JP1/Base.

6.3.2 Setting JP1 users

This section describes the JP1 users (standard users) for whom login authentication is performed from the authentication server. JP1 users must be set only from the hosts that are authentication servers (the primary authentication servers).

You can use commands supported by JP1/Base to register or delete JP1 users or change their passwords. JP1/Base also supports a command that lists the registered JP1 users. For details on the commands, see *13. Commands*.

(1) Registering a JP1 user

To register a JP1 user on the authentication server, execute the following command:

```
jbsadduser JP1-user-name
```

For *JP1-user-name*, use lower-case characters. This command prompts you to enter a password. The password is case-sensitive. The following table lists the limit on the number of characters that can be specified for the JP1 user name and password.

Table 6-4: Character limit for JP1 user names and passwords

Item	Number of bytes	Prohibited characters
JP1 user name	1 to 31 bytes	`* / \ " ' ^ [ ] { } ( ) : ;` `| = , + ? < >` spaces and tabs
Password	6 to 32 bytes	`\ " :` spaces and tabs

(2) Changing a JP1 user's password:

To change the password of a registered JP1 user, execute the following command:

```
jbschgpasswd JP1-user-name
```

(3) Deleting a JP1 user:

To delete a registered JP1 user, execute the following command:

```
jbsrmuser JP1-user-name
```

(4) Listing all JP1 users

To list the registered JP1 users, execute the following command:

```
jbslistuser
```

6.3.3 Setting JP1 user operating permissions

You must set the JP1 user operating permissions from an authentication server (a primary authentication server). For this setting, you set what kind of operations are permitted to JP1 users (the JP1 permission level) when they operate JP1 resource groups, such as jobs and jobnets.

Note

> You can only set operating permissions for jobs and jobnets for which you have specified JP1 resource group names with JP1/AJS. For other jobs and jobnets, all types of access by all JP1 users are permitted.

You can either set operating permissions for multiple JP1 users simultaneously or register or delete operating permissions for individual JP1 users.

The following describes how to set operating permissions for JP1 users.

(1) Setting operating permissions for multiple JP1 users simultaneously

You can use a command to set operating permissions for multiple JP1 users simultaneously. To do this, define operating permissions in the user permission level file (`JP1_UserLevel`). After editing the file, execute the `jbsaclreload` command to apply the settings. For details on the `jbsaclreload` command, see *jbsaclreload* in *13. Commands*. For details on the user permission level file, see *User permission level file* in *14. Definition Files*.

(2) Registering operating permissions for individual JP1 users

To add or modify operating permissions for individual JP1 users, you must create a definition file that describes operating permissions given to each JP1 user you want to register.

You can create the definition file in any location. The file format is the same as that of the user permission level file (`JP1_UserLevel`). For details on the user permission level file, see *User permission level file* in *14. Definition Files*.

After preparing the definition file, execute the following command to register the information in the definition file with the authentication server:

```
jbssetacl -f definition-file-name
```

For details on the `jbssetacl` command, see *jbssetacl* in *13. Commands*.

(3) Deleting operating permissions for individual JP1 users

To delete operating permissions for a registered JP1 user, execute the following command:

```
jbsrmacl -u JP1-user-name
```

Note that this command deletes all operating permissions that have been given to the specified JP1 user.

For details on the `jbsrmacl` command, see *jbsrmacl* in *13. Commands*.

6.3.4 Copying settings from the primary authentication server

When using a secondary authentication server, you must set it up with the same information set on the primary authentication server. After completing the setup for the primary authentication server, therefore, you must copy the settings from the primary authentication server to the secondary authentication server. To copy the settings from the primary authentication server to the secondary authentication server:

1. On the primary authentication server, complete the settings for JP1 users and operating permissions.

   For details on how to set up JP1 users, see *6.3.2 Setting JP1 users*. For details on how to set up user operation permissions, see *6.3.3 Setting JP1 user operating permissions*.

2. Start the secondary authentication server.

   Start the JP1/Base service to start the secondary authentication server. You can use the `jbs_spmd_status` command to verify that the secondary authentication server has started. The secondary authentication server is running if the information shown by the command contains `jbssessionmgr`.

3. Copy the settings files from the primary authentication server, using FTP or some other method.

   Using FTP or some other method, copy the settings file from the primary authentication server to the secondary authentication server. Copy the following files: `JP1_AccessLevel`, `JP1_Group`, `JP1_Passwd`, and `JP1_UserLevel`.

   These files are located in the following directory:

   `/etc/opt/jp1base/conf/user_acl/`

   Copy the files to the same directory on the local host. For a logical host, the files are stored in the following directory:
   shared-directory-name`/jp1base/conf/user_acl/`

4. Use the `jbs_spmd_reload` command to apply the settings.

   Execute the `jbs_spmd_reload` command to apply the contents of the copied settings files. The settings take effect when the command terminates normally.

For details on the commands, see *13. Commands*.

Notes

- Ensure that the same version of JP1/Base is running on the primary and secondary authentication servers.

- If the secondary authentication server has not started, execute the following commands:

  ```
  cd /etc/opt/jp1base/conf
  ```

  ```
  cp -p jp1bs_spmd.conf.session.model jp1bs_spmd.conf
  ```

  Then, restart JP1/Base to start the authentication server.

- The settings files are text files. When transferring the files between different platforms, be careful about the character set. If you transfer them by FTP, be sure to use the ASCII transfer mode.

6.3.5 Setting user mapping

You can execute a command to register, in a batch, user mapping information that was written in a definition file, into common definition information. You can also add, modify, or delete specific user mapping information.

The following describes how to set user mapping.

(1) Setting user mapping information in one operation

You can set user mapping information in one operation from the user mapping definition file (`jp1BsUmap.conf`). For details on the user mapping definition file, see *User mapping definition file* in *14. Definition Files*.

After editing the user mapping definition file (`jp1BsUmap.conf`), execute the `jbsmkumap` command, which deletes all the mapping information registered in the common definition information, and replaces it with the information written in a user mapping definition file (`jp1BsUmap.conf`). To check the defined mapping relationships, execute the `jbsgetumap` command.

For details on the `jbsmkumap` and `jbsgetumap` commands, see *jbsmkumap* and *jbsgetumap* in *13. Commands*.

(2) Registering specific user mapping information

You can execute the `jbssetumap` command to add or modify specific user mapping information. You can either specify user mapping information directly with an option for the `jbssetumap` command or use a definition file containing user mapping information.

If you specify user-mapping information to register it in the common definition information, execute the following command:

```
jbssetumap {-u JP1-user-name| -ua}
           {-sh server-host-name| -sha}
           {-o OS-user-name [,OS-user-name]}
           [-no]
```

If you create a definition file and register user-mapping information in the file, execute the following command:

```
jbssetumap -f definition-file-name
```

You can store the definition file in any location. When you store the file, the file format must be the same as the user mapping definition file (`jp1BsUmap.conf`). For details on the format of the user mapping definition file, see *User mapping definition file* in *14. Definition Files*. For details on the `jbssetumap` command, see *jbssetumap* in *13. Commands*.

(3) Deleting specific user mapping information

To delete specific user mapping information from the common definition information, use the `jbsrmumap` command.

Execute the command as follows:

```
jbsrmumap -u JP1-user-name
```

For details on the `jbsrmumap` command, see *jbsrmumap* in *13. Commands*.

6.3.6 Notes on user management setup

Note the following when setting up user management:

When you set user management in a cluster system, you must first set up the environment for a cluster system as described in *3. Setting Up JP1/Base for Use in a Cluster System*. Then, set up user management as described in *6.3 User management setup (in UNIX)*. When setting user management, specify a logical host name for the `-h` option in each command.

When you operate an authentication server in a cluster system, the setting files for the authentication server are stored in the following directory:

shared-directory-name`/jp1base/conf/user_acl/`

If you are using a secondary authentication server, you must copy the settings files from the primary authentication server to the secondary authentication server. Note that the copy destination varies depending on whether you use the secondary authentication server in a cluster system:

When using a cluster system:

shared-directory-name`/jp1base/conf/user_acl/`

When not using a cluster system:

`/etc/opt/jp1base/conf/user_acl/`

After copying the settings files, execute the following command to apply the settings.

You need to specify the `-h` option only if you use the secondary authentication server in a cluster system:

`jbs_spmd_reload -h` *logical-host-name*

6.4 Setup for handling the blocked status (using a secondary authentication server)

In a JP1/Base system with a secondary authentication server, if connection to the primary authentication server fails, JP1/Base will use the secondary authentication server instead, blocking access to the primary authentication server. This section describes how to check and release the blocked status, and how to place an authentication server in the blocked status.

Note

> You cannot check, release, or set the blocked status if there is only one authentication server. The blocked status applies only in a JP1/Base system with two authentication servers in one user authentication block.

In the Windows version of JP1/Base, you can use the GUI or commands to work with blocked status settings. In the UNIX version, you use commands.

6.4.1 Blocked status settings using the GUI (Windows only)

The following explains how to specify settings for handling the blocked status.

To use the GUI to work with the blocked status:

1. From the Windows **Start** menu, choose **Programs**, **JP1_Base**, and then **Environment Settings**.

   The JP1/Base Environment Settings dialog box appears.

2. Click the **Authentication Server** tab.

   In the **Order of authentication server** area of the **Authentication Server** page, you can check, release, or set the blocked status.

(1) Checking the blocked status

In the **Order of authentication server** area, you can check whether an authentication server is blocked or not. If **Blocked** appears in the **Status** field, the authentication server is blocked. If nothing appears in this field, the authentication server is available.

(2) Releasing the blocked status

To release an authentication server from the blocked status:

1. In the **Order of authentication server** area, select an authentication server that has **Blocked** shown in the **Status** field.

2. Click the **Change** button.

   The Authentication Server dialog box appears. Clear **Set this authentication server in state of blockage**.

3. Click **OK** or **Apply**.

   Click the **OK** button to apply the changes and close the JP1/Base Environment Settings dialog box.

   Click the **Apply** button to apply the changes and leave the dialog box open.

To verify that the blocked status has been released, check the **Status** in the JP1/Base Environment Settings dialog box. If nothing appears in this field, then the authentication server has been released.

(3) Placing an authentication server in the blocked status

To place an authentication server in the blocked status:

1. In the **Order of authentication server** area, select an authentication server that has nothing shown in **Status**.
2. Click the **Change** button.

   The Authentication Server dialog box appears. Select **Set this authentication server in state of blockage**.
3. Click **OK** or **Apply**.

   Click the **OK** button to apply the changes and close the JP1/Base Environment Settings dialog box.

   Click the **Apply** button to apply the changes and leave the dialog box open.

To verify that the status is blocked, check the **Status** in the JP1/Base Environment Settings dialog box. If **Blocked** is shown, the authentication server has been blocked.

6.4.2 Blocked status settings using commands

The following explains how to use commands to work with the blocked status. Here we assume that the system administrator specified `server1` as the primary authentication server and `server2` as the secondary authentication server.

(1) Checking the blocked status

To check whether an authentication server is blocked, execute the following command:

```
jbslistsrv
```

For details on the `jbslistsrv` command, see *jbslistsrv* in *13. Commands*.

(2) Releasing the blocked status

To release an authentication server from the blocked status, execute the following command:

`jbsunblockadesrv -s` *authentication-server*

For details on the `jbsunblockadesrv` command, see *jbsunblockadesrv* in *13. Commands*.

(3) Placing an authentication server in the blocked status

To place an authentication server in the blocked status, execute the following command:

```
jbsblockadesrv -s authentication-server
```

For details on the `jbsblockadesrv` command, see *jbsblockadesrv* in *13. Commands*.

Chapter

7. Setting the Service Start and Stop Sequences (Windows Only)

You can define the sequences for starting and stopping services. This chapter describes how to set the service start and stop sequences.

7.1 Setting the service start and stop sequences

To set the sequence for starting and stopping services:

1. Create a start sequence definition file with the file name `JP1SVPRM.DAT`.

   To create the file, execute the `cpysvprm` command. For details on the `cpysvprm` command, see *cpysvprm (Windows only)* in *13. Commands*.

   At execution of the `cpysvprm` command, the JP1SVPRM.DAT file is created in the JP1/Base data folder (*installation-folder*`\conf\boot\`).#1 Always save under the file name JP1SVPRM.DAT after modifying#2 the start sequence definition file or creating a new one.

2. If necessary, open the `JP1SVPRM.DAT` file in a text editor and edit the contents.

   For details on editing a `JP1SVPRM.DAT` file, see *7.2 Editing a start sequence definition file*.

3. Change the startup method of the services set in the `JP1SVPRM.DAT` file from automatic to manual.#3

   From the Control Panel, open the Services dialog box and change the **Startup** setting for the set services.

4. Set the timing for starting the services.

   If both the OS and JP1/Base determine when services start, the system workload increases and services might fail to start at all. To avoid startup failure due to a conflict between service schedules, set the start timing that will be used by JP1/Base for starting services.

   You can check whether services started successfully within the specified time. For details, see *7.3 Setting the timing for starting services*.

5. Restart Windows.#4

#1

The JP1/Base data folder (*installation-folder*`\conf\boot\`) contains a file with the name `JP1SVPRM.DAT.MODEL`. Never edit this file directly.

#2

We recommend that you back up the `JP1SVPRM.DAT` file before modifying its contents.

#3

If the startup method of the services set in the JP1SVPRM.DAT file is not changed from automatic to manual, the services will not start as defined in the file. Also, if services did not start as defined, neither will they stop as defined in the file.

#4

To disable the startup control, execute the cpysvprm -d command. This command deletes the JP1SVPRM.DAT file. We recommend that you back up the JP1SVPRM.DAT file before deleting it in case you later need to register the same JP1SVPRM.DAT file again.

7.2 Editing a start sequence definition file

In the start sequence definition file (`JP1SVPRM.DAT`), define information about scheduling services to start and stop in a particular sequence. This section describes how to set this start and stop sequence.

7.2.1 Setting the service start sequence

To specify the start sequence by using the start sequence definition file (`JP1SVPRM.DAT`), perform the following procedure:

1. Non-JP1 services that you want to start before JP1 services

   Write the information in the `[FrontOtherService`*xxx*`]` section of the startup sequence definition file (`JP1SVPRM.DAT`), where *xxx* represents a specific service.

2. JP1 services

   Write the information in the `[Jp1`*xxx*`]` section of the startup sequence definition file (`JP1SVPRM.DAT`), where *xxx* represents a character string assigned to the specific service.

3. Non-JP1 services that you want to start after JP1 services

   Write the information in the `[OtherService`*xxx*`]` section of the startup sequence definition file (`JP1SVPRM.DAT`), where *xxx* represents a specific service.

A *section* is a control unit that makes explicit the method of processing for each service, and the way in which the service is processed under the startup control (that is, under JP1/Base Control Service).

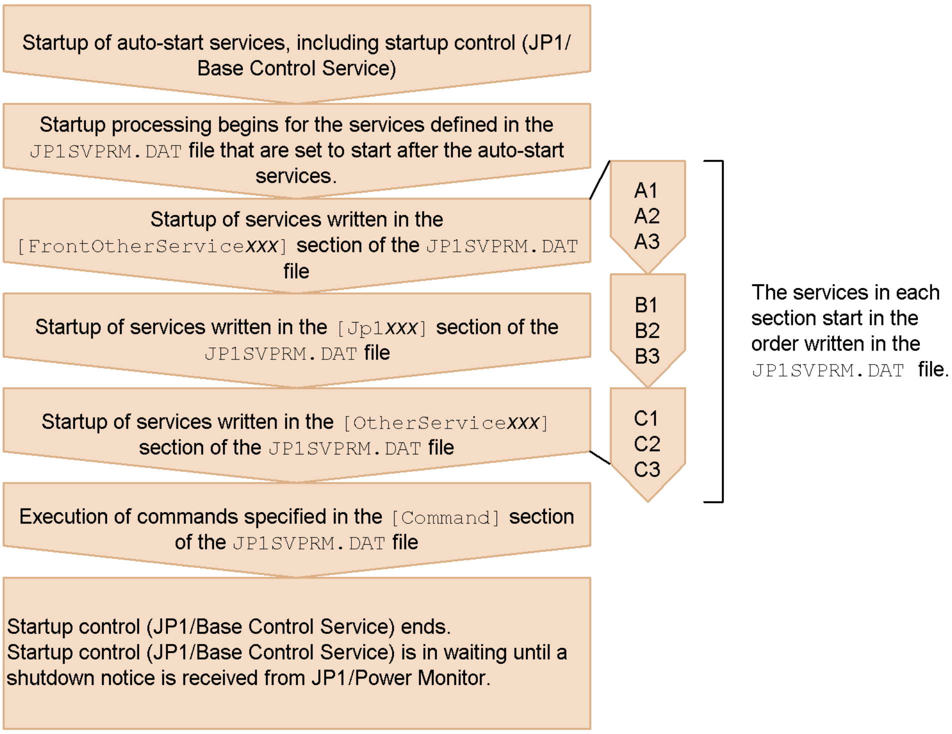
You can also control the startup sequence for the services that have been defined in the startup sequence definition file (`JP1SVPRM.DAT`) as follows:

- To start each service after the previous service's startup has finished
- To start each service before the previous service's startup has finished

For details on the forwarding settings file, see *Forwarding settings file* in *14. Definition Files*.

The following diagram shows the sequence in which services are activated at system startup.

Figure 7-1: Sequence for starting services when using the startup control


Startup of auto-start services, including startup control (JP1/Base Control Service)
Startup processing begins for the services defined in the JP1SVPRM.DAT file that are set to start after the auto-start services.
Startup of services written in the [FrontOtherService*xxx*] section of the JP1SVPRM.DAT file
Startup of services written in the [Jp1*xxx*] section of the JP1SVPRM.DAT file
Startup of services written in the [OtherService*xxx*] section of the JP1SVPRM.DAT file
Execution of commands specified in the [Command] section of the JP1SVPRM.DAT file
Startup control (JP1/Base Control Service) ends.
Startup control (JP1/Base Control Service) is in waiting until a shutdown notice is received from JP1/Power Monitor.
A1
A2
A3
B1
B2
B3
C1
C2
C3
The services in each section start in the order written in the JP1SVPRM.DAT file.

Legend:

A1, A2, and A3: Services written in that order in `[FrontOtherService`*xxx*`]`
B1, B2, and B3: Services written in that order in `[JP1`*xxx*`]`
C1, C2, and C3: Services written in that order in `[OtherService`*xxx*`]`

From the following two messages, the system administrator can verify that service startup completed successfully:

- KAVA4014-I#
- KAVA4036-I

#: Make sure that this message is output for each of the services defined in the start sequence definition file (`JP1SVPRM.DAT`).

7.2.2 Setting the service stop sequence

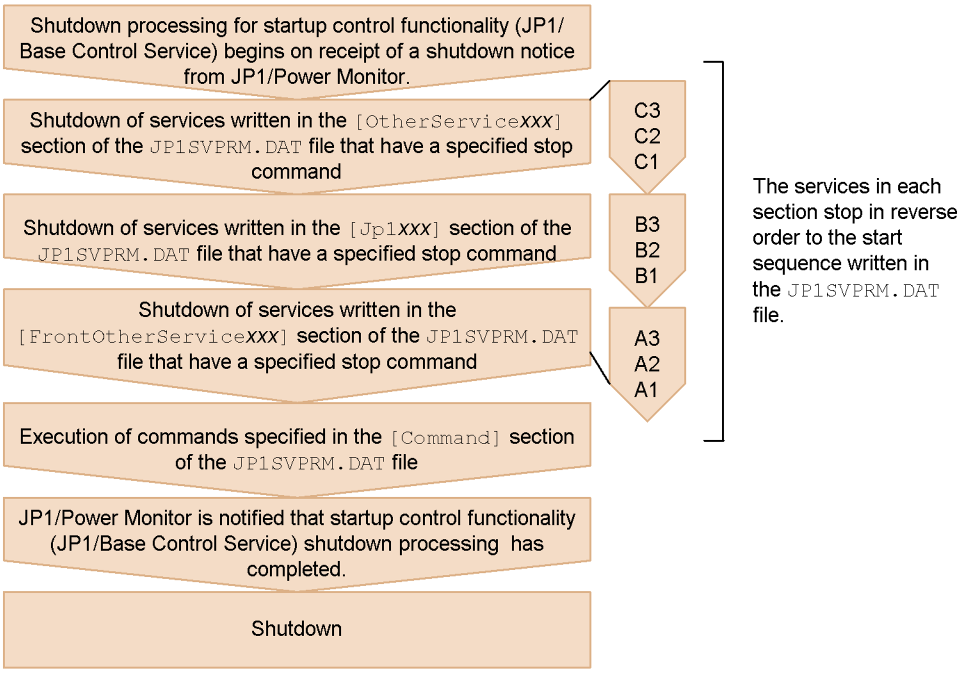
JP1/Power Monitor must be installed on the same host to control the sequence for stopping services. A stop command must be specified in the start sequence definition file (`JP1SVPRM.DAT`) file for each service that you want to control. The services that have a stop command specified in the file are shut down in reverse order from the service start sequence. When a combination of commands is used to shut down a service, you must write the commands in a batch file and specify the file name in `JP1SVPRM.DAT`.

You can control the services that have been defined in the startup sequence definition file (`JP1SVPRM.DAT`) in the following way:

- To end each service after the previous service's shutdown processing has finished

The following diagram shows the sequence in which services are stopped at system shutdown.

Figure 7-2: Sequence for stopping services when using the startup control


Shutdown processing for startup control functionality (JP1/Base Control Service) begins on receipt of a shutdown notice from JP1/Power Monitor.
Shutdown of services written in the [OtherServicexxx] section of the JP1SVPRM.DAT file that have a specified stop command
Shutdown of services written in the [Jp1xxx] section of the JP1SVPRM.DAT file that have a specified stop command
Shutdown of services written in the [FrontOtherServicexxx] section of the JP1SVPRM.DAT file that have a specified stop command
Execution of commands specified in the [Command] section of the JP1SVPRM.DAT file
JP1/Power Monitor is notified that startup control functionality (JP1/Base Control Service) shutdown processing has completed.
Shutdown
C3
C2
C1
B3
B2
B1
A3
A2
A1
The services in each section stop in reverse order to the start sequence written in the JP1SVPRM.DAT file.

Legend:

A1, A2, and A3: Services written in that order in `[FrontOtherService`*xxx*`]`
B1, B2, and B3: Services written in that order in `[JP1`*xxx*`]`
C1, C2, and C3: Services written in that order in `[OtherService`*xxx*`]`

At planned termination under JP1/Power Monitor, service shutdown processing is carried out as defined in the `JP1SVPRM.DAT` file. In this case, only services that have been activated by the startup control (JP1/Base Control Service) are stopped. Services that were already stopped when shutdown processing began or services that cannot be activated under the startup control are not stopped. To control the stop sequence at forced termination under JP1/Power Monitor, you must specify the forced termination option in the `[ControlValue]` section of the `JP1SVPRM.DAT` file.

From the following two messages, the system administrator can verify that service shutdown completed successfully:

- KAVA4023-I#
- KAVA4035-I

#: Make sure that this message is output for each of the services defined in the start sequence definition file (`JP1SVPRM.DAT`).

You can specify the start command, stop command, start processing timeout, and stop processing timeout for each service. You cannot specify service startup parameters for start commands or for stop commands.

7.3 Setting the timing for starting services

You can delay startup of the services in the start sequence definition file (`JP1SVPRM.DAT`) for a specified duration. This prevents any conflict with OS-driven service scheduling.

You can check whether services started successfully within the specified time. If a service failed to start, message KAVA4107-W is output to the Windows event log and to the integrated trace log. Check which service failed to start, and start it manually.

To enter delay settings:

1. Edit the service startup delay time / timer monitoring period definition file (`Jp1svprm_wait.dat`).

   Make a copy of the sample service startup delay time / timer monitoring period definition file (`Jp1svprm_wait.dat.sample`), save it with the file name `Jp1svprm_wait.dat`, and then edit the file.

   For details on the service startup delay time / timer monitoring period definition file, see *Service startup delay time / timer monitoring period definition file (Windows only)* in *14. Definition Files*.

2. Apply the settings.

   Restart the OS.

   Alternatively, stop all the services in the start sequence definition file (`JP1SVPRM.DAT`), and then restart the JP1/Base Control Service.

To disable the delay settings:

1. Delete or rename the service startup delay time / timer monitoring period definition file (`Jp1svprm_wait.dat`).

2. Disable the definitions.

   Restart the OS.

   Alternatively, stop all the services in the start sequence definition file (`JP1SVPRM.DAT`), and then restart the JP1/Base Control Service.

7.4 Notes on using startup control

Note the following points when using the startup control:

- Do not attempt to start or stop any services in the Services dialog box that opens from the Control Panel in Windows while Windows is starting up. If you do so, the services might not start correctly.
- Do not use the Services dialog box from the Control Panel in Windows to perform operations on any of the services defined in the start sequence definition file (`JP1SVPRM.DAT`). Starting or stopping these services in the Services dialog box could cause the `KAVA4003-E` message to appear, and could make automatic start and stop control by the JP1/Base Control Service fail to operate correctly.
- The startup control function is not available for the services running on logical hosts. The function is only available for the services running on physical hosts. Use cluster software to control startup of services on logical hosts.

Chapter

8. Setting up an Event Service Environment

This chapter explains how to set up the JP1/Base event service.

8.1 Process for setting up an event service environment

You must perform two tasks in order to configure an event service environment:

- Configure an event service operating environment
- Define how JP1 events will be forwarded

By default, the following settings have been set:

- Run the event server on the local host.
- Create the event database.

  By default, the event database is created in the following location:

  In Windows: *installation-folder*`\sys\event\servers\`

  In UNIX: `/var/opt/jp1base/sys/event/servers/`

  By default, the maximum size of the event database is 10,000,000 bytes.
- Acquire all JP1 events.
- Forward JP1 events to an upper server.#

  #: An *upper server* is a server set in the JP1/IM configuration definition file. Only JP1 events with the extended attribute `SEVERITY`, and with `Warning`, `Error`, `Critical`, `Alert`, or `Emergency` set as the value of that attribute, are forwarded from the local host. If no upper server has been set in the JP1/IM configuration definition file, JP1 events are not forwarded. If you want to forward JP1 events to a remote host other than the server set in the configuration definition file, modify the default setting.

The following explains the procedures for setting up an event service environment.

8.1.1 Determining which JP1 events to forward

First, determine which JP1 events to forward. Consider the following when determining which JP1 events to forward:

- Only important JP1 events need to be forwarded for error monitoring.

  According to the system configuration defined in JP1/IM - Manager, by default, only important JP1 events are sent to a higher-level server. The default setting is recommended if you intend to monitor the system for errors only. If you change the default, any JP1 events that are unnecessary for system operation should not be forwarded to a higher-level host.
- Consider the number of JP1 events to be forwarded per unit of time.

  Delays could occur in the transfer processing if there are a large number of JP1 events being forwarded.

Set the conditions so that the types of forwarded JP1 events will not be in close proximity or, if they do occur in quick succession, this situation does not continue for very long. For example, define a filter condition in the forwarding settings file (`forward`) so that only JP1 events with a severity level of *Warning* or higher will be sent.

- Consider the total number of JP1 events that will be stored on the higher-level host (manager or submanager).

  Delays could occur when the JP1 events are registered in the event database if there are a large number of JP1 events being forwarded to the higher-level host.

  Consider the number of hosts managed by the manager host, the number of JP1 events sent from each host, and the number of JP1 events generated on the local host. For example, define filter conditions in the forwarding settings file (`forward`) on each host so that only JP1 events with a severity level of *Warning* or higher will be sent from an agent to a submanager, and only JP1 events with a severity level of *Error* or higher will be sent from a submanager to the manager host.

- Consider the amount of traffic data on the network.

  Use the following equation to estimate the amount of data transferred on the network per JP1 event:

  $60^{\#1} + 600^{\#2}$ (bytes)

  #1: The amount of data transferred per JP1 event when a 16-byte remote event server name, with `close` as its communication type, is specified in the `remote-server` parameter in the event server settings file (`conf`). When `keep-alive` is specified as the communication type, this amount of data is transferred only for the first JP1 event.

  #2: For a JP1 event generated when a character string of approximately 100 bytes is trapped by a log file trap.

8.1.2 Setting up an event service environment

This section describes how to configure or modify an event service environment, and how to check the specified settings.

(1) Configuring the environment

To set up the event service environment:

1. Configure the event-service operating environment.

   Use the following files to configure an event-service operating environment:

   - Event server index file (`index`)

Defines directories that are used by the event server.

- Event server settings file (`conf`)

  Defines the operating environment for the event service.

- API settings file (`api`)

  Defines the method for connecting from the application program to the event server and the port to use for the connection.

For details on each definition file, see *Event server index file*, *Event server settings file*, and *API settings file* in *14. Definition Files*.

2. Define how JP1 events should be forwarded.

   Use the forwarding settings file (`forward`) to define which JP1 events to be forwarded to which event server. According to the system configuration defined in JP1/IM - Manager, by default, only severe-level JP1 events are sent to a higher-level server. The default setting is recommended if you intend to monitor the system for only errors.

   For details on the forwarding settings file, see *Forwarding settings file* in *14. Definition Files*.

3. Enable the setting.

   Start the event service to apply the settings.

   In Windows:

   The event service is set by default to start automatically when the system is started. For details on the startup control, see *7. Setting the Service Start and Stop Sequences (Windows Only)*.

   In UNIX:

   Execute the `jevstart` command.

(2) Modifying the event service operating environment

To modify the event service operating environment:

1. Edit the settings files.

   Edit the event server index file (`index`), event server settings file (`conf`), and API settings file (`api`).

2. Apply the new settings.

   Restart the event service to apply the new settings.

   In Windows:

   From the Control Panel, open the Services dialog box. Stop the **JP1/Base**

Event service, and then restart the service.

In UNIX:

Execute the `jevstop` command to stop the event service, and then execute the `jevstart` command to restart it.

Notes on overwrite installations

In Version 9, the `save-rep` flag has been added to the `options` parameter in the event server settings file (`conf`). Setting this flag saves the duplication prevention table of the event database to the file. If this flag is not set, the duplication prevention table is saved to memory. In this case, the table is deleted, and then re-created when the event server is restarted. As a result, it takes time to receive JP1 events forwarded from other hosts. We recommend that you set the `save-rep` flag in the event server that receives JP1 events forwarded from other hosts.

If you perform an overwrite installation from JP1/Base 08-00 or earlier, this flag will not be set. In this case, you must perform the following procedure to create the duplication prevention table in the file.

To create this table in the file:

1. Add the `save-rep` flag to the `options` parameter in the event server settings file.

   For details on the event server settings file, see *Event server settings file* in *14. Definition Files*.

2. Execute the `jevdbmkrep` command.

   For details on the `jevdbmkrep` command, see *jevdbmkrep* in *13. Commands*.

3. Start the event server.

(3) Modifying the settings for forwarding JP1 events

To modify the settings for forwarding JP1 events:

1. Edit the forwarding settings file (`forward`).
2. Apply the new settings.

   Reload the forwarding settings file (`forward`) or restart the event service to apply the new settings.

   - Reload the forwarding settings file (`forward`).

     You can apply the new settings while the system is operating. Execute the following:

     ```
     jevreload
     ```

- Restart the event service.

  In Windows: From the Control Panel, open the Services dialog box. Stop the **JP1/Base Event** service, and then restart it.

  In UNIX: Execute the `jevstop` command to stop the event service, and then execute the `jevstart` command to restart it.

(a) Collecting and distributing definition information from the manager host

With one operation, you can distribute the information in a forwarding settings file (`forward`) from a higher-level host defined in the JP1/IM - Manager system configuration to lower-level hosts. The forwarding settings are reloaded on each host as soon as the file is successfully distributed, after which event forwarding starts again, using the updated settings.

For details on this function, see *10. Collecting and Distributing Event Service Definitions (JP1/IM Only)*.

(b) Note on reloading the forwarding settings file (forward)

Any JP1 events being sent at the exact moment the forwarding settings file (`forward`) is reloaded are canceled and the transfers are regarded as having failed. For this reason, in the `forward-limit` parameter of the event server settings file (`conf`), you must set a retry timeout that will allow any JP1 events that could not be forwarded to be resent after the forwarding settings file is reloaded.

(c) Reloading the forwarding settings file when using JP1/IM - Manager

When the forwarding settings file (`forward`) contains a `to-upper` forwarding setting block, the JP1 events will be forwarded according to the JP1/IM - Manager system configuration. If the JP1/IM - Manager system configuration is changed, the forwarding settings file (`forward`) will be automatically updated when you execute the `jbsrt_distrib` command to distribute the new JP1/IM - Manager system configuration to each host. There is no need to execute the `jevreload` command on each host.

For details on the `jbsrt_distrib` command, see the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition file Reference*.

Note

> If your system consists of hosts on which JP1/Base 06-00 or JP1/Base 06-51 or later are installed, the configuration definition information will be distributed when the `jbsrt_distrib` command is executed. However, the forwarding settings file (`forward`) will not be reloaded on the hosts running JP1/Base version 06-00.
>
> You must restart the event service on the hosts running JP1/Base version 06-00.

(4) Checking whether the event service is active

Execute the following command to check whether the event service is active. If the return value is 0, then the event service is running.

```
jevstat
```

For details on the jevstat command, see *jevstat* in *13. Commands*.

(5) Checking the settings for forwarding JP1 events

Execute the following command to check the event forwarding settings for the active event services. The execution result will be displayed on screen in the format of the forwarding settings file (forward).

```
jbsgetopinfo -o forward
```

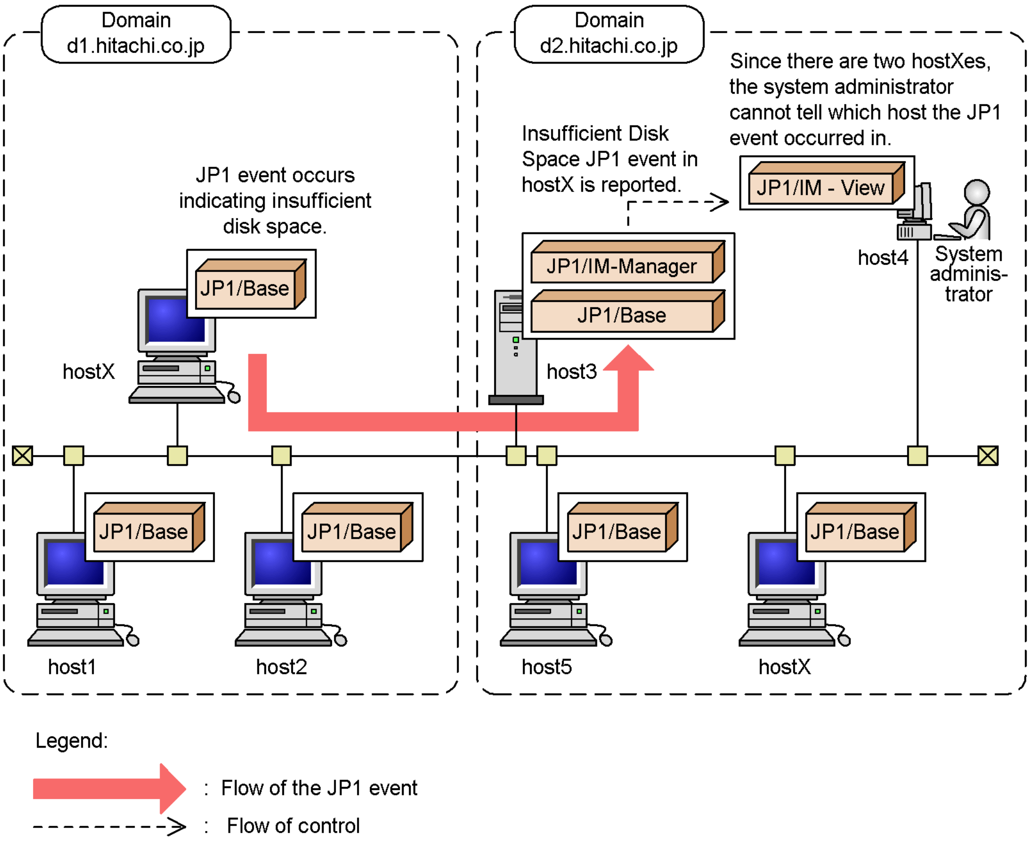
For details on the jbsgetopinfo command, see *jbsgetopinfo* in *13. Commands*.

8.1.3 Setting up an event server in a system that uses DNS services

Various problems might occur if you use the default event server in a system that has multiple domains. This subsection describes how to set up the event servers in a system that uses DNS services, based on the following example. Note that the following example assumes that the DNS returns the FQDN name as the local host name.

The following figure shows a system that contains two domains, d1.hitachi.co.jp and d2.hitachi.co.jp.

Figure 8-1: Example system containing two domains



In this example, a JP1 event indicating insufficient disk space occurs in the `hostX.d1.hitachi.co.jp` domain. A JP1 event is forwarded to `host3.d2.hitachi.co.jp` and displayed in JP1/IM - View on host4. The registered host name appears as *hostX*. Since *hostX* also exists in domain `d2.hitachi.co.jp` in the above figure, the system administrator cannot tell whether the JP1 event occurred at `hostX.d1.hitachi.co.jp` or at `hostX.d2.hitachi.co.jp`. JP1/IM - View has a window for monitoring from which programs it receives JP1 events. However, if the host running JP1/IM - View belongs to domain `d2.hitachi.co.jp`, it interprets *hostX* to be `hostX.d2.hitachi.co.jp` and displays the wrong information.

To avoid these sorts of problems with multiple domains, instead of the default event server, define an event server with a Fully Qualified Domain Name (FQDN-format event server).

Notes

- When you use an FQDN-format event server, the JP1/SES compatibility function or collection and distribution of event service definition information described in *J. Linking with Products That Use JP1/SES Events* might not be possible. Keep this in mind when using the JP1/SES compatibility function or collecting and distributing event service definition information.
- While using an FQDN-format event server, a JP1/AJS log file monitoring job on the physical host is not available. To use a JP1/AJS log file monitoring job, do not configure an FQDN-format event server as described in (1), and specify the local host name (the host name that is returned by the `hostname` command) in FQDN-format.

The following describes the procedure for setting up an FQDN-format event server. The procedure differs in Windows and UNIX. The procedures for Windows and UNIX are described below.

(1) Setting up an FQDN-format event server (Windows)

Follow these steps to set up an FQDN-format event server in Windows. The specified event server here is assumed to be `hostX.d1.hitachi.co.jp`.

1. Register the FQDN-format event server as a service by using the `jevregsvc` command.

   The `jevregsvc` command has the following format:

   ```
   jevregsvc -r hostX.d1.hitachi.co.jp
   ```

   Note

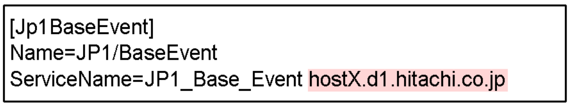
   If JP1/IM - Manager or JP1/AJS has been installed, dependencies exist with the default services. In Windows, to set up an FQDN-format event server, release the dependencies between JP1/IM - Manager or JP1/AJS and the default event services.

2. Open the event server index file (`index`) in a text editor. Change the event server name in the `server` parameter from `*` (default) to `@` or `hostX.d1.hitachi.co.jp`.

   If you change the parameter to `@`, you can use the JP1/SES compatibility function or collect and distribute event service definition information. If you change the parameter to `hostX.d1.hitachi.co.jp`, you can no longer use the JP1/SES compatibility function nor collect and distribute event service definition information. Choose whichever setting suits your system.

3. Open the start sequence definition (`JP1SVPRM.DAT`) file in a text editor. Edit the file to start the FQDN-format event server instead of the default event server.

   The entry in the edited start sequence definition (`JP1SVPRM.DAT`) file (only the part pertaining to the event server) is as follows:



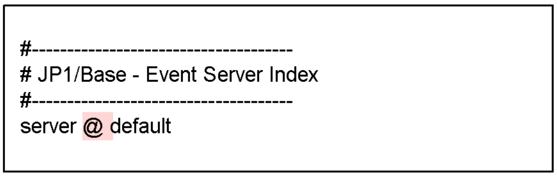
```
[Jp1BaseEvent]
Name=JP1/BaseEvent
ServiceName=JP1_Base_Event hostX.d1.hitachi.co.jp
```

(2) Setting up an FQDN-format event server (UNIX)

Follow these steps to set up an FQDN-format event server in UNIX. The specified event server here is assumed to be `hostX.d1.hitachi.co.jp`.

1. Open the event server index file (`index`) in a text editor. Change the event server name in the `server` parameter from `*` (default) to `@` or `hostX.d1.hitachi.co.jp`.

   If you change the parameter to `@`, you can use the JP1/SES compatibility function or collect and distribute event service definition information. If you change the parameter to `hostX.d1.hitachi.co.jp`, you can no longer use the JP1/SES compatibility function nor collect and distribute event service definition information. Choose whichever setting suits your system. The entry in the event server index file (`index`) when the event server name is changed to `@` is as follows:

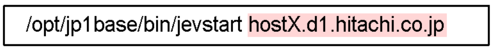


```
#-------------------------------------
# JP1/Base - Event Server Index
#-------------------------------------
server @ default
```

2. Open the `jbs_start` and `jbs_stop` scripts in a text editor. Edit the scripts to start and stop the FQDN-format event server instead of the default event server.

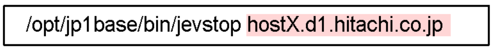
   The entries in the edited scripts (only the part pertaining to the event server) are as follows:

   Entry in the `jbs_start` script:



```
/opt/jp1base/bin/jevstart hostX.d1.hitachi.co.jp
```

   Entry in the `jbs_stop` script:



```
/opt/jp1base/bin/jevstop hostX.d1.hitachi.co.jp
```

8.2 Initializing the event database

Using the `jevdbswitch` command, you can initialize an event database while the event service is active. However, you must stop the event service and use the `jevdbinit` command to initialize an event database, if any of the following occur:

- There are not enough system resources.
- You cannot connect to the event service.
- A JP1 event is being forwarded to another event server.

The following describes the procedure for initializing an event database.

8.2.1 Initializing an event database while the event service is active

This subsection describes the procedure for initializing an event database while the event service is active. If a JP1 event is being forwarded to another event server, refer to *8.2.2 Initializing an event database while the event service is stopped* and initialize the event database.

To initialize an event database while the event service is active:

1. Back up the event database by using an OS command or by some other means.

   Back up the event database if you want to verify its contents. You can output the contents to a CSV file by using the `jevexport` command.

   For details on this command, see *jevexport* in *13. Commands*.

2. Execute the `jevdbswitch` command twice.

   Execute the `jevdbswitch` command two times to swap the event database out and in again.

   The first time you execute this command, the active database (database currently in use) is replaced by the standby database. Also, the existing data in the standby database is erased. The second time you execute the `jevdbswitch` command, the existing data is cleared from both the active and standby databases.

   For details on the `jevdbswitch` command, see *jevdbswitch* in *13. Commands*.

Note

> The procedure above cannot be used to clear out the memory in which the events are stored. A maximum of 2,000 events can be stored in memory during the transfer retry processing. If you want to delete the events by clearing the memory, initialize the event database by referring to the procedure described in *8.2.2 Initializing an event database while the event service is stopped*.

8.2.2 Initializing an event database while the event service is stopped

The procedure for initializing an event database while the event service is stopped depends on whether JP1 events are being forwarded from the event server to be initialized. The following describes the procedure for initializing an event database for each case.

(1) When JP1 events are forwarded from the event server to be initialized

Work out the start serial number from the JP1 events forwarded to another event server and initialize the event database:

1. On the destination event server, locate the serial number of the last JP1 event forwarded from the event server to be initialized.

   Locate the serial number in either of the following ways. If JP1 events are forwarded to more than one event server, search on all the destination event servers.

   Event search in JP1/IM - View:

   > Perform an event search from JP1/IM - View to find the JP1 events registered on the destination event server.
   >
   > For details on searching for JP1 events, see the manual *Job Management Partner 1/Integrated Management - Manager Administration Guide*.

   Outputting the event database contents to a CSV file:

   > Using the `jevexport` command, output the contents of the event database on the destination event server to a CSV file for verification.
   >
   > For details on this command, see *jevexport* in *13. Commands*.

2. Execute the `jevdbinit` command. In the `-s` option, specify the start serial number in the event database.

   Execute the following:
   `jevdbinit -s` *event-database-serial-number-found-at-step1*`+1 {-b | -n}`

   The event database is re-created using the start serial number specified in the `-s` option.

(2) When JP1 events are not forwarded from the event server to be initialized

Execute the following command to initialize the event database:
`jevdbinit {-b | -n}`

This command deletes and re-creates the event database. The data serial numbers are inherited from the original database.

If the database is corrupted and you want to back it up, specify the -b option. If you do not want to back up the database, specify the -n option. You can output the contents to a CSV file by using the jevexport command.

For details on the jevdbinit command and backed up databases, see *jevdbinit* in *13. Commands*.

Initialization fails at execution of the jevdbinit command if the serial numbers in the event database cannot be carried over. If the KAJP1789-E message is output, re-create the event database by specifying 0 as the start serial number in the -s option.

```
jevdbinit -s 0 {-b | -n}
```

8.3 Outputting the event database to a CSV file

This section describes how to convert the contents of an event database into the comma separated value (CSV) format and output the records to a CSV file. Use this procedure when you want to preserve the event database records as a CSV file or when you need to verify the contents of a backed up event database. To output the event database to a CSV file, execute the following command:

```
jevexport [-h event-server-name]
          [-i event-database-file-name]
          [-o output-file-name]
          [-f filter-file-name]
          [-t ON | OFF]
          [-k items-file-name]
          [-a]
```

For details on this command, see *jevexport* in *13. Commands*. The output format of a CSV file is described below.

8.3.1 Output format of a CSV file

The output format of a CSV file is as follows:

- Strings are enclosed with double quotation marks (").
- Data items are separated by commas.
- Each record ends with a linefeed.
- Strings containing null data are still output and enclosed with double quotation marks (").
- When outputting the numeric data, use numbers.
- For extended attributes, only the attribute value is output for the 12 types of common information. Both the attribute name and attribute value are output for program-specific information.
- Program-specific information is output in alphabetical order of the attribute names.
- You can change the data items output from column 28 by modifying the items file.

  The items output to the CSV file are explained in further detail below.

8.3.2 Items output to the CSV file

The following explains the items that are output from the event database to a CSV file. The items that are actually output to the file depend on whether you specified the `-k` option when executing the `jevexport` command.

The output items in each case are listed separately below.

(1) Items output when the -k option is specified in the jevexport command

If you specify the `-k` option when executing the `jevexport` command, the extended attributes (program-specific information) specified in the items file are output to the CSV file. The items are output from column 28 in the same order as specified in the items file. Each item is output as an extended attribute name paired with its value. If a non-existent extended attribute is written in the items file, a null value is output to the corresponding column for that item.

The following table lists the items that are output when the `-k` option is specified in the `jevexport` command. The title name is output when the `-a` option is specified.

Table 8-1: Items output when the -k option is specified in the jevexport command

Col.	Attribute name	Title name	Contents	Format	Remarks
1	Serial number	Serial number	Order in which events (including local events) arrive at this event server, regardless of the source. This attribute is not preserved for JP1 event transfers between event servers. This attribute is mainly used to prevent delays or duplication when a user program acquires JP1 events or when JP1/Base forwards a JP1 event to another event server.	Number	--
2	`ID` (basic code)	Event ID(basic code)	Basic code of the event ID. An event ID is expressed as an eight-byte value. The upper four bytes represent the basic code.	Number	Hexadecimal of 1 to 8 digits
3	`ID` (extended code)	Event ID(extended code)	Extended code of the event ID. The lower four bytes represent the extended code.	Number	Hexadecimal of 1 to 8 digits
4	`PROCESSID`	Source process ID	Process ID of the application program that issued the event.	Number	Number
5	`TIME`	Registered time	Time of event registration on the source event server (based on the source host clock).	Number	Cumulative seconds since UTC 1970-01-01 00:00:00

Col.	Attribute name	Title name	Contents	Format	Remarks
6	`ARRIVEDTIME`	Arrived time	Time an event was registered on the local event server. This attribute is not preserved for JP1 event transfers between event servers.	Number	Cumulative seconds since UTC 1970-01-01 00:00:00
7	`REASON`	Registered reason	Reason for registration of the JP1 event on this event server. This attribute is not preserved for JP1 event transfers between event servers. One of the following codes is set: `1`: Event issued by the local event server to the local event server `3`: Event issued by the remote event server to the local event server `4`: Event forwarded from the remote event server to the local event server according to the environment settings	Number	--
8	`USERID`	Source user ID	User ID of the source process.	Number	In Windows and Java, set to a fixed value (-1 to 65,535) according to the environment settings.
9	`GROUPID`	Source group ID	Group ID of the source process.	Number	In Windows and Java, set to a fixed value (-1 to 65,535) according to the environment settings.
10	`USERNAME`	Source user name	User name of the source process.	Character string	--
11	`GROUPNAME`	Source group name	Group name of the source process.	Character string	Null string in Windows and Java

Col.	Attribute name	Title name	Contents	Format	Remarks
12	SOURCESERVER	Source event server name	Name of the source event server. Set to the event server name of the host on which a JP1 event occurred, even if the event is forwarded to another event server.	Character string	--
13	SOURCESEQNO	Source specific serial number	Serial number in the event database on the source host.	Number	Unchanged during an event transfer.
14	CODESET	Code set	Name of the character code-set in which the message, detailed information, and extended attributes are written.	Character string	--
15	MESSAGE	Message	Message text indicating the JP1 event contents.	Character string	--
16	SEVERITY	Event level	Urgency of the JP1 event. The following levels are used, starting from the most severe: Emergency, Alert, Critical, Error, Warning, Notice, Information, Debug	Character string	Extended attribute value 1
17	USER_NAME	User name	Name of the user who executed the job.	Character string	Extended attribute value 2
18	PRODUCT_NAME	Product name	Name of the program that issued the JP1 event. The program names set in this attribute include: /HITACHI/JP1/AJS /HITACHI/JP1/AOM /HITACHI/JP1/IM /HITACHI/JP1/NBQ /HITACHI/JP1/NQSEXEC	Character string	Extended attribute value 3
19	OBJECT_TYPE	Object type	Object type as one of the following: JOB, JOBNET, ACTION, ACTIONFLOW, PRINTJOB, PRINTQUEUE, PRINTER, BATCHQUEUE, PIPEQUEUE	Character string	Extended attribute value 4

Col.	Attribute name	Title name	Contents	Format	Remarks
20	OBJECT_NAME	Object name	Object name (job, jobnet, and so on). For a hierarchy of objects such as a jobnet, the lowest element is set.	Character string	Extended attribute value 5
21	ROOT_OBJECT_TYPE	Root object type	Object type. Normally the same as OBJECT_TYPE, but when there is a hierarchy of objects as in a jobnet, the type of ROOT_OBJECT_NAME is used. The range of values is the same as for OBJECT_TYPE.	Character string	Extended attribute value 6
22	ROOT_OBJECT_NAME	Root object name	Name of the unit for execution instructions during user operation. Normally the same as OBJECT_NAME, but when there is a hierarchy of objects as in a jobnet, the name of the top-level object is set.	Character string	Extended attribute value 7
23	OBJECT_ID	Object ID	Object ID. When paired with PRODUCT_NAME, the OBJECT_ID uniquely identifies an instance of the object within the JP1 system. (The format is product-dependent. This information is used when a user launches the monitor screen for a JP1 program from the Tool Launcher in JP1/IM - View.)	Character string	Extended attribute value 8
24	OCCURRENCE	Occurrence	The event that occurred in relation to the object shown in OBJECT_NAME. The values set in this attribute include: END, LATEEND, LATESTART, NOTICE, PAUSE, START, SWITCH	Character string	Extended attribute value 9
25	START_TIME	Start time	Time at which execution started or restarted, as the number of seconds since UTC 1970-01-01 00:00:00. This item is not always set.	Character string	Extended attribute value 10

Col.	Attribute name	Title name	Contents	Format	Remarks
26	`END_TIME`	End time	Time at which execution or re-execution completed, as the cumulative seconds since UTC 1970-01-01 00:00:00. This item is not always set.	Character string	Extended attribute value 11
27	`RESULT_CODE`	Result Code	Completion code (numeric literal). This item is not always set.	Character string	Extended attribute value 12
28	Program-specific extended attribute name 1	Program-specific extended attribute	Program-specific extended attribute name	Character string	--
29	Program-specific extended attribute value 1	Not output.	Program-specific extended attribute value	Character string	--
: :	: :	: :	: :	: :	: :
m-1	Program-specific extended attribute name *n*	Not output.	Program-specific extended attribute name	Character string	--
m	Program-specific extended attribute value *n*	Not output.	Program-specific extended attribute value	Character string	--

Legend:

m: Number of items output to the CSV file

n: Number of program-specific extended attribute names and associated values

(2) Items output when the -k option is omitted in the jevexport command

If you omit the `-k` option when executing the `jevexport` command, the data from column 28 and on in the CSV file differs from the items that are output when the `-k` option is specified. The following table lists the items that are output from column 28 and on when the `-k` option is omitted. For details on the items that are output from columns 1 to 27, see *Table 8-1 Items output when the -k option is specified in the jevexport command*. The title name is output when the `-a` option is specified.

Table 8-2: Items output when the -k option is omitted in the jevexport command

Col.	Attribute name	Title name	Contents	Format	Remarks
28	Program-specific extended attributes count	Program-specific extended attributes count	Number of program-specific extended attributes	Number	Number (0 to *n*)
29	Program-specific extended attribute name 1	Program-specific extended attribute	Program-specific extended attribute name	Character string	--
30	Program-specific extended attribute value 1	Not output.	Program-specific extended attribute value	Character string	--
: :	: :	: :	: :	: :	: :
m-1	Program-specific extended attribute name *n*	Not output.	Program-specific extended attribute name	Character string	--
m	Program-specific extended attribute value *n*	Not output.	Program-specific extended attribute value	Character string	--

Legend:

m: Number of items output to the CSV file

n: Number of program-specific extended attribute names and associated values

8.4 Notes on using the event service

Note the following points when using the event service:

- If you install JP1/Base on a Windows computer, but change the default setting to disable the event service, the performance of programs that use the event service might be affected. If you do not want to start the event service, add the following definition to the API settings file `api` (sets the event service environment):

  ```
  server local-host-name close  0.0.0.0  jp1imevtapi
  ```

  In *local-host-name*, specify the same name as the host name output by the `hostname` command. Adding this definition will prevent any impact on program performance. Do not write this definition in the API settings file if you want to start the event service.

- The event service will only operate in an environment that allows conversion from a local host name to an IP address, or from a local IP address to a local host name. Be sure to set up the `hosts` file or DNS server to enable these conversions.

- When you specify an IP address with the `ports` parameter in the event server settings file (`conf`) configured by default during the program installation, the JP1 event registration and acquisition programs might not be able to access event services if you assign an IP address that does not correspond to a host name returned by the `hostname` command. In this case, modify the API settings (`api`) file.

  Example:

  Settings in the `conf` file (the `ports` parameter line):

  ```
  ports 192.168.1.2 jp1imevt jp1imevtapi
  ```

  Settings in the `api` file:

  ```
  server     *     keep-alive
  server  host-name keep-alive 192.168.1.2
  ```

  Note: For *host-name*, specify the value returned by the `hostname` command.

- The event service does not support the use of external characters in basic or extended attributes for JP1 events. Any external characters contained in character string attributes might not appear correctly in JP1/IM - View and other programs. Forwarding settings files (`forward`) and action definition files for log file trapping and event log trapping also do not support external characters. If you specify an external character, JP1/Base might fail to forward or trap any JP1 events.

Chapter

9. Setting Up the Event Converters

SNMP traps and messages output to log files can be converted into JP1 events and handled by the event service.

This chapter describes how to set up the event converters provided by JP1/Base. To convert the SNMP traps managed by the pre-Version 6 NNM into JP1 events, see *I. Converting SNMP traps*.

9.1 Converting application program log files

Use log file trapping to convert application logs into JP1 events. Because the log messages that are converted differ for each user, no default is set for the log file trapping function. To use this function, you need to set log file traps for each user.

The following describes how to set up a log file trap.

9.1.1 Setting up a log file trap

The following describes the procedures for starting a log file trap, changing the settings, checking the operating status, checking the settings, and stopping a log file trap. Set up a log file trap in the following files:

- Action definition file for log file trapping

  Specify the format of the monitored log file, the retry settings when monitoring fails and any other settings.

- Log information definition file (`jevlogd.conf`)

  Specify the maximum size and number of storable log files used for log file trapping. You can use the default settings under normal circumstances.

(1) Starting a log file trap

To start a log file trap:

1. Create an action definition file for log file trapping.
2. Execute the `jevlogstart` command.

   The log file trapping starts, the ID is output to the standard output or to the `syslog` file. Take note of this ID as you will need it when stopping a log file trap or updating a definition file.

   Also, you can specify a monitoring target name using the `jevlogstart` command. After the monitoring target name is specified, use the `jevlogstop`, `jevlogreload`, and `jevlogstat` commands to specify and operate the monitoring target names.

   For details on the `jevlogstart` command, see *jevlogstart* in *13. Commands*.

(2) Changing a setting

The following describes how to change settings in the action definition file for log file trapping and the log information definition file (`jevlogd.conf`).

(a) Changing a setting in the action definition file for log file trapping

1. Edit the action definition file for log file trapping.

2. Apply the settings.

    If a parameter other than MARKSTR or ACTDEF is modified:

    Restart the log file trapping function. Execute jevlogstop {*ID-number*|-a *monitoring target name*}, and then execute the jevlogstart command.

    If the modified parameter is MARKSTR or ACTDEF:

    Execute jevlogreload { *ID-number*|-a *monitoring target name*} without stopping log file trapping to apply the settings.

For details on the jevlogstart command, see *jevlogstart* in *13. Commands*.

For details on the jevlogreload command, see *jevlogreload* in *13. Commands*.

(b) Changing a setting in the log information definition file

1. Edit the log information definition file (jevlogd.conf).
2. Restart the log-file trap management service (or daemon).

(3) Checking the operating status

To check the operating status of a log file trap, execute the following command. From the return value, you can verify the status of the log file trap specified by the ID number in the command argument or monitoring target name.

```
jevlogstat{ID-number|-a monitoring target name}
```

You can also use the following command to display a list of IDs and monitoring target names of the log file traps in progress:

```
jevlogstat ALL
```

For details on the jevlogstat command, see *jevlogstat* in *13. Commands*.

(4) Checking the settings

To check the action definition information of the active log file trap, execute the following command. The execution result will be displayed on screen in the format of the action definition file for log file trapping.

```
jbsgetopinfo -o logtrap [-i ID-number|-a monitoring target name]
```

For details on the jbsgetopinfo command, see *jbsgetopinfo* in *13. Commands*.

(5) Stopping a log file trap

To stop a log file trap, execute the following command:

```
jevlogstop {ID-number|-a monitoring target name}
```

To stop all the active log file traps, execute the following command:

```
jevlogstop ALL
```

For details on the `jevlogstop` command, see *jevlogstop* in *13. Commands*.

(6) Starting a log file trap automatically

Upon restarting the system, active log file traps stop and are not restarted automatically. To restart the log file traps automatically when you restart the system, use the following procedure:

- In Windows, create batch files and use the JP1/Base startup control to set up the batch files.

  Create batch files and specify the appropriate `jevlogstart` command in each file. After that, in the start sequence definition file (`JP1SVPRM.DAT`), write `ReadyCommand=` followed by each batch file name specified by full path.

  For details on the start sequence definition file, see *Start sequence definition file (Windows only)* in *14. Definition Files*.

- In UNIX, specify the `jbs_start` command.

  Specify the command so that the log file trapping starts after the event service and the log-file trap management daemon have started.

- Execute the `jevlogstart` command as a JP1/AJS job.

9.1.2 Notes on log file trapping

Note the following points when you use log file trapping:

- Stop the log file trap before you edit or delete a log file that is being monitored by log file trapping. If you attempt to edit or delete a log file while the trap is in progress, the monitoring position in the file might change and the trap will fail to convert the data correctly.

- The log file trapping function cannot extract data written to a log file unless the data has actually been written to a disk. This means that sometimes you might not be able to retrieve log messages as soon as they occur because the data has not been written to a disk yet.

- It will take a long time for the first JP1 event to be generated if the log write-position is near the end of the file.

Notes on monitoring the integrated trace log or `syslog` file

When you use a log file trap to monitor the integrated trace log or `syslog` file, attempts to transfer the log data to JP1 events might fail repeatedly. In such a case, the transfer error message KAJP1037-E is output to the integrated trace log or `syslog` file. If you specify the settings as the following to monitor the integrated trace log or `syslog` file, the transfer error message KAJP1037-E will also be converted into a JP1 event. If the default setting is used for the forwarding settings file (`forward`), the JP1 transfer-failure events will also be forwarded.

Setting example:

When monitoring the integrated trace log or `syslog` file:

```
ACTDEF=<Error>11 "KAJP....-E"
ACTDEF=<Error>11 "-E"
```

When monitoring the `syslog` file:

```
ACTDEF=<Error>11 "error"
```

To prevent the event transfer from looping, change the setting in the action definition file for log file trapping, so that a log file trap will not trap the KAJP1037-E message. A setting example is shown below.

Setting example 1:

```
MARKSTR="KAJP1037-E"
```

Setting example 2:

```
ACTDEF=<Error>11 "KAJP....-E"
        !"KAJP1037-E"
```

Using JP1/AJS log file monitoring jobs

If you wish to use a JP1/AJS log file monitoring job, you must first start both the Windows log-file trap management service (or UNIX log file trap management daemon) and the event service. JP1/AJS log file monitoring jobs are executed using the JP1/Base log file trapping function.

For details on log file monitoring jobs, see the *Job Management Partner 1/ Automatic Job Management System 2 Planning and Administration Guide*, *Job Management Partner 1/Automatic Job Management System 3 System Design (Configuration) Guide*, *Job Management Partner 1/Automatic Job Management System 3 System Design (Work Tasks) Guide*, and the *Job Management Partner 1/ Automatic Job Management System 3 Administration Guide*.

9.2 Converting Windows event logs

Use the event log trapping function to convert Windows event logs into JP1 events. By default, JP1/Base converts the system log, and the error and warning logs output by the application program, that are displayed in the Windows event viewer.

The following describes how to set up an event log trap.

9.2.1 Procedures for setting up event log trapping

The following describes the procedures for starting and stopping event log trapping. Set up a event log trap in the following files:

- Action definition file for event log trapping

  Specify the conditions for converting event log data into a JP1 event and the event-log monitoring interval.

(1) Starting the event log trapping function

The following describes the procedure for starting the event log trapping function:

To change the settings:

1. Edit the action definition file for event log trapping (`ntevent.conf`).
2. Start the event-log trapping service.

   From the Control Panel, open the Services dialog box and start the **JP1/Base EventlogTrap** service.

Notes

- If the event server is inactive and no connection retry setting has been entered in the action definition file, the server will fail to start.
- If no action definition file for event log trapping (`ntevent.conf`) exists, or if the file is invalid, the service will fail to start and this information will be output to the event log and integrated trace log.
- If an invalid log type or invalid regular expression is specified in a filter condition in the action definition file for event log trapping (`ntevent.conf`), by default that condition is considered invalid, but the service is successfully started or the settings are successfully reloaded. Alternatively, you can specify that service startup and reloading of settings should fail when a filter condition is invalid. For details, see the `filter-check-level` parameter of *Action definition file for event log trapping (Windows only)* in *14. Definition Files*.
- Event log entries are monitored starting from the time the trapping service

starts. Entries before the service starts cannot be monitored.

(2) Changing a setting while a trap is active

To change the settings:

1. Edit the action definition file for event log trapping (`ntevent.conf`).
2. Apply the settings.

   If you changed the `server` parameter:

   Restart the event-log trapping service.

   If you changed a parameter other than `server`:

   Do not stop the event-log trapping service. Instead, execute the `jeveltreload` command to apply the changes.

(3) Check the settings

To check the action definition information of the active event log trap, execute the following command. The execution result will be displayed on screen in the format of the action definition file for log file trapping (`ntevent.conf`).

```
jbsgetopinfo -o evttrap
```

For details on the `jbsgetopinfo` command, see *jbsgetopinfo* in *13. Commands*.

(4) Stopping the event log trapping function

To stop event log trapping, stop the event-log trapping service. From the Control Panel, open the Services dialog box and stop the **JP1/Base EventlogTrap** service.

(5) Starting the event log trapping function automatically

Upon restarting the system, active event log traps stop and are not restarted automatically. If you want to start an event log trap automatically after the system is restarted, use the JP1/Base startup control to automatically start event log trapping.

In the start sequence definition file (`JP1SVPRM.DAT`), delete the hash mark (#) at the beginning of the following parameter lines:

```
#[Jp1BaseEventlogTrap]
#Name=JP1/BaseEventlogTrap
#ServiceName=JP1_Base_EventlogTrap
```

For details on the start sequence definition file, see *Start sequence definition file (Windows only)* in *14. Definition Files*.

9.2.2 Notes on event log trapping

(1) Notes on using the defaults

Note the following points when you are using the defaults set in the action definition file for event log trapping (ntevent.conf) and forwarding settings file (forward).

- When the action definition file for event log trapping (ntevent.conf) and the forwarding settings file (forward) are used with their defaults and a JP1 event fails to transfer, the error message KAJP1037-E will be output to the event log and converted into a JP1 event. The converted JP1 event is then resent, and another transfer error will occur.

  To prevent the event transfer from looping, change the setting in the action definition file for event log trapping (ntevent.conf), so that the KAJP1037-E message will not be trapped. For an example on how to set up ntevent.conf, see *Action definition file for event log trapping (Windows only)* in *14. Definition Files*.

- If the event log can no longer acquire events, a message will be output to the integrated trace log, but the JP1 event will not be output. To output the JP1 event, change the setting of the action definition file for event log trapping (ntevent.conf). For details on ntevent.conf, see *Action definition file for event log trapping (Windows only)* in *14. Definition Files*.

(2) Notes on using JP1/AJS Windows event-log monitoring jobs

If you wish to use a JP1/AJS Windows event-log monitoring job, you must first start the event log trapping service. JP1/AJS Windows event log monitoring jobs are executed under this JP1/Base function.

Set the event log trapping action definition file (ntevent.conf) so that it contains the condition for event monitoring by JP1/AJS. This condition is the logical product of the settings defined in JP1/AJS and the settings defined in the action definition file for event log trapping (ntevent.conf). For details on Windows event log monitoring jobs, see the *Job Management Partner 1/Automatic Job Management System 2 Planning and Administration Guide*, *Job Management Partner 1/Automatic Job Management System 3 System Design (Configuration) Guide*, *Job Management Partner 1/Automatic Job Management System 3 System Design (Work Tasks) Guide*, and the *Job Management Partner 1/Automatic Job Management System 3 Administration Guide*.

Chapter

10. Collecting and Distributing Event Service Definitions (JP1/IM Only)

This chapter explains how the manager host can collect event service definitions in a system consisting of JP1/Base and JP1/IM, and distribute definitions to each managed host.

10.1 Communication settings for definition and operation information (linked with IM configuration management)

After JP1/Base is linked with IM configuration management of JP1/IM, the definition and operation information of JP1/Base can be managed from IM configuration management viewer. For details on linking with IM configuration management, see the *Job Management Partner 1/Integrated Management - Manager Overview and System Design Guide*.

To link JP1/Base to IM configuration management, you must first specify the hosts that can access the host access control definition file. Only the hosts specified in the host access control definition file have access permission, access attempts from unspecified hosts will all be rejected. For details on the host access control definition file, see *Host access control definition file* in *14. Definition Files*.

10.2 Collecting event service definitions

When you execute the collection command (`jevdef_get`) on the manager host, it collects definitions in the specified definition files from all managed hosts defined in the JP1/IM system configuration. The command also outputs the definitions to the standard output. For details on the `jevdef_get` command, see *jevdef_get* in *13. Commands*.

Notes

- If the `jevdef_get` command fails to collect definitions due to an error on a managed host, the system outputs an error message to the standard error output without outputting definitions for that host to the standard output.
- The message returned from the source hosts during the execution of the `jevdef_get` command is output in the language specified by each host.

10.2.1 Output format

The collected definitions are output as the following:

```
# JP1/Base - Event Server file-type-information by jevdef_get
# Time which acquired the following definitions : date-and-time

[target-host-1]
definitions
[target-host-2]
definitions
       :
```

For *file-type*, the name of the target definition file is displayed. The display is `forward` for the forwarding settings file, `event log trap` for the action definition file for event log trapping, and `log file trap` for the action definition file for log file trapping.

For *definitions*, all information in the definition file is displayed, including hash marks (#) and blank lines.

10.2.2 Collection example

The following shows an example of what might be output when collecting definitions in the forwarding settings file (`forward`):

```
# JP1/Base - Event Server forward-information by jevdef_get
# Time which acquired the following definitions : 2003/07/21
15:23:22

[SubHost_A]
to ManagerHost
```

```
E.SEVERITY IN Error
OR
E.PRODUCT_NAME IN /HITACHI/JP1/AOM
end-to

[SubHost_B]
to ManagerHost
E.SEVERITY IN Error
OR
E.PRODUCT_NAME IN /HITACHI/JP1/AOM
end-to

[SubHost_C]
to ManagerHost
E.SEVERITY IN Error
OR
E.PRODUCT_NAME IN /HITACHI/JP1/AOM
end-to

[JP1host_1]
to SubHost_A
E.SEVERITY IN Error Warning
OR
E.PRODUCT_NAME IN /HITACHI/JP1/AOM
end-to

[JP1host_2]
to SubHost_A
E.SEVERITY IN Error Warning
OR
E.PRODUCT_NAME IN /HITACHI/JP1/AOM
end-to
```

10.3 Distributing event service definitions

The following describes how the manager host distributes definitions to managed hosts. The manager host distributes definitions to the managed hosts defined in the JP1/IM - Manager system configuration on the manager host. It can distribute definitions to all managed hosts or just particular managed hosts.

To distribute definitions to managed hosts:

1. Edit the distribution definition file.

   In the distribution definition file, define the destination hosts and the definitions you want to distribute. You must prepare a distribution definition file for each definition file for which you want to distribute definitions.

   For details on the distribution definition file, see *Distribution definition file* in *14. Definition Files*.

2. Execute the `jevdef_distrib` command.

   The definitions are distributed and the settings are applied. For details on the `jevdef_distrib` command, see *jevdef_distrib* in *13. Commands*.

Notes

- If definitions are already set on a destination host, the `jevdef_distrib` command first deletes the existing definitions before distributing definitions.
- The message returned from the destination hosts during the execution of the `jevdef_get` command is output in the language specified on each host.

Chapter
11. Setting Local Actions

When a failure or another specific JP1 event occurs, you can use the JP1/Base local action function to automatically execute pre-registered commands.

This chapter explains how to set up local actions.

11.1 Setting a local action

This section describes how to set up a local action.

11.1.1 Defining a local action

The procedure for defining a local action is described below:

1. Register local action definitions to the common definition information.

   You can change the setting of the following items in the common definition information:

   - File size of the local action execution log (1,024 KB by default)
   - Numbers of local action execution logs to store (4 by default)
   - Local action pausing (local actions are not paused by default)

   To change the above settings:

   1-1 Copy the model file (`jp1bs_lcact_setup.conf.model`) for the common definition settings file (local action function) and give the file a name.

   1-2 Edit the copied file.

   1-3 Execute the following command:

   `jbssetcnf` *file-edited-in-step-1-2*

   Local action definitions are registered to the common definition information.

   For details on the `jbssetcnf` command, see *jbssetcnf* in *13. Commands*.

   For details on the common definition settings file (local action function), see *Common definition settings file (local action function)* in *14. Definition Files*. If the common definition settings file (local action function) contains an error, the set values are invalidated and the default settings are used.

2. Create and edit the local action execution definition file (`jbslcact.conf`).

   You can define the following items in the local action execution definition file.

   Required items:

   - Execution conditions of the local action
   - JP1 user name
   - Execution command

   Option items:

   - Environment variable file name

- Same action suspending
- Number of actions in queue
- Number of actions to be executed simultaneously
- Loading of the user profile (Windows only)

For details on the local action execution definition file, see *Local action execution definition file* in *14. Definition Files*. If the local action execution definition file contains an error, the command cannot be executed.

3. Specify user mapping for JP1 users.

   Specify user mapping for the JP1 users required for the execution of each action. For details on how to specify user mapping, see *6.1 User management setup (in Windows)* or *6.3 User management setup (in UNIX)*.

4. Edit the local action environment variable file.

   Define the environment variables required for the execution of the local action execution commands. For details on the local action environment variable file, see *Local action environment variable file* in *14. Definition Files*. If the local action environment variable file contains an error, the commands cannot be executed.

5. Restart all of the JP1/Base services.

   To apply the information, execute the `jbs_spmd_reload` command. For details on the `jbs_spmd_reload` command, see *jbs_spmd_reload* in *13. Commands*.

11.1.2 Changing local action settings

To change the execution conditions or execution commands of local actions:

1. Edit the local action execution definition file (`jbslcact.conf`).

   For details on the local action execution definition file, see *Local action execution definition file* in *14. Definition Files*.

2. Restart all JP1/Base services to enable the settings for the local action execution definition file (`jbslcact.conf`).

   To apply the information, execute the `jbs_spmd_reload` command. For details on the `jbs_spmd_reload` command, see *jbs_spmd_reload* in *13. Commands*.

The settings for the local actions generated after the restart of JP1/Base services are enabled.

If the local action execution definition file (`jbslcact.conf`) contains an error, the local actions are paused.

11.1.3 Checking the operating status of a local action

To check the status of a process executed by the local action, execute the following command:
`jbslistlcact`

Information about the action in execution or in the queue is output.

To cancel an action in execution or in the queue, execute the following command:
`jbscancellcact`

The action specified in the command is canceled. If an action in execution is canceled, any child processes generated during the execution are also canceled.

For details on the `jbslistlcact` command and the `jbscancellcact` command, see *jbslistlcact* and *jbscancellcact* in *13. Commands*.

11.1.4 Pausing a local action

The following describes how to temporarily pause a local action to conduct maintenance or other operations.

To pause a local action:

1. Edit the common definition settings file (local action function) you used when defining the local action.

   Set the `PAUSE` parameter to `00000001` (pause). For details on the common definition settings file (local action function), see *Common definition settings file (local action function)* in *14. Definition Files*.

2. Execute the following command:

   ```
   jbssetcnf file-edited-in-step-1
   ```

   The information specified for pausing the local action is registered to the common definition information. For details on the `jbssetcnf` command, see *jbssetcnf* in *13. Commands*.

3. Apply the specified common definition information.

   To apply the information, execute the `jbs_spmd_reload` command. For details on the `jbs_spmd_reload` command, see *jbs_spmd_reload* in *13. Commands*.

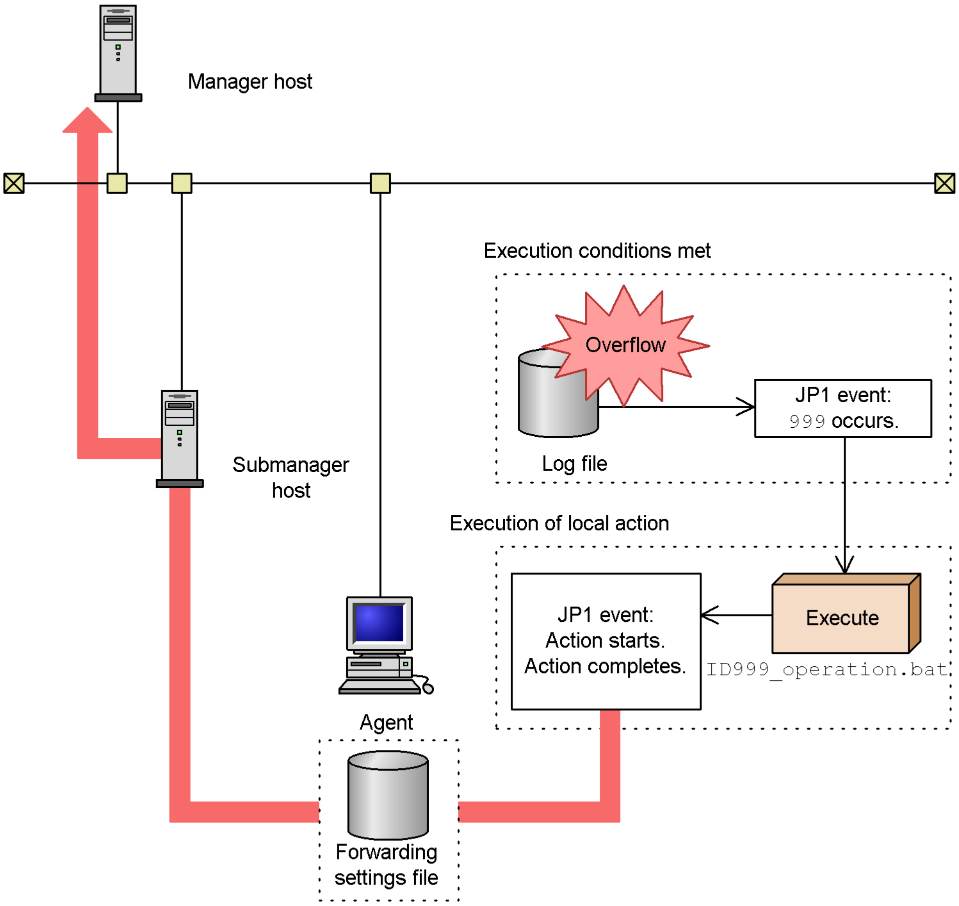
When a local action is paused, the local action remains in the state of having been started, and event acquisition stops. The actions in execution or in the queue are not canceled.

When a local action is unpaused, the events registered after the local action was unpaused become the targets of the action. For details on how to unpause a local action, see *Common definition settings file (local action function)* in *14. Definition Files*.

11.2 Example of operating a local action

The following example describes how to set up and operate a local action. In this example, the local action executes a batch file (`ID999_operation.bat`), which contains commands for operations such as backing up log files, and starting the data collection tool, when a JP1 event (event ID: `999`) indicating a log file overflow occurs in a system configuration similar to the one illustrated in the following figure.

Figure 11-1: Example of operating a local action



11.2.1 Setting the local action execution definition file

First of all, you need to set the local action execution definition file. The following explains how to set up the local action execution definition file and provides an example of the file.

The settings in the local action execution definition file are as follows:

- Set up the file so that the batch file (ID999_operation.bat) that contains measures against log file overflow will execute when a JP1 event (event ID:999) indicating a log file overflows occurs.
- An OS user with batch file execution permission needs to specify the name of the mapped JP1 user (jp1user01) in order to execute a local action.
- To report to the manager host that an action has been executed, make sure that JP1 events are issued for the start and end of a local action, and that the events are transferred to the manager host.

An example of local action execution definition file:

```
# Measure of JP1 Event ID: 999
act ID999_action
  cnd
    B.ID IN 999
  end-cnd
  usr jp1user01
  cmd "D:\EventOperation\ID999_operation.bat"
  evt yes/yes
end-act
```

For details on how to enable the specified local action execution definition file, see *11.1.1 Defining a local action*.

11.2.2 Setting the forwarding settings file

Send the action start event and action end event to a higher-level manager host. The following explains how to set up the event service forwarding settings file and provides an example of the file.

Items to specify in the forwarding settings file:

- Set up the file so that the action start event (00004780), action end event (00004781), action end event (not executable) (00004782), and action end event (cancellation) (00004783) will be forwarded from the agent host to a submanager host.
- Furthermore, set up the file so that the events will be forwarded from the submanager host to a higher-level manager host.

An example of setting the forwarding settings file

```
# Forwarding of a local action event
to-upper
  B.ID RANGE 4780 4783
```

```
end-to
```

For details on how to enable the specified forwarding settings file, see *8.1.2 Setting up an event service environment*.

11.3 Notes on local actions

Note the following point when using the local action function:

- Do not use perform the OS shutdown command from a local action.

Chapter

12. Modifying Settings During JP1/ Base Operation

This chapter describes the times when changes made in JP1/Base settings during JP1/Base operation take effect. It also describes the procedures required to modify the system environment, such as IP addresses, or host names, during JP1/Base operation.

12.1 Modifying settings for JP1/Base

The following table shows when changes made in JP1/Base settings during JP1/Base operation take effect. For details of how to modify settings, see the relevant section. In the *See:* column, the upper row indicates the relevant section for Windows and the lower row indicates that for UNIX.

Item	When settings are reflected	See:
JP1/Base troubleshooting settings	If you modify settings for restarting an abnormally ended process, the new settings take effect when you restart JP1/Base or execute the reload command.	*2.4.2*
	If you modify the settings for issuing a JP1 event at abnormal termination of a process controlled by the process management function or at failover of the authentication server, you must restart JP1/Base and the products that require JP1/Base (JP1/IM and JP1/AJS) after executing the command.	*2.4.2*

Item	When settings are reflected	See:
User management settings	You can modify the authentication server settings while JP1/Base is active if no jobs, automated actions, or commands that use JP1/IM or JP1/AJS are being executed. The new settings take effect when you click the **OK** button in the GUI or when you execute the command.	*6.1.1* *6.3.1*
	You can modify the JP1 user settings any time after the authentication server has started. The new settings take effect when you click the **OK** button in the GUI or when you execute the command. However, if the JP1 user who changed the settings is still logged in, the new settings will not take effect until the JP1 user logs in again. You do not need to restart JP1/Base.	*6.1.2*, *6.2.2* *6.3.2*
	You can modify the authority levels for JP1 resource groups any time after the authentication server has started. The new settings take effect when you click the **OK** button in the GUI or when you execute the command. You do not need to restart JP1/Base.	*6.1.3* *6.3.3*
	If you are using a secondary authentication server, the settings take effect when you copy the setting files from the primary authentication server to the secondary authentication server.	*6.1.4* *6.3.4*
	You can modify the settings of login authentication linking with the directory server any time after the authentication server has started. If you modify the settings in the directory server linkage definition file (`jp1bs_ds_setup.conf`), the new settings will take effect after you execute the command.	*6.2.1*
	You can modify the user mapping settings without stopping JP1/Base. The new settings take effect when you click the **OK** button in the GUI or when you execute the command.	*6.1.6* *6.1.7* *6.3.5*
Settings for service start and stop sequences (Windows only)	If you modify the start sequence definition file (`JP1SVPRM.DAT`), the new settings take effect once you restart Windows.	*Start sequence definition file (Windows only)*
Event service environment settings	If you modify settings in the event server index file (`index`), the new settings take effect once you restart the event service.	*Event server index file*

Item	When settings are reflected	See:
	If you modify settings in the event server settings file (`conf`), the new settings take effect once you restart the event service.	*Event server settings file*
	If you modify settings in the forwarding settings file (forward), the new settings take effect once you execute the reload command.	*Forwardi ng settings file*
	If you modify settings in the API settings file (`api`), the new settings take effect once you restart the event service.	*API settings file*
Event conversion settings	If you modify settings in the action definition file for log file trapping, the definitions of some parameters take effect once you execute the reload command.	*Action definition file for log file trapping*
	If you modify settings in the action definition file for event log trapping (`ntevent.conf`), the new settings take effect once you execute the reload command.	*Action definition file for event log trapping (Windows only)*
Health check settings	If you modify settings in the health check definition file (`jbshc.conf`), the new settings take effect when you restart JP1/Base or execute the `jbs_spmd_reload` command.	*Health check definition file*
Settings for Hitachi Network Objectplaza Trace Library (HNTRLib2)	Settings take effect when you restart the Hitachi Network Objectplaza Trace Library (HNTRLib2).	*hntr2util (Windows only), hntr2util (UNIX only), hntr2conf, hntr2getc onf*
Communication settings	If you modify `jp1hosts` information, the settings take effect once you execute the command and then restart JP1/Base.	*4.3.2*
	If you modify the protocol for JP1/Base, the settings take effect once you execute the command and then restart JP1/Base, the products requiring JP1/Base (JP1/IM and JP1/AJS), and the programs that depend on JP1/Base.	*4.3.3*

Item	When settings are reflected	See:
	If you modify the protocol for the event service, the settings take effect once you restart JP1/Base, the products requiring JP1/Base (JP1/IM and JP1/AJS), and the programs that depend on JP1/Base.	*4.3.4*
Local action functionality settings	If you modify settings in the local action execution definition file, the new settings will take effect after you start or reload JP1/Base.	*Local action execution definition file*

12.2 Modifying settings on a JP1/Base host

This section describes the effects of changing the host name, IP address, or system time of a computer running JP1/Base and the follow-up tasks required when you change these settings.

12.2.1 Effects and follow-up tasks when changing host names

This subsection describes the functionality that is affected by changing host names, and the tasks you must perform after the change.

(1) User authentication

If you change the host name of the authentication server in Windows, in the JP1/Base Environment Settings dialog box, display the **Authentication Server** page. Then, change the host name. For UNIX, use the `jbssetusrsrv` command to change the host name. The user authentication function is not affected unless the host name of the authentication server is changed.

(2) User mapping

For the user mapping function, perform the following carefully so that none of the host names remain unchanged.

(a) When the manager host name is changed

On every agent host for which remote command execution is issued from a manager, check the mapping definition file that is on the agent host.

The second field *server-host-name* in *JP1-user-name*:*server-host-name*:*user-list* in the mapping definition file needs to be changed when the manager host name is changed.

To change the information:

1. Execute the `jbsgetumap` command and acquire the text file.
2. Change the applicable server host name to the new server host name.

   You do not need to change the server host name if the old server host name is `*`.
3. After you change the server host name, execute the `jbsmkumap` command and register the new definition.

For details on the commands, see *jbsgetumap* and *jbsmkumap* in *13. Commands*.

Note

If you are using domain names for DNS operation, specify a host name in Fully Qualified Domain Name (FQDN) format in *server-host-name*.

(b) When the agent host name is changed

Changing an agent host name has no effect.

(3) Event service

If you have specified host names in the environment settings files (all in the text format) of the event service, you need to correct them completely. Only the host names set by users need to be corrected. Default names do not need to be corrected. Since the event service does not automatically store default host names, you need not worry about correcting them.

(4) When using JP1/IM - Manager

When you use `Read from Selected Event` for an event search, you need to set `hosts` so the machine that uses JP1/IM - Manager can reference the old host name (for example, to make `ping` *old-host-name* successful). If you do not need this type of operation, you do not need to change the settings regarding the event service.

For JP1/IM - Manager, the system is configured using the configuration definition file. Therefore, each time a host name is changed, the system configuration needs to be redistributed (by executing the `jbsrt_distrib` command). Unless the system configuration is redistributed, JP1 events might not be forwarded correctly. For details on how to redistribute the system configuration, see the manual *Job Management Partner 1/Integrated Management - Manager Administration Guide*.

Note

> For a JP1 event that was issued while an old host name was still in use, JP1/IM - View displays the old host name as the registered host name even after the host name is changed. When you perform a search, the old host name is also used as the registered host name. You cannot use this type of JP1 event to display the monitor screen for JP1/AJS.

(5) When using a cluster system

If you change a logical host name in a cluster system environment, delete the previous logical host name. And then, complete the same setup for the new logical host name.

In Windows:

> For details on deleting a logical host name, see *3.4.6 Deleting logical hosts*. For details on setting up a cluster system, see *3.4.3 Setup*.

In UNIX:

> For details on deleting a logical host name, see *3.5.6 Deleting logical hosts*. For details on setting up a cluster system, see *3.5.3 Setup*.

(6) Hitachi Network Objectplaza Trace Library (HNTRLib2)

It is not necessary to restart Hitachi Network Objectplaza Trace Library (HNTRLib2) after changing the host name. However, if you do not so, the previous logical host name is output to the header of the integrated trace log.

12.2.2 Effects and follow-up tasks when changing IP addresses

This subsection describes the tasks that you need to perform when an IP address is changed. Perform the following procedure when you change only an IP address.

To perform the required task:

1. Stop all the programs that use the event service and then restart the programs.
2. Stop JP1/Base and then restart JP1/Base.

12.2.3 Follow-up tasks when changing the system time

This subsection describes the procedure and precautions for changing the system time while JP1/Base is running.

When you are synchronizing the system clock using a Network Time Protocol (NTP) server or other method in which the system time never becomes a past time, you can do so without stopping JP1/Base. Also, you do not need to follow the procedure below.

(1) Moving the system time backward

Avoid changing the system time to a past date or time.

Event searches with a specified arrival time might operate incorrectly if you move the system time backward to correct a fast system time, for example.

If you intentionally moved the system time forward for testing purposes or some other reason, follow the steps below to change the system time back again. If JP1/AJS has already started, refer to the changing procedure in the manuals *Job Management Partner 1/Automatic Job Management System 2 Planning and Administration Guide*, *Job Management Partner 1/Automatic Job Management System 3 System Design (Configuration) Guide*, *Job Management Partner 1/Automatic Job Management System 3 System Design (Work Tasks) Guide*, and *Job Management Partner 1/ Automatic Job Management System 3 Administration Guide*.

To change the system time back again:

1. Stop JP1/IM - Manager.
2. Stop JP1/Base.
3. Stop all services that use the startup control.
4. Change the system time to the current date and time.
5. Delete the event database by using the `jevdbinit` command.
6. Start JP1/Base.
7. Restart JP1/IM - Manager.

(2) Moving the system time forward to correct a slow system time

You do not need to stop the JP1/Base service to move the system time forward, but you must stop JP1/AJS if it is active. For details on the procedure, see the manuals *Job Management Partner 1/Automatic Job Management System 2 Planning and Administration Guide*, *Job Management Partner 1/Automatic Job Management System 3 System Design (Configuration) Guide*, *Job Management Partner 1/Automatic Job Management System 3 System Design (Work Tasks) Guide*, and *Job Management Partner 1/Automatic Job Management System 3 Administration Guide*.

Chapter
13. Commands

This chapter explains the syntax of JP1/Base commands.

List of commands

List of commands

The commands available in JP1/Base are listed below. In the table, Windows or UNIX support is abbreviated as follows:

Legend:

Yes: Supported

No: Not supported

Superuser means *Administrators* in a Windows system.

Command used for startup control

Functional overview	Command name	Windows	UNIX	Required execution permission
Creates a `JP1SVPRM.DAT` file.	`cpysvprm` (Windows only)	Yes	No	None

Command for checking the network setup

Functional overview	Command name	Windows	UNIX	Required execution permission
Checks network setup.	`jp1ping`	Yes	Yes	None

Commands for starting, stopping, and setting up JP1/Base processes other than the event service

Functional overview	Command name	Windows	UNIX	Required execution permission
Starts HNTRLib2.	`hntr2mon` (UNIX only)	No	Yes	Superuser
Stops HNTRLib2.	`hntr2kill` (UNIX only)	No	Yes	Superuser
Changes HNTRLib2 settings.	`hntr2util` (Windows only)	Yes	No	Superuser
	`hntr2util` (UNIX only)	No	Yes	Superuser
	`hntr2conf`	Yes	Yes	Superuser

Functional overview	Command name	Windows	UNIX	Required execution permission
Displays the HNTRLib2 settings.	`hntr2getconf`	Yes	Yes	None
Outputs the names of program products that use HNTRLib2.	`hntr2getname` (Windows only)	Yes	No	Superuser
Sets up JP1/Base.	`jp1base_setup` (UNIX only)	No	Yes	Superuser
Starts JP1/Base including the event service.	`jbs_start` (UNIX only)	No	Yes	Superuser
Stops JP1/Base including the event service.	`jbs_stop` (UNIX only)	No	Yes	Superuser
Starts JP1/Base processes other than the event service.	`jbs_spmd` (UNIX only)	No	Yes	Superuser
Stops JP1/Base processes other than the event service.	`jbs_spmd_stop`	Yes	Yes	Superuser
Checks the status of JP1/Base processes other than the event service.	`jbs_spmd_status`	Yes	Yes	Superuser
Reloads JP1/Base processes other than the event service.	`jbs_spmd_reload`	Yes	Yes	Superuser
Sets up JP1/Base for use in a cluster system.	`jp1bshasetup` (Windows only)	Yes	No	Superuser
	`jp1base_setup_cluster` (UNIX only)	No	Yes	Superuser
	`jbs_setup_cluster` (Windows only)	Yes	No	Superuser
Starts JP1/Base in a cluster system.	`jbs_start.cluster` (UNIX only)	No	Yes	Superuser
Stops JP1/Base in a cluster system.	`jbs_stop.cluster` (UNIX only)	No	Yes	Superuser
Forcibly terminates all active JP1/Base processes in a cluster system.	`jbs_killall.cluster` (UNIX only)	No	Yes	Superuser
Starts the JP1/Base administrator console.	`jbsadmin` (Windows Vista only)	Yes	No	Superuser

Command for upgrading

Functional overview	Command name	Windows	UNIX	Required execution permission
Migrates the command execution logs of JP1/Base Version 7 or earlier to the file format used in Version 8.	jcocmdconv	Yes	Yes	Superuser

Commands for user management

Functional overview	Command name	Windows	UNIX	Required execution permission
Sets an authentication server.	jbssetusrsrv (UNIX only)	No	Yes	Superuser
	jbssetupsrv (Windows only)	Yes	No	Superuser
Lists authentication servers.	jbslistsrv	Yes	Yes	Superuser
Blocks an authentication server.	jbsblockadesrv	Yes	Yes	Superuser
Unblocks an authentication server.	jbsunblockadesrv	Yes	Yes	Superuser
Registers a JP1 user.	jbsadduser	Yes	Yes	Superuser
Deletes a JP1 user.	jbsrmuser	Yes	Yes	Superuser
Lists registered JP1 users.	jbslistuser	Yes	Yes	Superuser
Changes the password of a registered JP1 user.	jbschgpasswd	Yes	Yes	Superuser
Registers JP1 user operating permissions.	jbssetacl	Yes	Yes	Superuser
Deletes JP1 user operating permissions.	jbsrmacl	Yes	Yes	Superuser
Displays registered JP1 user operating permissions.	jbslistacl	Yes	Yes	Superuser
Creates user mapping definitions and registers the information in the common definitions.	jbsmkumap	Yes	Yes	Superuser
Registers specific mapping information.	jbssetumap	Yes	Yes	Superuser

Functional overview	Command name	Windows	UNIX	Required execution permission
Deletes specific mapping information.	`jbsrmumap`	Yes	Yes	Superuser
Lists registered mapping information.	`jbsgetumap`	Yes	Yes	Superuser
Maintenance program for OS users' password management	`jbspassmgr` (Windows only)	Yes	No	Superuser
Registers an OS user or changes the password of a registered OS user.	`jbsumappass` (Windows only)	Yes	No	Superuser
Deletes an OS user.	`jbsrmumappass` (Windows only)	Yes	No	Superuser
Batch-register password information in the common definitions.	`jbsmkpass` (Windows only)	Yes	No	Superuser
Lists operating permission definitions registered on the authentication server.	`jbsacllint`	Yes	Yes	Superuser
Reloads operating permission definitions to the authentication server.	`jbsaclreload`	Yes	Yes	Superuser
Changes the directory server to be linked.	`jbschgds` (Windows only)	Yes#	No	Superuser
Checks the settings of the directory server to be linked.	`jbschkds` (Windows only)	Yes#	No	Superuser

#: Windows XP Professional, Windows Server 2003, and Windows Server 2008 are supported.

Commands for the event service

Functional overview	Command name	Windows	UNIX	Required execution permission
Reloads the forwarding settings file.	`jevreload`	Yes	Yes	Superuser
Initializes the event database.	`jevdbinit`	Yes	Yes	Superuser
Reorganizes a duplication prevention table	`jevdbmkrep`	Yes	Yes	Superuser
Switches the event database.	`jevdbswitch`	Yes	Yes	Superuser
Outputs the event database to a CSV file.	`jevexport`	Yes	Yes	None

Functional overview	Command name	Windows	UNIX	Required execution permission
Adds a service to the event server.	`jevregsvc` (Windows only)	Yes	No	Superuser
Manually starts the event service.	`jevstart` (UNIX only)	No	Yes	Superuser
Manually stops the event service.	`jevstop` (UNIX only)	No	Yes	Superuser
Checks the status of the event service.	`jevstat`	Yes	Yes	Superuser
Registers a JP1 event on the event server.	`jevsend`	Yes	Yes	None
Registers a JP1 event in the event server and verifies its arrival at the destination server.	`jevsendd`	Yes	Yes	None
Reloads the action definition file for event log trapping.	`jeveltreload` (Windows only)	Yes	No	Superuser
Starts the log-file trap management daemon.	`jevlogdstart` (UNIX only)	No	Yes	Superuser
Stops the log-file trap management daemon.	`jevlogdstop` (UNIX only)	No	Yes	Superuser
Starts the log file trap.	`jevlogstart`	Yes	Yes	Superuser
Stops the log file trap.	`jevlogstop`	Yes	Yes	Superuser
Reloads the action definition file for log file trapping.	`jevlogreload`	Yes	Yes	Superuser
Checks the operating status of the log file trap.	`jevlogstat`	Yes	Yes	Superuser
Collects event service definitions.	`jevdef_get`	Yes	Yes	Superuser
Distributes event service definitions.	`jevdef_distrib`	Yes	Yes	Superuser

Utility commands for operations and maintenance on ISAM (indexed sequential access method) files

Functional overview	Command name	Windows	UNIX	Required execution permission
Adds, deletes or reorganizes keys.	`Jiskeymnt`	Yes	Yes	Superuser

Functional overview	Command name	Windows	UNIX	Required execution permission
Converts a file.	`Jisconv`	Yes	Yes	Superuser
Checks a file.	`Jischk`	Yes	Yes	Superuser
Extracts data from a file.	`Jisext`	Yes	Yes	Superuser
Supports resource settings.	`Jislckreg` (UNIX only)	No	Yes	Superuser
Displays records.	`Jisprt`	Yes	Yes	Superuser
Deletes a resource.	`Jisrsdel` (UNIX only)	No	Yes	Superuser
Displays key definition information.	`Jisinfo`	Yes	Yes	Superuser
Compresses files.	`Jiscond`	Yes	Yes	Superuser
Extends the lock table.	`Jislckext`	Yes	Yes	Superuser
Displays lock table information.	`Jismlcktr` (Windows only)	Yes	No	Superuser
Deletes lock entry information.	`Jislckfree` (Windows only)	Yes	No	Superuser
Checks and releases file or record locks.	`Jislckclear` (Windows only)	Yes	No	Superuser
Copies files.	`Jiscpy`	Yes	Yes	Superuser
Extracts records.	`Jisktod`	Yes	Yes	Superuser

Commands for getting, setting, and deleting operating information and common definition

Functional overview	Command name	Windows	UNIX	Required execution permission
Collects operating information.	`jbsgetopinfo`	Yes	Yes	Superuser
Collects common definition information.	`jbsgetcnf`	Yes	Yes	Superuser
Registers common definition information.	`jbssetcnf`	Yes	Yes	Superuser

Functional overview	Command name	Windows	UNIX	Required execution permission
Deletes common definition information.	`jbsunsetcnf`	Yes	Yes	Superuser
Registers the `jp1hosts` information in the common definition information.	`jbshostsimport`	Yes	Yes	Superuser
Checks the `jp1hosts` information registered in the common definition information.	`jbshostsexport`	Yes	Yes	Superuser

Commands for troubleshooting

Functional overview	Command name	Windows	UNIX	Required execution permission
Collects data if an error occurs.	`jbs_log.bat` (Windows only)	Yes	No	Superuser
	`jbs_log.sh` (UNIX only)	No	Yes	Superuser

Command for the configuration definition

Functional overview	Command name	Windows	UNIX	Required execution permission
Distributes the JP1/IM configuration definition information to lower-level hosts.	`jbsrt_distrib`	Yes	Yes	Superuser
Collects the JP1/IM configuration definition information from the lower-level hosts, and then updates the information.	`jbsrt_sync`	Yes	Yes	Superuser
Deletes the JP1/IM configuration definition information.	`jbsrt_del`	Yes	Yes	Superuser
Displays the JP1/IM configuration definition information.	`jbsrt_get`	Yes	Yes	Superuser

Command for local actions, automated actions, and command execution

Functional overview	Command name	Windows	UNIX	Required execution permission
Outputs a list of the waiting or running local actions.	`jbslistlcact`	Yes	Yes	Superuser
Cancels the waiting or running local actions.	`jbscancellcact`	Yes	Yes	Superuser
Configures the JP1/IM command execution environment.	`jcocmddef`	Yes	Yes	Superuser
Outputs the JP1/IM command execution logs.	`jcocmdlog`	Yes	Yes	None
Deletes the commands executed by JP1/IM - View or automated actions.	`jcocmddel`	Yes	Yes	Superuser
Checks the operating status of the commands executed by JP1/IM - View or automated actions.	`jcocmdshow`	Yes	Yes	Superuser

In the following pages, the commands listed above are explained in alphabetical order.

JP1/Base administrator console (for Windows Vista or Windows Server 2008)

(1) Overview of the JP1/Base administrator console

JP1/Base provides a number of administrator commands that require the administrator privilege to execute the commands.

The JP1/Base administrator console can be used as the command prompt to execute the administrator commands.

If User Account Control (UAC) for Windows is enabled, you must execute the command from the administrator console.

(2) Starting the administrator console

From the Windows **Start** menu, choose **Programs**, **JP1_Base**, and then **Administrator Console**.

(3) Stopping the administrator console

Enter the `exit` command from the command prompt, or click the **Close** button (**X**).

(4) Customizing the behavior

You can customize the configuration to be used when starting the JP1/Base administrator console to set an environment variable or change a current path by editing the profile batch program provided by the JP1/Base administrator console.

The profile batch program is located in *installation-folder*`\conf\jbsadmin\profile.bat`.

Default settings defined in the profile batch program:

```
@echo off

rem #--------------------------------------------------------
rem # In this space you can set the profile information (such as an environment
variable)
rem # for the administrator console of Job Management Partner1/Base.
rem #--------------------------------------------------------

echo Job Management Partner 1/Base - Administrator Console

@echo on
```

For example, to specify `logical` for the environment variable `JP1_HOSTNAME`, enter the following definition in the profile batch program file:

```
@echo off

rem #--------------------------------------------------------
rem # In this space you can set the profile information (such as an environment
variable)
rem # for the administrator console of Job Management Partner1/Base.
rem #--------------------------------------------------------

echo Job Management Partner 1/Base - Administrator Console
set JP1_HOSTNAME=logical

@echo on
```

cpysvprm (Windows only)

Function

The `cpysvprm` command creates a start sequence definition file (`JP1SVPRM.DAT`).

Format

```
cpysvprm [-n file-name]
cpysvprm -d
```

Required execution permission

None. (If User Account Control (UAC) for Windows is enabled, you must execute the command from the administrator console.)

Command directory

installation-folder`\bin\`

Arguments

- `-n` *file-name*

This option copies the specified file to create a `JP1SVPRM.DAT` file in the JP1/Base data folder (*installation-folder*`\conf\boot\`). Specify the file name using its full path. If you omit this option, the system creates a `JP1SVPRM.DAT` file based on the sample `JP1SVPRM.DAT.MODEL` file provided in the JP1/Base data folder.

- `-d`

This option deletes the `JP1SVPRM.DAT` file from the JP1/Base data folder. Note that specifying the `-d` option disables startup control.

Notes

- Be sure to back up the file specified in the `-n` option, or the `JP1SVPRM.DAT.MODEL` file.
- Do not directly edit the `JP1SVPRM.DAT.MODEL` file provided in the JP1/Base data folder (*installation-folder*`\conf\boot\`).

hntr2conf

Function

The `hntr2conf` command changes the size, number, and output path of the integrated trace logs output by the Hitachi Network Objectplaza Trace Library (HNTRLib2).

This command allows you to set the same settings (the size, number of, and output path of the integrated trace logs) as can be set by using the `hntr2util` command, which utilizes a GUI.

Format

```
hntr2conf [-f log-file-name]
          [-b log-file-size]
          [-n number-of-log-files]
          [-s buffer-file-size]
          [-w monitoring-period]
          [-i monitoring-interval]
          [-m number-of-messages]
          [-l command-log-file-name]
          [-h]
```

Required execution permission

In Windows: Administrators (If User Account Control (UAC) for Windows is enabled, you must execute the command from the administrator console.)

In UNIX: Superuser

Command directory

In Windows:

system-drive`\Program Files\Hitachi\HNTRLib2\bin\`

In UNIX:

`/opt/hitachi/HNTRLib2/bin/`

Arguments

- `-f` *log-file-name*

  Specify the output path and name prefix of the integrated trace log file. A file name of the integrated trace log will consist of the specified prefix and `[1-16].log`.

- `-b` *log-file-size*

  Specify the size of the integrated trace logs (8 to 8,192 KB).

- `-n` *number-of-log-files*

  Specify the number of integrated trace logs (1 to 16). The specified number of integrated trace logs are created in the output directory that is specified by using the `-f` option.

- `-s` *buffer-file-size*

  Specify the buffer file size (8 to 2,048 KB). Do not modify the default setting.

- `-w` *monitoring-period*

  Specify the period for monitoring the log file (1 to 300 seconds). Do not modify the default setting.

- `-i` *monitoring-interval*

  Specify the interval for monitoring the log file (1 to 3,600 seconds). Do not modify the default setting.

- `-m` *number-of-messages*

  Specify the maximum number of messages output by the command (0 to 500). Do not modify the default setting.

- `-l` *command-log-file-name*

  If you want to save the command outputs to a log file, specify the destination file name.

- `-h`

  This argument enables you to display online Help.

Notes

- For the appropriate size of the integrated trace logs file, see *Note* for the `hntr2util` command.
- If you modified the settings for the Hitachi Network Objectplaza Trace Library (HNTRLib2), you must restart it. For details on restarting the Hitachi Network Objectplaza Trace Library (HNTRLib2), see *Note* for the `hntr2util` command.

Return values

`0`	Normal end
`1`	Wrong arguments
`2`	The user who executed the command does not have the administrative privilege (in Windows).
`10`	The log output file specified by the `-f` option does not exist.
`11`	The log file size specified by the `-b` option is too small.
`12`	The buffer file size specified by the `-s` option is bigger than the log file size.

13 to 17	Internal error
99	System error

hntr2getconf

Function

The `hntr2getconf` command outputs the settings of the integrated trace logs output by the Hitachi Network Objectplaza Trace Library (HNTRLib2), such as the size, number, and output path of the integrated trace logs.

This command allows you to set the same settings (the size, number of, and output path of the integrated trace logs) as can be set by using the `hntr2util` command, which utilizes a GUI.

Format

```
hntr2getconf [-f]
               [-b]
               [-n]
               [-s]
               [-w]
               [-i]
               [-m]
               [-l command-log-file-name]
               [-h]
```

Required execution permission

In Windows: None.

In UNIX: None.

Command directory

In Windows:

system-drive`\Program Files\Hitachi\HNTRLib2\bin\`

In UNIX:

`/opt/hitachi/HNTRLib2/bin/`

Arguments

- `-f`

  Outputs the output paths and names of the integrated trace logs output by the Hitachi Network Objectplaza Trace Library (HNTRLib2).

- `-b`

  Outputs the size of the integrated trace logs.

- `-n`

  Outputs the number of integrated trace logs.

- `-s`

  Output the buffer file size.

- `-w`

  Outputs the monitoring period.

- `-i`

  Outputs the monitoring interval.

- `-m`

  Outputs the number of messages.

- `-l` *command-log-file-name*

  If you want to save the command output to a log file, specify the destination file name.

- `-h`

  Outputs online Help information.

Return values

`0`	Normal end
`1`	Wrong arguments
`13` to `17`	Internal error
`99`	System error

Example

The following shows an example of output.

When only one option is specified (in Windows):

```
> hntr2getconf.exe -b
8
>
```

When multiple options are specified (in UNIX):

```
$ hntr2getconf -b -n
LogSize=8
LogFNum=4
$
```

If multiple options are specified, the system outputs the settings in the order that the options are specified, using the corresponding key names. The following table shows the correspondence between option names and key names.

Key name	Option name
LogFile	`-f`
LogSize	`-b`
LogFNum	`-n`
MapSize	`-s`
WatchDog	`-w`
IntervalSec	`-i`
MaxMsgNum	`-m`

hntr2getname (Windows only)

Function

The `hntr2getname` command outputs the names of the program products that use the Hitachi Network Objectplaza Trace Library (HNTRLib2) to the standard output.

Format

```
hntr2getname
```

Required execution permission

Administrators. (If User Account Control (UAC) for Windows is enabled, you must execute the command from the administrator console.)

Command directory

system-drive`\Program Files\Hitachi\HNTRLib2\bin\`

Return values

`-1`	Abnormal end
`0` to `126`	Number of the program products that use HNTRLib2
`127`	More than 126 program products use HNTRLib2

hntr2kill (UNIX only)

Function

The `hntr2kill` command terminates the Hitachi Network Objectplaza Trace Library (HNTRLib2).

Format

```
hntr2kill
```

Required execution permission

Superuser

Command directory

```
/opt/hitachi/HNTRLib2/bin/
```

hntr2mon (UNIX only)

Function

The `hntr2mon` command starts the Hitachi Network Objectplaza Trace Library (HNTRLib2).

Format

```
hntr2mon -d &
```

Required execution permission

Superuser

Command directory

```
/opt/hitachi/HNTRLib2/bin/
```

hntr2util (UNIX only)

Function

The hntr2util command changes the size, number, and output path of the integrated trace logs output by the Hitachi Network Objectplaza Trace Library (HNTRLib2).

At command execution, the following menu appears.

```
Hitachi Network Objectplaza Trace Library 2 - Configuration Utility  Rel 1.0

  Select the item you want to change.  (Type 1-5 or e)

    1: Size of a log file.      256 KB
    2: Number of log files.       4
    3: Size of buffer.           64 KB
    4: Watch dog time.           10 Sec
    5: Name of log files.      /var/opt/hitachi/HNTRLib2/spool/hntr2*.log

    e: Exit

  Enter the number>
```

The menu has the following items.

1

Enter the log file size. (8 to 4,096 KB)

2

Enter the number of log files. (1 to 16)

3 and 4

Do not modify.

5

Enter the output path.

Format

```
hntr2util
```

Required execution permission

Superuser

Command directory

```
/opt/hitachi/HNTRLib2/bin/
```

Notes

- The following shows the amount of log data that each program outputs each day. You should consider these values when specifying log file sizes. The value of each calculation formula provides the amount of log data output during normal operation. You should specify a larger size to handle errors.

  Process management

  `3.1` x *number-of-starts-and-stops-per-day* (kilobytes)

  The above formula obtains the amount of log data for a single product. Estimate the amount of log data for each of JP1/Base, JP1/IM, and JP1/AJS.

  Authentication server

  `0.2` x *number-of-logins-from-JP1/AJS - View* `+ 0.2` x *number-of-command-executions* (kilobytes)

  JP1/IM

  `(0.16 +` *automated-action-command-length*`)` x *number-of-times-automated-action-runs-per-day* `+ 0.4` x *number-of-times-automated-action-is-changed-from-JP1/IM - View* `+ 0.16` x *number-of-logins-from-JP1/IM - View-to-JP1/IM - Manager* `+ (0.16 +` *command-length-on-command-execution-screen*`)` x *number-of-command-executions-per-day* (kilobytes)

  JP1/AJS

  number-of-times-startup-conditions-are-satisfied x `0.2` (kilobytes)

- If you modified the settings for the Hitachi Network Objectplaza Trace Library (HNTRLib2), you must restart it according to the following procedure:

  1. Stop the integrated trace collection process by executing the following command:

     ```
     /opt/hitachi/HNTRLib2/bin/hntr2kill
     ```

  2. Start the integrated trace collection process by executing the following command:

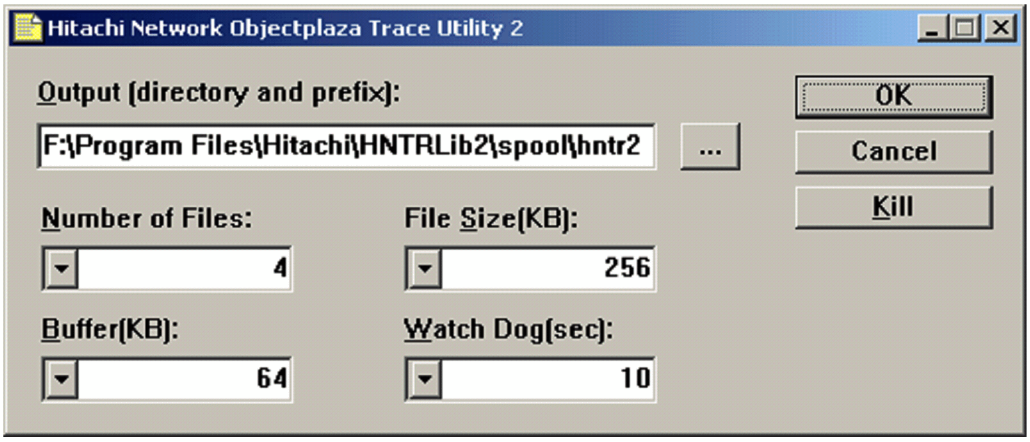
     ```
     /opt/hitachi/HNTRLib2/bin/hntr2mon -d &
     ```

hntr2util (Windows only)

Function

The `hntr2util` command changes the size, number, and output path of the integrated trace logs output by the Hitachi Network Objectplaza Trace Library (HNTRLib2).

At command execution, the following dialog box appears.



Hitachi Network Objectplaza Trace Utility 2

Output (directory and prefix): F:\Program Files\Hitachi\HNTRLib2\spool\hntr2

Number of Files: 4

File Size(KB): 256

Buffer(KB): 64

Watch Dog(sec): 10

In this dialog box, you can set the size, number, and output path of the HNTRLib2 log files. The dialog box has the following components.

Output (directory and prefix)

> Enter the output directory and the file name prefix. The default is *system-drive*`\Program Files\Hitachi\HNTRLib2\spool\hntr2*.log`.

Number of Files

> Enter the number of log files (1 to 16). The default is 4. The specified number of log files are created in the output directory that you specified in **Output**.

File Size (KB)

> Specify the log file size (8 to 4,096 KB). The default is 256 KB.

Buffer (KB) and **Watch Dog (sec)**

> Do not modify.

OK button

> Applies the entered settings and closes the dialog box.

Cancel button

Closes the dialog box without applying the entered settings.

Kill button

Terminates the monitoring process currently executing. You can stop the HNTRLib2 service (service name: **Hitachi Network Objectplaza Trace Monitor 2**) using the **Kill** button, but you should normally do this from the Services dialog box that opens from the Windows Control Panel.

Format

```
hntr2util
```

Required execution permission

Administrators

Command directory

system-drive`\Program Files\Hitachi\HNTRLib2\bin\`

Notes

- The following shows the amount of log data that each program outputs each day. You should consider these values when specifying log file sizes. The value of each calculation formula provides the amount of log data output during normal operation. You should specify a larger size to handle errors.

  Process management

  `3.1 x` *number-of-starts-and-stops-per-day* (kilobytes)

  The above formula obtains the amount of log data for a single product. Estimate the amount of log data for each of JP1/Base, JP1/IM, and JP1/AJS.

  Authentication server

  `0.2 x` *number-of-logins-from-JP1/AJS - View* `+ 0.2 x` *number-of-command-executions* (kilobytes)

  JP1/IM

  `(0.16 +` *automated-action-command-length*`) x` *number-of-times-automated-action-runs-per-day* `+ 0.4 x` *number-of-times-automated-action-is-changed-from-JP1/IM - View* `+ 0.16 x` *number-of-logins-from-JP1/IM - View-to-JP1/IM - Manager* `+ (0.16 +` *command-length-on-command-execution-screen*`) x` *number-of-command-executions-per-day* (kilobytes)

  JP1/AJS

  number-of-times-startup-conditions-are-satisfied `x 0.2` (kilobytes)

- If you modified the settings for the Hitachi Network Objectplaza Trace Library (HNTRLib2), you must restart it. From the Control Panel, open the Services dialog box, and then restart the HNTRLib2 service (service name: **Hitachi Network Objectplaza Trace Monitor 2**).

jbs_killall.cluster (UNIX only)

Function

The `jbs_killall.cluster` command forcibly terminates active JP1/Base processes on a logical host. Using this command, you can terminate:

- The main process
- Configuration management processes
- Processes executed by remote command
- Authentication server processes (if an authentication server is being used)
- Event service

Format

`jbs_killall.cluster [`*logical-host-name*`]`

Required execution permission

Superuser

Command directory

`/etc/opt/jp1base/`

Arguments

- *logical-host-name*

Specify the name of a logical host set in JP1/Base. If you omit this option, the host name set in the environment variable `JP1_HOSTNAME` is assumed. If you omit this option and nothing is set in `JP1_HOSTNAME`, the command ends abnormally.

Notes

- The `jbs_killall.cluster` command determines the host by using the first 15 bytes and forcibly terminates the associated process. You cannot kill a process for a logical host name that exceeds 15 bytes.
- At failover, a process might not stop and failover might not succeed, even if you execute the `jbs_stop.cluster` command. You can use the `jbs_killall.cluster` command to forcibly terminate any processes that did not stop.

Return values

0	Normal end

1 or more	Abnormal end

jbs_log.bat (Windows only)

Function

The `jbs_log.bat` command is a tool for collecting data if an error occurs in JP1/Base. The command collects data such as JP1/Base maintenance information, system information output by the OS, and integrated trace logs.

This tool is a batch file. It cannot be customized.

Executing this tool creates a `jp1default` folder in the specified data folder. If you specify the `-h` option, in addition to the `jp1default` folder, a folder with the name of the logical host is created. Two further folders, `base_1st` and `base_2nd` are created in each of these folders, and the data collected by `jbs_log.bat` is copied under them. If necessary, you can compress the collected data by using an archiving tool. The following table shows the folder organization and the files stored in each directory.

Command folder	Collected data
data-folder`\jp1_default\base_1st\conf\`	Settings and definition files
data-folder`\jp1_default\base_1st\log\`	Log file
data-folder`\jp1_default\base_1st\allusers\jp1_default\JP1Base\log`	Log file
data-folder`\jp1_default\base_1st\allusers\`*logical-host-name*`\JP1Base\log`	Log file
data-folder`\jp1_default\base_1st\sys\`	OS system information
data-folder`\jp1_default\base_1st\sys\tmp\event\`	Event server settings
data-folder`\jp1_default\base_1st\sys\OPI`	Information on the operation of services
data-folder`\jp1_default\base_1st\default\`	Common definition information
data-folder`\jp1_default\base_1st\plugin\conf\`	Plug-in service settings file
data-folder`\jp1_default\base_1st\spool\`	Integrated trace logs
data-folder`\jp1_default\base_2nd\log\Command\`	Command execution log files
data-folder`\jp1_default\base_2nd\sys\`	Event database
data-folder`\`*logical-host-name*`\base_1st\conf\`	Settings and definition files for the logical host (if applicable)

Command folder	Collected data
*data-folder**logical-host-name*\base_1st\log\	Log data for the logical host (if applicable)
*data-folder**logical-host-name*\base_1st\event\	Event server settings for the logical host (if applicable)
*data-folder**logical-host-name*\base_1st\sys\OPI	Information on the operation of services for the logical host
*data-folder**logical-host-name*\base_2nd\sys\	Command execution log files for the logical host (if applicable)
*data-folder**logical-host-name*\base_2nd\event\	Event database for the logical host (if applicable)

For details on the types of data that you can collect with this tool, see *16.3 Data that must be collected when an error occurs*.

Format

```
jbs_log.bat [-h logical-host-name]
            [data-folder]
            [-r]
            [-t]
            [-u]
            [-p]
            [-q]
```

Required execution permission

None. (If User Account Control (UAC) for Windows is enabled, you must execute the command from the administrator console.)

Command directory

installation-folder\tools\

Arguments

■ -h *logical-host-name*

Specify the logical host if you are using JP1/Base in a cluster system. When this option is specified, the command collects information about the physical hosts and logical host. If you omit this option, the command collects information about the physical hosts only. There is no need to specify this argument unless you are running a cluster system.

This command does not use the logical host name set in the environment variable JP1_HOSTNAME. You must therefore specify the logical host name in this option if you are using JP1/Base in a cluster system.

- *data-folder*

  Specify the folder name by full path or by relative path from the current directory in which you are executing the command. If the path contains a space, enclose the space in double quotation marks (`"`).

  If you specify a non-existing folder, a new folder will be created with that name.

  If the specified folder already exists, it will be deleted and recreated. Do not specify the name of a folder containing files you want to keep.

  If you omit this option, the `jp1log` folder under the folder specified in the environment variable `TEMP` is assumed. As the `TEMP` setting differs according to the OS and user, check the setting by clicking **System** in the Control Panel.

- `-r`

  Specify this option if you do not want to collect command execution logs (ISAM).

- `-t`

  Specify this option if you do not want to collect data in the `hosts` and `services` files.

- `-u`

  Specify this option if you do not want to collect crash dumps.

- `-p`

  Specify this option if you do not want to collect data in the event database.

- `-q`

  Specify this option if you do not want the system to wait for your response about whether a data collection process will continue.

  When the `-q` option is omitted, a confirmation message appears and your response is waited.

Return values

`0`	Normal end
`8`	Abnormal end • Invalid argument • Unable to find the folder containing data to be collected.

jbs_log.sh (UNIX only)

Function

The `jbs_log.sh` command is a tool for collecting data if an error occurs in JP1/Base. The command collects data such as JP1/Base maintenance information, system information output by the OS, and integrated trace logs.

This tool is a shell script. It cannot be customized.

When you execute this tool, the specified directories or files are archived using the `tar` command in the root directory, and then compressed using the `compress` command. The compressed files are stored in the *data-directory* specified in the `-f` option, or in the `/tmp/jp1base/` directory if you did not set the `-f` option. The following table shows the directory organization for the compressed files.

Command directory	Collected data
data-directory`/jp1_default_base_1st/var/opt/jp1base/conf/`	Settings and definition files
data-directory`/jp1_default_base_1st/var/opt/jp1base/log/`	Log file
data-directory`/jp1_default_base_1st/var/opt/jp1base/log/sys/`	• OS system information • `jbs_spmd_status` command execution results
data-directory`/jp1_default_base_1st/var/opt/jp1base/sys/tmp/event/`	Event server settings
data-directory`/jp1_default_base_1st/var/opt/jp1base/sys/OPI`	Information on the operation of services
data-directory`/jp1_default_base_1st/var/opt/jp1base/plugin/conf/`	Plug-in service settings file
data-directory`/jp1_default_base_1st/var/opt/hitachi/HNTRLib2/spool/`	Integrated trace logs
data-directory`/jp1_default_base_1st/opt/jp1/hcclibcnf/`	Common definition information
data-directory`/jp1_default_base_2nd/var/opt/jp1base/Command/`	Command execution log files
data-directory`/jp1_default_base_2nd/var/opt/jp1base/sys/event/`	Event database
data-directory`/jp1_default_base_2nd/usr/tmp/jp1_ses/`	Settings file for SES compatibility
data-directory`/jp1_default_base_2nd/usr/lib/jp1_ses/`	
data-directory`/jp1_default_base_2nd/usr/bin/jp1_ses/`	

Command directory	Collected data
data-directory/jp1_default_base_2nd/tmp/	
data-directory/jp1_default_base_2nd/var/opt/jp1_ses/	
data-directory/*logical-host-name*_base_1st/etc/opt/jp1base/log/	Log files for the logical host
data-directory/*logical-host-name*_base_1st/etc/opt/jp1base/conf/	Settings and definition files for the logical host (if applicable)
data-directory/*logical-host-name*_base_1st/*shared-directory*/event/	Event server settings for the logical host (if applicable)
data-directory/*logical-host-name*_base_1st/*shared-directory*/jp1base/sys/OPI	Information on the operation of services for the logical host
data-directory/*logical-host-name*_base_2nd/*shared-directory*/event/	Event database for the logical host (if applicable)
data-directory/*logical-host-name*_base_2nd/var/opt/jp1base/COMMAND/	Command execution log files for the logical host (if applicable)

For details on the types of data that you can collect with this tool, see *16.3 Data that must be collected when an error occurs*.

Format

```
jbs_log.sh [-f data-directory]
              [-k]
              [-p]
              [-r]
              [-t]
              [-u]
              [-q]
              [-h logical-host-name]
              [directory-name-or-file-name...]
```

Required execution permission

Superuser

Command directory

`/opt/jp1base/tools/`

Arguments

- `-f` *data-directory*

  Specify the directory for storing the collected information by absolute path, without any spaces. If you include a space, the character string before the space is taken as the directory name and the characters after the space are regarded as another argument.

  If you omit the `-f` option, JP1/Base creates the following files:

  For a physical host:

  `/tmp/jp1base/jp1_default_base_1st.tar.Z`

  `/tmp/jp1base/jp1_default_base_2nd.tar.Z`

  For a logical host:

  `/tmp/jp1base/`*logical-host-name*`_base_1st.tar.Z`

  `/tmp/jp1base/`*logical-host-name*`_base_2nd.tar.Z`

- `-k`

  Specify this option if you do not want to collect log data related to the pre-Version 6 program JP1/SES.

- `-p`

  Specify this option if you do not want to collect data in the event database.

- `-r`

  Specify this option if you do not want to collect command execution logs (ISAM).

- `-t`

  Specify this option if you do not want to collect data from the `/etc/hosts`, `etc/services`, or `/etc/passwd` files.

- `-u`

  Specify this option if you do not want to collect analysis information from core files.

- `-q`

  Specify this option if you do not want the system to wait for your response about whether a data collection process will continue.

  When the `-q` option is omitted, a confirmation message appears and your response is waited.

- *directory-name-or-file-name*

  Specify this argument to collect one or more specific files or directories using the data collection tool. Specify the name(s) by full path(s). Use spaces to delimit multiple names.

- `-h` *logical-host-name*

  Specify the logical host if you are using JP1/Base in a cluster system. When this option is specified, the command collects information about the physical hosts and logical host. If you omit this option, the command collects information about the physical hosts only. There is no need to specify this argument unless you are running a cluster system.

  This command does not use the logical host name set in the environment variable `JP1_HOSTNAME`. You must therefore specify the logical host name in this option if you are using JP1/Base in a cluster system.

Return values

`0`	Normal end
`8`	• Invalid argument • The specified logical host name does not exist. • The shared directory of the specified logical host is not mounted. • Unable to copy the file because the program has not been installed. • The user replied `NO` when asked whether the device file is ready. • The user replied `NO` when asked whether the file being output might overwrite the existing file. • Unable to read the specified additional file. • The specified additional file does not exist. • Unable to write to the output directory. • Unable to create the output directory.

jbs_setup_cluster (Windows only)

Function

The `jp1base_setup_cluster` command sets the operating environment of a JP1/Base logical host. If you set the operating environment of a JP1/Base in a cluster system, execute this command at the primary node and the secondary node.

At the primary node:

Specify the logical host name and the shared folder name. Specify the other options as required. Since this command attempts to create definition files and log files in the specified shared folder, you must mount a shared disk before executing this command.

At the secondary node:

Specify the logical host name only. The command sets the environment based on the information specified at the primary node. Note that you must copy the common definition information from the primary node to the secondary node before you set the operating environment of the secondary node. For details on copying the common definition information, see the descriptions for the `jbsgetcnf` and `jbssetcnf` commands.

Format

```
jbs_setup_cluster -h logical-host-name
                  [[-d shared-folder[-a authentication-server]] [-v] | -r]
```

Required execution permission

Administrators. (If User Account Control (UAC) for Windows is enabled, you must execute the command from the administrator console.)

Command directory

installation-folder`\bin\`

Arguments

- `-h` *logical-host-name*

Specify the name of the logical host you want to set up or delete. You can enter a character string that is from 1 to 196 bytes to specify the logical host.

- `-d` *shared-folder*

Specify this option only when setting the operating environment of the primary node. Specify the shared folder in which to save information to be carried over at failover. The shared directory to be specified must be in *shared-folder*. The environment settings for operating JP1/Base are saved in the specified shared folder. If you execute this command with this option specified, the command creates the folders shown in the following table and copies the definition files from *installation-folder*`\jp1base\conf` to the appropriate shared folder.

Folder	Files to be contained
shared-folder`\jp1base\conf\`	Definition files
shared-folder`\jp1base\log\`	Log file
shared-folder`\event\`	Event server settings file

■ `-a` *authentication-server*

Specify the host name of the authentication server to which the logical host will connect. If you omit this option, the command assumes the same authentication server as that specified in the operating environment of the physical host.

■ `-v`

Specify this option to view all messages when you set the operating environment of the logical host.

■ `-r`

Specify this option to delete the logical host. You can execute this option on both the primary and secondary server. This procedure deletes the common definition information of the logical host for JP1/Base, JP1/IM, JP1/Power Monitor, and JP1/AJS, and deletes those services. However, shared files and shared directories remain on the shared disk. Delete these files and directories manually.

Notes

- Complete this setup on every node.
- At execution of this command, the TCP/IP communication protocol is changed from socket binding to IP addressing. This change affects settings for the logical hosts to be created and their constituent physical hosts. For details on the socket binding method used for TCP/IP communication, see the documentation for the OS you are using.
- In the `jbs_setup_cluster` command, you cannot specify the communication protocol of the event service. To specify a communication protocol, edit the event server settings file (`conf`).
- Do not execute this command when JP1/Base is active.
- At command execution, the logical host name and *folder-on-shared-disk*`\event` are automatically set to the event server index file (*installation-folder*`\conf\event\index`) for the event service on the local disk.

A logical host name and communication type (`keep-alive`) is also automatically set to the API setting file (*installation-folder*`\conf\event\api`) for the event service on the local disk. The event server settings file (`conf`) and forwarding settings file (`forward`) are created under *folder-on-shared-disk*`\event`.

Return values

`0`	Normal end
`1`	Abnormal end

jbs_spmd (UNIX only)

Function

The `jbs_spmd` command starts JP1/Base processes other than the event service. If a failure occurs in a process other than the event service, there is no need to stop the event service. Stop all the other services by using the `jbs_spmd_stop` command, and then restart them by using the `jbs_spmd` command. For details on stopping JP1/Base processes other than the event service, see the `jbs_spmd_stop` command.

Format

```
jbs_spmd [-h logical-host-name]
         [-HA]
```

Required execution permission

Superuser

Command directory

`/opt/jp1base/bin/`

Arguments

■ `-h` *logical-host-name*

When using JP1/Base in a cluster system, specify the logical host in which services will start. You can enter a character string that is from 1 to 255 bytes to specify the logical host. If you omit this option, the host name set in the environment variable `JP1_HOSTNAME` is assumed. If the environment variable `JP1_HOSTNAME` is not set, the physical host name is assumed.

■ `-HA`

Specify this option to end process management in a cluster system if at least one of the managed processes terminates abnormally.

Notes

- To check whether JP1/Base processes started at execution of this command, execute the `jbs_spmd_status` command.
- You cannot execute the `jbs_spmd` command two or more times concurrently on a single host.
- If you execute the `jbs_spmd` command as a remote shell command, you must terminate the standard input, standard output, and standard error output by assigning `/dev/null` to those beforehand. The remote shell command might not terminate after JP/Base processes started.

Return values

0	Normal end
Other than 0	Abnormal end

jbs_spmd_reload

Function

The `jbs_spmd_reload` command reloads JP1/Base processes other than the event service.

Format

```
jbs_spmd_reload [-h logical-host-name]
                [-t timeout-in-seconds]
```

Required execution permission

In Windows: Administrators (If User Account Control (UAC) for Windows is enabled, you must execute the command from the administrator console.)

In UNIX: Superuser

Command directory

In Windows:

installation-folder`\bin\`

In UNIX:

`/opt/jp1base/bin/`

Arguments

- `-h` *logical-host-name*

When using JP1/Base in a cluster system, specify the logical host in which services will be reloaded. You can enter a character string that is from 1 to 255 bytes to specify the logical host. If you omit this option, the host name set in the environment variable `JP1_HOSTNAME` is assumed. If the environment variable `JP1_HOSTNAME` is not set, the physical host name is assumed.

- `-t` *timeout* (in seconds)

Specify how long the system should wait for the `jbs_spmd_reload` command to complete execution. The specifiable range is 0 to 32,767. If the `jbs_spmd_reload` command does not complete execution within the specified time, execution is assumed to have failed. The default is 60 seconds.

Notes

- It is not possible to reload environment settings for the event service. If you modify the settings, you must restart the event service for the new settings to take effect.

- You cannot execute multiple instances of the `jbs_spmd_reload`, `jbs_spmd_status`, or `jbs_spmd_stop` command at the same time on a single host.
- If the `jbs_spmd_reload` is executed on the authentication server host during users log in from the viewer such as JP1/IM - View, login authentication will be disabled. In this case, reattempt to log in.

Return values

`0`	Normal end
Other than `0`	Abnormal end

jbs_spmd_status

Function

The `jbs_spmd_status` command checks whether JP1/Base processes other than the event service have started or stopped. If the processes have started normally, the `jbs_spmd_status` command returns the following information.

If an authentication server has been set:

```
jbssessionmgr
jbsroute
jcocmd
jbsplugin
jbshcd
jbshchostd
jbssrvmgr
jbslcact
jbscomd
```

If an authentication server has not been set:

```
jbsroute
jcocmd
jbsplugin
jbshcd
jbshchostd
jbssrvmgr
jbslcact
jbscomd
```

For details on the processes managed by JP1/Base, see *B. List of Processes*.

Format

```
jbs_spmd_status [-h logical-host-name]
                    [-t timeout-in-seconds]
```

Required execution permission

In Windows: Administrators (If User Account Control (UAC) for Windows is enabled, you must execute the command from the administrator console.)

In UNIX: Superuser

Command directory

In Windows:

installation-folder`\bin\`

In UNIX:

`/opt/jp1base/bin/`

Arguments

- `-h` *logical-host-name*

When using JP1/Base in a cluster system, specify the logical host where you want to check whether JP1/Base processes have started or stopped. You can enter a character string that is from 1 to 255 bytes to specify the logical host. If you omit this option, the host name set in the environment variable `JP1_HOSTNAME` is assumed. If the environment variable `JP1_HOSTNAME` is not set, the physical host name is assumed.

- `-t` *timeout* (in seconds)

Specify how long the system should wait for the `jbs_spmd_status` command to complete execution. The specifiable range is 0 to 32,767. If the `jbs_spmd_status` command does not complete execution within the specified time, execution is assumed to have failed. The default is 60 seconds.

Note

You cannot execute multiple instances of the `jbs_spmd_status`, `jbs_spmd_reload`, or `jbs_spmd_stop` command at the same time on a single host.

Return values

`0`	All processes are active.
`1`	An error has occurred in, for example, the communication with the process management, or, a shared folder (shared directory) is not mounted while using JP1/Base in a cluster system.
`4`	Some processes are active.
`8`	All of the child processes have stopped.
`12`	The request is being processed or a timeout occurs (retry is acceptable).

jbs_spmd_stop

Function

The `jbs_spmd_stop` command stops JP1/Base processes other than the event service. This command is useful for stopping other processes, but not the event service, if a failure occurs in a process. For details on restarting stopped processes, see the `jbs_spmd` command.

Format

```
jbs_spmd_stop [-h logical-host-name]
                [-kill]
```

Required execution permission

In Windows: Administrators (If User Account Control (UAC) for Windows is enabled, you must execute the command from the administrator console.)

In UNIX: Superuser

Command directory

In Windows:

installation-folder`\bin\`

In UNIX:

`/opt/jp1base/bin/`

Arguments

- `-h` *logical-host-name*

When using JP1/Base in a cluster system, specify the logical host whose processes you want to stop. You can enter a character string that is from 1 to 255 bytes to specify the logical host. If you omit this option, the host name set in the environment variable `JP1_HOSTNAME` is assumed. If the environment variable `JP1_HOSTNAME` is not set, the physical host name is assumed.

- `-kill`

Specify this option to forcibly terminate processes.

Notes

- To check whether JP1/Base processes stopped, execute the `jbs_spmd_status` command.
- This command does not terminate the log-file trap management daemon. To terminate the log-file trap management daemon, first execute the

jbs_spmd_stop command, and then execute the jevlogdstop command.

- You cannot execute multiple instances of the jbs_spmd_stop, jbs_spmd_reload, or jbs_spmd_status command at the same time on a single host.

Return values

0	Normal end
Other than 0	Abnormal end

jbs_start (UNIX only)

Function

The jbs_start command starts JP1/Base (the event service, process management including user management, and the log-file trap management daemon).

To automatically start JP1/Base by executing this command, run the following script after completing JP1/Base installation and setup:

```
cd /etc/opt/jp1base
cp -p jbs_start.model jbs_start
```

Format

```
jbs_start
```

Required execution permission

Superuser

Command directory

```
/etc/opt/jp1base/
```

Notes

- After issuing the startup request to the JP1/Base processes, this command ends with the return value 0. To verify the proper state of the processes, after the jbs_start command has finished, use the jbs_spmd_status command.
- If you execute the jbs_start command as a remote shell command, you must terminate the standard input, standard output, and standard error output by assigning /dev/null to those beforehand. The remote shell command might not terminate after JP/Base processes started.

Return values

0	Normal end
1	More than one argument was specified.

jbs_start.cluster (UNIX only)

Function

In a cluster system, the `jbs_start.cluster` command starts JP1/Base (the event service, process management functions including the user management function, and the log-file trap management daemon). To execute this command, you must first register it in your cluster software.

The following commands are executed within this command:

- `jevstart` *logical-host-name*
- `jbs_spmd -h` *logical-host-name*

Format

`jbs_start.cluster` *logical-host-name*

Required execution permission

Superuser

Command directory

`/etc/opt/jp1base/`

Arguments

■ *logical-host-name*

Specify the logical host for which you want to execute this command.

Notes

- After issuing the startup request to the JP1/Base processes, this command ends with the return value 0. To verify the proper state of the processes, after the `jbs_start.cluster` command has finished, use the `jbs_spmd_status` command.
- If you execute the `jbs_start.cluster` command as a remote shell command, you must terminate the standard input, standard output, and standard error output by assigning `/dev/null` to those beforehand. The remote shell command might not terminate after JP/Base processes started.

Return values

`0`	Normal end
`1`	More than one argument was specified.

jbs_stop (UNIX only)

Function

The `jbs_stop` command stops JP1/Base (the event service and process management including user management).

To automatically stop JP1/Base by executing this command, run the following script after completing JP1/Base installation and setup:

```
cd /etc/opt/jp1base
cp -p jbs_stop.model jbs_stop
```

Format

```
jbs_stop
```

Required execution permission

Superuser

Command directory

```
/etc/opt/jp1base/
```

Notes

- This command does not stop the log-file trap management daemon, which runs on both the logical and physical hosts. You can stop the daemon by executing the `jevlogdstop` command after executing the `jbs_stop` command. However, if the log-file trap management daemon is active on the logical host, executing the `jevlogdstop` command will disable log file trapping on that logical host. Before executing the `jevlogdstop` command, make sure that the log file trapping is not being used on the logical host.
- After issuing the stop request to the JP1/Base processes, this command ends with the return value 0. To check whether the processes have stopped correctly, after the `jbs_stop` command has finished, use the `jbs_spmd_status` command.

Return values

`0`	Normal end
`1`	More than one argument was specified.

jbs_stop.cluster (UNIX only)

Function

The `jbs_stop.cluster` command stops JP1/Base (the event service and process management including user management) in a cluster system. To execute this command, you must first register it in your cluster software.

The following commands are executed within this command:

- `jevstop` *logical-host-name*
- `jbs_spmd_stop -h` *logical-host-name*

Format

`jbs_stop.cluster` *logical-host-name*

Required execution permission

Superuser

Command directory

`/etc/opt/jp1base/`

Arguments

■ *logical-host-name*

When using JP1/Base in a cluster system, specify the logical host for which you want to execute this command.

Notes

- The `jbs_stop.cluster` command does not stop the log-file trap management daemon, which is used on both the logical and physical hosts. You can stop the daemon by executing the `jevlogdstop` command after executing the `jbs_stop.cluster` command. However, if the log-file trap management daemon is active on the physical host, executing the `jevlogdstop` command will disable log file trapping on that physical host. Before executing the `jevlogdstop` command, make sure that the log file trapping is not being used on the physical host.
- After issuing the stop request to the JP1/Base processes, this command ends with the return value 0. To check whether the processes have stopped correctly, after the `jbs_stop.cluster` command has finished, use the `jbs_spmd_status` command.
- In a cluster system that monitors during stop processing, modify the command that terminates JP1/Base (the event service and process management including

user management), as follows:

```
cd /etc/opt/jp1base
cp -p jbs_stop.cluster.retry.model jbs_stop.cluster
```

Return values

0	Normal end
1	More than one argument was specified.

jbsacllint

Function

The `jbsacllint` command sorts definition information about the operating permissions of JP1 users registered on the authentication server, and outputs it to the standard output. The listed definitions are the access permission level (`JP1_AccessLevel`) file and user permission level (`JP1_UserLevel`) file.

Format

`jbsacllint [-h` *logical-host-name*`]`

Required execution permission

In Windows: Administrators (If User Account Control (UAC) for Windows is enabled, you must execute the command from the administrator console.)

In UNIX: Superuser

Command directory

In Windows:

installation-folder`\bin\`

In UNIX:

`/opt/jp1base/bin/`

Arguments

- `-h` *logical-host-name*

When using JP1/Base in a cluster system, specify the logical host for which you want to execute this command. If you omit this option, the host name set in the environment variable `JP1_HOSTNAME` is assumed. If the environment variable `JP1_HOSTNAME` is not set, the physical host name is assumed.

Note

You can use this command on the authentication server to show the definitions.

Return values

`0`	Normal end
`2`	Invalid arguments
`4`	Insufficient system resource such as memory
`32`	An error occurred during initialization of the communication functionality

128	Inconsistency in internal processing (a C++ exception)
255	Other error

jbsaclreload

Function

The `jbsaclreload` command reloads the definition information about the operating permissions of JP1 users to the authentication server. The listed definitions are the access permission level (`JP1_AccessLevel`) file and user permission level (`JP1_UserLevel`) file.

Format

```
jbsaclreload [-h logical-host-name]
             [-s authentication-server-name]
```

Required execution permission

In Windows: Administrators (If User Account Control (UAC) for Windows is enabled, you must execute the command from the administrator console.)

In UNIX: Superuser

Command directory

In Windows:

installation-folder`\bin\`

In UNIX:

`/opt/jp1base/bin/`

Arguments

- `-h` *logical-host-name*

When using JP1/Base in a cluster system, specify the logical host for which you want to execute this command. The command will reload the definitions about the JP1 user operating permissions set on the specified logical host.

- `-s` *authentication-server-name*

Specify the authentication server on which to reload the definitions about JP1 user operating permissions. When you specify this option, the `-h` option is ignored.

Note

The `-s` option takes precedence if you specify both the `-h` and `-s` options. If you omit both options, the host name set in the environment variable `JP1_HOSTNAME` is assumed as the logical host. If you omit both options and nothing is set in `JP1_HOSTNAME`, the definitions set on the physical host are reloaded.

Return values

0	Normal end
2	Invalid arguments
4	Insufficient system resource such as memory
8	The authentication server has not started or is not responding
16	An error occurred in the authentication server side processing
32	An error occurred during initialization of the communication functionality
128	Inconsistency in internal processing (a C++ exception)
255	Other error

jbsadduser

Function

The `jbsadduser` command registers a JP1 user. Use this command when using the local host as the authentication server. This command prompts you to enter a password for the JP1 user you want to register. When you specify the `-p` option, the system registers the specified password without prompting you for the entry of a password. If you specify the `-ds` option, you do not need to enter a password when registering linked users.

The `-ds` option enables you to register linked users without passwords.

Format

```
jbsadduser [-h logical-host-name]
           [-s authentication-server-name]
           [-p password | -ds#]
            JP1-user-name
```

#: The `-ds` option can only be specified in Windows (except Windows Vista).

Required execution permission

In Windows: Administrators (If User Account Control (UAC) for Windows is enabled, you must execute the command from the administrator console.)

In UNIX: Superuser

Command directory

In Windows:

installation-folder`\bin\`

In UNIX:

`/opt/jp1base/bin/`

Arguments

- `-h` *logical-host-name*

When using JP1/Base in a cluster system, specify the logical host for which you want to execute this command. The JP1 user will be registered on the authentication server set for this logical host.

- `-s` *authentication-server-name*

Specify the authentication server on which to register the JP1 user. When you set this option, the `-h` option is ignored.

- `-p` *password*

  Specify the password for the standard user. This specification is case sensitive. You can enter a character string that is from 6 to 32 bytes to specify the password. For the password, you can use ASCII characters excluding tab characters, spaces, and some special characters (`\ " :`). When you specify this option, the system registers the specified password without prompting the entry of a password.

- `-ds`

  This option can only be specified in Windows (except Windows Vista).

  You can register linked users by using this option. When a JP1 user who has been registered as a linked user by using this option, the JP1 user must use a password managed by the directory server.

- *JP1-user-name*

  Specify the user name to be registered as a JP1 user. You can use alphanumeric characters to specify a JP1 user name but the characters must be lower case. You can enter a character string that is from 1 to 31 bytes to specify the logical host. Note that you cannot use tab characters, space, or any of the following characters in the JP1 user name: `* / \ " ' ^ [ ] { } ( ) : ; | = , + ? < >`

Notes

- Type the `-h` option and logical host name, and the `-s` option and authentication server name, before the JP1 user name.
- The `-s` option takes precedence if you specify both the `-h` and `-s` options. If you omit both options, the host name set in the environment variable `JP1_HOSTNAME` is assumed as the logical host. If you omit both options and nothing is set in `JP1_HOSTNAME`, the JP1 user is registered on the authentication server set for the physical host.

Return values

0	Normal end
1	The user has been already registered
2	Invalid arguments
4	Insufficient system resource such as memory
32	Invalid password
128	Inconsistency in internal processing (a C++ exception)
255	Other error

jbsadmin (Windows Vista only)

Function

The `jbsadmin` command starts the JP1/Base administrator console. JP1/Base administrator console provides a number of administrator commands that require the administrator privilege to execute the commands.

Format

```
jbsadmin
```

Required execution permission

Administrators

Command directory

installation-folder`\bin\`

jbsblockadesrv

Function

The `jbsblockadesrv` command blocks access to the specified authentication server.

Format

```
jbsblockadesrv [-h logical-host-name]
                   -s authentication-server-name
```

Required execution permission

In Windows: Administrators (If User Account Control (UAC) for Windows is enabled, you must execute the command from the administrator console.)

In UNIX: Superuser

Command directory

In Windows:

installation-folder`\bin\`

In UNIX:

`/opt/jp1base/bin/`

Arguments

- `-h` *logical-host-name*

When using JP1/Base in a cluster system, specify the logical host for which the destination authentication server is set. If you omit this option, the host name set in the environment variable `JP1_HOSTNAME` is assumed. If the environment variable `JP1_HOSTNAME` is not set, the physical host name is assumed.

- `-s` *authentication-server-name*

Specify the name of the authentication server to be placed in blocked status.

Return values

`0`	The authentication server has been blocked.
`1`	The authentication server is already blocked.
`17`	The authentication server cannot be blocked.
Other than `0`, `1`, or `17`	Abnormal end

Example

Suppose that the primary authentication server is `server1`, and the secondary authentication server is `server2`. When you execute the `jbsblockadesrv` command to block `server2`, the following information appears:

```
jbsblockadesrv -s server2
primary:server1
secondary:server2:blocked
```

jbscancellcact

Function

The `jbscancellcact` command cancels the waiting or running local actions. If the command is canceled while it is being executed, the executed process and its child processes are also canceled.

Format

```
jbscancellcact [-h logical-host-name]
                  action-number
```

Required execution permission

In Windows: Administrators (If User Account Control (UAC) for Windows is enabled, you must execute the command from the administrator console.)

In UNIX: Superuser

Command directory

In Windows:

installation-folder`\bin\`

In UNIX:

`/opt/jp1base/bin/`

Arguments

- `-h` *logical-host-name*

  Specify the logical host if you are using JP1/Base in a cluster system. If you omit this option, the host name set in the environment variable `JP1_HOSTNAME` is assumed. If the environment variable `JP1_HOSTNAME` is not set, the physical host name is assumed.

- *action-number*

  Specify an action number of the local action that you want to cancel. To check an action number, execute the `jbslistlcact` command to display a list of action numbers.

Return values

`0`	Normal end
`1`	The specified action does not exist as a waiting action or running action.
`255`	Other error

jbschgds (Windows only)

Function

The `jbschgds` command temporarily changes the directory server to be linked. This command should be executed on an authentication server where the directory server linkage function has been enabled.

Format

```
jbschgds [-h logical-host-name]
            {-f definition-file | -d}
```

Required execution permission

Administrators. (If User Account Control (UAC) for Windows is enabled, you must execute the command from the administrator console.)

Command directory

installation-folder`\bin\`

Arguments

- `-h` *logical-host-name*

  When using JP1/Base in a cluster system, specify the logical host for which you want to execute this command. If you omit this option, the host name set in the environment variable `JP1_HOSTNAME` is assumed. If the environment variable `JP1_HOSTNAME` is not set, the physical host name is assumed.

- `-f` *definition-file*

  Specify a directory server modification file. You can name the definition file and determine where it is stored at your choice. For details on the directory server modification file, see *Directory server modification file (Windows only)* in *14. Definition Files*.

- `-d`

  Specify this option for canceling the temporary change of the directory server to be linked.

Return values

`0`	Normal end
`2`	Invalid arguments
`4`	Insufficient system resource such as memory

64	No execution permission
128	Inconsistency in internal processing (a C++ exception)
255	Other error

jbschgpasswd

Function

The `jbschgpasswd` command changes the password of a registered JP1 user. This command prompts you to enter the current password and a new password. You can enter a character string that is from 6 to 32 bytes for the password. The new password can be the same as the current one.

Format

```
jbschgpasswd [-h logical-host-name]
             [-s authentication-server-name]
             [-op old-password -np new-password]
             JP1-user-name
```

Required execution permission

In Windows: Administrators (If User Account Control (UAC) for Windows is enabled, you must execute the command from the administrator console.)

In UNIX: Superuser

Command directory

In Windows:

installation-folder`\bin\`

In UNIX:

`/opt/jp1base/bin/`

Arguments

- `-h` *logical-host-name*

When using JP1/Base in a cluster system, specify the logical host for which you want to execute this command. The command changes the password of the JP1 user registered on the authentication server set for this logical host.

- `-s` *authentication-server-name*

Specify the authentication server on which to change the JP1 user's password. When you set this option, the `-h` option is ignored.

- `-op` *old-password*

Specify the old password you want to change. Specify this option together with the `-np` option. When you specify the `-op` and `-np` options, the system registers the password specified with the `-np` option without prompting for the entry of a password.

- `-np` *new-password*

  Specify the new password. Specify this option with the `-op` option.

- *JP1-user-name*

  Specify the JP1 user name whose password you wish to change.

Notes

- Type the `-h` option and logical host name, and the `-s` option and authentication server name, before the JP1 user name.
- The `-s` option takes precedence if you specify both the `-h` and `-s` options. If you omit both options, the host name set in the environment variable `JP1_HOSTNAME` is assumed as the logical host. If you omit both options and nothing is set in `JP1_HOSTNAME`, this command changes the password of the JP1 user registered on the authentication server set for the physical host.

Return values

`0`	Normal end
`1`	The user does not exist, the entered old password is incorrect, or you attempted to change a linked user's password.
`2`	Invalid arguments
`4`	Insufficient system resource such as memory
`8`	The authentication server has not started or is not responding
`16`	An error occurred in the authentication server side processing
`32`	Invalid password
`128`	Inconsistency in internal processing (a C++ exception)
`255`	Other error

jbschkds (Windows only)

Function

The `jbschkds` command displays the settings of the directory server linkage, the result on connecting to the directory server, and the result of user authentication, while the directory server linkage is enabled. The following are displayed:

- Whether the directory server linkage function is enabled
- Directory server name
- Port number
- Whether SSL is to be used
- Distinguished name
- Result on connecting to the directory server
- Result of user authentication

This command should be executed on an authentication server where the directory server linkage function has been enabled.

Format

```
jbschkds [-h logical-host-name]
         [-u JP1-user-name -p password]
```

Required execution permission

Administrators. (If User Account Control (UAC) for Windows is enabled, you must execute the command from the administrator console.)

Command directory

installation-folder`\bin\`

Arguments

- `-h` *logical-host-name*

When using JP1/Base in a cluster system, specify the logical host for which you want to execute this command. If you omit this option, the host name set in the environment variable `JP1_HOSTNAME` is assumed. If the environment variable `JP1_HOSTNAME` is not set, the physical host name is assumed.

- `-u` *JP1-user-name*

Specify a JP1 user name that is authenticated on the directory server.

- `-p` *password*

  Specify the password for the user specified by the `-u` option.

Return values

`0`	Normal end
`2`	Invalid arguments
`4`	Insufficient system resource such as memory
`64`	No execution permission
`128`	Inconsistency in internal processing (a C++ exception)
`255`	Other error

Example

The following shows examples of output.

When the directory server linkage function is disabled

```
>jbschkds
The directory server linkage functionality is disabled.
```

When the directory server linkage function is enabled and the user successfully authenticated

```
>jbschkds -u jp1user -p password
Directory server settings:
Directory server name:host-A
Port number: 636
SSL Use
Distinguished naem=jp1user,CN=Users,DC=netmanage,DC=local
The directory server is now connected.
User authentication succeeded.
```

When the directory server linkage function is enabled and the directory server connection failed.

```
>jbschkds
Directory server settings:
Directory server name:host-A
Port number: 636
SSL Use
KAVA5810-E A connection to the directory server could not be
established.
Server Down
```

jbsgetcnf

Function

The `jbsgetcnf` command collects all common definition information. Also, this command outputs the common definition information to the standard output.

Format

`jbsgetcnf [-h` *logical-host-name*`] >` *backup-file-name*

Required execution permission

In Windows: Administrators (If User Account Control (UAC) for Windows is enabled, you must execute the command from the administrator console.)

In UNIX: Superuser

Command directory

In Windows:

installation-folder`\bin\`

In UNIX:

`/opt/jp1base/bin/`

Arguments

- `-h` *logical-host-name*

When using JP1/Base in a cluster system, specify the logical host from which you want to collect the definition information. If you omit this option, the physical host name is assumed.

This command does not use the logical host name set in the environment variable `JP1_HOSTNAME`. For this reason, you must specify the logical host in this option when using JP1/Base in a cluster system. If you specify an invalid argument other than this option, all the arguments from the invalid argument are ignored.

- *backup-file*

Specify the name of the backup file in which to save the common definition information.

Return values

`0`	Normal end
`-1`	Abnormal end

jbsgetopinfo

Function

The `jbsgetopinfo` command collects operating information, converts it to the definition file format, and outputs to the standard output. Definitions for forwarding events, log file traps, and event log traps can be collected as operating information.

Format

```
jbsgetopinfo [-h logical-host-name]
             [-o operating-information-name, ...]
             [-i ID-number | -a monitoring-target-name]
```

Required execution permission

In Windows: Administrators (If User Account Control (UAC) for Windows is enabled, you must execute the command from the administrator console.)

In UNIX: Superuser

Command directory

In Windows:

installation-folder`\bin\`

In UNIX:

`/opt/jp1base/bin/`

Arguments

- `-h` *logical-host-name*

  Specify the name of the logical host from which you want to collect operating information. If you omit this option, the host name set in the environment variable `JP1_HOSTNAME` is assumed. If the environment variable `JP1_HOSTNAME` is not set, the physical host name is assumed.

- `-o` *operating-information-name*`, ...`

  Specify the name of the operating information you want to collect. If you omit this option, the system assumes that all of the operating information names are specified. When multiple operating information names are specified, separate the names with commas.

  You can specify any of the following operating information names.

  - `forward`

    Outputs definitions in the forwarding settings file in use. For details on the forwarding settings file, see *Forwarding settings file* in *14. Definition Files*.

- `logtrap`

  Outputs definitions in the action definition file for log file trapping in use. If you want to collect operating information from the logical host, operating information of the physical host are actually collected. For details about the format of the action definition file for log file trapping, see *Action definition file for log file trapping* in *14. Definition Files*.

- `evttrap`

  Outputs definitions in the action definition file for event log trapping in use. If you want to collect operating information from the logical host, operating information of the physical host are actually collected. `evttrap` is only for Windows. For details about the format of the action definition file for event log trapping, see *Action definition file for event log trapping (Windows only)* in *14. Definition Files*.

■ `-i` *ID-number* `|-a` *monitoring-target-name*

This option is valid only when `logtrap` is specified as an operating information name. For *ID-number*, specify the ID number of the log file trap that you want to collect operating information. For *monitoring-target-name*, specify a monitoring target name of the log file trap that you want to collect operating information. Specify either *ID-number* or *monitoring-target-name*. If `logtrap` is specified as an operating information name and this option is omitted, definitions of all the active log file traps are collected.

Notes

- If definitions corresponding to the specified operating information name do not exist, it causes an error. If multiple operating information names are specified, only existing definitions are output.
- If a log file trap corresponding to the specified ID number or monitoring target name does not exist, no definition is output.

Return values

`0`	Normal end
`1`	Invalid argument
`2`	No operating information
`248`	The operating information file is corrupted.
`249`	The specified logical host name does not exist.
`250`	The reloaded settings have not been reflected.

251	Other user is now accessing.
252	No execution permission
253	UAC error
254	Insufficient memory
255	Other error

jbsgetumap

Function

The `jbsgetumap` command displays the user mapping relationships that have already been registered.

This command imports the registered user mapping relationships, exports them into the mapping definition file (`jp1BsUmap.conf`) registered by the `jbsmkumap` command, and then outputs the file to the standard output.

Format

`jbsgetumap [-h` *logical-host-name*`]`

Required execution permission

In Windows: Administrators (If User Account Control (UAC) for Windows is enabled, you must execute the command from the administrator console.)

In UNIX: Superuser

Command directory

In Windows:

installation-folder`\bin\`

In UNIX:

`/opt/jp1base/bin/`

Arguments

■ `-h` *logical-host-name*

When using JP1/Base in a cluster system, specify the logical host whose mapping relationships you want to display. If you omit this option, the host name set in the environment variable `JP1_HOSTNAME` is assumed. If the environment variable `JP1_HOSTNAME` is not set, the physical host name is assumed.

Return values

`1`	Normal end
`0`	Abnormal end

jbshostsexport

Function

The `jbshostsexport` command collects `jp1hosts` information registered in the common definition information, and then outputs it to the standard output.

Format

`jbshostsexport [-h` *logical-host-name*`] >` *jp1hosts-definition-file-name*

Required execution permission

In Windows: Administrators (If User Account Control (UAC) for Windows is enabled, you must execute the command from the administrator console.)

In UNIX: Superuser

Command directory

In Windows:

installation-folder`\bin\`

In UNIX:

`/opt/jp1base/bin/`

Arguments

- `-h` *logical-host-name*

When using JP1/Base in a cluster system, specify the logical host whose `jp1hosts` information you want to collect. If you omit this option, the host name set in the environment variable `JP1_HOSTNAME` is assumed. If the environment variable `JP1_HOSTNAME` is not set, the physical host name is assumed.

- *jp1hosts-definition-file-name*

Specify the name of the file in which to collect the `jp1hosts` data.

Return values

`0`	Normal end
`1`	Message processing error
`2`	Command argument error
`3`	Permission check error
`4`	Common definition error

jbshostsimport

Function

The `jbshostsimport` command registers the `jp1hosts` information into the common definition information. The order of the hosts in the `jp1hosts` data registered in the common definition information is not fixed.

Format

```
jbshostsimport { {-o|-r} jp1hosts-definition-file-name | -d }
                           [-h logical-host-name]
```

Required execution permission

In Windows: Administrators (If User Account Control (UAC) for Windows is enabled, you must execute the command from the administrator console.)

In UNIX: Superuser

Command directory

In Windows:

installation-folder`\bin\`

In UNIX:

`/opt/jp1base/bin/`

Arguments

- `{-o|-r}` *jp1hosts-definition-file-name*

  Specify the file name that defines the `jp1hosts` data to be registered in the common definition information. If you specify the `-o` option, the existing `jp1hosts` data registered in the common definition information is not deleted, and the newer `jp1hosts` data is added (the existing host that is the same as the newer one is overwritten). If you specify the `-r` option, all of the existing `jp1hosts` data registered in the common definition information are deleted, and the newer `jp1hosts` data is registered. For details about the format of `jp1hosts` definition file, see *jp1hosts definition file* in *14. Definition Files*.

- `-d`

  Specify this option when you need to delete the `jp1hosts` data registered in the common definition information.

- `-h` *logical-host-name*

  When using JP1/Base in a cluster system, specify the logical host whose `jp1hosts` data you want to register or delete. If you omit this option, the host name set in the environment variable `JP1_HOSTNAME` is assumed. If the environment variable `JP1_HOSTNAME` is not set, the physical host name is assumed.

Note

Do not use the following commands when JP1/Base is active.

Return values

0	Normal end
1	Message processing error
2	Command argument error
3	Permission check error
4	Common definition error
5	Syntax error
6	File I/O error

jbslistacl

Function

The `jbslistacl` command lists the operating permissions assigned to the registered JP1 users.

Format

```
jbslistacl [-h logical-host-name]
           [-s authentication-server-name]
```

Required execution permission

In Windows: Administrators (If User Account Control (UAC) for Windows is enabled, you must execute the command from the administrator console.)

In UNIX: Superuser

Command directory

In Windows:

installation-folder`\bin\`

In UNIX:

`/opt/jp1base/bin/`

Arguments

- `-h` *logical-host-name*

  When using JP1/Base in a cluster system, specify the logical host for which you want to execute this command. The command lists the operating permissions assigned to the JP1 users registered on the authentication servers set for this logical host.

- `-s` *authentication-server-name*

  Specify an authentication server to list the operating permissions assigned to the JP1 users registered on that authentication server. When you set this option, the `-h` option is ignored.

Note

The `-s` option takes precedence if you specify both the `-h` and `-s` options. If you omit both options, the host name set in the environment variable `JP1_HOSTNAME` is assumed as the logical host. If you omit both options and nothing is set in `JP1_HOSTNAME`, the command lists the JP1 users registered on the authentication server(s) set for the physical host.

Return values

0	Normal end
1	The user is not registered in the authentication server.
2	Invalid arguments
4	Insufficient system resource such as memory
8	The authentication server has not started or is not responding
16	An error occurred in processing of the authentication server.
32	An error occurred during initialization of the communication functionality
128	Inconsistency in internal processing (a C++ exception)
255	Other error

jbslistlcact

Function

The `jbslistlcact` command lists the waiting or running local actions.

Format

`jbslistlcact [-h` *logical-host-name*`]`

Required execution permission

In Windows: Administrators (If User Account Control (UAC) for Windows is enabled, you must execute the command from the administrator console.)

In UNIX: Superuser

Command directory

In Windows:

installation-folder`\bin\`

In UNIX:

`/opt/jp1base/bin/`

Arguments

- `-h` *logical-host-name*

Specify the logical host if you are using JP1/Base in a cluster system. If you omit this option, the host name set in the environment variable `JP1_HOSTNAME` is assumed. If the environment variable `JP1_HOSTNAME` is not set, the physical host name is assumed.

Return values

`0`	Normal end
`1`	No waiting or running local action.
`255`	Other error

Output example

The following shows an example output by executing the `jbslistlcact` command:

```
act-No      act-Name      Status      Command
1122        JOB10         running      abc.exe
1334        JOB22         waiting      xyz.bat
```

`act-No` is an action number, `act-Name` is an action name, `Status` is an action execution status, and `Command` is a first string of a command. If an attribute variable name is specified in a command, the variable will be expanded.

jbslistsrv

Function

The `jbslistsrv` command lists the target authentication server names set in the common definition information on the screen.

Format

`jbslistsrv [-h` *logical-host-name*`]`

Required execution permission

In Windows: Administrators (If User Account Control (UAC) for Windows is enabled, you must execute the command from the administrator console.)

In UNIX: Superuser

Command directory

In Windows:

installation-folder`\bin\`

In UNIX:

`/opt/jp1base/bin/`

Arguments

- `-h` *logical-host-name*

When using JP1/Base in a cluster system, specify the logical host for which the destination authentication server is set. If you omit this option, the host name set in the environment variable `JP1_HOSTNAME` is assumed. If the environment variable `JP1_HOSTNAME` is not set, the physical host name is assumed.

Return values

`0`	Normal end
Other than `0`	Abnormal end

Example

The following shows some examples of use.

Example 1

Suppose that the primary authentication server is `server1`, and the secondary authentication server is `server2`. The following information appears when you execute the `jbslistsrv` command:

```
jbslistsrv
primary:server1
secondary:server2
```

Example 2

Suppose that the primary authentication server is `server1`, and the secondary authentication server is `server2`. If `server1` is in blocked status, the following information appears when you execute the `jbslistsrv` command:

```
jbslistsrv
primary:server1:blocked
secondary:server2
```

Example 3

If only one authentication server is set (authentication server name:`server1`), the following information appears when you execute the `jbslistsrv` command:

```
jbslistsrv
primary:server1
```

jbslistuser

Function

The `jbslistuser` command lists the registered JP1 users.

Format

```
jbslistuser [-h logical-host-name]
            [-s authentication-server-name]
            [-ld]
            [-ds#]
```

#: The `-ds` option can only be specified in Windows (except Windows Vista).

Required execution permission

In Windows: Administrators (If User Account Control (UAC) for Windows is enabled, you must execute the command from the administrator console.)

In UNIX: Superuser

Command directory

In Windows:

installation-folder`\bin\`

In UNIX:

`/opt/jp1base/bin/`

Arguments

- `-h` *logical-host-name*

When using JP1/Base in a cluster system, specify the logical host for which you want to execute this command. The command lists the JP1 users registered on the authentication servers set for this logical host.

- `-s` *authentication-server-name*

Specify an authentication server to list the JP1 users registered on that authentication server. When you set this option, the `-h` option is ignored.

- `-ld`

This option enables you to output the date and time at which user data was last modified for each user (`yyyy/mm/dd HH:MM:SS` format). The last modified date and time is updated when a JP1 user was registered or a password was changed. Note that the last modified date and time for a JP1 user, who was registered before upgrading to JP1/Base Version 8, who was initialized when installing JP1/Base for the first time, or who has been set as a linkage user, is displayed by using hyphens (`----/--/-- --:--:--`). After a password is changed in the JP1/Base Environment Settings dialog box or by using the password change command (`jbschgpasswd`), the last modified data and time is displayed.

If you specify the `-ds` option, this option is ignored.

- `-ds`

  This option can only be specified in Windows (except Windows Vista).

  When this option is specified, only the linked users are displayed.

Notes

- The `-s` option takes precedence if you specify both the `-h` and `-s` options. If you omit both options, the host name set in the environment variable `JP1_HOSTNAME` is assumed as the logical host. If you omit both options and nothing is set in `JP1_HOSTNAME`, the command lists the JP1 users registered on the authentication server(s) set for the physical host.
- The `-ds` option takes precedence if both the `-ld` and the `-ds` options are specified.

Return values

0	Normal end
1	The user is not registered in the authentication server.
2	Invalid arguments
4	Insufficient system resource such as memory
8	The authentication server has not started or is not responding
16	An error occurred in the authentication server side processing
128	Inconsistency in internal processing (a C++ exception)
255	Other error

Example

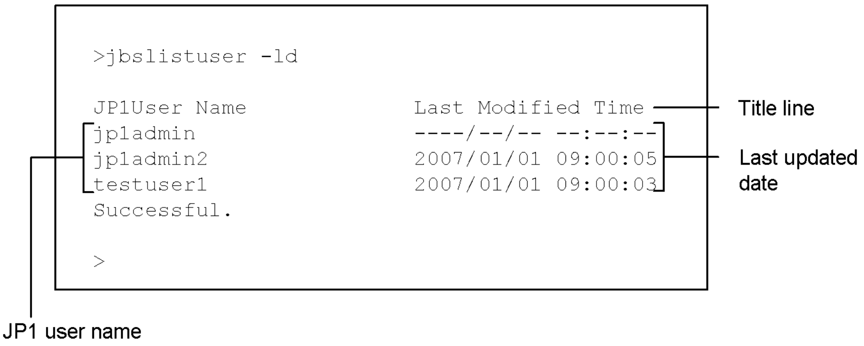
The following shows examples of output where the standard users `jp1admin`, `jp1admin2` and the linked user `testuser1` have been registered on the authentication server:

When no option is specified:

```
>jbslistuser
jp1user account[0]:jp1admin
jp1user account[1]:jp1admin2
```

```
jp1user account[2]:testuser1
Successful.
```

When the `-ld` option is specified:



```
>jbslistuser -ld

JP1User Name             Last Modified Time
jp1admin                 ----/--/-- --:--:--
jp1admin2                2007/01/01 09:00:05
testuser1                2007/01/01 09:00:03
Successful.

>
```

When the `-ds` option is specified:

```
>jbslistuser -ds
jp1user account[0]:testuser1
Successful.
```

The following shows an example of output where the standard users `jp1admin` and `jp1admin2` and no linked users have been registered on the authentication server:

When the `-ds` option is specified:

```
>jbslistuser -ds
No jp1user account.
Failed.
```

jbsmkpass (Windows only)

Function

The `jbsmkpass` command batch-registers password management information. Executing this command deletes all the password information registered in the common definition information, and batch-registers the password information set in a password definition file.

Format

```
jbsmkpass [-h logical-host-name]
               -f password-definition-file
```

Required execution permission

Administrators. (If User Account Control (UAC) for Windows is enabled, you must execute the command from the administrator console.)

Command directory

installation-folder`\bin\`

Arguments

- `-h` *logical-host-name*

  When using JP1/Base in a cluster system, specify the logical host for which you want to register the password management information. If you omit this option, the host name set in the environment variable `JP1_HOSTNAME` is assumed. If the environment variable `JP1_HOSTNAME` is not set, the physical host name is assumed.

- `-f` *password-definition-file*

  Specify the password definition file to import. The system performs a syntax check on the specified file and returns an error if any formatting mistakes are found. If the password information is correct, the file contents are batch-registered in the common definition information. For details on the format of the password definition file, see *Password definition file (Windows only)* in *14. Definition Files*.

Notes

- At command execution, all the password management information registered in the common definition information is deleted, and the password information written in the password definition file is batch-registered in its place. If you want to keep any of the previous password information, include that information in the password definition file.
- In Windows, you need to grant specific Windows user permissions to the OS user who is to execute this command, and to the OS user specified in the user mapping,

respectively. For details, see *6.1.5 Before setting user mapping*.

Return values

1	Normal end
0	Abnormal end

jbsmkumap

Function

The `jbsmkumap` command imports the user mapping definition file (`jp1BsUmap.conf`) and registers the contents in the common definition information. Executing this command deletes all the mapping information in the common definition information, and replaces it with the information set in the user mapping definition file (`jp1BsUmap.conf`). If the format of the user mapping definition file (`jp1BsUmap.conf`) is incorrect, the command returns an error.

Format

```
jbsmkumap [-h logical-host-name]
          [-f user-mapping-definition-file-name]
```

Required execution permission

In Windows: Administrators (If User Account Control (UAC) for Windows is enabled, you must execute the command from the administrator console.)

In UNIX: Superuser

Command directory

In Windows:

installation-folder`\bin\`

In UNIX:

`/opt/jp1base/bin/`

Arguments

- `-h` *logical-host-name*

When using JP1/Base in a cluster system, specify the logical host for which you want to register the user mapping information. If you omit this option, the host name set in the environment variable `JP1_HOSTNAME` is assumed. If the environment variable `JP1_HOSTNAME` is not set, the physical host name is assumed.

- `-f` *user-mapping-definition-file-name*

Specify the name of the definition file containing the mapping information. If you omit this option, information is imported from the default user mapping definition file (`jp1BsUmap.conf`). For details on the format of the user mapping definition file, see *User mapping definition file* in *14. Definition Files*.

Notes

- At command execution, all the mapping information in the common definition information is deleted, and the information written in the mapping definition file is registered in its place. If you want to keep any of the previous mapping information, include that information in the mapping definition file.
- To check the settings done by this command, use the `jbsgetumap` command.

Return values

`1`	Normal end
`0`	Abnormal end

jbspassmgr (Windows only)

Function

The `jbspassmgr` command displays the Password Manager dialog box. The user can perform the following operations in the Password Manager dialog box:

- Register a new user.
- Change a password.
- Delete a registered user.

The users registered or deleted in the Password Manager dialog box are users registered in the OS.

Format

```
jbspassmgr
```

Required execution permission

Administrators

Command directory

installation-folder`\bin\`

Note

In Windows, you need to grant specific Windows user permissions to the OS user who is to execute this command, and to the OS user specified in the user mapping, respectively. For details, see *6.1.5 Before setting user mapping*.

jbsrmacl

Function

The `jbsrmacl` command deletes all the operating permissions assigned to a specified JP1 user.

Format

```
jbsrmacl [-h logical-host-name]
         [-s authentication-server-name]
         -u JP1-user-name
         [-i]
```

Required execution permission

In Windows: Administrators (If User Account Control (UAC) for Windows is enabled, you must execute the command from the administrator console.)

In UNIX: Superuser

Command directory

In Windows:

installation-folder`\bin\`

In UNIX:

`/opt/jp1base/bin/`

Arguments

- `-h` *logical-host-name*

When using JP1/Base in a cluster system, specify the logical host for which you want to delete the operating permissions of the JP1 user. If you omit this option, the host name set in the environment variable `JP1_HOSTNAME` is assumed. If the environment variable `JP1_HOSTNAME` is not set, the physical host name is assumed.

- `-s` *authentication-server-name*

Specify the name of the authentication server from which you want to delete the operating permissions. When you set this option, the `-h` option is ignored.

- `-u` *JP1-user-name*

Specify the JP1 user name for which you want to delete operating permissions.

- `-i`

When you specify this option, a confirmation message appears before the operating permissions for the specified JP1 user are deleted. The deletion processing is executed only if you type `y` or `Y` in response to the message.

Note

The `-s` option takes precedence if you specify both the `-h` and `-s` options. If you omit both options, the host name set in the environment variable `JP1_HOSTNAME` is assumed as the logical host. If you omit both options and nothing is set in `JP1_HOSTNAME`, the operating permissions are registered for the physical host.

Return values

`0`	Normal end
`1`	The user is not registered in the authentication server.
`2`	Invalid arguments
`4`	Insufficient system resource such as memory
`8`	The authentication server has not started or is not responding
`16`	An error occurred in processing of the authentication server.
`32`	An error occurred during initialization of the communication functionality
`128`	Inconsistency in internal processing (a C++ exception)
`255`	Other error

jbsrmumap

Function

The `jbsrmumap` command deletes specific user mapping information from common definitions.

Format

```
jbsrmumap [-h logical-host-name]
             {-u JP1-user-name | -ua}
             [-sh server-host-name | -sha]
             [-i]
```

Required execution permission

In Windows: Administrators (If User Account Control (UAC) for Windows is enabled, you must execute the command from the administrator console.)

In UNIX: Superuser

Command directory

In Windows:

installation-folder`\bin\`

In UNIX:

`/opt/jp1base/bin/`

Arguments

- `-h` *logical-host-name*

When using JP1/Base in a cluster system, specify the logical host for which you want to delete the user mapping information. If you omit this option, the host name set in the environment variable `JP1_HOSTNAME` is assumed. If the environment variable `JP1_HOSTNAME` is not set, the physical host name is assumed.

- `-u` *JP1-user-name*

Specify the JP1 user name for which you want to delete mapping information.

- `-ua`

Specify this option to delete mapping information for which an asterisk (*) is specified for the JP1 user name.

- `-sh` *server-host-name*

Specify the server host name defined for the JP1 user specified in the `-u` option. If you omit this option, all mapping information for the JP1 user specified in the `-u` option will be deleted. You can only specify this option when the `-sha` option is not specified.

- `-sha`

  This option causes the system to delete mapping information for which an asterisk (*) is specified for the server host name for the JP1 user name specified in the `-u` option. You can only specify this option when the `-sh` option is not specified.

- `-i`

  When you specify this option, a confirmation message appears before the user mapping information is deleted. The deletion processing is executed only if you type `y` or `Y` in response to the message.

Return values

`0`	Normal end
`1`	Invalid arguments
`2`	The user executing the command does not have an appropriate privilege.
`5`	An error occurred during access to the common definitions.
`6`	Insufficient system resource such as memory
`10`	An error occurred during locking of the common definitions.
`255`	Other error

jbsrmumappass (Windows only)

Function

The `jbsrmumappass` command deletes an OS user registered in the JP1/Base password management information.

Format

```
jbsrmumappass [-h logical-host-name]
              -u OS-user-name
```

Required execution permission

Administrators. (If User Account Control (UAC) for Windows is enabled, you must execute the command from the administrator console.)

Command directory

installation-folder`\bin\`

Arguments

- `-h` *logical-host-name*

  When using JP1/Base in a cluster system, specify the logical host for which you want to delete the OS user. If you omit this option, the host name set in the environment variable `JP1_HOSTNAME` is assumed. If the environment variable `JP1_HOSTNAME` is not set, the physical host name is assumed.

- `-u` *OS-user-name*

  Specify the OS user name to be deleted from the password management information.

Return values

`0`	Normal end
Other than `0`	Abnormal end

jbsrmuser

Function

The `jbsrmuser` command deletes a JP1 user.

Format

```
jbsrmuser [-i]
           [-h logical-host-name]
           [-s authentication-server-name]
           JP1-user-name
```

Required execution permission

In Windows: Administrators (If User Account Control (UAC) for Windows is enabled, you must execute the command from the administrator console.)

In UNIX: Superuser

Command directory

In Windows:

installation-folder`\bin\`

In UNIX:

`/opt/jp1base/bin/`

Arguments

- `-i`

  When you specify this option, a confirmation message asks you to confirm that you want to delete the specified JP1 user name. The deletion processing is executed only if you type `y` or `Y` in response to the message.

- `-h` *logical-host-name*

  When using JP1/Base in a cluster system, specify the logical host for which you want to execute this command. The command deletes the JP1 user registered on the authentication server(s) set for this logical host.

- `-s` *authentication-server-name*

  Specify the authentication server from which to delete the JP1 user. When you set this option, the `-h` option is ignored.

- *JP1-user-name*

  Specify the JP1 user name to be deleted.

Notes

- Type the -h option and logical host name, and the -s option and authentication server name, before the JP1 user name.
- The -s option takes precedence if you specify both the -h and -s options. If you omit both options, the host name set in the environment variable JP1_HOSTNAME is assumed as the logical host. If you omit both options and nothing is set in JP1_HOSTNAME, the JP1 user is deleted from the authentication server(s) set for the physical host.

Return values

0	Normal end
1	The user has been deleted already
2	Invalid arguments
4	Insufficient system resource such as memory
8	The authentication server has not started or is not responding
16	An error occurred in the authentication server side processing
32	An error occurred during initialization of the communication functionality
128	Inconsistency in internal processing (a C++ exception)
255	Other error

jbsrt_del

Function

The `jbsrt_del` command deletes the configuration definition information of the host which you execute this command.

Format

```
jbsrt_del [-h logical-host-name]
```

Required execution permission

In Windows: Administrators (If User Account Control (UAC) for Windows is enabled, you must execute the command from the administrator console.)

In UNIX: Superuser

Command directory

In Windows:
installation-folder`\bin\`

In UNIX:
`/opt/jp1base/bin/`

Arguments

- `-h` *logical-host-name*

When using JP1/Base in a cluster system, specify the logical host for which you will execute the command. If you omit this option, the host name set in the environment variable `JP1_HOSTNAME` is assumed. If the environment variable `JP1_HOSTNAME` is not set, the physical host name is assumed. There is no need to specify this argument unless you are running a cluster system.

Return values

0	Normal end
1	Abnormal end

jbsrt_distrib

Function

The `jbsrt_distrib` command is executed on a manager host (i.e. host on which JP1/IM - Manager is installed).

This command distributes information defined in the configuration definition file from the host on which the command is executed to lower-level hosts, and then the definitions are enabled.

If the configuration definition information has already been set, the existing configuration definition is deleted, and then the new configuration definition is distributed.

Before executing this command, JP1/Base must have started on the target lower-level hosts to which the configuration definition is distributed. If JP1/Base has not started yet on a target host, the configuration definition will not be distributed to the host. If this happens, a message is displayed during command execution, notifying you that the configuration information cannot be set. By continuing the process, the configuration definition is distributed to other hosts on which JP1/Base has started. To distribute the configuration definition to a host to which it cannot be distributed, start JP1/Base on the host, and then re-execute the `jbsrt_distrib` command. When a message asking you to delete the configuration definition information appears, enter `n` to distribute the configuration definition to the host. This completes the distribution of the configuration definition in the entire system.

The following configuration definition file is referenced by this command:

In Windows:

installation-folder`\conf\route\jbs_route.conf`
shared-folder`\jp1base\conf\route\jbs_route.conf (when the -h option is specified)`

In UNIX:

`/etc/opt/jp1base/conf/route/jbs_route.conf`
shared-directory`/jp1base/conf/route/jbs_route.conf (when the -h option is specified)`

For details on the format of the definition file, see the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition file Reference*.

Format

`jbsrt_distrib [-h` *logical-host-name*`]`

Required execution permission

In Windows: Administrators (If User Account Control (UAC) for Windows is enabled, you must execute the command from the administrator console.)

In UNIX: Superuser

Command directory

In Windows:
installation-folder`\bin\`

In UNIX:
`/opt/jp1base/bin/`

Arguments

- `-h` *logical-host-name*

When using JP1/Base in a cluster system, specify the logical host for which you will execute the command. If you omit this option, the host name set in the environment variable `JP1_HOSTNAME` is assumed. If the environment variable `JP1_HOSTNAME` is not set, the physical host name is assumed. There is no need to specify this argument unless you are running a cluster system.

Return values

`0`	Normal end
`1`	Abnormal end

jbsrt_get

Function

The `jbsrt_get` command displays the configuration definition information of the host for which you will execute this command.

If you execute this command with the `-h` option on a secondary server in a cluster system, no definition is displayed. In that case, execute this command on a primary server.

Format

`jbsrt_get [-h` *logical-host-name*`]`

Required execution permission

In Windows: Administrators (If User Account Control (UAC) for Windows is enabled, you must execute the command from the administrator console.)

In UNIX: Superuser

Command directory

In Windows:
installation-folder`\bin\`

In UNIX:
`/opt/jp1base/bin/`

Arguments

■ `-h` *logical-host-name*

When using JP1/Base in a cluster system, specify the logical host for which you will execute the command. If you omit this option, the host name set in the environment variable `JP1_HOSTNAME` is assumed. If the environment variable `JP1_HOSTNAME` is not set, the physical host name is assumed. There is no need to specify this argument unless you are running a cluster system.

Return values

`0`	Normal end
`1`	Abnormal end

Output example

An example of output from this command is shown below.

```
** configuration definition information **

upper-level host : parent_host
local host        : myhost
lower-level hosts: child_host1
                   : child_host2
                   : [child_host1]
                   : child_host3
```

jbsrt_sync

Function

The `jbsrt_sync` command is executed on a manager host (i.e. host on which JP1/IM - Manager is installed).

This command collects configuration definition information from lower-level hosts, and then updates the configuration definition in the system. This command is executed after the system configuration definition is divided and defined.

Format

`jbsrt_sync [-h` *logical-host-name*`]`

Required execution permission

In Windows: Administrators (If User Account Control (UAC) for Windows is enabled, you must execute the command from the administrator console.)

In UNIX: Superuser

Command directory

In Windows:
installation-folder`\bin\`

In UNIX:
`/opt/jp1base/bin/`

Arguments

- `-h` *logical-host-name*

When using JP1/Base in a cluster system, specify the logical host for which you will execute the command. If you omit this option, the host name set in the environment variable `JP1_HOSTNAME` is assumed. If the environment variable `JP1_HOSTNAME` is not set, the physical host name is assumed. There is no need to specify this argument unless you are running a cluster system.

Return values

`0`	Normal end
`1`	Abnormal end

jbssetacl

Function

The `jbssetacl` command registers operating permissions for individual JP1 users.

Format

```
jbssetacl [-h logical-host-name]
                [-s authentication-server-name]
                -f definition-file-name
                [-no]
```

Required execution permission

In Windows: Administrators (If User Account Control (UAC) for Windows is enabled, you must execute the command from the administrator console.)

In UNIX: Superuser

Command directory

In Windows:

installation-folder`\bin\`

In UNIX:

`/opt/jp1base/bin/`

Arguments

- `-h` *logical-host-name*

  When using JP1/Base in a cluster system, you register JP1 user operating permissions with the primary authentication server configured on the logical host specified with this option.

- `-s` *authentication-server-name*

  Specify the authentication server on which you want to register the JP1 user operating permissions. When you omit this option, the `-h` option is ignored.

- `-f` *definition-file*

  Specify the name of the definition file containing JP1 user operating permissions. The file format is the same as that of the user permission level file (`JP1_UserLevel`). You can give the definition file any name and store it in any location. For details on the format of the user permission level file, see *User permission level file* in *14. Definition Files*.

- `-no`

  This option causes the system to return an error without registering operating permissions if the specified JP1 user has already been assigned operating permissions.

Note

The `-s` option takes precedence if you specify both the `-h` and `-s` options. If you omit both options, the host name set in the environment variable `JP1_HOSTNAME` is assumed as the logical host. If you omit both options and nothing is set in `JP1_HOSTNAME`, the operating permissions are registered for the physical host.

Return values

0	Normal end
2	Invalid arguments
4	Insufficient system resource such as memory
8	The authentication server has not started or is not responding
16	An error occurred in processing of the authentication server.
32	An error occurred during initialization of the communication functionality
64	File format error
128	Inconsistency in internal processing (a C++ exception)
255	Other error

jbssetcnf

Function

The `jbssetcnf` command registers the information in the specified definition file into the common definition information.

Format

`jbssetcnf` *definition-file-name*

Required execution permission

In Windows: Administrators (If User Account Control (UAC) for Windows is enabled, you must execute the command from the administrator console.)

In UNIX: Superuser

Command directory

In Windows:

installation-folder`\bin\`

In UNIX:

`/opt/jp1base/bin/`

Arguments

- *definition-file*

Specify the definition file you want to add to the common definition information. The definition file name must be specified by using a full path.

Return values

`0`	Normal end (returned even if no definition file was specified)
`-1`	Abnormal end

jbssetumap

Function

The `jbssetumap` command registers specific user mapping information into the common definition information.

Format

```
When using a definition file:
jbssetumap [-h logical-host-name]
            -f definition-file-name
            [-no]
When not using a definition file:
jbssetumap [-h logical-host-name]
            {-u JP1-user-name | -ua}
            {-sh server-host-name| -sha}
            -o OS-user-name [,OS-user-name...]
            [-no]
```

Required execution permission

In Windows: Administrators (If User Account Control (UAC) for Windows is enabled, you must execute the command from the administrator console.)

In UNIX: Superuser

Command directory

In Windows:

installation-folder`\bin\`

In UNIX:

`/opt/jp1base/bin/`

Arguments

- `-h` *logical-host-name*

  When using JP1/Base in a cluster system, specify the logical host for which you want to register the user mapping information. If you omit this option, the host name set in the environment variable `JP1_HOSTNAME` is assumed. If the environment variable `JP1_HOSTNAME` is not set, the physical host name is assumed.

- `-f` *definition-file-name*

  Specify the name of the definition file containing the mapping information you want to register or modify. You can store the definition file in any location. You can use any file name when you store the file, but the file format must be the same as the user mapping definition file (`jp1BsUmap.conf`). For details on the format of the user mapping definition file, see *User mapping definition file* in *14. Definition Files*.

When you specify this option, you cannot specify the `-u`, `-ua`, `-sh`, or `-sha` option.

- `-u` *JP1-user-name*

  Specify the name of the JP1 user for which you want to register or modify mapping information. You can only specify this option when the `-ua` option is not specified.

- `-ua`

  Specify an asterisk (`*`) for the JP1 user name. Entering an asterisk (`*`) grants the rights of the users specified in *user-list* to all JP1 users. You can only specify this option when the `-u` option is not specified.

- `-sh` *server-host-name*

  Specify the name of the server host where the JP1 user issues operating instructions. You can only specify this option when the `-sha` option is not specified.

- `-sha`

  Specify an asterisk (`*`) for the server host name. This option enables the JP1 users to operate from any server host. You can only specify this option when the `-sh` option is not specified.

- -o *OS-user-name*

  Specify the OS user name to which you want to map the JP1 user. You can use a comma (`,`) as a delimiter to specify multiple OS users.

- `-no`

  This option causes the system to return an error without registering mapping information if the specified mapping information has already been registered for the specified JP1 user.

Note

To check the settings done by this command, execute the `jbsgetumap` command.

Return values

`0`	Normal end
`1`	Invalid arguments
`2`	The user executing the command does not have an appropriate privilege.
`3`	An error occurred during reading of the user mapping definition file.
`4`	The user mapping definition file contains a syntax error.

5	An error occurred during access to the common definitions.
6	Insufficient system resource such as memory
10	An error occurred during locking of the common definitions.
255	Other error

jbssetupsrv (Windows only)

Function

The `jbssetupsrv` command registers or deletes the authentication servers (the primary authentication and secondary authentication servers). When you want to change an authentication server setting from a local host to a remote host or visa versa, modify the startup settings of the authentication server.

Format

```
jbssetupsrv [-h logical-host-name]
            {primary-authentication-server [secondary-authentication-server] |
                 -d [authentication-server-name]}
                [-f]
```

Required execution permission

Administrators. (If User Account Control (UAC) for Windows is enabled, you must execute the command from the administrator console.)

Command directory

installation-folder`\bin\`

Arguments

- `-h` *logical-host-name*

  When using JP1/Base in a cluster system, specify the logical host for which you want to register the authentication server. If you omit this option, the host name set in the environment variable `JP1_HOSTNAME` is assumed. If the environment variable `JP1_HOSTNAME` is not set, the physical host name is assumed. You can enter a character string that is from 1 to 196 bytes to specify the logical host.

- *primary-authentication-server*

  Specify the authentication server (primary authentication server) to be used in routine operation.

- *secondary-authentication-server*

  Specify the authentication server (secondary authentication server) to operate in reserve. Specify this option if you are using two authentication servers in one user authentication block. If you omit this option, JP1/Base assumes that only one authentication server is used in the user authentication block.

- `-d` *authentication-server-name*

  Specify the authentication server or servers that you want to delete. If you specify -d without *authentication-server-name*, all the authentication servers on the specified logical host are deleted.

- `-f`

This option forcibly starts JP1/Base so that you can modify the startup settings of the authentication server. This option enables you to change an authentication server setting from a local host to a remote host or visa versa while JP1/Base is running.

Note

When a secondary authentication server has been registered and you delete only the primary authentication server, the secondary authentication server becomes the primary authentication server.

Return values

`0`	Normal end
`1`	Abnormal end

jbssetusrsrv (UNIX only)

Function

The `jbssetusrsrv` command specifies the authentication server (primary authentication server and secondary authentication server). Use this command when using JP1/IM and JP1/AJS.

Execute this command on the following hosts:

- Host used as an authentication server
- Host on which JP1/IM - Manager, JP1/AJS - Manager, or JP1/AJS - Agent is installed

Format

```
jbssetusrsrv [-h logical-host-name]
             primary-authentication-server
             [secondary-authentication-server]
```

Required execution permission

Superuser

Command directory

`/opt/jp1base/bin/`

Arguments

- `-h` *logical-host-name*

  When using JP1/Base in a cluster system, specify the logical host for which you want to register the authentication server. If you omit this option, the host name set in the environment variable `JP1_HOSTNAME` is assumed. If the environment variable `JP1_HOSTNAME` is not set, the physical host name is assumed.

- *primary-authentication-server*

  Specify the authentication server (primary authentication server) to be used in routine operation.

- *secondary-authentication-server*

  Specify the authentication server (secondary authentication server) to operate in reserve. Specify this option if you are using two authentication servers in one user authentication block. If you omit this option, JP1/Base assumes that only one authentication server is used in the user authentication block.

Return values

`0`	Normal end
`1`	Abnormal end

jbsumappass (Windows only)

Function

The `jbsrmumappass` command registers an OS user in the JP1/Base password management information. This command also enables you to change the registered OS user's password.

Format

```
jbsumappass [-h logical-host-name]
            -u OS-user-name
            [-p password]
```

Required execution permission

Administrators. (If User Account Control (UAC) for Windows is enabled, you must execute the command from the administrator console.)

Command directory

installation-folder`\bin\`

Arguments

- `-h` *logical-host-name*

When using JP1/Base in a cluster system, specify the logical host for which you want to register the OS user or change an OS user's password. If you omit this option, the host name set in the environment variable `JP1_HOSTNAME` is assumed. If the environment variable `JP1_HOSTNAME` is not set, the physical host name is assumed.

- `-u` *OS-user-name*

Specify the OS user name that you want to register or whose password you want to change.

As the OS user name, you can specify not only a user name but also the name of the domain to which the local host belongs or the local host name. To specify a domain name or local host name, use a backslash (\) as a separator between the domain or local host name and user name (for example, `domain\user1` or `server\user1`). If you specify a domain name, JP1/Base checks if the specified OS user is a user who belongs to that domain. If the specified OS user name is not a user of the domain, you cannot register the user under the OS user name. If you specify a local host name, JP1/Base checks whether the OS user name you entered is a local user. If the specified OS user name is a local user, you cannot register the user under the OS user name.

If you do not specify a domain name or local host name, JP1/Base checks whether the specified OS user is a local user. If the entered OS user is not a local user, JP1/Base checks whether it is a user in a domain containing a trusted domain. If the specified OS user name is not a local user or a user of the domain, you cannot register the user under the OS user name.

To register an OS user name with the Windows domain controller, use the format *domain-name\user-name*. As the domain controller does not differentiate between a domain user and local user, the user name will be treated as a domain user.

- `-p` *password*

  Specify the password for the *OS-user-name*. Omit this option if the OS user has no password.

Note

In Windows, you need to grant specific Windows user permissions to the OS user who is to execute this command, and to the OS user specified in the user mapping, respectively. For details, see *6.1.5 Before setting user mapping*.

Return values

`0`	The OS user's password was updated.
`1`	The OS user has been registered.
Other than `0` or `1`	Abnormal end

jbsunblockadesrv

Function

The `jbsunblockadesrv` command unblocks an authentication server.

Format

```
jbsunblockadesrv [-h logical-host-name]
                              -s authentication-server-name
```

Required execution permission

In Windows: Administrators (If User Account Control (UAC) for Windows is enabled, you must execute the command from the administrator console.)

In UNIX: Superuser

Command directory

In Windows:

installation-folder`\bin\`

In UNIX:

`/opt/jp1base/bin/`

Arguments

- `-h` *logical-host-name*

  When using JP1/Base in a cluster system, specify the logical host for which the destination authentication server is set. If you omit this option, the host name set in the environment variable `JP1_HOSTNAME` is assumed. If the environment variable `JP1_HOSTNAME` is not set, the physical host name is assumed.

- `-s` *authentication-server-name*

  Specify the name of the authentication server to be released from blocked status.

Return values

`0`	The authentication server has been unblocked.
`1`	The authentication server is already unblocked.
Other than `0` or `1`	Abnormal end

Example

Suppose that the primary authentication server is `server1` (blocked), and the secondary authentication server is `server2`. When you execute the `jbsunblockadesrv` command to unblock `server1`, the following information appears:

```
jbsunblockadesrv -s server1
primary:server1
secondary:server2
```

jbsunsetcnf

Function

The `jbsunsetcnf` command deletes a specified logical host from the common definition information.

Format

```
jbsunsetcnf [-i]
             -h logical-host-name
             [-c component-name]
             [-n subkey]
```

Required execution permission

In Windows: Administrators (If User Account Control (UAC) for Windows is enabled, you must execute the command from the administrator console.)

In UNIX: Superuser

Command directory

In Windows:

installation-folder`\bin\`

In UNIX:

`/opt/jp1base/bin/`

Arguments

- `-i`

  When you specify this option, a confirmation message asks you to confirm that you want to delete the common definition information for the specified logical host. The deletion processing is executed only if you type `y` or `Y` in response to the message.

- `-h` *logical-host-name*

  Specify the logical host name to be deleted from the logical hosts registered in the common definition information.

- `-c` *component-name*

  Specify the component name to be deleted for the logical host registered in the common definition information.

- `-n` *subkey*

  Specify the subkey of the component to be deleted for the logical host registered in the common definition information. This option is valid only when the `-c` option is specified.

Notes

- As a general rule, execute this command with the `-i` option specified.
- Do not execute this command when JP1/Base is active.

Return values

`0`	Normal end (also returned if the specified logical host does not exist)
`-1`	Delete processing failed.

jcocmdconv

Function

The `jcocmdconv` command migrates the command execution logs of JP1/Base Version 7 or earlier to the command execution logs (ISAM) used in JP1/Base Version 8 or later. If you do not execute this command, the command execution logs accumulated in Version 7 or earlier cannot be accessed.

After upgrading to JP1/Base Version 8 or later from a previous version, execute this command only once on the manager host where the command execution logs reside. When using JP1/Base in a cluster system, execute the `jcocmdconv` command on both the physical host and logical host. The `jcocmdconv` command can be executed at the same time on both the physical host and logical host. However, you cannot execute multiple instances of the `jcocmdconv` command at the same time on the physical host.

Format

`jcocmdconv [-h` *logical-host-name*`]`

Required execution permission

In Windows: Administrators (If User Account Control (UAC) for Windows is enabled, you must execute the command from the administrator console.)

In UNIX: Superuser

Command directory

In Windows:

installation-folder`\bin\`

In UNIX:

`/opt/jp1base/bin/`

Arguments

- `-h` *logical-host-name*

Specify the logical host if you are using JP1/Base in a cluster system. If you omit this option, the host name set in the environment variable `JP1_HOSTNAME` is assumed. If the environment variable `JP1_HOSTNAME` is not set, the physical host name is assumed. There is no need to specify this argument unless you are running a cluster system.

Note

Execute this command after installing the Version 8 JP1/Base and JP1/IM - Manager, and before starting JP1/IM - Manager. If you start JP1/IM - Manager before executing this command, a message about an automated action or command execution might be entered in the command execution log in Version 8 format. If the command execution log files (ISAM) are updated in this way before you execute the jcocmdconv command, the log accumulated in the previous version cannot be migrated.

Return values

0	Normal end
2	Invalid parameter
3	No logical host
4	Memory error
5	Disk file error
6	A file already exists at the save-to destination.
7	The command was canceled by a signal.
8	Execution permission error
32	An error occurred during access to the common definitions.
41	File access error
42	Another jcocmdconv command is being executed.
255	Other error

jcocmddef

Function

The `jcocmddef` command configures and references the command execution environment. Two types of arguments are provided: one type to be specified on the manager host (host on which JP1/IM - Manager is installed), and the other type to be specified only on the host that executes the command. For details on these arguments, see the following description.

Format

```
jcocmddef [ [-show] |
          [-default]
          [-rsptime response-monitoring-time]
          [-record number-of-records]
          [-group host-group-definition-file-name]
          [-loaduserprofile {ON|OFF}]
          [-queuenum number-of-commands-in-queue]
          [-execnum number-of-commans-to-be-executed-concurrently]
          [-open {ON|OFF}]
          [-flush {ON|OFF}]
          [-cmdevent {0 | 1 | 2 | 3 | 4 | 5 | 6 | 7}]
          [-actevent {0 | 1 | 2 | 3 | 4 | 5 | 6 | 7}]
          [-actresult {ON|OFF}]
          [-host logical-host-name]
          [-runevinterval
interval-of-issuing-the-elapsed-time-notification-event]
          [-actlimit {ON [transferred-data-amount-(number-of-lines)] |
OFF}]
          [-cmdlimit {ON [transferred-data-amount-(number-of-lines)] |
OFF}]
         [-queuethreshold threshold-for-number-of-commands-in-queue] ]
```

Required execution permission

In Windows: Administrators (If User Account Control (UAC) for Windows is enabled, you must execute the command from the administrator console.)

In UNIX: Superuser

Command directory

In Windows:
installation-folder`\bin\`

In UNIX:

`/opt/jp1base/bin/`

Arguments

- `-show`

  This option enables you to display the current definitions. You can only specify this option when the other options are not specified. If you omit all of the options including this option, the current definitions are displayed, which is the same result as when only the `-show` option is specified.

- `-default`

  This option resets the values of the following options to their defaults: `-rsptime`, `-record`, `-loaduserprofile`, `-queuenum`, `-execnum`, `-open`, `-flush`, `-cmdevent`, `-actevent`, `-actresult`, `-runevinterval`, `-actlimit`, `-cmdlimit`, and `-queuethreshold`. The `-default` option takes precedence if you specify this option with any other options.

- `-rsptime` *response-monitoring-time*

  This option is set on a manager host (i.e. host on which JP1/IM - Manager is installed).

  Specify the monitoring time for response from the executed command. The specifiable range is 0 to 600 (in seconds). When 0 is specified, no monitoring occurs. The default is 60 seconds.

  If there is no response from the executed command within the specified response monitoring time, the `KAVB2002-I` message is output.

  The value specified in this option is valid when JP1/Base is restarted.

- `-record` *number-of-records*

  This option is set on a manager host (i.e. host on which JP1/IM - Manager is installed).

  Specify the number of records as an upper limit of command execution logs for commands that are executed in the Execute Command window of JP1/IM - View or by an automated action.

  The specifiable range is 1 to 196,600. The default is 20,000 records.

  The number of records to be used in one command execution is (*number-of-command-output-rows* + 3) records. One record is 6,520 bytes. You cannot change the record size.

  If there are not enough records, the result of automated actions might not be displayed properly.

  The changed number of records is valid when the command execution logs (ISAM) are deleted. When deleting the command execution logs (ISAM), note that you cannot restore the logs for the previously executed automated actions or the command executions. For details on the procedure for, and notes on, deleting the command execution logs (ISAM), see the section describing how to change the maximum number of records in the chapter *Troubleshooting* in the manual *Job Management Partner 1/Integrated Management - Manager Administration Guide*.

- `-group` *host-group-definition-file-name*

  This option is set on a manager host (i.e. host on which JP1/IM - Manager is installed).

  Specify a host group definition file in which the command execution hosts have been defined. For details on the format of the definition file, see the manual *Job Management Partner 1/Integrated Management - Manager Command and Definition file Reference*.

  If a host group has not been defined in the host group definition file, the host group will be deleted.

- `-loaduserprofile {ON|OFF}`

  This option is set on the host that executes the command.

  Specify whether OS users' profiles are read by executing this command. If you specify `ON`, profiles are read. If you specify `OFF`, profiles are not read. The values `ON` and `OFF` are not case sensitive. The default is `OFF`.

  The value specified in this option is valid when JP1/Base is restarted.

  This option is for Windows.

- `-queuenum` *number-of-commands-in-queue*

  This option is set on the host that executes the command.

  Specify the maximum number of commands that can reside in the queue on the host that executes the command, if the command is executed by using the automated action functionality. The specifiable range is 0 to 65,535. The default is 1,024. If you specify `0`, you cannot execute multiple instances of a command at the same time on the target host.

  If the number of automated actions in queue exceeds the value of *number-of-commands-in-queue*, the `KAVB2058-E` message appears.

  The value specified in this option is valid when JP1/Base is restarted.

- `-execnum` *number-of-commans-to-be-executed-concurrently*

  This option is set on the host that executes the command.

  Specify the maximum number of commands to be executed concurrently on the host that executes the command, if the command is executed by using the automated action functionality. The specifiable range is 1 to 48. The default is 1. You can specify a different value for each host on which the command is executed.

The value specified in this option is valid when JP1/Base is restarted.

This option is useful if the command execution takes a long time and you want a command further down the queue to be executed ahead of the command that takes a while to execute, or if a large number of automated actions occur and you want to speed up processing.

If you specify `2` or a larger number, multiple commands are executed at the same time, so the executed commands might not end in the same order as they started in. Therefore, if you need to operate the system considering the end order of automated actions, do not specify this option.

■ `-open {ON|OFF}`

This option is set on a manager host (i.e. host on which JP1/IM - Manager is installed).

Set whether an execution log is output leaving the command execution log files (ISAM) still being opened. If you specify `ON`, an execution log is output leaving the command execution log files still being opened. If you specify `OFF`, an execution log is output not leaving the command execution log files still being opened. The default is `OFF`. This option is valid only for the command execution log for automated actions, and it is invalid for command execution log for the Execute Command window of JP1/IM - View.

To enable the `-open` setting, you must restart JP1/Base.

■ `-flush {ON|OFF}`

This option is set on a manager host (i.e. host on which JP1/IM - Manager is installed).

Set whether command execution logs are written to the disks for each row. If this option is enabled, you can restart JP1/Base and reference the execution logs when an unexpected shutdown occurs. If you specify `ON`, the execution logs are written to the disks for each row. If you specify `OFF`, the system buffers the execution logs, instead of writing to the disks for each row. The default is `OFF`.

If `-flush` is enabled, automated action and command execution performance might deteriorate. This is because a disk write operation occurs for each row.

To enable the `-flush` setting, you must restart JP1/Base.

■ `-cmdevent {0 | 1 | 2 | 3 | 4 | 5 | 6 | 7}`

This option is set on a manager host (i.e. host on which JP1/IM - Manager is installed).

If you want to issue an event (command execution-related event) before, during, or after a command is executed, you must specify the level of the event to be issued. You can specify any one of the event levels listed in the following table. The default is `0`.

Table 13-1: Event levels (command execution-related)

Event Level	Event ID	Description
0	None	Does not issue a command executed-related event.
1	00003FA0	Issues an event when command execution begins.
2	00003FA1	Issues an event when command execution ends.
3	00003FA0, 00003FA1	Issues an event when command execution begins and ends.
4	00003FA2	Issues an event when command execution ends abnormally.
5	00003FA0, 00003FA2	Issues an event when command execution begins and ends abnormally.
6	00003FA1, 00003FA2	Issues an event when command execution ends normally or ends abnormally.
7	00003FA0, 00003FA1, 00003FA2	Issues an event when command execution begins and ends normally, or when command execution ends abnormally.

The value specified in this option is valid when JP1/Base is restarted.

■ `-actevent {0 | 1 | 2 | 3 | 4 | 5 | 6 | 7}`

This option is set on a manager host (i.e. host on which JP1/IM - Manager is installed).

If you want to issue an event (action status notification-related event) when the status of an action changes, you must specify the level of the event to be issued. You can specify any one of the event levels listed in the following table. The default is `0`.

Table 13-2: Event levels (automated action status notification-related)

Event level	Event ID	Description
0	None	Do not issue an action status notification-related event.
1	000020E0, 000020E3	Issues an event when the status of an action changes to Sending, Queued, or Running.
2	000020E1, 000020E4	Issues an event when the status of an action changes to Finished, Canceled, or Forcibly terminated.
3	000020E0, 000020E1, 000020E3, 000020E4	Issues an event when the status of an action changes to Sending, Queued, Running, or Finished.
4	000020E2, 000020E5	Issues an event when the status of an action changes to Unexecutable or Failed.

Event level	Event ID	Description
5	`000020E0`, `000020E2`, `000020E3`, `000020E5`	Issues an event when the status of an action changes to Sending, Queued, Running, Unexecutable, or Failed.
6	`000020E1`, `000020E2`, `000020E4`, `000020E5`	Issues an event when the status of an action changes to Finished, Canceled, Forcibly terminated, Unexecutable, or Failed.
7	`000020E0`, `000020E1`, `000020E2`, `000020E3`, `000020E4`, `000020E5`	Issues an event when the status of an action changes to Sending, Queued, Running, Finished, Canceled, Forcibly terminated, Unexecutable, or Failed.

The value specified in this option is applied when JP1/IM - Manager restarts, or when the `jco_spmd_reload` command is used to reload the manager.

To issue an action status notification-related event, JP1/IM - Manager refers to the action information file. If the action information file becomes full and is overwritten, the manager cannot refer to the action information that was overwritten. This makes it impossible to issue an action status notification-related event. In such a case, a warning event (`000020E6` or `000020E7`) or an error event (`000020E8`) is issued.

■ `-actresult {ON|OFF}`

This option is set on a manager host (i.e. host on which JP1/IM - Manager is installed).

This option specifies whether results of commands executed by the automated action function are to be recorded in the command execution log. If you record execution results, specify `ON`. If you do not record them, specify `OFF`.

The values `ON` and `OFF` are not case sensitive. The default is `ON`. If you want detailed command execution results, you must specify `ON`.

If `OFF` is specified, performance of the JP1/Base controller improves. This is because output to the command execution log file (ISAM) is suppressed. However, because the return values from commands executed as automated actions are the only items of information that are not discarded, no detailed command execution result is output. (As a result, only the KAVB2401-I message is output to **Message** in the **Action Log Details** window of JP1/IM - View.)

The value specified in this option is valid when JP1/IM - Manager is restarted.

■ `-host` *logical-host-name*

Specify the logical host if you are using JP1/Base in a cluster system. If you omit this option, the host name set in the environment variable `JP1_HOSTNAME` is assumed. If the environment variable `JP1_HOSTNAME` is not set, the physical host name is assumed.

If this option is specified and a setting for an active or standby server is changed, make sure that the settings in each server match.

- `-runevinterval` *interval-of-issuing-the-elapsed-time-notification-event*

  This option is set on the host that executes the command.

  This option specifies how often to issue an event that indicates a specified amount of time has elapsed since a command was started in the Execute Command window of JP1/IM - View, or since a command was started as an automated action. The specifiable range is 0 to 86,400. The default is 600 seconds (10 minutes).

  An event with the event ID `00003FA3` (execution elapsed time notification event) is issued and the KAVB2402-W message appears after the specified amount of time has elapsed. If `0` is specified, no event is issued.

  The value specified in this option is valid when JP1/Base is restarted.

- `-actlimit {ON [`*transferred-data-amount-(number-of-lines)*`] | OFF}`

  This option is set on the host that executes the command.

  If the results of commands executed by the automated action function are transferred to the manager, you can use this option to specify whether to suppress the amount of result data transferred. You can also specify the maximum amount of result data that can be transferred when data transfer is suppressed. The specifiable range is 0 to 196,600. The default setting is `ON` (suppressed), and the default maximum amount is 1,000. If the JP1/Base version running on the command-executing host is 07-51 or earlier, or if the version has upgraded to 08-00 or later, the default setting for this option is `OFF` (unsuppressed).

  To suppress the amount of command execution result data to be transferred, specify this option to `ON`, and specify the total number of lines as the maximum amount of data (assuming 256 bytes per line). 1,000 lines is the default.

  If you do not want to suppress the amount of data to be transferred, specify the setting to be `OFF`.

  If you do not want to output a large amount of result data for commands executed by the automated action function, or if you want to prevent an executed command from entering an infinite loop due to an invalid operation, we recommend using this setting. If you enable this setting, only a small amount of data is output.

  If command execution results exceed the maximum value, the KAVB2070-W message is output.

  To enable the `-actlimit` setting, you must restart JP1/Base.

- `-cmdlimit {ON [`*transferred-data-amount-(number-of-lines)*`] | OFF}`

  This option is set on the host that executes the command.

  If the results of commands executed in the Execute Command window of JP1/IM -

View are transferred to the manager, you can use this option to specify whether to suppress the amount of result data transferred. You can also specify the maximum amount of result data that can be transferred when data transfer is suppressed. The specifiable range is 0 to 196,600. The default setting is `ON` (suppressed), and the default maximum amount is 1,000. If the JP1/Base version running on the command-executing host is 07-51 or earlier, or if the version has been upgraded to 08-00 or later, the default setting for this option is `OFF` (unsuppressed).

To suppress the amount of command execution result data to be transferred, specify this option to `ON`, and specify the total number of lines as the maximum amount of data (assuming 256 bytes per line). 1,000 lines is the default.

If you do not want to suppress the amount of data to be transferred, specify the setting to be `OFF`.

If you do not want to output a large amount of result data for commands executed in the Execute Command window of JP1/IM - View, or if you want to prevent an executed command from entering an infinite loop due to an invalid operation, we recommend using this setting. If you enable this setting, only a small amount of data is output.

If command execution results exceed the maximum value, the KAVB2070-W message is output.

To enable the `-cmdlimit` setting, you must restart JP1/Base.

■ `-queuethreshold` *threshold-for-number-of-commands-in-queue*

This option is set on the host that executes the command.

If you want to monitor the number of queued commands on the command-executing host that are waiting to be executed by the automated action function, you can use this option to specify a threshold for the number of commands that can be prequeued. The specifiable range is 0 to 65,535. The default is 10.

When `0` is specified, a threshold is not monitored.

If a non-zero value is specified and that value is reached, a warning JP1 event is issued and the KAVB2071-W message is output. If the number of prequeued commands returns to 0, a recovery JP1 event is issued and the KAVB2072-I message is output.

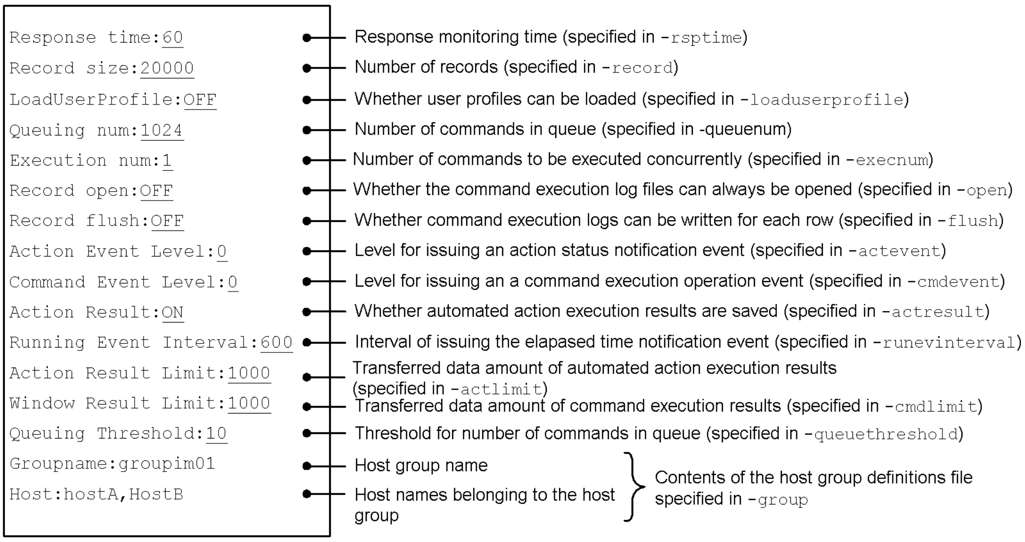
Threshold monitoring allows you to detect the accumulation of actions in the JP1/Base queue. This helps you to prevent execution delays before they occur.

To enable the `-queuethreshold` setting, you must restart JP1/Base.

Output format

When a `jcocmddef` command is executed, all the parameters (including parameters that have been changed) are displayed. The output format is shown below.

Figure 13-1: jcocmddef command output format



```
Response time:60
Record size:20000
LoadUserProfile:OFF
Queuing num:1024
Execution num:1
Record open:OFF
Record flush:OFF
Action Event Level:0
Command Event Level:0
Action Result:ON
Running Event Interval:600
Action Result Limit:1000
Window Result Limit:1000
Queuing Threshold:10
Groupname:groupim01
Host:hostA,HostB
```

Response monitoring time (specified in -rsptime)

Number of records (specified in -record)

Whether user profiles can be loaded (specified in -loaduserprofile)

Number of commands in queue (specified in -queuenum)

Number of commands to be executed concurrently (specified in -execnum)

Whether the command execution log files can always be opened (specified in -open)

Whether command execution logs can be written for each row (specified in -flush)

Level for issuing an action status notification event (specified in -actevent)

Level for issuing an a command execution operation event (specified in -cmdevent)

Whether automated action execution results are saved (specified in -actresult)

Interval of issuing the elapased time notification event (specified in -runevinterval)

Transferred data amount of automated action execution results (specified in -actlimit)

Transferred data amount of command execution results (specified in -cmdlimit)

Threshold for number of commands in queue (specified in -queuethreshold)

Host group name

Host names belonging to the host group

Contents of the host group definitions file specified in -group

Legend:

__ (underscore): Indicates the default value.

Return values

0	Normal end
-1	Abnormal end

jcocmddel

Function

JP1/IM requests command execution in the Execute Command window of JP1/IM - View, or uses the automated action function to request command execution. This command allows you to terminate and delete commands on a JP1/Base host that are being executed or queued in the above manner.

Use this command when a command execution problem occurs, such as when a wrong command is executed while the system is being used, or when a time-consuming command prevents the next command from being executed. Before you execute this command, use the `jcocmdshow` command to check the target command's status and confirm that it is not required (can be deleted).

Format

```
jcocmddel [-h logical-host-name]
            [-s target-host-name]
            [-f]
            [command-ID | ALL]
```

Required execution permission

In Windows: Administrators (If User Account Control (UAC) for Windows is enabled, you must execute the command from the administrator console.)

In UNIX: Superuser

Command directory

In Windows:
installation-folder`\bin\`

In UNIX:
`/opt/jp1base/bin/`

Arguments

- `-h` *logical-host-name*

Specify the logical host if you are using JP1/Base in a cluster system. If you omit this option, the host name set in the environment variable `JP1_HOSTNAME` is assumed. If the environment variable `JP1_HOSTNAME` is not set, the physical host name is assumed. There is no need to specify this argument unless you are running a cluster system.

- `-s` *target-host-name*

  Specify the name of the target host on which the command to be deleted exists. You can enter a character string that is from 1 to 255 bytes to specify the host. If you omit this option, the local host is assumed.

- `-f`

  Specify this option if you want to suppress the confirmation message that is displayed when a command is deleted. If you specify this option, the selected command is forcibly deleted.

- *command-ID* | `ALL`

  Specify a command to be deleted. To delete a specific command, you must specify the corresponding command ID shown when the `jcocmdshow` command is executed. To delete all commands that are currently being executed or queued, specify `ALL`.

  Use spaces to delimit multiple command IDs.

Return values

`0`	Normal end
`1`	The command ID was not found, or some commands have been deleted from the JP1/Base command execution management.
`2`	Invalid argument
`4`	Insufficient system resources
`8`	No permission to execute commands
`16`	An error occurred during communication with JP1/Base command execution management.
`32`	An error occurred during access to the common definitions.
`64`	No response from the target host
`65`	Version incompatible with the target host
`128`	Internal error
`129`	Maximum connections error
`255`	Other error

Example

In this example, the command `1234` that is currently being executed on the target host `host01 is deleted.`

```
jcocmddel -s host01 1234
```

Output example

```
jcocmddel -s host01 1234
KAVB2291-Q Do you want to delete the specified command ID(s) [Y/
y or N/n] ->
KAVB2293-I The command(s) were deleted successfully from command
execution control.
```

jcocmdlog

Function

The `jcocmdlog` command is executed on a manager host (i.e. host on which JP1/IM - Manager is installed).

This command outputs a history of commands executed in the Execute Command window of JP1/IM - View, or a history of commands executed by the automated action function. The history is output to the standard output in CSV format.

Format

```
jcocmdlog [-window]
            [-act]
            [-dir execution-log-directory]
            [-h logical-host-name]
            [-ext]
            [-date {date-time | [start-date-time],[end-date-time]}]
```

Required execution permission

In Windows: None (If User Account Control (UAC) for Windows is enabled, you must execute the command from the administrator console.)

In UNIX: None.

Command directory

In Windows:
installation-folder`\bin\`

In UNIX:
`/opt/jp1base/bin/`

Arguments

- `-window`

Outputs a history of commands executed in the Execute Command window of JP1/IM - View.

- `-act`

Outputs a history of commands executed by the automated action function.

If neither `-window` or `-act` option is specified, a history of commands is output for commands executed in the Execute Command window of JP1/IM - View, and for commands executed by the automated action function.

If you use the `jcocmddef` command (with `-actresult OFF`) to suppress output, the output result will not contain detailed information. (Only the KAVB2401-I message is output.) Detailed information is output by default, or if output suppression has been disabled with the `jcocmddef` command (with `-actresult ON`).

■ `-dir` *execution-log-directory*

Directs execution log output to the specified directory. If you omit this option, output is directed to the current execution log.

■ `-h` *logical-host-name*

Specify the logical host if you are using JP1/Base in a cluster system. If you omit this option, the host name set in the environment variable `JP1_HOSTNAME` is assumed. If the environment variable `JP1_HOSTNAME` is not set, the physical host name is assumed. If you specify the `-dir` option, this option is ignored.

■ `-ext`

Outputs the reception times for commands executed in the Execute Command window of JP1/IM - View, and for commands executed by the automated action function. The display format is *YYYY*/*MM*/*DD*, *hh*:*mm*:*ss*. The executed command names and messages are enclosed by double quotation marks. If an executed command name or a message contains a double quotation mark, another double quotation mark is added to the right or left of the command name or message. If you do not specify the `-ext` option, the display format for reception times is *YYYY*/*MM*/*DD*, *hh*:*mm*:*ss*. The executed command names or messages are not enclosed by double quotation marks.

Examples

- When the `-ext` option is specified:
```
Window,2005/04/01,14:16:23,hostA,"jcochstat -k HELD -n
1003",2420,0,"KAVB2013-I Terminated the ""jcochstat -k HELD
-n 1003"" command. pid=2420 terminate code=0"
```

- When the `-ext` option is not specified:
```
Window,04/01/05 14:16:23,hostA,jcochstat -k HELD -n
1003,2420,0,KAVB2013-I Terminated the "jcochstat -k HELD -n
1003" command. pid=2420 terminate code=0
```

■ `-date` {*date-time* | [*start-date-time*],[*end-date-time*]}

Specifies a date and time range for log output. If you omit this option, the whole log is output.

Specify the date and time or starting and ending date and time in the format date (*YYYYMMDD*: years, months, and days) and time (*hhmmss*: hours, minutes, and seconds) shown below. You can omit the time.

- `-date` *date-time*

Outputs log data recorded on a specified date or during a specified time period.

(Example) `-date 2005030317`

Outputs log data recorded during the 17th hour on 2005/03/03 (17:00:00 to 17:59:59).

- `-date` [*start-date-time*],[*end-date-time*]

  Outputs log data recorded during the time period for the specified starting and ending date and time.

  If you omit the time, the following is assumed:

  Start: 000000 (00:00:00)

  End: 235959 (23:59:59)

  - `-date` *start-date-time*`,`*end-date-time*

    Outputs log data recorded during the time period for the specified starting and ending date and time.

    (Example) `-date 2005030317,2005030416`

    Outputs log data recorded during the time period from 2005/03/03 17:00:00 to 2005/03/04 16:59:59.

  - `-date` *start-date-time*,

    Outputs log data recorded on or after the specified starting date and time.

    (Example) `-date 200503031724,`

    Outputs log data recorded on or after 2005/03/03 17:24:00.

  - `-date ,`*end-date-time*

    Outputs log data recorded on or before the specified ending date and time.

    (Example) `-date ,200503031724`

    Outputs log data recorded on or before 2005/03/03 17:24:59.

  - `-date ,`

    This is the same as omitting the `-date` option. Thus, all log data is output.

Return values

`0`	Normal end
`4`	Processing was interrupted because the command execution log file was being used.
`-1`	Abnormal end

Output format

Command execution results are output in the comma-separated value (CSV) format. The format for each output record is as follows:
execution-type`,` *message-reception-time*`,` *command-executing-host-name*`,`
executed-command`,` *process-ID*`,` *termination-code*`,` *message*

The execution type value is either `Window` (indicates that the command was executed in the Execute Command window of JP1/IM - View) or `Action` (indicates that the command was executed by the automated action function).

There is a maximum of 256 bytes per line of command execution result output. If the output result exceeds 256 bytes, the output is split into multiple lines.

A field that contains no data is simply output as a comma.

jcocmdshow

Function

JP1/IM requests command execution from the Execute Command window of JP1/IM - View, or uses the automated action function to request command execution. This command allows you to check the statuses of commands on a JP1/Base host that are being executed or queued in the above manner.

Use this command when a command execution problem occurs, such as when a wrong command is executed while the system is being used, or when a time-consuming command prevents the next command from being executed. This command provides the following formation:

- `ID`: A unique ID assigned to a command being executed or queued in command execution management
- `STATUS`: The execution status of a command in command execution management (R indicates that the command is being executed, and `Q` indicates that the command is currently queued.)
- `TYPE`: The name of the function requesting command execution (`WIN` indicates that it was requested from JP1/IM -View, and `ACT` indicates that it was requested by the automated action function.)
- `USER`: The name of the JP1 user requesting command execution
- `STIME`: The time that command execution management received the command from JP1/IM
- `ETIME`: The length of time that has elapsed since command execution started
- `COMMAND`: The name of the command being executed or queued

For safety reasons, we recommend that you use this command to check the status of a command that you want to delete. Before you use the `jcocmddel` command to delete the command, confirm that it is not required (can be deleted).

Format

```
jcocmdshow [-h logical-host-name]
             [-s target-host-name]
             [-window]
             [-act]
             [-state {r|q}]
             [-ph command-submitting-host-name]
             [-v]
```

Required execution permission

In Windows: Administrators (If User Account Control (UAC) for Windows is enabled, you must execute the command from the administrator console.)

In UNIX: Superuser

Command directory

In Windows:
installation-folder`\bin\`

In UNIX:
`/opt/jp1base/bin/`

Arguments

- `-h` *logical-host-name*

  Specify the logical host if you are using JP1/Base in a cluster system. If you omit this option, the host name set in the environment variable `JP1_HOSTNAME` is assumed. If the environment variable `JP1_HOSTNAME` is not set, the physical host name is assumed. There is no need to specify this argument unless you are running a cluster system.

- `-s` *target-host-name*

  Specify the name of the target host that contains commands whose execution statuses are to be checked. You can enter a character string that is from 1 to 255 bytes to specify the host. If you omit this option, the local host is assumed.

- `-window`

  If you want to check the execution statuses of commands for which execution was requested from the Execute Command window of JP1/IM - View, specify this option. If you specify both this option and the `-act` option, or if you omit both options, the command displays the execution statuses of commands for which execution was requested by the Execute Command window of JP1/IM - View and the automated action function.

- `-act`

  If you want to check the execution statuses of commands for which the automated action function requested execution, specify this option. If you specify both this option and the `-window` option, or if you omit both options (`-window` and `-act`), the command displays the execution statuses of commands for which execution was requested by the Execute Command window of JP1/IM - View and the automated action function.

- `-state {r|q}`

  Specify a command execution status. If you want to know which commands are *running*, specify `r`. Likewise, if you want to know which commands are *queued*, specify `q`.

  If you omit this option, information on the commands that are *running* and *queued* is output.

- `-ph` *command-submitting-host-name*

  If you want to know which commands were submitted from a specific host, specify this option.

- `-v`

  If you want to vertically display information output by the `jcocmdshow` command, specify this option.

  If you omit this option, the information items output by the `jcocmdshow` command are not displayed on individual lines.

Return values

`0`	Normal end
`1`	No command available in JP1/Base command execution management
`2`	Invalid argument
`4`	Insufficient system resources
`8`	No permission to execute commands
`16`	An error occurred during communication with JP1/Base command execution management.
`32`	An error occurred during access to the common definitions.
`64`	No response from the target host
`65`	Version incompatible with the target host
`128`	Internal error
`129`	Maximum connections error
`255`	Other error

Example

In this example, the execution statuses of commands being executed on the target host `host01` are displayed.

```
jcocmdshow -s host01
```

Output example

When the -v option is omitted:

```
jcocmdshow -s host01
ID   STATUS TYPE USER     STIME           ETIME     COMMAND
1234 R      WIN  jp1admin Feb 13 18:55:29 000:01:05
"C:\WINNT\system32\notepad.exe"
```

When the -v option is specified:

```
jcocmdshow -s host01 -v
ID       :1234
STATUS   :R
TYPE     :WIN
USER     :jp1admin
STIME    :Feb 13 18:55:29
ETIME    :000:01:05
COMMAND  :"C:\WINNT\system32\notepad.exe"
```

jevdbinit

Function

The `jevdbinit` command initializes the event database. At command execution, the existing data is deleted and the event database is re-created.

The new start serial number is the number you specify or the number carried over from the event database before the data was deleted.

You can create a backup of the event database before initialization. Using the `jevexport` command, you can output the backup file to a CSV-format file. You cannot restore the backup file.

For details on the event database initialization, see 8.2 *Initializing the event database*.

Format

```
jevdbinit [-h event-server-name]
          [-s start-serial-number-in-event-database]
          [-f]
          {-b | -n}
```

Required execution permission

In Windows: Administrators (If User Account Control (UAC) for Windows is enabled, you must execute the command from the administrator console.)

In UNIX: Superuser

Command directory

In Windows:
installation-folder`\bin\`

In UNIX:
`/opt/jp1base/bin/`

Arguments

- `-h` *event-server-name*

Specify the name of the event server at which to initialize the event database. If you omit this option, the logical host name set in the environment variable `JP1_HOSTNAME` is assumed as the event server name. If the environment variable `JP1_HOSTNAME` is not set, the event server name is assumed to be the same as the local host name. Specify the event server name as a character string of no more than 255 bytes.

- `-s` *start-serial-number-in-event-database*

Specify the start serial number of the event database when it is re-created after initialization. The database will be created with the serial number specified in this option. The specifiable range is 0 to 2,147,483,647.

If you omit this option, the serial numbers carry on from the deleted event database.

- `-f`

If you omit this option, a message asks if you are sure you want to execute the command. (The displayed message is `Is This OK?[Y/N].`) Specify this option if user confirmation is unnecessary.

- `-b`

Specify this option to back up the event database before it is initialized. You must specify either `-b` or `-n`.

The backup files are saved to the same directory as the event database. The following files are backed up:

Event database file name	Backup file name
`IMEvent{0|1}.idx`	`0IMEvent{0|1}.idx`
`IMEvent{0|1}.dat`	`0IMEvent{0|1}.dat`
`IMEvent{0|1}.fwd`	`0IMEvent{0|1}.fwd`

Note that the disk space occupied by the event database doubles when it is backed up. If you have kept a previous database backup file, it will be deleted when you specify the `-b` option.

- `-n`

Specify this option if you do not want to back up the event database before it is initialized. You must specify either `-b` or `-n`. If you have kept a previous database backup file, it will remain when you specify the -n option.

Notes

- You cannot execute this command while the event service is active.
- You cannot start the event service while this command is executing.
- If the event database is empty, executing this command returns a value of 7 (indicating that the event database is corrupted), but you can ignore this result.

Return values

0	Normal end

1	Invalid argument
2	Insufficient execution permission
3	I/O error
4	Insufficient memory
5	Undefined event server name
6	No event database
7	The event database is corrupt.
8	The event database cannot be initialized because the event service is active.
255	Other error

jevdbmkrep

Function

The `jevdbmkrep` command reconstructs the duplication prevention table file for the event database.

For details on the duplication prevention table, see *1.4.2 Event database*.

Format

```
jevdbmkrep [-h event-server-name]
              [-f]
```

Required execution permission

In Windows: Administrators (If User Account Control (UAC) for Windows is enabled, you must execute the command from the administrator console.)

In UNIX: Superuser

Command directory

In Windows:
installation-folder`\bin\`

In UNIX:
`/opt/jp1base/bin/`

Arguments

- `-h` *event-server-name*

Specify the name of an event server that contains the duplication prevention table file to be reconstructed. If you omit this option, the logical host name set in the environment variable `JP1_HOSTNAME` is assumed as the event server name. If the environment variable `JP1_HOSTNAME` is not set, the event server name is assumed to be the same as the local host name. Specify the event server name as a character string of no more than 255 bytes.

- `-f`

If you omit this option, a message asks if you are sure you want to execute the command. (The displayed message is `Is This OK?[Y/N].`) Specify this option if user confirmation is unnecessary.

Notes

- If the event database is large, it might take a long time for this command to finish.
- You cannot execute this command while the event service is active. You cannot

start the event service while this command is executing.

- If the event database is empty, the command will fail with a return value of 6 (indicates there is no event database).

Return values

0	Normal end
1	Invalid argument
2	Insufficient execution permission
3	I/O error
4	Insufficient memory
5	Undefined event server name
6	No event database
7	The event database is corrupt.
8	Cannot reconstruct the duplication prevention table file because the event service is running.
255	Other error

jevdbswitch

Function

The `jevdbswitch` command forcibly switches the event database in which events are actually registered from the active database to the standby database on the event server where the event service is running.

When the standby event database is swapped in, its existing contents are deleted. If you execute this command twice in succession, both event databases are initialized. If you want to preserve the JP1 events already registered in the event database, use the `jevexport` command to output the event database in CSV format before you initialize the database.

For details on initializing an event database by using the `jevdbswitch` command, see *8.2 Initializing the event database*.

Format

```
jevdbswitch [-h event-server-name]
            [-f]
```

Required execution permission

In Windows: Administrators (If User Account Control (UAC) for Windows is enabled, you must execute the command from the administrator console.)

In UNIX: Superuser

Command directory

In Windows:

installation-folder`\bin\`

In UNIX:

`/opt/jp1base/bin/`

Arguments

- `-h` *event-server-name*

Specify the event server on which to swap the event database in which events are actually registered from the active database to the standby database. If you omit this option, the logical host name set in the environment variable `JP1_HOSTNAME` is assumed as the event server name. If the environment variable `JP1_HOSTNAME` is not set, the event server name is assumed to be the same as the local host name. Specify the event server name as a character string of no more than 255 bytes.

- `-f`

  If you omit this option, a message asks if you are sure you want to execute the command. (The displayed message is `Is This OK?[Y/N]`.) Specify this option if user confirmation is unnecessary.

Return values

`0`	Normal end
`1`	Invalid argument
`2`	Insufficient execution permission
`3`	I/O error
`4`	Insufficient memory
`5`	Undefined event server name
`8`	Unable to connect to the event service.
`9`	Unable to detect whether the event databases have been switched.
`255`	Other error

jevdef_distrib

Function

The `jevdef_distrib` command distributes event service definitions and adds them to a specified destination.

Format

```
jevdef_distrib {-f [distribution-definition-file-name] |
                 -e [distribution-definition-file-name] |
                 -l [distribution-definition-file-name]}
                [-h logical-host-name]
                [-n]
```

Required execution permission

In Windows: Administrators (If User Account Control (UAC) for Windows is enabled, you must execute the command from the administrator console.)

In UNIX: Superuser

Command directory

In Windows:

installation-folder`\bin\`

In UNIX:

`/opt/jp1base/bin/`

Arguments

■ `-f` [*distribution-definition-file-name*]

Specify the `-f` option to distribute definitions in the forwarding settings file (`forward`). If you have prepared a distribution definition file named `jev_forward.conf`, you can execute the command without specifying the file name. If you have prepared a distribution definition file with another name, specify the name of the file. You cannot specify a directory name. Create a distribution definition file for each forwarding settings file in the appropriate location, as described in *Distribution definition file* in *14. Definition Files*.

If you specify this option, regular expressions in the definition file on the distribution source host are checked for syntax errors. You can execute the `jevreload` command to perform a syntax check on the distribution destination host. The syntax check on the source host checks basic regular expressions (JP1-unique regular expressions in Windows). Therefore, if the destination host is set up to use extended regular expressions, use the `-n` option to suppress the syntax check on the source host.

- `-e` [*distribution-definition-file-name*]

  Specify the `-e` option to distribute definitions in the action definition file for event log trapping (`ntevent.conf`). If you have prepared a distribution definition file named `jev_ntevent.conf`, you can execute the command without specifying the file name. If you have prepared a distribution definition file with another name, specify the name of the file. You cannot specify a directory name. Create a distribution definition file for each forwarding settings file in the appropriate location, as described in *Distribution definition file* in *14. Definition Files*. This command distributes definitions only to Windows hosts.

  If the destination agent is a logical host, the action definition file for event log trapping is distributed. The action definition file is then reloaded onto the physical host (the primary host) of the distribution agent host.

- `-l` [*distribution-definition-file-name*]

  Specify the `-l` option to distribute definitions in the action definition file for log file trapping. If you have prepared a distribution definition file named `jev_logtrap.conf`, you can execute the command without specifying the file name. If you have prepared a distribution definition file with another name, specify the name of the file. You cannot specify a directory name. Create a distribution definition file for each forwarding settings file in the appropriate location, as described in *Distribution definition file* in *14. Definition Files*.

  If the destination agent is a logical host, the action definition file for log file trapping is distributed. The action definition file is then reloaded onto the physical host (the primary host) of the distribution agent host.

- `-h` *logical-host-name*

  Specify this option when executing the command on a logical host. If you omit this option, the host name set in the environment variable `JP1_HOSTNAME` is assumed. If the environment variable `JP1_HOSTNAME` is not set, the host name is assumed to be the same as the local host.

  If you specify the `-e` option, the action definition file for event log trapping specified on the physical host of the command-executing host (primary host) is distributed.

  If you specify the `-l` option, the action definition file for log file trapping specified on the physical host of the command-executing host (primary host) is distributed.

- `-n (valid when the -f option is specified)`

  If you want to disable syntax checking on the source host, specify this option. Because the regular expression specifications depend on the platform and the regular expression type (basic regular expression or extended regular expression), we recommend specifying this option in the following cases:

  - The distribution definition file for a forwarding settings file (`forward`) contains a regular expression, and the source platform differs from the destination platform.

- The destination host is specified to use extended regular expressions.

If you specify the `-e` or `-l` option, syntax is not checked on the source host. However, specifying the `-n` option with either of these two options does not produce an error.

If you specify this option when the event server is running on the destination, a reloading result is output as a command execution result. However, a syntax check on the source host is not performed. If the event server is not running on the destination, no filter condition error can be detected. In order to detect a filter condition error, the event server must be running on the destination. You can use the return value from the `jevdef_distrib` command to determine whether the event server is running.

Notes

- You can execute the `jevdef_distrib` command only from a host where JP1/IM - Central Console Version 7 or JP1/IM - Manager Version 8 or later is installed.
- If the manager host has a submanager running JP1/IM - Central Console Version 7 or JP1/IM - Manager Version 8 or later in a lower layer, you can also execute the `jevdef_distrib` command from the submanager. If you execute the `jevdef_distrib` command concurrently from both the manager host and the submanager, the definitions distributed last are valid.
- Definitions are distributed to the destinations specified in the distribution definition file.
- When the `jevdef_distrib` command is executed, the `jbsplugin` process (in Windows) or the `jbsplugin` daemon (in UNIX) must be running on destination hosts.
- If any of the destination hosts are not started when the `jevdef_distrib` command is executed, the command displays a message stating that it could not change definitions on those hosts. In such a case, ensure that the hosts are started and then redistribute the definitions.
- If definitions are already set on a destination host, the `jevdef_distrib` command first deletes the existing definitions before distributing definitions.
- If a host specified in the distribution definition file has not been defined in the JP1/IM configuration definition file, the `jevdef_distrib` command results in an error, distributing definitions to any host.
- If the same host is specified more than once in the distribution definition file, the `jevdef_distrib` command results in an error, without distributing definitions to any host.
- If the version of JP1/Base running on a destination host is 06-71 or earlier, the `jevdef_distrib` command does not distribute definitions to that host, and

proceeds to the next destination.

- If an error occurs on a destination host due to failed reloading, the command continues processing with the previous definitions being valid but it rewrites the definitions with the distributed definitions. You should re-execute the `jevdef_distrib` command for a host where reloading has failed.
- The host names and error messages for destination hosts that have caused an error are output to the standard error output.
- When you distribute definitions in the action definition file for log file or event log trapping, the `jevlogreload` or `jeveltreload` command is executed on the destination host. If trap processing is in progress, the system waits until the trap processing finishes before executing the reload command. If an event occurs while the `jevlogreload` or `jeveltreload` command is being executed, the event will be converted according to the newly loaded definitions after the reload command has finished.
- When you distribute definitions, do *not* change the attribute parameter values (`FILETYPE`, `HEADLINE`, `HEADSIZE`, and `RECTYPE`) of the definition file for log file trapping. Use the values specified at startup. If you modify any of these parameters and distribute the definitions, the definitions on destination hosts are updated but an error occurs when the `jevlogreload` command is executed.

Return values

`0`	Normal end
`1`	Invalid argument
`2`	The log-file trap management service or log-file trap management daemon is inactive.
`3`	An error occurred during acquisition of configuration definition information.
`4`	Insufficient system resource such as memory
`10`	The distribution definition file contains an error.
`11`	An error occurred during opening of the distribution definition file.
`12`	Error at the destination
`255`	Other error

jevdef_get

Function

You can use this command to collect event service definitions.

Format

```
jevdef_get {-f | -e | -l [action-definition-file-for-log-file-trapping]}
               [-h logical-host-name]
```

Required execution permission

In Windows: Administrators (If User Account Control (UAC) for Windows is enabled, you must execute the command from the administrator console.)

In UNIX: Superuser

Command directory

In Windows:

installation-folder`\bin\`

In UNIX:

`/opt/jp1base/bin/`

Arguments

- `-f`

Specify the `-f` option to collect definitions in the forwarding settings file (forward).

- `-e`

Specify the `-e` option to collect definitions in the action definition file for event log trapping (`ntevent.conf`). This command collects definitions only when the source host is running Windows.

If the target agent is a logical host, definitions are collected from an action definition file for event log trapping. This file is on the physical host (primary host) of the target agent host.

- `-l [`*action-definition-file-name*`]`

This argument enables you to collect definitions from an action definition file for log file trapping. If you have created an action definition file with an arbitrary name on the source host, specify the name of the file.

If the target agent is a logical host, definitions are collected from an action definition file for log file trapping. This file is on the physical host (primary host) of the target agent host.

- `-h` *logical-host-name*

  Specify this option when executing the command on a logical host. If you omit this option, the host name set in the environment variable `JP1_HOSTNAME` is assumed. If the environment variable `JP1_HOSTNAME` is not set, the host name is assumed to be the same as the local host.

Notes

- When the `jevdef_get` command is executed, the `jbsplugin` process (in Windows) or the `jbsplugin` daemon (in UNIX) must be running on source hosts.
- If the version of JP1/Base running on a source host is 06-71 or earlier, the `jevdef_get` command does not distribute definitions to that host, and proceeds to the next source host.
- If an error occurs on a collection source host, the command does not collect definitions from that host and proceeds to the next source host.
- The host names and error messages for source hosts that have caused an error are output to the standard error output.
- Each line of collected definition output is made up of no more than 1,023 bytes. If a line exceeds 1,023 bytes, it is not output.

Return values

`0`	Normal end
`1`	Invalid argument
`2`	The log-file trap management service or log-file trap management daemon is inactive.
`3`	An error occurred during acquisition of configuration definition information.
`4`	Insufficient system resource such as memory
`10`	Error at the collection source host
`255`	Other error

jeveltreload (Windows only)

Function

The `jeveltreload` command reloads the action definition file for event log trapping (`ntevent.conf`).

Format

```
jeveltreload
```

Required execution permission

Administrators. (If User Account Control (UAC) for Windows is enabled, you must execute the command from the administrator console.)

Command directory

installation-folder`\bin\`

Notes

- If the command is executed while trapping is in progress, the command waits until trapping is completed before reloading the file.
- If you change the `server` parameter, you must restart the event-log trapping service. If you execute this command without restarting the service, an error occurs and the action definition file cannot be reloaded.

Return values

`0`	Normal end
`1`	Invalid arguments
`2`	The service is inactive.
`3`	The action definition file contains a syntax error.
`4`	An error occurred during opening of the action definition file.
`5`	Insufficient system resource such as memory
`6`	Permission check error
`255`	Other error

jevexport

Function

The `jevexport` command outputs the event database to a CSV file.

Format

```
jevexport [-h event-server-name]
          [-i event-database-file-name]
          [-o output-file-name]
          [-f filter-file-name]
          [-t {ON | OFF}]
          [-k items-file-name]
          [-a]
```

Required execution permission

In Windows: None.

In UNIX: None.

Command directory

In Windows:

installation-folder`\bin\`

In UNIX:

`/opt/jp1base/bin/`

Arguments

- `-h` *event-server-name*

  Specify an event server name to be output to a CSV file. If you omit this option, the logical host name set in the environment variable `JP1_HOSTNAME` is assumed as the event server name. If the environment variable `JP1_HOSTNAME` is not set, the event server name is assumed to be the same as the local host name. Specify the event server name as a character string of no more than 255 bytes.

  You cannot specify this option with the `-i` option.

- `-i` *event-database-file-name*

  Specify an event database file name to be output to a CSV file. You can specify the file name of an event database backed up by an OS backup command or the `jevdbinit` command. If you omit the path, the current directory is assumed.

  You cannot specify this option with the `-h` option.

- `-o` *output-file-name*

  Specify a CSV file name by a character string that is no more than 255 bytes. If you specify an existing file, the event database contents will replace the data in that file. If you omit this option, the contents are output to a file named `imevexport.csv` in the current directory. JP1 events are output in date order, starting from the oldest.

- `-f` *filter-file-name*

  Specify a text file that contains the conditions for outputting selected JP1 events registered in the event database. The text file name must be no more than 255 bytes. In a filter file, you can specify each filter in the same format used for an event filter. For details, see *Event filter syntax* in *14. Definition Files*. If you omit this option, all JP1 events registered in the event database will be output to the CSV file.

  Note

  > If the locale (for example, specified for the environment variable `LANG`) when executing the `jevexport` command differs from the character code used for character strings specified as conditions for JP1 events, no JP1 events are output to the CSV file.

- `-t {ON | OFF}`

  Specify `ON` to convert the time notation from the number of seconds since UTC 1970-01-01 00:00:00 to *YYYYMMDDhhmmss* format. This applies to the registration time and arrival time of JP1 events, and the `START_TIME` and `END_TIME` (common information of extended attributes). Specify `OFF` if you do not want to convert the time notation. If you omit this option, operation is the same as specifying `OFF`.

- `-k` *items-file-name*

  Specify a text file that contains the names of the extended attributes (program-specific information) to be output to the CSV file. The text file name must be no more than 255 bytes. When the `-k` option is specified, the command outputs only the extended attributes (program-specific information) from the event database that are written in the items file. All program-specific information is output to CSV files by default. All the shared information items for basic attributes and extended attributes are output.

  The coding conventions are as follows:

  - Write the names of the program-specific information that you want to output to a CSV file, starting from the beginning of the file (byte 1).
  - Either omit the program-specific items that you do not want to output, or comment them out (write a # at the start of the line).
  - Write an @ prefix before the names of program-specific items expressed in number of seconds since UTC 1970-01-01 00:00:00.

    This converts them into *YYYYMMDDhhmmss* format.

If no value is specified for a program-specific item, and the item's name has the prefix `@`, the name is converted to the year format, assuming `0`. For example, the value `TZ=JST-9` is converted to `19700101090000`.

The following examples illustrate these conventions for writing an items file.

```
AAA    <-  No time conversion
@BBB   <-  Convert to YYYYMMDDhhmmss format.
#CCC   <-  Comment line
```

- `-a`

Specify this option to output the title names of the basic attribute and extended attribute as header lines at the top of the CSV file. As the program-specific information in the extended attributes is output as pairs of attribute names and values, the extended attribute name is output as a title for the first pair only and is omitted thereafter.

Notes

- If a space appears in the output file name, filter file name, or items file name, enclose the file name in double quotation marks (`"`).
- If the event database is switched while this command is running, the command immediately stops CSV output and outputs a message. In such a case, the output information in the CSV file is not guaranteed. You can re-execute the command to output valid information.
- The command guarantees CSV output as much as the size of the event database specified in the event server setting file (`conf`). If you want to save all event information, you should periodically use the `-f` option to execute a filter file containing the `WITHIN` comparison keyword or other keywords before the event database is switched. For details on the event database size, see *Event server settings file* in *14. Definition Files*.
- When you use this command to output events in JP1/SES format to a CSV file, events that include double quotation marks might be incorrectly converted, since events in JP1/SES format do not have the code set.
- The event ID is output in CSV format as a hexadecimal number. Your spreadsheet software might display an event ID in exponential format if it matches a exponential representation (for example, `000020E0`). You can view the event ID in text format by opening the file as plain text.
- If you output a corrupted event database to the CSV file, the uncorrupted data will be output normally, but message `KAJP1765-W` will be output for the corrupted records.

Return values

`0`	Normal end

1	Invalid argument
2	Output to a CSV file was canceled during processing of the command.
3	A corrupted record was detected in the event database.
255	Other error

Example

The following shows some examples of use.

From the event database named Service, extract only the JP1 events that match the filter conditions written in the file filter.txt, convert the program-specific information specified in the file conf.txt into CSV format, and output the data to the file csvconv.csv.

```
jevexport -h Service -o csvconv.csv -f filter.txt -k conf.txt
```

jevlogdstart (UNIX only)

Function

The `jevlogdstart` command starts the log-file trap management daemon.

Format

```
jevlogdstart
```

Required execution permission

Superuser

Command directory

```
/opt/jp1base/bin/
```

Return values

`0`	Normal end
`255`	Abnormal end

jevlogdstop (UNIX only)

Function

The `jevlogdstop` command stops the log-file trap management daemon.

Format

```
jevlogdstop
```

Required execution permission

Superuser

Command directory

`/opt/jp1base/bin/`

Note

The log-file trap management daemon runs on both the logical and physical hosts. Executing this command disables the log-file traps. Therefore, before executing this command, make sure that the log file trapping is not active on the logical or any of the physical hosts.

Return values

`0`	Normal end
`1`	Invalid argument
`2`	The log-file trap management daemon is inactive.
`255`	Other error

jevlogreload

Function

The `jevlogreload` command reloads the action definition file for log file trapping. This command can only reload the values of the `MARKSTR` and `ACTDEF` parameters in the action definition file you specify with the `jevlogstart` command upon startup.

Format

`jevlogreload` {*ID-number*|`-a` *monitoring-target-name* | `ALL` }

Required execution permission

In Windows: Administrators (If User Account Control (UAC) for Windows is enabled, you must execute the command from the administrator console.)

In UNIX: Superuser

Command directory

In Windows:

installation-folder`\bin\`

In UNIX:

`/opt/jp1base/bin/`

Arguments

ID-number

Specify the ID number of the log file trap that you want to reload. Process IDs are output to the standard output at execution of the `jevlogstart` command.

- `-a` *monitoring-target-name*

  Specify the monitoring target name of the log file trap that you want to reload. You must use the `-a` option of the `jevlogstart` command to specify the monitoring target name.

- `ALL`

  Reloads all log file traps started by the `jevlogstart` command.

Note

If you specify a value different from that specified upon startup for any parameter other than `MARKSTR` and `ACTDEF`, the command fails to reload the file and results in an error. If you want to modify a parameter other than `MARKSTR` and `ACTDEF`, restart the log file trapping. If the command is executed while trapping is in progress, the command waits until trapping is completed before reloading the file.

Return values

`0`	Normal end
`1`	Invalid argument
`2`	The log-file trap management service or log-file trap management daemon is inactive.
`3`	No log file trap with the specified ID or monitoring target name exists (the trap has already stopped). No log file traps exist (when `ALL` is specified).
`4`	The action definition file contains an error.
`5`	An error occurred during opening of the action definition file.
`6`	Insufficient system resource such as memory
`7`	The event server is inactive.
`8`	Permission check error
`10`	Reload failed partially.
`255`	Other error

jevlogstart

Function

The `jevlogstart` command starts the log file trapping. This command searches the specified log file for lines that satisfy the conditions specified in the action definition file for log file trapping. It converts each of the matched lines into a JP1 event, and then registers each event in the event server. Before executing this command, you must create an action definition file for log file trapping.

Log files that use different output data formats cannot be handled together by the log file trapping function. In such a case, execute the log file trapping function for each individual log file.

Format

```
jevlogstart [-f action-definition-file-for-log-file-trapping]
            [-t file-monitoring-interval-in-seconds]
            [-m data-size-for-conversion-in-bytes]
            [-h]
            [-n display-command-name-for-UNIX only]
            [-p log-data-source-program-name]
            [-r]
            [-s destination-event-server-name]
            [-a monitoring-target-name]
            log-file-name1 [...log-file-name32(100)]
```

Required execution permission

In Windows: Administrators (If User Account Control (UAC) for Windows is enabled, you must execute the command from the administrator console.)

In UNIX: Superuser

Command directory

In Windows:

installation-folder`\bin\`

In UNIX:

`/opt/jp1base/bin/`

Arguments

■ `-f` *action-definition-file-name*

Specify the name of the action definition file for log file trapping in no more than 256 bytes. If you specify a relative path, make sure that the full path when the directory name is added will not exceed 256 bytes. Specify a path relative to the current directory where you execute the command. You can omit this option if you have already created a `jevlog.conf` file in the `conf` folder, and have specified the action definitions in that file.

The `jevlog.conf` file resides in the following directory.

In Windows:

installation-folder`\conf\`

In UNIX:

```
/etc/opt/jp1base/conf/
```

- `-t` *file-monitoring-interval* (in seconds)

Specify the interval for monitoring the log file. The specifiable range is 1 to 86,400 seconds (24 hours). If you omit this option, the default is 10.

Monitoring a log file in `WRAP1`, `WRAP2`, or `HTRACE` format

If the wrap-around frequency is too high or if the monitoring interval is too long, the file might be overwritten before the log file trap reads the data and some entries might be missed. To prevent entries from being missed, use the following equation to estimate the monitoring interval:

log-file-size (bytes) x *number-of-log-files* > *output-size-per-second* (bytes) x *monitoring-interval* (seconds)

- `-m` *data-size-for-conversion* (in bytes)

Specify how much data is to be converted into a JP1 event each time a specified log file is read. Specify the number of bytes (1 to 1,024) from the start of a line. The end-of-line character is converted into an end-of-line symbol (`\0`). This symbol is included in the specified data size. If a line read from a log file exceeds the specified number of bytes, the size of the converted data equals the number of bytes specified by `-m`, minus one byte.

The value specified in this option indicates the valid range of a line of data in the input log files. Thus, for regular expressions specified in the `MARKSTR` and `ACTDEF` parameters in the action definition file for log file trapping, the system check applies only to the regular expressions that are within the range specified in the `-m` option. Regular expressions that select columns outside this range are not checked. If you omit this option, the default is 512. The end-of-line character is converted into an end-of-line symbol (`\0`).

- `-h`

Specify this option to read the log from the start of the file. If you execute the `jevlogstart` command after the program has started, the log already output by the program will not be read. By specifying the `-h` option, however, you can read the log data from the start of the file. If the log file is a wrap-around file, the trapping service first reads all the log data from the start of the file to the end of the file (EOF), and then finds the current pointer and reads the latest data.

■ `-n` *display-command-name* (for UNIX only)

This option is available for UNIX only.

Specify the display name of the command for the log file trapping. The command name specified in this option is displayed in the result of the `ps` command. Specify the command name in no more than 256 bytes. If you omit this option, *log-file-name*`1` is assumed as the display command name.

■ `-p` *log-data-source-program-name*

Specify the name of the program that outputs the log data. This name will appear in the Event Console window of JP1/IM - View.

The program name is shown as follows.

In Windows:

`/HITACHI/JP1/NT_LOGTRAP/`*log-data-source-program-name*

In UNIX:

`/HITACHI/JP1/UX_LOGTRAP/`*log-data-source-program-name*

If you omit this option, the program name is shown as `/HITACHI/JP1/NT_LOGTRAP` (in a Windows system) or `/HITACHI/JP1/UX_LOGTRAP` (in a UNIX system).

■ `-r`

When the `-r` option is specified, if a specified log file does not exist when the log file trapping starts, the system keeps trying to access the file, according to the interval specified in the `-t` option, until the file is created. When file open processing succeeds, the trapping service starts searching the log data.

When the `-r` option is omitted, the log file trapping cancels access and terminates the processing if a specified log file does not exist when the log file trapping starts.

■ `-s` *destination-server-name*

Specify this option to change the destination server for JP1 event registration to the server specified here. Only an event server running on the local host can be specified. If you omit this option, the local host name is assumed as the event server name (host name returned by the `hostname` command). Specify a destination server name in no more than 255 bytes. Specify the destination server name in no more than 255 bytes.

This option is primarily for use in a cluster system.

If an event service on a physical host starts with FQDN in an environment with a short name for the local host name, you can use this option to explicitly specify the event server name in the FQDN format.

- `-a` *monitoring-target-name*

  Specify a monitoring target name as an alias for the ID number. You can enter a character string that is no more than 30 bytes for the target name. You can use alphanumeric characters, hyphens, and underscores for the target name. However, the name must start with an alphanumeric character. Event server names are case sensitive.

- *log-file-name*`1[...`*log-file-name*`32(100)]`

  Specify each name of the monitored log file in no more than 256 bytes. If you specify a relative path, make sure that the full path when the directory name is added will not exceed 256 bytes. Specify a path relative to the current directory where you execute the command. A log file name cannot start with hyphen (`-`).

  You can specify no more than 32 log files in a Windows system, or 100 for UNIX. Remember that since the number of files that can be accessed concurrently is system-dependent, the maximum number of files that can be actually specified might be fewer than 32 (or 100) in some cases. In a UNIX system, one process is required for monitoring one log file. Therefore, the `ps` command lists the command names in the form *log-file-name*`.child`.

  Some types of log files cannot be monitored. For details on the formats of log files that can or cannot be monitored, see *1.5.1 (1) Types of log files that can be monitored*.

Notes

- Start the log file trapping before you start the program that outputs the log you want to monitor. Trapping will not be performed correctly if the trapping is started while data is already being output to the specified log file. If you wish to specify a log file that does not yet exist, use the `-r` option to keep the log file trapping waiting for the file.
- Before executing the `jevlogstart` command, ensure that the log-file trap management service (in Windows) or log-file trap management daemon (in UNIX) is running.

Return values

`0`	Normal end
`1`	Invalid argument
`2`	The log-file trap management service or log-file trap management daemon is inactive.
`3`	The event service is inactive.
`4`	A monitoring target with the same name has already been started (output only when the `-a` option is specified).

255	Other error

The jevlogstart command outputs an ID number to the standard output. The ID number is required to stop log file trapping.

Example

These examples are for Windows.

Example 1

Search for and read data from log file c:\log\logfile1.log. Use the defaults for all arguments except the log file name. The action definition file for log file trapping is jevlog.conf in the JP1/Base conf folder, the monitoring interval is 10 seconds, and the data size for event conversion is 512 bytes.

```
jevlogstart c:\log\logfile1.log
```

Example 2

Search for and read data from log file c:\log\logfile1.log, using the action definition file for log file trapping c:\conf\configfile.conf.

```
jevlogstart -f c:\conf\configfile.conf c:\log\logfile1.log
```

Example 3

Search for and read data from log files c:\log\logfile1.log and c:\log\logfile2.log, using a monitoring interval of 5 seconds.

```
jevlogstart -t 5 c:\log\logfile1.log c:\log\logfile2.log
```

jevlogstat

Function

The `jevlogstat` command shows the operating status of log file trapping. This command returns the operating state of the log file trap that has the ID number or monitoring target name specified in the command argument.

Format

`jevlogstat {`ID-*number*`|-a` *monitoring-target-name* `| ALL }`

Required execution permission

In Windows: Administrators (If User Account Control (UAC) for Windows is enabled, you must execute the command from the administrator console.)

In UNIX: Superuser

Command directory

In Windows:

installation-folder`\bin\`

In UNIX:

`/opt/jp1base/bin/`

Arguments

- *ID-number*

Specify the ID number of the log file trap that you want to check. Process IDs are output to the standard output at execution of the `jevlogstart` command.

- `-a` *monitoring-target-name*

Specify the monitoring target name of the log file trap that you want to check. You must use the `-a` option of the `jevlogstart` command to specify the monitoring target name.

- `ALL`

This argument enables you to show the IDs for all the log file traps triggered by the `jevlogstart` command. If you specify a monitoring target name for a trap, the trap ID and the monitoring target name are shown.

Return values

`0`	The specified log file trap is active. If `ALL` is specified, at least one active log file trap is active.

`1`	Invalid argument
`2`	The log-file trap management service or log-file trap management daemon is inactive.
`3`	No log file trap with the specified ID exists (the trap has already stopped).
`255`	Other error

jevlogstop

Function

The `jevlogstop` command stops the log file trapping.

Format

`jevlogstop [-w] {` *ID-number* `| -a` *monitoring-target-name* `| ALL }`

Required execution permission

In Windows: Administrators (If User Account Control (UAC) for Windows is enabled, you must execute the command from the administrator console.)

In UNIX: Superuser

Command directory

In Windows:

installation-folder`\bin\`

In UNIX:

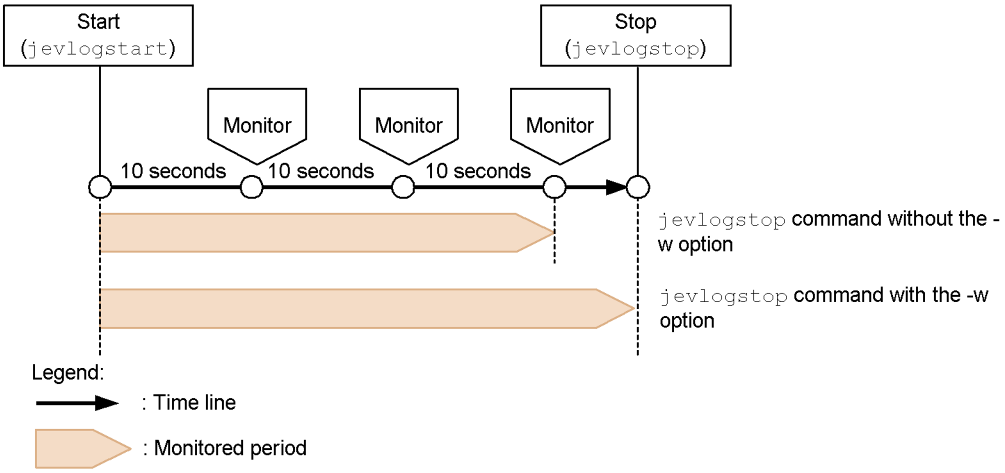
`/opt/jp1base/bin/`

Arguments

- `-w`

This option enables log data to be forcibly read before log file trapping stops, regardless of the monitoring interval. Monitoring continues until the time when the `jevlogstop` command is executed. If you omit this option, the log data output between the last monitoring and `jevlogstop` command execution is not monitored. The following figure shows how the stop timing differs depending on whether this option is specified.

Figure 13-2: Stop timing options for log file monitoring



This command might take a long time to complete, depending on the amount of log data to be read and the number of JP1 events held during retry processing. Take care when using this option to stop log file trapping at failover in a cluster system.

■ *ID-number*

Specify the ID number of the log file trap that you want to stop. Process IDs are output to the standard output at execution of the `jevlogstart` command.

■ `-a` *monitoring-target-name*

Specify the name of the log file trap monitoring target to be stopped. You must use the `-a` option of the `jevlogstart` command to specify the monitoring target name.

■ `ALL`

Stops all log file traps started by the `jevlogstart` command.

Return values

`0`	Normal end
`1`	Invalid argument
`2`	The log-file trap management service or log-file trap management daemon is inactive.
`3`	No log file trap with the specified ID or monitoring target name exists (the trap has already stopped). No log file traps exist (when `ALL` is specified).
`255`	Other error

jevregsvc (Windows only)

Function

For the following cases, this command is used to add or delete an event server service in a Windows environment:

- When using a cluster system#
- When a logical host is used in a non-cluster environment#
- When configuring an event server on a system using DNS

#: Because the `jp1bshasetup` command automatically executes this command, there is no need to execute it manually.

Format

```
jevregsvc -r [event-server-name]
jevregsvc -u [event-server-name]
```

Required execution permission

Administrators. (If User Account Control (UAC) for Windows is enabled, you must execute the command from the administrator console.)

Command directory

installation-folder`\bin\`

Arguments

- `-r` *event-server-name*

Adds the service provided by the event server. When no event server name is specified, the local host name is assumed.

- `-u` *event-server-name*

Deletes the service provided by the event server. When no event server name is specified, the local host name is assumed.

Note

Make sure that the event server name exactly matches the name specified in the event server index file, including the case of the characters.

Return values

`0`	Normal end
`1`	Invalid argument

255	Other error

jevreload

Function

The `jevreload` command reloads the forwarding settings file (`forward`).

Format

```
jevreload [-h event-server-name]
```

Required execution permission

In Windows: Administrators (If User Account Control (UAC) for Windows is enabled, you must execute the command from the administrator console.)

In UNIX: Superuser

Command directory

In Windows:

installation-folder`\bin\`

In UNIX:

`/opt/jp1base/bin/`

Arguments

- `-h` *event-server-name*

Specify the name of the event server on which you want to reload the forwarding settings file (`forward`). If you omit this option, the logical host name set in the environment variable `JP1_HOSTNAME` is assumed as the event server name. If the environment variable `JP1_HOSTNAME` is not set, the event server name is assumed to be the same as the local host name. Specify the event server name as a character string of no more than 255 bytes.

Return values

`0`	Normal end
`1`	Invalid argument
`2`	The specified event server has not started.
`3`	The forwarding settings file contains an error.
`255`	Other error

Example

The following shows some examples of use.

Reload the forwarding settings file (`forward`) on event server `evserver1`.

```
jevreload -h evserver1
```

jevsend

Function

The `jevsend` command registers a JP1 event in an event server.

Format

```
jevsend [-i event-ID]
          [-m message]
          [[-e extended-attribute-name=extended-attribute-value]...]
          [-d destination-event-server-name]
          [-s source-event-server-name]
```

Required execution permission

In Windows: None.

In UNIX: None.

Command directory

In Windows:

installation-folder`\bin\`

In UNIX:

`/opt/jp1base/bin/`

Arguments

■ `-i` *event-ID*

Specify the event ID of the JP1 event to be registered. The specifiable range is `0` to `1FFF`, and `7FFF8000` to `7FFFFFFF`. If you omit this option, the default is 0.

■ `-m` *message*

Specify the message text of the JP1 event to be registered. The length of the message text can be no more than 1,023 bytes.

■ `-e` *extended-attribute-name=extended-attribute-value*

Specify the extended attributes of the JP1 event to be registered. Specify the attributes in separate lines, in the form `-e` *extended-attribute-name=extended-attribute-value*. Do not insert a blank (such as a space or tab character) between the equals sign and extended attribute value. Extended attributes are a set of no more than 100 of the following items. The total length of all the attribute values must not exceed 10,000 bytes.

Extended attribute	Contents	Format
Extended attribute name	Name that expresses the attribute meaning.	Character string of no more than 32 bytes, consisting of alphanumeric characters, and underscores (first character an alphabetic character; all characters upper case)
Extended attribute value	Contents of the attribute	Character string (0 to 10,000 bytes)

JP1 events with `SEVERITY` specified as an extended attribute name are listed in the Event Console window of JP1/IM - View. For the `SEVERITY` extended attribute, specify one of the values listed in *15.1.2 Extended attributes*. Be sure to write the first character in upper case.

- `-d` *destination-event-server-name*

Specify an event server name if you want to send the JP1 event to a different event server than the server specified in the forwarding settings file (`forward`). Specify the event server name as a character string of no more than 255 bytes.

Notes

- No error occurs if the specified event server is undefined, inactive, or unreachable due to a network failure.
- A JP1 event forwarded with this option specified cannot be acquired from the event server of the local host.
- When the event server of a remote host is specified in this option, the retry setting in the `forward-limit` parameter in the event server settings file (`conf`) does not apply to event forwarding.

- `-s` *source-event-server-name*

When the `-d` option is specified, this option sets the event server to be used for forwarding the event. When the `-d` option is omitted, this option sets the event server for registering the event. You can only specify an event server that runs on the local host. If you omit this option, the logical host name set in the environment variable `JP1_HOSTNAME` is assumed as the event server name. If the environment variable `JP1_HOSTNAME` is not set, the event server name is assumed to be the same as the local host name. Specify the event server name as a character string of no more than 255 bytes.

This option is primarily for use in a cluster system.

Notes

- Insert one or more spaces between each option and its value.

- If you want to enter one or more spaces in a message text or extended attribute value, enclose the text or value in double quotation marks (").
- The number of bytes that can be specified in the command options is system-dependent. Set the length within the limits of the OS.

Return values

0	Normal end
1	Invalid argument
255	Other error

Example

Example 1

Register the JP1 event that has the event ID 111, and that outputs a message reading "BaseEvent_Sample."

```
jevsend -m BaseEvent_Sample -i 111
```

Example 2

Register the JP1 event that has the event ID 111, and that has extended attribute name EXTATTR and extended attribute value Extend Value.

```
jevsend -i 111 -e EXTATTR="Extend Value"
```

Example 3

Register the JP1 event that has the following extended attributes:

- Extended attribute name EXTATTR and extended attribute value extattr
- Extended attribute name INCLUDESPACE and extended attribute value include space

```
jevsend -e EXTATTR=extattr -e INCLUDESPACE="include space"
```

Example 4

Register the JP1 event that has the event ID 111, and that has the extended attribute name SEVERITY and extended attribute value Information.

```
jevsend -i 111 -e SEVERITY=Information
```

jevsendd

Function

The `jevsendd` command registers the JP1 events to the event server and checks whether the registration was successful. Even if a JP1 event is not registered when an event service is running, you can still use this command to check whether the event is registered.

Format

```
jevsendd [-i event-ID]
          [-m message]
          [[-e extended-attribute-name=extended-attribute-value]...]
         -d destination-event-server-name
         [-s source-event-server-name]
         [-f initial-polling-interval-in-seconds]
         [-p polling-interval-in-seconds]
         [-t checking-times]
```

Required execution permission

In Windows: None.

In UNIX: None.

Command directory

In Windows:

installation-folder`\bin\`

In UNIX:

`/opt/jp1base/bin/`

Arguments

- `-i` *event-ID*

  Specify the event ID of the JP1 event to be registered. The specifiable range is `0` to `1FFF`, and `7FFF8000` to `7FFFFFFF`. If you omit this option, the default is 0.

- `-m` *message*

  Specify the message text of the JP1 event to be registered. The length of the message text can be no more than 1,023 bytes.

- `-e` *extended-attribute-name=extended-attribute-value*

  Specify the extended attributes of the JP1 event to be registered. Specify the attributes in separate lines, in the form `-e` *extended-attribute-name=extended-attribute-value*. Do not insert a blank (such as a space or tab character) between the equals sign and extended attribute value. Extended attributes are a set of no more than 100 of the following items. The total length of all the attribute values must not exceed 10,000 bytes.

Extended attribute	Contents	Format
Extended attribute name	Name that expresses the attribute meaning.	Character string of no more than 32 bytes, consisting of alphanumeric characters, and underscores (first character an alphabetic character; all characters upper case)
Extended attribute value	Contents of the attribute	Character string (0 to 10,000 bytes)

JP1 events with `SEVERITY` specified as an extended attribute name are listed in the Event Console window of JP1/IM - View. For the `SEVERITY` extended attribute, specify one of the values listed in *15.1.2 Extended attributes*. Be sure to write the first character in upper case.

- `-d` *destination-event-server-name*

Specify the name of the destination event server. Specify the event server name as a character string of no more than 255 bytes.

Notes

- A JP1 event forwarded with this option specified cannot be acquired from the event server of the local host.
- When the event server of a remote host is specified in this option, the retry setting in the `forward-limit` parameter in the event server settings file (`conf`) does not apply to event forwarding.

- `-s` *source-event-server-name*

Specify the name of the event server to be used for forwarding the event. You can only specify an event server that runs on the local host. If you omit this option, the logical host name set in the environment variable `JP1_HOSTNAME` is assumed as the event server name. If the environment variable `JP1_HOSTNAME` is not set, the event server name is assumed to be the same as the local host name. Specify the event server name as a character string of no more than 255 bytes.

This option is primarily for use in a cluster system.

- `-f` *initial-polling-interval* (in seconds)

Specify the timeout for the first arrival verification after sending the JP1 event to the destination server, from 1 to 10 seconds. If you omit this option, the default is 3 seconds.

- `-p` *polling-interval* (in seconds)

  Specify the interval to the second and further arrival verifications if the JP1 event has not arrived by the first arrival verification, from 3 to 600 seconds. If you omit this option, the default is 10 seconds.

- `-t` *checking-times*

  Specify how many times to perform an arrival verification after the first verification, from 0 to 999 times. If you omit this option, the default is 0.

Notes

- Insert one or more spaces between each option and its value.
- If you want to enter one or more spaces in a message text or extended attribute value, enclose the text or value in double quotation marks (`"`).
- A double quotation mark (`"`) preceded with a backslash (`\"`) is interpreted as a double quotation mark.
- If the special characters shown below are to be included, enclose them in double quotation marks (`"`).

  `# ; | & ( ) ^ < >` space, and `/`or tab characters
- The number of bytes that can be specified in the command options is system-dependent. Set the length within the limits of the OS.
- This command does not return control until the arrival is verified or an error is detected.

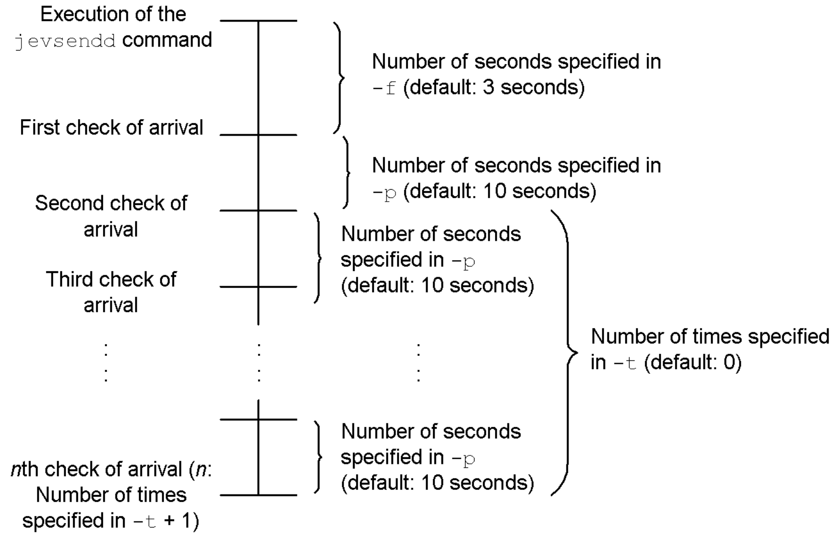
Return values

`0`	Normal end
`1`	Invalid argument
`2`	Processing is continuing (if the arrival cannot be verified within the maximum time for waiting for arrival).
`3`	Transfer failed
`255`	Other error

- Further explanation

  The following figure shows the flow of processing with the `-f`, `-p`, and `-t` options specified.

Figure 13-3: Behavior when the -f, -p, and -t options are specified


Execution of the jevsendd command
First check of arrival
Second check of arrival
Third check of arrival
nth check of arrival (n: Number of times specified in -t + 1)
Number of seconds specified in -f (default: 3 seconds)
Number of seconds specified in -p (default: 10 seconds)
Number of seconds specified in -p (default: 10 seconds)
Number of seconds specified in -p (default: 10 seconds)
Number of times specified in -t (default: 0)

You can use the following expression to obtain the maximum time for waiting for arrival:
Maximum-time-for-waiting-for-arrival =
(*number-of-seconds-specified-in--*f*-option*) +
(*number-of-seconds-specified-in--*p*-option*) x
(*number-of-times-specified-in--*t*-option*)

If the command cannot check the arrival within the maximum time, it outputs an error message and terminates.

jevstart (UNIX only)

Function

The `jevstart` command enables you to manually start an event server.

Format

```
jevstart [event-server-name]
```

Required execution permission

Superuser

Command directory

`/opt/jp1base/bin/`

Arguments

- *event-server-name*

Specify the event server to be started. When no event server is specified, the event server name is assumed to be that of the local host.

Return values

`0`	Normal end
`255`	Abnormal end

jevstat

Function

The `jevstat` command enables you to check the operating status of event service processes (`jevservice`). For details on event service processes, see *B. List of Processes*.

Format

```
jevstat [event-server-name]
          [-t timeout-in-seconds]
```

Required execution permission

In Windows: Administrators (If User Account Control (UAC) for Windows is enabled, you must execute the command from the administrator console.)

In UNIX: Superuser

Command directory

In Windows:

installation-folder`\bin\`

In UNIX:

`/opt/jp1base/bin/`

Arguments

■ *event-server-name*

Specify the event server name at which to check whether event service processes have started or stopped in, for example, the cluster system. Event server names are case sensitive. If you omit this option, the host name set in the environment variable `JP1_HOSTNAME` is assumed. If the environment variable `JP1_HOSTNAME` is not set, the physical host name is assumed. Specify the event server name as a character string of no more than 255 bytes.

■ `-t` *timeout* (in-seconds)

Specify how long the system should wait for the `jevstat` command to complete execution. The specifiable range is 1 to 32,767. If the `jevstat` command does not complete execution within the specified time, execution is assumed to have failed. The default is 60 seconds.

Notes

- If a `jevstat` command is executed immediately after an event service starts, the following error message might be output: KAJP1706-E A connection to the event server cannot be established. In such a case, execute the jevstat command a few seconds after the event service starts.

- If the jevstat command is executed and the following message is output to an integrated trace log, the command might have timed out: KAJP1775-E An attempt to send or receive communication data has failed. (maintenance information). Re-execute the jevstat command, specifying how long to wait for the command to complete execution in the -t option.

Return values

0	All processes are active.
1	Abnormal termination (command processing error)
4	Some processes are active.
8	All of the child processes have stopped.
12	Abnormal termination (error returned by the event server)

Further explanation

When using JP1/Base in a cluster system on UNIX, you can use the jevstat command in the abnormality detection script of the logical host. In this case, you should be aware that the names of the event server to be run on the logical host are case sensitive and must be specified accordingly. Refer to the event server index file (index) in which the event server names for the logical host are defined as you specify them.

The following shows a definition example of the event server index file (index), and the execution result of the jevstat command run using the index file.

Definition example of the event server index file (index)

```
server * default
server HOSTZZ /jp1/share/
```

Examples of jevstat commands and their results:

jevstat command execution examples	Execution results
jevstat	Outputs the status of the event server on the physical host.
jevstat hostzz	Outputs an error message indicating that the specified event server name was not found.
jevstat HOSTZZ	Outputs the status of the event server on the logical host.

Example

Examples of the `jevstat` command for Windows and UNIX are shown below.

In Windows:

```
E:\>jevstat
KAJP1771-I Processing to report the status of the event
service HOST1 will now start.
Display the running processes
process name        process ID
jevservice        1234
KAJP1772-I All the processes are running.
```

In UNIX:

```
$ /opt/jp1base/bin/jevstat
KAJP1771-I Processing to report the status of the event
service HOST1 will now start.
Display the running processes
process name        process ID
jevservice        2098
KAJP1772-I All the processes are running.
```

`KAJP1772-I` is a message shown when all the necessary processes for the event server have been started.

jevstop (UNIX only)

Function

The `jevstop` command enables you to manually stop an event server.

Format

```
jevstop [event-server-name]
```

Required execution permission

Superuser

Command directory

```
/opt/jp1base/bin/
```

Arguments

- *event-server-name*

Specify the event server to be started. When no event server is specified, the event server name is assumed to be that of the local host.

Return values

`0`	Normal end
`255`	Abnormal end

Jischk

Function

The `Jischk` command checks the logical structure of ISAM files. The command displays messages if the files have errors. Based on the specified level, the command checks the contents and relationship of the constituent files in the ISAM files.

In UNIX, if the key file is invalid, this command can output key definition parameters indicating key information. By using these parameters, you can use the `Jiskeymnt` command to reorganize the key file.

Format

In Windows:

`Jischk [-l` *level*`]` *file-names* `...`

In UNIX:

`Jischk [-l` *level*`][-p]` *file-names* `...`

Required execution permission

In Windows: Administrators (If User Account Control (UAC) for Windows is enabled, you must execute the command from the administrator console.)

In UNIX: Superuser

Command directory

In Windows:

installation-folder`\bin\`

In UNIX:

`/opt/jp1base/bin/`

Arguments

- `-l` *level*

Specify the level for checking the specified files. Specifying a larger value in this option performs a more detailed (and longer) check.

`1`

In Windows, the command checks only the key file.

In UNIX, the command checks the key definition file and the key file.

`2`

In Windows, the command checks the key file, as well as the relationship between the key file and the data file.

In UNIX, the command checks the key definition file and the key file, as well as the relationship between the key file and data file.

`3`

The command checks the following items:

- Key definition file (in UNIX only)
- Key file
- Relationship between the key file and the data file
- Structure of the data file
- Number of records

If you omit the `-l` option, 1 is assumed.

- `-p`

Specify this option to output the key definition parameters for the `Jiskeymnt` command (adding, deleting or reorganizing keys) if the key file is invalid. This option is available for UNIX only.

- *file-name*

Specify one or more files you want to check. If you do not specify the full path name of a file, the command assumes that the file is located in the current directory at the current drive. When you specify more than one file name, use at least one space to separate each file name. You can also use the wildcard character (`*`) to specify files. In Windows, if you want to specify a file name that includes spaces, enclose the file name in double quotation marks (`"`).

Example:

The following shows examples in Windows.

- Specify all the files in the `c:\data` directory.

```
Jischk -l3 c:\data\*
```

- Specify the file names beginning with `SAMPLE` in the `c:\data` directory.

```
Jischk -l3 c:\data\SAMPLE*
```

Notes

- The command immediately stops if an I/O error occurs or a specified file does not exist even when the command has processed some files.
- In Windows, if you want to redirect the check result to a text file, specify the destination file name after >. The following shows an example.

Example:

```
Jischk -l3 sample > chk.txt
```

Return values

`0`	Normal end
`1`	Abnormal end
`2`	Abnormal end (returned if the file contains an inconsistency)

Jiscond

Function

The `Jiscond` command eliminates unnecessary area from the specified data files to compress them. This command also reorganizes the key file.

Updating records in data files or deleting records from data files increases the area size of the data files. This command eliminates unnecessary data from the data files to reduce the area for the data files. Also, this command extracts keys to reorganize the key file, based on the key information in the key definition file. If no keys are defined in the key file, this command does not reorganize the key file.

Format

In Windows:

`Jiscond [-r] [-d dir` *work-folder-name*`] [-k | -q]` *file-name*

In UNIX:

`Jiscond [-T dir` *work-directory-name*`] [-k | -q]` *file-name*

Required execution permission

In Windows: Administrators (If User Account Control (UAC) for Windows is enabled, you must execute the command from the administrator console.)

In UNIX: Superuser

Command directory

In Windows:

installation-folder`\bin\`

In UNIX:

`/opt/jp1base/bin/`

Arguments

- `-r`

Specify this option to display the compression rate of the data file and key file. When you specify this option, the file compression utility command outputs the execution result including the ratio (percentage) of the compressed file size to the uncompressed file size.

- `-d dir` *work-folder-name*

The work files is used to sort key entries during file compression. This means that you must specify the directory for the work files. If you omit this option, the directory specified in the `TEMP` environment variable, the `tmp` directory, or the current directory is used. This option can only be specified in Windows.

- `-T dir` *work-directory-name*

  The work files is used to sort key entries during file compression. This means that you must specify the directory for the work files. If you omit this option, the `/tmp` or `/usr/tmp` directory is used. This option is available for UNIX only.

- `-k`

  Specify the `-k` option to reorganize the ISAM file while preventing it from becoming too large. If JP1 is operating for a long time, the size of the key file, which provides indexes for the ISAM database, increases without limit. You must reorganize the ISAM file periodically. This argument prevents the key file from becoming too large.

- `-q`

  Specify the `-k` option to reorganize the ISAM file but cancel the setting for preventing it from becoming too large. If you want to use a previous version of JP1, you must disable any functionality not supported by that version. This argument enables previous versions of JP1 to access the ISAM file.

- *file-name*

  Specify one or more files you want to check. If you do not specify the full path name of a file, the command assumes that the file is located in the current directory at the current drive. In Windows, if you want to specify more than one file, use at least one space to separate each file name. If you want to specify a file name that includes spaces, enclose the file name in double quotation marks (`"`). You can also use the wildcard character (`*`) to specify files.

  Example:

  The following shows examples in Windows.

  - Specify all the files in the `c:\data` directory.

  ```
  Jiscond c:\data\*
  ```

  - Specify the file names beginning with `SAMPLE` in the `c:\data` directory.

  ```
  Jiscond c:\data\SAMPLE*
  ```

Notes

- This command creates work files for compressing files. Be careful when you compress a large file because this command creates a copy of the data file and then creates a key file.
- In Windows, the command immediately stops if an I/O error occurs or a specified file does not exist even when the command has already processed some files.

- In Windows, the command takes some time to display the result if you specify the `-r` option.
- Your system might contain an ISAM file created on a shared disk for the primary and secondary nodes that have version 06-71 or earlier of JP1/Base. If you want to specify the option that prevents the ISAM file from becoming too large, upgrade to JP1/Base Version 7 or later on both the primary and secondary nodes. Then, set this option for the ISAM file on the shared disk.
- In the system containing an ISAM file created on a shared disk for the primary and secondary nodes, you can set the option that prevents the ISAM file from becoming too large. If you want to change the version of JP1/Base back to 06-71 or earlier in such a system, first cancel this option. Then, change the version of JP1/Base on the primary node and then on the secondary node.

Return values

`0`	Normal end
`1`	Abnormal end

Jisconv

Function

The `Jisconv` command converts a sequential file into an ISAM file. The `Jisconv` command also converts an ISAM file into a sequential file.

When records from an ISAM file where an error occurred are extracted to a sequential file, you can use this command to restore the ISAM file from the sequential file.

■ Converting a sequential file into an ISAM file

Based on the information in the key definition file, this command converts a sequential file into an ISAM file. This command also creates the key file if keys are defined in the ISAM file. However, if no keys are defined in the ISAM file, this command does not create the key file.

The sequential file (before conversion) and the ISAM file (after conversion) must have the same record type. The following table shows the possible combinations of record types.

Table 13-3: Possible combinations of record types (when converting a sequential file into an ISAM file)

Sequential file (before conversion)	**ISAM file (after conversion)**	
	Fixed length	**Variable length**
Fixed length	Yes	No
Variable length	No	Yes

Legend:

Yes: Conversion is possible.

No: Conversion is impossible.

The command handles the record length as follows.

- When the command converts a fixed-length sequential file into a fixed-length ISAM file, the command assumes the following as the record length of the source file (sequential file): the record length defined in the key definition file for the destination file (ISAM file).
- When the command converts a variable-length sequential file into a variable-length ISAM file, the command uses the record length of each record in the source file. If the record length of the source file is not within the range of the record lengths defined in the key definition file for the destination file, the

command assumes that the source record length is incorrect, and stops the conversion.

Notes

Note the following when converting a sequential file into an ISAM file:

- You must create the ISAM file for the converted data in advance.
- The command uses work files when converting the data into an ISAM file.

■ Converting an ISAM file into a sequential file

This command converts an ISAM data file into a sequential file. The command outputs records to the destination file in the same order as the physical order of records in the source file. This command does not output the records that were deleted from the source file.

The ISAM file (before conversion) and the sequential file (after conversion) must have the same record type. The following table shows the possible combinations of record types.

Table 13-4: Possible combinations of record types (when converting an ISAM file into a sequential file)

ISAM file (before conversion)	Sequential file (after conversion)	
	Fixed length	Variable length
Fixed length	Yes	No
Variable length	No	Yes

Legend:

Yes: Conversion is possible.

No: Conversion is impossible.

The command handles the record length as follows.

- When the command converts a fixed-length ISAM file into a fixed-length sequential file, the command assumes the following as the record length of the source file (ISAM file): the record length defined in the key definition file for the destination file (sequential file).
- When the command converts a variable-length ISAM file into a variable-length sequential file, the command assumes the following as the minimum record length and maximum record length for the destination file: the minimum record length and maximum record length defined in the key definition file for the source file.

Format

In Windows:

```
Jisconv [-f] -t type [-d dir work-folder-name] file-name-1
file-name-2
```

In UNIX:

```
Jisconv -t type [-T dir work-directory-name] file-name-1 file-name-2
```

Required execution permission

In Windows: Administrators (If User Account Control (UAC) for Windows is enabled, you must execute the command from the administrator console.)

In UNIX: Superuser

Command directory

In Windows:

installation-folder`\bin\`

In UNIX:

`/opt/jp1base/bin/`

Arguments

- `-f`

Specify this option if you do not want to display an overwrite confirmation message that appears if the file specified in *file-name-2* already exists. This option can only be specified in Windows.

- `-t` *type*

In *type*, specify either of the following keywords:

`SI`

The `Jisconv` command converts a sequential file into an ISAM file.

`IS`

When you specify this keyword, the command converts from an ISAM file into a sequential file.

- `-d dir` *work-folder-name*

The work files is used to sort key entries when converting the sequential file into an ISAM file. This means that you must specify the directory for the work files. If you omit this option, the directory specified in the `TEMP` environment variable, the `tmp` directory, or the current directory is used. This option can only be specified in

Windows.

- `-T dir` *work-directory-name*

  The work files is used to sort key entries when converting the sequential file into an ISAM file. This means that you must specify the directory for the work files. If you omit this option, the `/tmp` or `/usr/tmp` directory is used. This option can only be specified in UNIX.

- *file-name-1*

  Specify the name of the source file for conversion. If you do not specify the full path name of a file, the command assumes that the file is located in the current directory at the current drive.

  In Windows, if you want to specify a file name that includes spaces, enclose the file name in double quotation marks (`"`).

  In UNIX, if you specify a hyphen (`-`) in this argument when converting a sequential file into an ISAM file, the command uses the standard input as the source file.

- *file-name-2*

  Specify the name of the destination file for conversion. If you do not specify the full path name of a file, the command assumes that the file is located in the current directory at the current drive. If you specify the name of an existing file, the file specified in this argument replaces the existing one.

  In Windows, if you want to specify a file name that includes spaces, enclose the file name in double quotation marks (`"`).

  In UNIX, if you specify a hyphen (`-`) in this argument when converting an ISAM file into a sequential file, the command uses the standard output as the destination file.

Return values

`0`	Normal end
`1`	Abnormal end

Jiscpy

Function

The `Jiscpy` command is used to copy a specified ISAM file. You can use this command to copy more than one ISAM file to a specified directory.

Format

`Jiscpy` *copy-source-file-name copy-destination-file-name*
`Jiscpy` *copy-source-file-name-1* `[`*copy-source-file-name-2 ...*`]`
copy-destination-directory-name

Required execution permission

In Windows: Administrators (If User Account Control (UAC) for Windows is enabled, you must execute the command from the administrator console.)

In UNIX: Superuser

Command directory

In Windows:

installation-folder`\bin\`

In UNIX:

`/opt/jp1base/bin/`

Arguments

- *copy-source-file-name*

  Specify the ISAM data file to be copied.

- *copy-destination-file-name*

  Specify the name of the copy destination file.

- *copy-source-file-name-1* `[`*copy-source-file-name-2 ...*`]`

  Specify this when you copy more than one ISAM data files. Also, you must specify *copy-destination-directory-name* when you specify more than one ISAM data files.

- *copy-destination-directory-name*

  Specify the name of the directory to store the ISAM data file copied.

Note

To copy the ISAM data file successfully, you need to stop JP1/Base in advance.

Return values

`0`	Normal end
`1`	Abnormal end

Jisext

Function

The `Jisext` command extracts as many valid records as possible from an ISAM data file where an error occurred and then restores the extracted records to a sequential file. In UNIX, this command also outputs the key definitions for the ISAM file.

This command verifies the records in a data file from the file's beginning until the command encounters an error, and outputs the verified records to a sequential file. Then, this command verifies the records in the data file from the file's end until the command encounters an error, and outputs the verified records to the sequential file.

When this command extracts records, it determines the record type and record length from the definitions in the key definition file. Therefore, if the key definition file is damaged, you must specify the record type and record length as command options. If this command outputs a message notifying you of an error in a definition file, the key definition file is damaged. You can specify the record type and record length even when the key definition file is not damaged. In this case, this command extracts records by using the specified record type and length.

Format

In Windows:

```
Jisext [-f record-type:record-length] file-name-1 file-name-2
```

In UNIX:

```
Jisext {-p | -f record-type:record-length} file-name-1 [file-name-2]
```

Required execution permission

In Windows: Administrators (If User Account Control (UAC) for Windows is enabled, you must execute the command from the administrator console.)

In UNIX: Superuser

Command directory

In Windows:

installation-folder`\bin\`

In UNIX:

```
/opt/jp1base/bin/
```

Arguments

- `-p`

  Specify this option to output the key definition parameters to the standard output. You can only specify this option when the `-f` option is not specified. This option can only be specified in UNIX.

- `-f` *record-type*`:`*record-length*

  You can use this option to explicitly specify the record type and record length for the ISAM file. The specification of this option prevails over the specification in the key definition file. In UNIX, you can only specify this option when the `-p` option is not specified.

  record-type

  Specify either of the following keywords to specify the record type:

  `f`: Fixed length

  `v`: Variable length

  record-length

  Specify the record length (in bytes) in the range from 1 to 65,503.

  When the record type is variable-length, specify the maximum record length. When the record type is variable-length, the command assumes that the minimum record length is 1.

- *file-name-1*

  Specify the name of the source file (ISAM file) from which you want to extract records. If you do not specify the full path name of a file, the command assumes that the file is located in the current directory at the current drive. In Windows, if you want to specify a file name that includes spaces, enclose the file name in double quotation marks (`"`).

- *file-name-2*

  Specify the name of the destination file (sequential file) to which you want to output the extracted records. If you do not specify the full path name of a file, the command assumes that the file is located in the current directory at the current drive. If you specify the name of an existing file, the file specified in this argument replaces the existing one.

  In Windows, if you want to specify a file name that includes spaces, enclose the file name in double quotation marks (`"`).

  In HP-UX or Solaris, you must not omit this argument.

Return values

`0`	Normal end
`1`	Abnormal end

Jisinfo

Function

The `Jisinfo` command displays information about the files that constitute an ISAM file and information about keys.

This command displays the following information contained in the key definition file:

- Information about the data file:

  The record format, record length, and flags

- Information about the key file:

  The page length, key item names, number of key items, key file name, flags, number of key elements, key positions, key lengths, and key attributes

Format

`Jisinfo [-u] [-e]` *file-name*

```
(The -e option is only available in UNIX.)
```

Required execution permission

In Windows: Administrators (If User Account Control (UAC) for Windows is enabled, you must execute the command from the administrator console.)

In UNIX: Superuser

Command directory

In Windows:

installation-folder`\bin\`

In UNIX:

`/opt/jp1base/bin/`

Arguments

■ `-u`

Deleting or updating records increases the unused area for the data file and key file. If you specify this option, the command displays the percentage of the unused area size. If the percentage of the unused area size is high, you can use the file compression utility command to eliminate the unused area.

■ `-e`

This option is available for UNIX only.

Use this option to check the setting for ISAM file size capping. If ISAM file size capping is enabled, `Reuse` appears in the **Key File Reuse** field. If size capping is enabled in Windows, the function's status is always displayed.

- *file-name*

Specify the name of the file for which you want to display the key definition information. If you do not specify the full path name of a file, the command assumes that the file is located in the current directory at the current drive. When you specify more than one file name, use at least one space to separate each file name. You can also use the wildcard character (`*`) to specify files.

In Windows, if you want to specify a file name that includes spaces, enclose the file name in double quotation marks (`"`).

Example:

The following shows examples in Windows.

- Specify all the files in the `c:\data` directory.

```
Jisinfo c:\data\*
```

- Specify the file names beginning with `SAMPLE` in the `c:\data` directory.

```
Jisinfo c:\data\SAMPLE*
```

Notes

- The command immediately stops if an I/O error occurs or a specified file does not exist even when the command has processed some files.
- If you want to redirect the check result to a text file, specify the destination file name after `>`. The following shows an example.

  Example:

  ```
  Jisinfo sample > info.txt
  ```

- The command takes some time to display the result if you specify the `-u` option.
- If you execute the command with the `-u` option specified while another process is accessing the specified ISAM file, a file access error occurs.

Return values

0	Normal end
1	Abnormal end

Jiskeymnt

Function

The `Jiskeymnt` command adds or deletes keys. The `Jiskeymnt` command also reorganizes the key file. The key definition parameter file specifies the keys to be added, deleted or reorganized. Use a text editor or the `vi` editor (in UNIX) to create the key definition parameter file.

Adding keys

This command adds key item names and key definitions to the key definition file. This command also creates the key file for the keys to be added.

Deleting keys

This command deletes key item names and key definitions from the key definition file. This command also deletes the key file for the keys to be deleted.

Reorganizing keys

This command uses the current key definitions to re-create the key file for the specified keys.

Format

In Windows:

```
Jiskeymnt file-name
```

In UNIX:

```
Jiskeymnt [file-name ...]
```

Required execution permission

In Windows: Administrators (If User Account Control (UAC) for Windows is enabled, you must execute the command from the administrator console.)

In UNIX: Superuser

Command directory

In Windows:

installation-folder`\bin\`

In UNIX:

`/opt/jp1base/bin/`

Arguments

- *file-name*

Specify the name of the key definition parameter file containing the information about the ISAM file for which you want to add, delete or reorganize keys.

In Windows, if you want to specify a file name that includes spaces, enclose the file name in double quotation marks (").

In UNIX, you can omit a file name. If you omit a file name, the command imports the key definitions for the ISAM file from the standard input. When you specify more than one file name, use at least one space to separate each file name. You can also use the wildcard character (*) to specify files.

Example:

The following shows examples in Windows.

- Specify all the files in the `c:\data` directory.

```
Jiskeymnt c:\data\*
```

- Specify all the file names beginning with `SAMPLE` in the `c:\data` directory.

```
Jiskeymnt c:\data\SAMPLE*
```

Creating the key definition parameter file

The following shows how to create the key definition parameter file.

- Items to be specified in the file

The following table shows the items you need to specify in the key definition parameter file.

Table 13-5: Items in the key definition parameter file (for adding, deleting and reorganizing keys)

Keyword	Format	Contents
`fi-`	*file-name*#1	Specify the name of an ISAM file. You can include a path name in the file name. Follow the file naming rules of the OS you are using. In Windows, if the file name includes spaces, enclose the file name in double quotation marks ("). In UNIX, the maximum number of characters you can use in *file-name* is four characters fewer than the maximum file name length of the OS.
`an-`	*key-item-name*#2	Specify a key item name when you add a key.
`dn-`	*key-item-name*#2	Specify a key item name when you delete a key.

Keyword	Format	Contents
`rn-`	*key-item-name*[#2]	Specify a key item name when you reorganize a key. If you want to reorganize all keys, omit *key-item-name*.
`ke-`	`t=`*key-attribute* `,p=`*key-position* `,l=`*key-length* `[,ISDESC]`	Specify the details of a key when you add a key. You must specify this keyword when adding a key. When you want to specify a compound key, you must specify this keyword for each constituent element in the compound key.[#3] *key-attribute* In *key-attribute*, specify any of the following keywords: `c` for character type (`CHARTYPE`) `i` for two-byte integer type (`INTTYPE`) `l` for four-byte integer type (`LONGTYPE`) `f` for floating type (`FLOATTYPE`) `d` for double length type (`DOUBLETYPE`) *key-position* The value to be specified in *key-position* differs depending on the record type. Fixed-length record type:0 to (*record-length* - 1) Variable-length record type:0 to (minimum-*record-length* - 1) *key-length* The value to be specified in *key-length* differs depending on the key attribute. `c` (`CHARTYPE`): 1 to 255 `i` (`INTTYPE`): 2 `l` (`LONGTYPE`): 4 `f` (`FLOATTYPE`): 4 `d` (`DOUBLETYPE`): 8 `ISDESC` Indicates that key elements are in descending order. Omitting this keyword indicates that key elements are in ascending order.

Keyword	Format	Contents
`cp-`	Information about key duplication and compression	When you want to add a key, use four hexadecimal numbers to specify the information about key duplication and compression. Bit 15 specifies whether to assure the creation order of keys if key values are duplicated. `0`: Assures the creation order. `1`: Does not assure the creation order. Bit 14 specifies whether or not a sparse key exists. `0`: A sparse key does not exist. `1`: A sparse key exists. In Windows: Bits 1 to 13 are reserved bits and set to $(0000000000)_2$. In UNIX: Bits 4 to 13 are reserved bits and set to $(0000000000)_2$. In UNIX: Bits 1 to 3 specify the compression level#4 $(111)_2$: Performs complete compression. $(000)_2$: Does not compress. Bit 0 specifies whether to permit duplicate keys. `0`: Does not permit duplicate keys. `1`: Permits duplicate keys.
`sp-`	Sparse character	When you add a key, use two hexadecimal numbers to specify the internal value of the sparse character. Specify this parameter only when you specify the `cp` parameter.

#1: You cannot specify a file name that ends with `.KDF`, `.DRF` or `.K01` to `.K99`.

#2: You can use no more than 31 bytes to specify each key item name. You cannot specify `K01` to `K99` as a key item in the `an-` parameter.

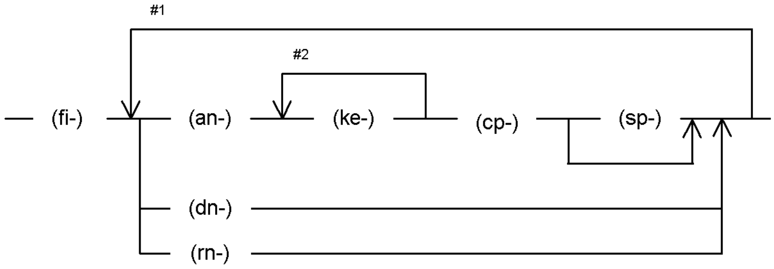
#3: You cannot specify more than one constituent element whose key attribute, key position, key length and key order (`ISDESC`) are the same.

#4: In this type of management for ISAM files, keys are compressed regardless of the compression level.

In the key definition parameter file, the specifications of the keys to be added, the keys to be deleted and the keys to be reorganized can coexist. You can specify more than one key for each operation type.

- Specifying parameters

The following shows how to specify parameters in the key definition parameter file.



#1 Repeat this part if you want to add, delete, or reorganize more than one key.

#2 When you add a compound key, repeat this part for each constituent item.

■ Notes on parameter specification

Remember the following points when you specify parameters in the key definition parameter file.

- Use at least one space to separate each parameter.

  Example:

  `fi-isamfile`Δ`rn-subkey1`Δ...

  (Legend) Δ: Space

- You cannot place a space in a parameter.

  Example:

  `ke-t=c`Δ`,p=10...`

  (Legend) Δ: Space

Notes

- You cannot add or delete primary keys.
- Addition or reorganization of keys uses work files.
- The command immediately stops if an I/O error occurs or a specified file does not exist even when the command has already processed some files.

Return values

`0`	Normal end
`1`	Abnormal end

Jisktod

Function

The `Jisktod` command extracts as many valid records as possible from a key file of an ISAM file where an error occurred and then restores the extracted records to a sequential file. However, this command exclusively locks the ISAM file to be restored. For this reason, before you execute this command, make sure that the ISAM file to be restored cannot be accessed.

The command validates the following logical structure of an ISAM file, and outputs the valid records managed by each key file to a sequential file:

- The logical structure of the definition file
- The size and logical record structure of each data file
- Consistency between the logical structure of key files and data files

If an error is detected during logical structure validation, a detailed message is output according to the specified message output level. If a fatal error is detected, the command ends abnormally and no sequential file is created. In such a case, the command attempts to extract as many valid records as possible, depending on the error that occurred.

When this command extracts records, it determines the record type and record length from the definitions in the key definition file. For this reason, if the key definition file is corrupt, no records can be extracted.

You can use the existing file conversion command (`Jisconv`) to convert the created sequential file into an ISAM file. The record type and length must be the same for both the sequential file and the target ISAM file.

Format

In Windows:

```
Jisktod [-k key-item-name]
          [-l message-output-level]
          [-b buffer-size]
          [-d work-folder-name]
          extraction-target-ISAM-file-name  sequential-file-name
Jisktod -c
          [-k key-item-name]
          [-l message-output-level]
          [-b buffer-size]
          [-d work-folder-name]
          validation-target-ISAM-file-name
```

In UNIX:

```
Jisktod [-k key-item-name]
         [-l message-output-level]
         [-b buffer-size]
         [-T work-directory-name]
         extraction-target-ISAM-file-name  sequential-file-name
Jisktod -c
        [-k key-item-name]
        [-l message-output-level]
        [-b buffer-size]
        [-T work-directory-name]
        validation-target-ISAM-file-name
```

Required execution permission

In Windows: Administrators (If User Account Control (UAC) for Windows is enabled, you must execute the command from the administrator console.)

In UNIX: Superuser

Command directory

In Windows:

installation-folder`\bin\`

In UNIX:

`/opt/jp1base/bin/`

Arguments

■ `-c`

Use this option only if you want to validate the logical structure of an ISAM file. The option determines whether records can be extracted from each key file of the specified ISAM file. After validating the logical structure of the ISAM file, if records that can be extracted from each key file and error message are detected, the command outputs the number of records that can be extracted. The number of records is output to the standard output.

This option allows you to specify the name of the ISAM file to be validated.

If this option is omitted, after the logical structure of the ISAM file is validated, the command extracts as many valid records as possible and restores them to a sequential file. If you omit this option, you must specify the name of the ISAM file from which valid records are to be extracted, and the name of a sequential file to which the valid records are to be output.

If you specify the `-k` option, you can explicitly specify a key file to be validated.

If you omit the `-k` option, all key files specified in the key definition file are validated. If an appropriate key file does not exist, the command does not validate the file, and instead proceeds to the next key file.

- `-k` *key-item-name*

  You must use the key definition display (`Jisinfo`) command to specify the key item name in a key file, and display it as key file information.

  If the `-c` option is specified when validating the logical structure of an ISAM file, select a key item name specified in the key file to be validated. If the `-c` option is specified and the `-k` option is omitted, all the key files specified in the key definition file are validated.

  If the `-c` option is omitted when extracting valid records from the ISAM file, select a key item name specified in the key file from which valid records are to be extracted. If both the `-c` and `-k` options are omitted in the operation to extract valid records, the files to be extracted are determined by the key file containing the first key item name shown as key file information. You can use the key definition display (`Jisinfo`) command to specify the key item name.

- `-l` *message-output-level*

  Specify whether messages detailing errors are to be output to the standard error output. The valid value is `0` or `1`. If you specify `1`, all messages, including detailed messages, are output to the standard error output. The default is `0`.

- `-b` *buffer-size* (MB)

  Specify a buffer size used for file input and output. The specifiable range is 0 to 256 (in MB). If you specify 0, no buffer is reserved. The default is 16.

- `-d` *work-folder-name*

  Work files are used to extract and sort valid records from key files. This means that you must specify the folder for the work files. If you omit this option, the current folder or a folder specified with the environment variable `temp` or `tmp` is used. This option can only be specified in Windows.

- `-T` *work-directory-name*

  Work files are used to extract and sort valid records from key files. This means that you must specify the directory for the work files. If you omit this option, `/tmp` or `/usr/tmp` is used. This option is available for UNIX only.

- *extraction-target-ISAM-file-name*

  If the `-c` option is omitted, you can specify an ISAM file as an extraction target. Specify the name of an ISAM file that contains the key file. The valid records are extracted from the key file. If you do not specify the full path name of a file, the command assumes that the file is located in the current directory at the current drive.

If you want to specify a file name that includes spaces, enclose the file name in double quotation marks (`"`).

If a definition file extension# accompanies the specified file name, the file name without the extension is assumed to be an ISAM file name. For all other extensions#, the combination of the file name and extension is assumed to be an ISAM file name.

#:

Windows: `.KDF`. This extension is not case sensitive.

UNIX: `.DEF`. This extension is case sensitive.

- *sequential-file-name*

If the `-c` option is omitted, you can specify the name of a sequential file to which valid records are to be output. These records are extracted from the ISAM file specified as the extraction target. If the specified file already exists, the file is overwritten.

If you do not specify the full path name of a file, the command assumes that the file is located in the current directory at the current drive. If you want to specify a file name that includes spaces, enclose the file name in double quotation marks (`"`).

An ISAM file extension# cannot be specified.

#:

Windows: `.KDF, .DRF, and .K01` to `.K99`. These extensions are not case sensitive.

UNIX: `.DEF, .DAT, and .K01` to `.K99`. These extensions are case sensitive.

- *validation-target-ISAM-file-name*

If the `-c` option is specified, you can specify an ISAM file as a validation target. Specify the name of an ISAM file whose logical structure is to be validated. If you do not specify the full path name of a file, the command assumes that the file is located in the current directory at the current drive. If you want to specify a file name that includes spaces, enclose the file name in double quotation marks (`"`).

If a definition file extension# accompanies the specified file name, the file name without the extension is assumed to be an ISAM file name. For all other extensions#, the combination of the file name and extension is assumed to be an ISAM file name.

#:

Windows: `.KDF`. This extension is not case sensitive.

UNIX: `.DEF`. This extension is case sensitive.

Notes

- If the -c option is omitted, two buffers are used for file input and output. Thus, the reserved buffer is twice the size of the value specified with the `-b` option.
- If an ISAM file has more than one key file, and if one of the key files has an invalid logical structure, the file conversion (`Jisconv`) command might fail when attempting to convert the ISAM file.

Return values

0	Normal end
1	Record that cannot be extracted was found.
2	Record that can be extracted was found, but its consistency is not fully maintained.
3	Argument error, invalid file, system error, internal inconsistency, or exclusive error

Example

The following examples show how to extract valid records from an ISAM file (`ISAMFILE`) to a sequential file (`SAMFILE`).

- Extracting records to a sequential file from an ISAM file that has a single key file:

```
>Jisktod ISAMFILE SAMFILE
KAIU347-I Checking of ISAM data file will now start.
            ISAM file name: ISAMFILE
KAIU348-I Checking of ISAM data file was finished normally.
            ISAM file name: ISAMFILE
KAIU321-I Extraction of ISAM file will now start.
            key item name: K01
            ISAM file name: ISAMFILE
            Output file: SAMFILE
KAIU323-I The record has been successfully extracted from the
key file.
            key item name: K01
            Number of extractions: 101
            Number of registrations: 101
            ISAM file name: ISAMFILE
            Output file: SAMFILE
```

- Extracting records to a sequential file from an ISAM file that has two key files (key item name: `K01` and `K02`):

1. The logical structure is validated for each key file.

```
>Jisktod -c -l 1 ISAMFILE
KAIU347-I Checking of ISAM data file will now start.
            ISAM file name: ISAMFILE
KAIU348-I Checking of ISAM data file was finished normally.
```

```
            ISAM file name: ISAMFILE
KAIU322-I Checking of ISAM key file will now start.
            key item name: K01
            ISAM file name: ISAMFILE
KAIU333-W The leaf page does not match the record key.  key
item name: K01 ISAM file name: ISAMFILE Offset: 0x00000000
KAIU342-W A definition file entry does not match the number
of key file records.
            Key item name: K01
            Number of valid records: 100
            Number of registrations: 101
            ISAM file name: ISAMFILE
KAIU340-W A record not managed from the key file exists.
            key item name: K01
            ISAM file name: ISAMFILE
            Offset: 0x00000000
KAIU328-W The integrity of part of the key file cannot be
guaranteed.
            key item name: K01
            Number of extractable items: 100
            Number of registrations: 101
            ISAM file name: ISAMFILE
KAIU322-I Checking of ISAM key file will now start.
            key item name: K02
            ISAM file name: ISAMFILE
KAIU324-I The state of the key file is normal.
            key item name: K02
            Number of extractable items: 101
            Number of registrations: 101
            ISAM file name: ISAMFILE
```

2. After the logical structures are validated in step 1, the normal key file (key item name: `K02`) is used to extract the records.

```
>Jisktod -k K02 ISAMFILE SAMFILE
KAIU347-I Checking of ISAM data file will now start.
            ISAM file name: ISAMFILE
KAIU348-I Checking of ISAM data file was finished normally.
            ISAM file name: ISAMFILE
KAIU321-I Extraction of ISAM file will now start.
            key item name: K02
            ISAM file name: ISAMFILE
            Output file: SAMFILE
KAIU323-I The record has been successfully extracted from the
key file.
            key item name: K02
            Number of extractions: 101
            Number of registrations: 101
            ISAM file name: ISAMFILE
```

```
Output file: SAMFILE
```

Jislckclear (Windows only)

Function

The `Jislckclear` command checks and clears the locked status of any files or records that were locked by a process that has disappeared because of circumstances such as the user forcibly ending a process of the JP1 product that accesses ISAM files.

Format

```
Jislckclear {-c | -d}
```

Required execution permission

Administrators. (If User Account Control (UAC) for Windows is enabled, you must execute the command from the administrator console.)

Command directory

installation-folder`\bin\`

Arguments

■ `-c`

This argument enables you to check whether there are any remaining files or records locked by a deleted process. If any lock information remains about a file or record used by the deleted process, message KAIU315-I is output to the standard error output.

■ `-d`

This argument enables you to release files or records locked by a deleted process.

Notes

- JP1 product processes currently accessing an ISAM file might be paused while this command is being executed.
- Between the time you check the lock information with the `-c` option and then clear the locks with the `-d` option, a file or record might be unlocked by another process that accesses ISAM files. For this reason, the number of locks displayed by the `-c` option might not match the number of released locks displayed by the `-d` option.

Return values

`0`	Normal end
`1`	Normal end (locks displayed or cleared)
`2`	Normal end (processing suspended because there is no lock information)

3	Abnormal end (no execution permission)
4	Abnormal end (invalid argument)
5	Abnormal end (system call error)
99	Abnormal end (program logic error)

Jislckext

Function

The `Jislckext` command extends or decreases the number of entries in the lock table. If you need to display the status of the lock table before or after executing the `Jislckext` command, the steps are as follows.

In Windows:

1. Specify the `-t` option of the `Jislckext` command to obtain the number of current lock entries.

   Specify and run the command as follows:
   ```
   Jislckext -t
   ```

2. Change the number of entries.

   Specify and run the command as follows:
   `Jislckext` *number-of-entries*

3. Specify the `-t` option of the `Jislckext` command to verify that the number of the lock entries has been changed.

   Specify and run the command as follows:
   ```
   Jislckext -t
   ```

In UNIX:

1. Use the `ipcs` command to check the segment size of the shared memory.

   Specify and run the command as follows:
   ```
   ipcs -ma | grep 0x88
   ```

2. Calculate the number of entries.

   You can use the following expression to obtain the number of entries:
   `(`*ipcs-command-execution-result* `- 36972) / 104`

3. Change the number of entries.

   Specify and run the command as follows:
   `Jislckext` *number-of-entries*

4. Use the `ipcs` command to verify that the segment size of the shared memory has been changed:
   ```
   ipcs -ma | grep 0x88
   ```

Format

```
Jislckext number-of-entries
```

Required execution permission

In Windows: Administrators (If User Account Control (UAC) for Windows is enabled, you must execute the command from the administrator console.)

In UNIX: Superuser

Command directory

In Windows:

installation-folder`\bin\`

In UNIX:

`/opt/jp1base/bin/`

Arguments

■ *number-of-entries*

Recreates the lock table with the specified number of entries.

Notes

- If the lock table is being used by another process, this command returns the number of entries in use.
- You must stop the JP1/Base service and JP1/AJS service to change the number of entries in the lock table. You must also complete ISAM file operations, maintenance utility commands, and commands for operating on JP1/AJS jobnets.
- The lock table can have a maximum of 32,767 entries.

Return values

`0`	Normal end
`1`	Abnormal end

Jislckfree (Windows only)

Function

The `Jislckfree` command deletes the lock entry information specified with the PID from the ISAM lock table in system shared memory. It thus cancels the exclusive use of the file or record. The command ends normally if the specified PID is not found in the specified ISAM lock table. If the specified ISAM lock table is not found (the JP1 product using that ISAM is not started), the command ends abnormally, outputting the `SetSecurity DescriptorDacl Error` error message.

Format

`Jislckfree -p` *PID*

Required execution permission

Administrators. (If User Account Control (UAC) for Windows is enabled, you must execute the command from the administrator console.)

Command directory

installation-folder`\bin\`

Arguments

`-p` *PID*

For *PID*, specify the ID of the process that is exclusively using the ISAM file or record.

Notes

- All lock command entry information specified with the PID is deleted from the ISAM lock table. Do not execute this command while the JP1 product specified with the PID is running.
- You can use the `Jismlcktr` command to determine the PID of the process for which you want to delete lock entry information.

Return values

`0`	Normal end
`1`	Abnormal end

Jislckreg (UNIX only)

Function

The `Jislckreg` command helps you set up the resources to be used for ISAM.

ISAM databases provided in JP1 products use common resources in the system so that any product intensively accessing the ISAM database might interfere with accesses by other JP1 products, resulting in degraded performance. You can split resources used for ISAM to improve access performance. For details of the setting method, see the manual for each JP1 product.

Format

```
Jislckreg {-r | -c | -i | -s}
```

Required execution permission

Superuser

Command directory

`/opt/jp1base/bin/`

Arguments

■ `-r`

Specify this option to set up the resources to be used for ISAM (shared memory and semaphores) according to the current setting file (`/etc/opt/jp1base/conf/Jismdef.ini`). You do not need to specify this option for this command because ISAM resources are set up automatically when JP1/Base is started.

■ `-c`

Specify this option to check the syntax of the setting file (`/etc/opt/jp1base/conf/Jismdef.ini`).

■ `-i`

Specify this option to display the current resource setting information in the system.

■ `-s`

Specify this option to display the amount of system resources currently being used according to the setting file (`/etc/opt/jp1base/conf/Jismdef.ini`).

Notes

- Stop all JP1 services before modifying settings in the file.
- After modifying the setting file, execute the `Jisrsdel` command before

restarting all JP1 services.

Return values

0	Normal end
1	Abnormal end

Jismlcktr (Windows only)

Function

The `Jismlcktr` command displays the information in the ISAM lock table. The following shows the display format.

```
*** REG INFO ***
ISM_FILENO_ENV[1024]             Number of file lock tables                     Registry
                                                                                information
ISM_LOCKENTRY_ENV[1024]          Number of lock entries
************** Lock Tabel *****************
tableCount:1024                  Number of file lock tables

fileCount:3                      Number of file lock tables in use

[1]C:\TEMP\TEST11.KDF            File lock table information
 usedEntryCount:1                Number of entries in use
--- PID --- TID --- fd --- Offset --- lngth --- mode --- time ---
[1] 255     188     160       0        1        1    03/05/14 10:35:07
                                                                                Lock table
[2]C:\TEMP\TEST11.DRF                                                           information
 usedEntryCount:2
--- PID --- TID --- fd --- Offset --- lngth --- mode --- time ---
[1] 255     188      20       0        1        2    03/05/14 10:35:11
[2] 255     188      20      82        1        2    03/05/14 10:35:15

[3]C:\TEMP\TEST11.K01
  usedEntryCount:0
--- PID --- TID --- fd --- Offset --- lngth --- mode --- time ---
```

Format

```
Jismlcktr
```

Required execution permission

Administrators. (If User Account Control (UAC) for Windows is enabled, you must execute the command from the administrator console.)

Command directory

installation-folder`\bin\`

Jisprt

Function

The `Jisprt` command edits and displays the records in the data file in the specified format: the dump, character, or hexadecimal format.

This command stops displaying the records when:

- The command has displayed all the records in the data file.
- The command has displayed all the records in the specified range.
- The command has displayed as many records as specified in *record-count*.

Format

```
Jisprt [-t type]
{[-k key-item][-s start-key-value[:x]][-e end-key-value[:x]]|-d}
[-c record-count]
file-name
```

Required execution permission

In Windows: Administrators (If User Account Control (UAC) for Windows is enabled, you must execute the command from the administrator console.)

In UNIX: Superuser

Command directory

In Windows:

installation-folder`\bin\`

In UNIX:

`/opt/jp1base/bin/`

Arguments

■ `-t` *type*

In *type*, specify any of the following keywords as the record display format:

- `d` (dump format)
- `c` (character format)
- `h` (hexadecimal format)

If you omit this option, the command assumes that `d` is specified.

- `-k` *key-item*

  In *key-item*, specify the key item name of the key on which the record display order is based. If you omit this option, the command sorts records by primary keys.

- `-s` *start-key-value*`[:x]`

  In *start-key-value*, specify the value of the first key from which the command displays keys. If you omit this option, the command displays keys starting from the one having the smallest value. If you specify the value in hexadecimal, add the suffix `:x`.

- `-e` *end-key-value*`[:x]`

  In *end-key-value*, specify the value of the last key to which the command displays keys. If you omit this option, the command displays keys up to the one having the largest value. If you specify the value in hexadecimal, add the suffix `:x`.

- `-d`

  Specify this option to display records in the order in which they are physically contained in the data file. You can only specify this option when the `-k` *key-item*, `-s` *start-key-value*`[:x]` and `-e` *end-key-value*`[:x]` options are not specified.

- `-c` *record-count*

  In *record-count*, specify the number of records you want to display.

- *file-name*

  Specify the name of the file you want to display.

Note

If you want to redirect the record information to a text file, specify the destination file name after `>`.

Example:

```
Jisprt sample > prt.txt
```

Return values

`0`	Normal end
`1`	Abnormal end

Jisrsdel (UNIX only)

Function

The `Jisrsdel` command deletes resources to be used for ISAM.

Format

```
Jisrsdel
```

Required execution permission

Superuser

Command directory

```
/opt/jp1base/bin/
```

Note

Ensure that all JP1 services are stopped before attempting to execute this command. If the command is executed when a JP1 service is running, it might corrupt the ISAM file.

Return values

`0`	Normal end
`1`	Abnormal end

jp1base_setup (UNIX only)

Function

The `jp1base_setup` command sets the operating environment of JP1/Base. Execute this command before using JP1/Base, either in a cluster system or a non-cluster system.

Format

```
jp1base_setup
```

Required execution permission

Superuser

Command directory

```
/opt/jp1base/bin/
```

Notes

- If you are installing JP1/Base over an existing JP1/Base program, there is no need to set up the operating environment by executing the `jp1base_setup` command.

  If you reinstall JP1/Base Version 6 on a host that has JP1/IM installed, and then execute the `jp1base_setup` command, the values set using the `jcocmddef` command in JP1/IM are reset to their defaults. You will need to set the values again, using the `jcocmddef` command.
- If you execute the `jp1base_setup` command after setting up a logical host, the communication protocol for a physical host is set to the ANY binding method. In that case, change the communication protocol to the IP binding method, as follows:
  1. Create a file containing the following contents:

     ```
     [JP1_DEFAULT\JP1BASE]
     "JP1_BIND_ADDR"="IP"
     ```
  2. Execute the `jbssetcnf` command to set the above file in the common definitions.
- Do not execute this command when JP1/Base is active.

Return values

`0`	Normal end
`1`	Abnormal end

jp1base_setup_cluster (UNIX only)

Function

The `jp1base_setup_cluster` command sets the operating environment of a JP1/Base logical host. Execute this command if you want to use JP1/Base in a cluster system. First set the environment for the primary node, and then set the environment for the secondary node.

Format

```
jp1base_setup_cluster -h logical-host-name
                   [-d shared-directory[-a authentication-server] [-s] [-v]]
```

Required execution permission

Superuser

At the primary node:

Specify the logical host name and the shared directory name. Specify the other options as required. Since this command attempts to create files in the specified shared directory, you must mount a shared disk before executing this command.

At the secondary node:

Specify the logical host name only. The command sets the environment based on the information specified at the primary node. Note that you must copy the common definition information from the primary node to the secondary node before you set the operating environment of the secondary node. Use the `jbsgetcnf` and `jbssetcnf` commands to copy the information.

Command directory

`/opt/jp1base/bin/`

Arguments

■ `-h` *logical-host-name*

Specify the name of the logical host you want to set up.

Notes

- Register the logical host name in the `hosts` file and in the name server to enable TCP/IP communication.
- If you do not want to operate JP1/Base by DNS, do not specify the host name in the FQDN (Fully Qualified Domain Name) format. For example, if the FQDN is `jp1v6.soft.hitachi.co.jp`, specify `jp1v6`.

- `-d` *shared-directory*

Specify this option only when setting the operating environment of the primary node. Specify the shared directory in which to save information to be carried over at failover. The shared directory to be specified must be in *shared-directory*. The environment settings for operating JP1/Base are saved in the specified shared directory. If you execute this command with this option specified, the command creates the directories shown in the following table and copies the definition files from `/etc/opt/jp1base/conf/` to the appropriate shared directory.

Directory	Files to be contained
shared-directory`/jp1base/conf/`	Definition files
shared-directory`/jp1base/log/`	Log file
shared-directory`/event/`	Event server settings file

Modify the definition files as required.

- `-a` *authentication-server*

Specify the host name of the authentication server to which the logical host will connect. If you omit this option, the command assumes the same authentication server as that specified in the operating environment of the physical host.

- `-s`

Specify this option if you want to run an authentication server on the logical host. If you specify this option, the authentication server is activated when JP1/Base starts. If you omit this option, no authentication server will be activated when JP1/Base starts.

- `-v`

Specify this option to view all messages when you set the operating environment of the logical host.

Notes

- Complete this setup on every node.
- At execution of this command, the *logical-host-name* and *directory-name-on shared-disk*`/event/` are automatically set in the event server index file (`/etc/opt/jp1base/conf/event/index`) of the event service on the local disk. A logical host name and communication type (`keep-alive`) is also automatically set to the API setting file (`/etc/opt/jp1base/conf/event/api`) for the event service on the local disk. An event server settings file (`conf`) and forwarding settings file (`forward`) are created in the *directory-name-on shared-disk*`/event/` directory.
- At execution of this command, the TCP/IP communication protocol is changed

from socket binding to IP addressing. This change affects settings for the logical hosts to be created and their constituent physical hosts. For details on the socket binding method used for TCP/IP communication, see the documentation for the OS you are using.

- In the `jp1base_setup_cluster` command, you cannot specify the communication protocol of the event service. To specify a communication protocol, edit the event server settings file (`conf`).
- Do not execute this command when JP1/Base is active.

Example

The following shows an example of this command when the logical host name is `lnode0` and the shared directory is `/shdsk/lnode0`.

At the primary node:

```
jp1base_setup_cluster -h lnode0 -d /shdsk/lnode0 -a lnode0
-s
```

The above command sets the operating environment of the logical host, creates shared directories and files on a shared disk, and sets up an authentication server.

At the secondary node:

```
jp1base_setup_cluster -h lnode0
```

jp1bshasetup (Windows only)

Function

The `jp1bshasetup` command displays the **Settings for Base Cluster System** dialog box for setting the operating environment of the JP1/Base logical hosts. Execute this command if you want to use JP1/Base in a cluster system.

Format

```
jp1bshasetup
```

Required execution permission

Administrators

Command directory

installation-folder`\bin\`

Note

Do not execute this command when JP1/Base is active.

jp1ping

Function

The `jp1ping` command converts the host name specified in the argument into an IP address by using the network functionality (`gethostbyname`) managed by the OS, and then executes the `ping` command on the acquired IP address.

Use this command to check the validity of network settings for a host that has multiple network interfaces (a host assigned multiple IP addresses for a single host name).

Format

`jp1ping [-h` *logical-host-name*`]`
host-name

Required execution permission

In Windows: None.

In UNIX: None.

Command directory

In Windows:

installation-folder`\bin\`

In UNIX:

`/opt/jp1base/bin/`

Arguments

- `-h` *logical-host-name*

When using JP1/Base in a cluster system, specify the logical host for which you want to execute the `jp1ping` command. If you omit this option, the host name set in the environment variable `JP1_HOSTNAME` is assumed. If the environment variable `JP1_HOSTNAME` is not set, the physical host name is assumed.

- *host-name*

Specify the name of a host on the network.

Return values

`0`	Normal end
Other than `0`	Abnormal end (but the command ends normally if the command usage is displayed after command execution without any arguments specified)

Example

The following shows a result (output example) of executing the `jp1ping` command to check what IP address `server1` is using:

```
C:\>jp1ping server1
LogicalHostnameKey : no define. use JP1_DEFAULT
jp1hosts           : no entry. extract hostlist is disabled.
Search jp1hosts    : server1 is not found.
Resolved Host List : server1 ->
server1.hitachi.co.jp(172.16.0.10, 172.16.0.20),
Check with ping command ---

Pinging 172.16.0.10 with 32bytes of data:

Reply from 172.16.0.10: bytes=32 time<10ms TTL=128
Reply from 172.16.0.10: bytes=32 time<10ms TTL=128
Reply from 172.16.0.10: bytes=32 time<10ms TTL=128
Reply from 172.16.0.10: bytes=32 time<10ms TTL=128

Pinging 172.16.0.20 with 32bytes of data:

Reply from 172.16.0.20: bytes=32 time<10ms TTL=128
Reply from 172.16.0.20: bytes=32 time<10ms TTL=128
Reply from 172.16.0.20: bytes=32 time<10ms TTL=128
Reply from 172.16.0.20: bytes=32 time<10ms TTL=128
C:\>
```

From the output, you can tell that the host name `server1` resolved to the two IP addresses 172.16.0.10 and 172.16.0.20, and that the pinging to the NIC is actually enabled.

Chapter
14. Definition Files

This chapter describes the JP1/Base definition files and the format and syntax of event filters.

List of definition files

The JP1/Base definition files are shown in the following table.

Table 14-1: List of definition files

Function	Definition file name and explanation
Startup control	*Start sequence definition file (Windows only)* Sets the sequence for starting and stopping services.
	Service startup delay time/timer monitoring period definition file (Windows only) Sets the length of time for service startup to be delayed and monitored.
Event service	*Event server index file* Specifies the directory to be used by the event server.
	Event server settings file Defines the operating environment for the event services.
	Forwarding settings file Defines which JP1 events are forwarded and the destination event server.
	API settings file Defines the method for connecting from the application program to the event server and the port to use for the connection.
Event conversion	*Action definition file for log file trapping* Specifies the conditions for converting log data into JP1 events and the retry settings when monitoring fails.
	Log information definition file Specifies the maximum size and number of storable log files that are used for log file trapping.
	Action definition file for event log trapping (Windows only) Specifies the conditions for converting event log data into JP1 events and the event-log monitoring interval.
Event service definition information collection and distribution	*Distribution definition file* Specifies the definition information to distribute and the destination host.
User management	*Password definition file (Windows only)* Specifies password information for multiple OS users.
	User permission level file Specifies operating permissions for JP1 resource groups accessed by JP1 users.

Function	Definition file name and explanation
	Directory server modification file (Windows only) Sets the common definition information in order to temporarily switch over the directory server when the linked directory server cannot be used due to a failure.
	Directory server linkage definition file (Windows only) Sets the common definition information in order to specify the directory server, when login authentication is performed by linkage to the directory server.
	User mapping definition file Sets mapping information for multiple JP1 users.
Health check function	*Health check definition file* Specifies how to report an error detected by the health check function and what other hosts to monitor by using the health check function.
	Common definition settings file (health check function) Sets the common definition information to enable the health check function.
Process management	*JP1/Base parameter definition file* Sets the common definition information. This file specifies whether to issue a JP1 event when the process is abnormally stopped or when the authentication server is switched.
	Extended startup process definition file Specifies the settings in order to automatically restart a process abnormally terminated.
Communication settings	*jp1hosts definition file* Sets the common definition information to modify the unique host information specifically for JP1/Base.
	Host access control definition file Sets access permissions to control access attempts from other hosts, for example, when providing information to the IM configuration management function of JP1/IM.
Local action function	*Local action environment variable file* Sets the environment variables to execute the command specified by the local action function.
	Local action execution definition file Specifies the commands and execution conditions of the local action function.
	Common definition settings file (local action function) Specifies whether to enable the local action function and sets the log information to the common definition information.

Event filter syntax

Event filters uses event IDs or source user names to filter out JP1 events. Event filters are specified in the following places:

- Forwarding settings file (`forward`)
- Local action execution definition file
- `jevexport` command
- JP1 event acquisition function (`JevGetOpen`)#
- Extended attribute mapping settings file#

#: For details, see *J.4 Converting JP1/SES events into JP1 events*.

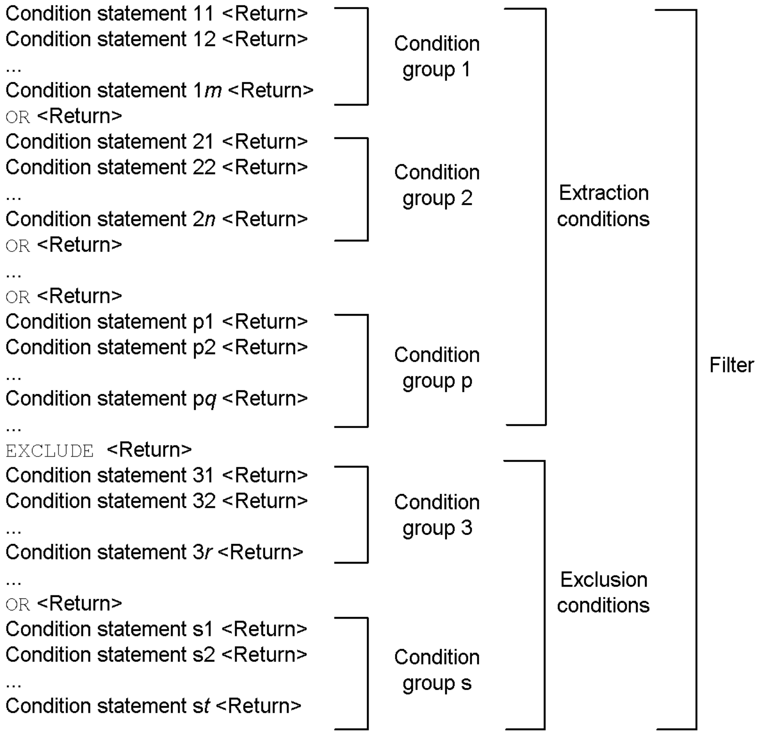
Event filter format

An *event filter* is a set of one or more condition groups. A *condition group* is a set of one or more condition statements. A *condition statement* is a line of conditions, and a number of such lines together constitute a condition group. The only statement you can write between condition groups is the single word `OR`. The maximum length of one line is 1,024 bytes. An event filter can be no more than 64 KB total.

A condition group is satisfied only if all the condition statements in the group are satisfied. The event filter conditions are satisfied if one or more of the condition groups are satisfied.

The following figure shows the concept of an event filter.

Figure 14-1: Concept of an event filter


Condition statement 11 <Return>
Condition statement 12 <Return>
...
Condition statement 1*m* <Return>
OR <Return>
Condition statement 21 <Return>
Condition statement 22 <Return>
...
Condition statement 2*n* <Return>
OR <Return>
...
OR <Return>
Condition statement p1 <Return>
Condition statement p2 <Return>
...
Condition statement p*q* <Return>
...
EXCLUDE <Return>
Condition statement 31 <Return>
Condition statement 32 <Return>
...
Condition statement 3*r* <Return>
...
OR <Return>
Condition statement s1 <Return>
Condition statement s2 <Return>
...
Condition statement s*t* <Return>
Condition group 1
Condition group 2
Condition group p
Condition group 3
Condition group s
Extraction conditions
Exclusion conditions
Filter

In JP1/Base 09-00 or later versions, you can write exclusion condition for event filters.

Define an exclusion condition when you want to exclude a specific JP1 event from the JP1 events that satisfy the extraction conditions.

Only the statement `EXCLUDE` can be written between the extraction conditions and the exclusion conditions. `EXCLUDE` can only be written once for each filter. The condition groups stated before `EXCLUDE` are extraction conditions; the condition groups stated after `EXCLUDE` are exclusion conditions. The format for exclusion conditions is the same as the format for extraction conditions.

Because exclusion conditions are not required, filters that were created in an earlier version of JP1/Base can still be used in version 09-00 or later, without having to modify the filters.

Condition statement format

Write condition statements in the following format:

attribute-name △ *comparison-keyword* △ *operand-1* △ *operand-2* △ . . .

△ is a separator representing one or more continuous spaces or tab characters. When multiple operands are specified, the condition statement is satisfied even if only one of them is true. Spaces, tab characters, CR, LF, and percent signs cannot be written as ordinary characters in the operands, but can be represented as two-digit hexadecimal codes, as follows:

- Space: `%20`
- Tab: `%09`
- CR: `%0d`
- LF: `%0a`
- %: `%25`

Characters other than space, tab character, CR, LF, and % symbols can also be represented using hexadecimal codes.

Note

If a condition statement contains a machine dependent character, the statement cannot be correctly applied.

■ Attribute name

The following table contains the attribute names that can be used in filter condition statements.

Table 14-2: Attribute names in filter condition statements

Attribute name	Contents	Type and format
`B.SEQNO`	Serial number in the event database	Number (0 to 2,147,483,647)
`B.ID`	Event ID	Event ID[#1]
`B.PROCESSID`	Source process ID	Number (0 to 2,147,483,647)
`B.TIME`	Registered time	Number (0 to 2,147,483,647 = cumulative seconds since UTC 1970-01-01 00:00:00)
`B.ARRIVEDTIME`	Arrived time	Number (0 to 2,147,483,647 = cumulative seconds since UTC 1970-01-01 00:00:00)
`B.REASON`	Reason to register the event into the event database	Number (1 to 4)

Attribute name	Contents	Type and format
B.USERID	Source user ID	Number (-1 to 2,147,483,647)
B.GROUPID	Source group ID	Number (-1 to 2,147,483,647)
B.USERNAME	Source user name	Character string#3
B.GROUPNAME	Source group name	Character string#3
B.SOURCESERVER	Source event server name	Character string#3
B.DESTSERVER	Destination event server name	Character string#3
B.SOURCESEQNO	Source serial number	Number (0 to 2,147,483,647)
B.CODESET	Code set	Character string#3
B.MESSAGE	Message	Character string#3
E.*extended-attribute-name*#2	Extended attribute	Character string#3

#1: Event IDs are different from character strings and numbers. For details, see the paragraph beginning with *When the attribute value is an event ID...* in the *Conditions* column of Table 14-3.

#2: For the format of extended attribute names, see *15.1.2 Extended attributes*.

#3: Character strings are case sensitive.

■ Comparison keywords

The following table shows how to specify comparison keywords in filter condition statements.

Table 14-3: Comparison keywords in filter condition statements

Comparison keywords	Number of operands	Conditions
IN	1 or more	The attribute value must match one of the operands. When the attribute value is of the string literal type, the operand can be any character string. When the attribute value is a number, the operand must be a character string that can be interpreted as a signed integer. Other operands are never matched. When the attribute value is an event ID, the operand must be a string in the form *x*:*y* or *x* (where *x* and *y* are hexadecimals of 1-8 digits). *x* represents the base code and *y* represents the extended code of the event ID. Other operands are never matched.

Comparison keywords	Number of operands	Conditions
NOTIN	1 or more	Negation of the IN comparison keyword
BEGIN	1 or more	The attribute value is of the string literal type, and must begin with one of the character strings specified in the operands. A numeric attribute value, or an attribute value that is an event ID, fails the condition.
RANGE	2	The condition statement is satisfied when the attribute name is B.TIME or B.ARRIVEDTIME, and the following conditions are satisfied: • The attribute value is a number, or a character string interpreted as a number (0 to 2,147,483,647) • *operand-1* and *operand-2* are 14-digit numeric literals • When the attribute value is interpreted as the cumulative seconds since UTC 1970-01-01 00:00:00, and converted to a numeric literal in *yyyymmddHHMMSS* format based on the time zone of the event server operating environment, and *operand-1* <= *attribute value* <= *operand-2*. When the attribute value is a number, specified in an attribute name other than B.TIME or B.ARRIVEDTIME: The condition is satisfied if *operand-1* and *operand-2* are interpreted as numbers, and *operand-1* <= *attribute value* <= *operand-2*. When the attribute value is of string literal type: The condition is satisfied if *operand-1* <= *attribute value* <= *operand-2* when the value is compared in order of its character codes. When the attribute value is an event ID: If *operand-1* and *operand-2* are strings in the form *x*:*y* (where *x* and *y* are hexadecimals of 1 to 8 digits), the whole interpreted as a 16-digit hexadecimal with *y* representing the upper 8 digits (extended code) and *x* representing the lower 8 digits (basic code), the condition is satisfied if *operand-1* <= *attribute value* <= *operand-2*. Attribute values of all other types fail the condition.
TRANGE	2	The condition is satisfied if: • The attribute value is a number, or a character string interpreted as a number (0 to 2,147,483,647) • *operand-1* and *operand-2* are 14-digit numeric literals • When the attribute value is interpreted as the cumulative seconds since UTC 1970-01-01 00:00:00, and converted to a numeric literal in *yyyymmddHHMMSS* format based on the time zone of the event server operating environment, and *operand-1* <= *attribute value* <= *operand-2*. Attribute values of all other types fail the condition.
DEFINED	0	The condition is satisfied if *attribute-name* represents an extended attribute, and the specified extended attribute is defined. If the extended attribute is undefined, the condition fails. This condition is necessarily true when *attribute-name* represents a basic attribute.
NOTDEFINED	0	Negation of the DEFINED comparison keyword

Comparison keywords	Number of operands	Conditions
`SUBSTR`	1 or more	The condition is satisfied if the attribute value is a string literal type, and includes one of the character strings specified in the operands. A numeric attribute value, or an attribute value that is an event ID, fails the condition.
`NOTSUBSTR`	1 or more	Negation of the `SUBSTR` comparison keyword
`REGEX`#1	1 or more	Regular expression comparison keyword. The condition is satisfied if the attribute value is of the string literal type, and matches one of the regular expressions specified in the operands. For details on regular expressions, see *F. Syntax of Regular Expressions*.
`WITHIN`#2	2	The condition statement is satisfied when the attribute name is `B.TIME` or `B.ARRIVEDTIME`, and the following conditions are satisfied: • The attribute value is a number, or a character string interpreted as a number (1 to 2,147,483,647) • *operand-1* is `M` (minutes), `H` (hours), or `D` (day). • *operand-2* is a character string that can be handled as a number (unsigned). • When *operand-1* is `M` (minutes) or `H` (hours): When the attribute value is interpreted as the cumulative seconds since UTC 1970-01-01 00:00:00, and converted to a numeric literal in *yyyymmddHHMMSS* format based on the time zone of the event server operating environment, and (current time - *operand-2* <= *attribute value* <= current time). • When *operand-1* is `D` (day): When the attribute value is interpreted as the cumulative seconds since UTC 1970-01-01 00:00:00, and converted to a numeric literal in *yyyymmddHHMMSS* format based on the time zone of the event server operating environment, and 00:00:00 on [today's date - (*operand-2* - 1)] <= *attribute value* <= 24:59:59 on today.

#1: `REGEX` is a comparison keyword introduced in version 06-71. If you use a file containing a REGEX definition in a version of JP1/Base other than version 06-71 or later, the REGEX part is ignored. Even when you specify machine-type-dependent characters as a regular expression, they are handled as an ordinary character string.

#2: `WITHIN` is a comparison keyword introduced in JP1/Base Version 07-00. You can specify this keyword in a filter file used for the jevexport command. If you define `WITHIN` with a command other than the `jevexport` command provided by JP1/Base 07-00 and later versions, the definition of `WITHIN` is handled as an error, resulting in the same operation as with versions 06-71 and earlier.

Examples of event filter settings

The following examples show how to set an event filter.

- Example 1: Select the JP1 event whose event ID consists of basic code `111` and extended code 0.

```
B.ID IN 111:0
or
B.ID IN 111
or
B.ID IN 00000111:00000000
```

- Example 2: Select JP1 events whose source user ID is 103.

```
B.USERID IN 103
or
B.USERID RANGE 103 103
```

- Example 3: Select JP1 events whose source event server names are reysol.

```
B.SOURCESERVER IN reysol
```

- Example 4: Select JP1 events that issued messages beginning with KAJP or KAVA.

```
B.MESSAGE BEGIN KAJP KAVA
```

- Example 5: Select JP1 events whose issued messages begin with the words Hello, world. Use the code %20 to represent the space between the comma and "w".

```
B.MESSAGE BEGIN Hello,%20world
```

- Example 6: Select JP1 events whose event IDs are other than 222:0, and whose source user names are ann.

```
B.ID NOTIN 222
B.USERNAME IN ann
```

- Example 7: Select JP1 events that have extended attributes with the attribute name TASK_NAME, and that have inventory_management set as the value of the attribute.

```
E.TASK_NAME IN inventory_management
```

- Example 8: Select JP1 events that have extended attributes with the attribute name TASK_NAME (the attribute value is irrelevant).

```
E.TASK_NAME DEFINED
```

- Example 9: Select JP1 events that occurred on or after June 16, 2002#.

```
B.TIME TRANGE 20020616000000 99999999999999
```

- Example 10: Select JP1 events that have:
  - `Warning` or `Error` set as the value of the extended attribute `SEVERITY`, and for which the extended attribute `PRODUCT_NAME` is defined
  - `www.hitachi.co.jp` set as the source event server, and `/HITACHI/JP1/AJS` set as the value of the extended attribute `PRODUCT_NAME`

```
E.SEVERITY IN Warning Error
E.PRODUCT_NAME DEFINED
or
B.SOURCESERVER IN www.hitachi.co.jp
E.PRODUCT_NAME IN /HITACHI/JP1/AJS
```

- Example 11: Select JP1 events that occurred within 30 minutes before the current time (current time:01:30:00 on July 16, 2003)#.

```
B.TIME WITHIN M 30
(Same as B.TIME TRANGE 20030716013000 20030716010000)
```

- Example 12: Select JP1 events that occurred within 24 hours before the current time (current time:01:21:21 on July 16, 2003)#.

```
B.TIME WITHIN M 24
(Same as B.TIME TRANGE 20030715012121 20030716012121)
```

- Example 13: Select JP1 events that occurred in the last two days, including today (today: July 16, 2003)#.

```
B.TIME WITHIN D 2
(Same as B.TIME TRANGE 20030715000000 20030716235959)
```

- Example 14: Select the JP1 event whose event ID is `101` or `102,` or whose severity level has an error. However, JP1 events whose source event server names are `host3` are not selected.

```
B.ID IN 101,102
or
E.SEVERITY IN Error
EXCLUDE
B.SOURCESERVER IN host3
```

#: Based on the time in the event server environment

Start sequence definition file (Windows only)

Format

```
# Comment
[ControlValue]
ForcedTerminateExec=YES

[FrontOtherServiceXXX]
Name=any-name
ServiceName=name-of-the-service-to-start-and-stop
StartCommand=command-to-execute-at service-startup
StopCommand=command-to-execute-at-service-stop
Parallel=YES
Wait=maximum-wait-time(in seconds)-for-completion-of-service-startup-processing
StopWait=maximum-wait-time(in seconds)-for-completion-of-service-stop-processing

[Jp1XXX]
Name=any-name
ServiceName=name-of-the-service-to-start-and-stop
StartCommand=command-to-execute-at service-startup
StopCommand=command-to-execute-at-service-stop
Parallel=YES
Wait=maximum-wait-time(in seconds)-for-completion-of-service-startup-processing
StopWait=maximum-wait-time(in seconds)-for-completion-of-service-stop-processing

[OtherServiceXXX]
Name=any-name
ServiceName=name-of-the-service-to-start-and-stop
StartCommand=command-to-execute-at service-startup
StopCommand=command-to-execute-at-service-stop
Parallel=YES
Wait=maximum-wait-time(in seconds)-for-completion-of-service-startup-processing
StopWait=maximum-wait-time(in seconds)-for-completion-of-service-stop-processing

[Command]
ReadyCommand=command-to-execute-after-all-service-startup-processing-has-completed
StopReadyCommand=command-to-execute-after-all-service-stop-processing-has-completed
```

File name

`JP1SVPRM.DAT` (Start sequence definition file)

`JP1SVPRM.DAT.MODEL` (Start sequence definition file model file)

Storage destination directory

installation-folder`\conf\boot\`

Description

This file specifies the startup and stop sequences for the JP1 series product services, non-JP1 series product services, and the commands and batch files to be executed after the services have started or stopped.

Application of settings

Execute the `cpysvprm` command to create the start sequence definition file (`JP1SVPRM.DAT`). Restart Windows to apply the settings. For details on the `cpysvprm` command, see *cpysvprm (Windows only)* in *13. Commands*.

Definition details

The parameters of the start sequence definition file (`JP1SVPRM.DAT`) are described below. In the start sequence definition file (`JP1SVPRM.DAT`), you can specify file names that are longer than 8 characters or include spaces. To insert a comment line, prefix the line with `#`. The characters following `#` and up to the next linefeed constitute a comment.

`[ControlValue]`

Specify parameters in this section to perform a sequenced stop of services when a forced termination is performed from JP1/Power Monitor. You can specify just `ForcedTerminateExec=` in this section.

For a JP1/Power Monitor planned termination, JP1/Base always performs service stop processing as defined in the start sequence definition file (`JP1SVPRM.DAT`), even if you omit the `[ControlValue]` section.

`ForcedTerminateExec=`

Specify `YES` to execute service stop processing at forced termination from JP1/Power Monitor. If you specify any other value or omit this parameter, JP1/Base will not perform service stop processing at forced termination from JP1/Power Monitor.

`[FrontOtherServiceXXX]`

In this section, write information about the non-JP1 services that you want to start *before* services provided by JP1 programs. In *xxx*, write any name using no more than 60 alphanumeric characters. Letters are not case sensitive.

`[Jp1XXX]`

In this section, specify information about the services provided by JP1 products. *xxx* represents a product name. For services provided by JP1 products, *xxx* has been written in the supplied file `JP1SVPRM.DAT.MODEL`. You can also specify any name in *xxx* to add a service that is not included in the model file. Write no more than 60 alphanumeric characters. Letters are not case sensitive.

`[OtherServiceXXX]`

In this section, write information about the non-JP1 services that you want to start *after* services provided by JP1 programs. In *xxx*, write any name using no more than 60 alphanumeric characters. Letters are not case sensitive.

`Name=`

Specify this parameter in the `[FrontOtherService`*xxx*`]`, `[Jp1`*xxx*`]`, and `[OtherService`*xxx*`]` sections. You can write any identifier in `Name=`.

`ServiceName=`

Specify this parameter in the `[FrontOtherService`*xxx*`]`, `[Jp1`*xxx*`]`, and `[OtherService`*xxx*`]` sections. Write the name of the service that you want to start and stop. If you omit this parameter, start and stop will not be controlled.

The service name written in this parameter might differ from the service name displayed in the Services dialog box, which opens from the Control Panel. For details, check with the manufacturer of the particular program.

`StartCommand=`

Specify this parameter in the `[FrontOtherService`*xxx*`]`, `[Jp1`*xxx*`]`, and `[OtherService`*xxx*`]` sections. Specify a command to be executed at service startup. Only one command can be specified.

`StopCommand=`

Specify this parameter in the `[FrontOtherService`*xxx*`]`, `[Jp1`*xxx*`]`, and `[OtherService`*xxx*`]` sections. Specify a command to be executed at service stop. If you omit this parameter, stop processing will not be performed. Only one command can be specified.

`Parallel=`

Specify this parameter in the `[FrontOtherService`*xxx*`]`, `[Jp1`*xxx*`]`, and `[OtherService`*xxx*`]` sections. Specify `YES` to start the service in parallel, during start processing of another service. If you specify any other value or omit this parameter, start processing for this service will begin after completion of start processing for the preceding service.

The `Parallel=` *parameter* is enabled when the service start sequence is being controlled. When the service stop sequence is being controlled, stop processing for this service will begin after the completion of shutdown processing for the preceding service, regardless of the `Parallel=` *parameter* setting.

`Wait=`

Specify this parameter in the `[FrontOtherService`*xxx*`]`, `[Jp1`*xxx*`]`, and `[OtherService`*xxx*`]` sections. Specify the maximum wait time (in seconds) for completion of service start processing. If start processing has not completed within the specified time, JP1/Base begins start processing for the next service. The specifiable range is from `1` to `86400` (seconds). The default is `60`.

`StopWait=`

Specify this parameter in the `[FrontOtherService`*xxx*`]`, `[Jp1`*xxx*`]`, and `[OtherService`*xxx*`]` sections. Specify the maximum wait time (in seconds) for completion of service stop processing. If stop processing has not completed within the specified time, JP1/Base begins stop processing for the next service. The default is `60` seconds. The specifiable range is `1` to `86400` seconds (24 hours).

`[Command]`

In this section, write information about the command or batch file to be executed after all services have started or stopped. You can write simply `ReadyCommand=` or `StopReadyCommand=` in this section.

`ReadyCommand=`

Write this parameter in the `[Command]` section. Specify a command to be executed after completion of start processing for all services. To execute multiple commands, prepare a batch file and specify the batch file name in `ReadyCommand=`.

`StopReadyCommand=`

Write this parameter in the `[Command]` section. Specify a command to be executed after the processing for all of the services has completed. To execute multiple commands, prepare a batch file and specify the batch file name in `StopReadyCommand=`.

Notes

- The square brackets enclosing section names are mandatory. Make sure that each section name is enclosed with square brackets when writing the start sequence definition file (`JP1SVPRM.DAT`).
- Write each section name once only. If the start sequence definition file (`JP1SVPRM.DAT)` contains duplicate section names, only the first one is used.
- Do not write duplicate names or command names in parameters within a section. If a section contains duplicate names or command names, the first one is valid.
- Sections can be written in any order in the start sequence definition file (`JP1SVPRM.DAT)`. However, processing within the `[FrontOtherService`*xxx*`]`, `[Jp1`*xxx*`]`, and `[OtherService`*xxx*`]` sections will be executed in the order written.
- When writing information about services that are linked by dependency relationships, write the main service first, followed by the dependent services. If

you write the dependent services before the main service, the main service will start automatically when the dependent services start. As a result, JP1/Base will not perform stop processing for the main service.

- The command set in `StopCommand=` can only be used for a service that starts under the startup control (a service started by setting the `StartCommand=` parameter). Stop processing will not be executed, even if a command is set in `StopCommand=`, when the service is already active when the startup control begins.
- Commands that require interactive operation or launch a GUI window cannot be specified in `StartCommand=`, `StopCommand=`, `ReadyCommand=`, or `StopReadyCommand=`.

  If you specify such commands, the service will end abnormally.
- Commands specified in `StartCommand=`, `StopCommand=`, `ReadyCommand=`, or `StopReadyCommand=` cannot access other machines in the network. If you specify a command that performs an operation for another machine in the network, an error will occur during execution.
- To specify the full path of a command name that includes a space, enclose the command name with double quotation marks (`"`). If the path does not include a space, you do not have to used double quotation marks. You can specify an argument in a command.
- The service stop sequence is not controlled if you quit by clicking the Windows **Start** menu and choosing **Shut Down**. To control the sequence in which services stop, you must execute shutdown from JP1/Power Monitor.
- The service stop sequence cannot be controlled if you stop the JP1/Base Control Service manually, even if stop sequence control is defined in the start sequence definition file (`JP1SVPRM.DAT)`.
- If you want to start a particular service automatically or manually without using the JP1/Base Control Service, add comment delimiters to the service definition in the start sequence definition file (JP1SVPRM.DAT). Also, add comment delimiters to all the service definitions having dependencies with that service. Enter a hash mark (`#`) at the beginning of every line that is a definition of a service.

  Having edited the start sequence definition file (`JP1SVPRM.DAT`) in this way, you can then work with that service in the Services dialog box that opens from the Control Panel in Windows. If you start the services automatically or manually without adding comment delimiters, the KAVA4003-E message might appear and the system might not operate correctly.

Definition examples

The following shows examples of settings in the start sequence definition file

(JP1SVPRM.DAT).

```
# Enter the following definition to stop services in sequence
when there is a forced termination from JP1/Power Monitor.
[ControlValue]
ForcedTerminateExec=YES

# Specify the services you want to start before the JP1 services.
[FrontOtherService1]
Name=ABC
ServiceName=ABC
StartCommand="c:\Program Files\ABC\start.exe" -start
StopCommand="c:\Program Files\ABC\start.exe" -stop
[FrontOtherService2]
Name=DEF
ServiceName=def_serv

# Specify the services provided by JP1 products.
[Jp1BaseStart]
Name=JP1/Base
ServiceName=JP1Base
StopCommand="jbs_spmd_stop.exe"
[Jp1BaseEvent]
Name=JP1/Base Event
ServiceName=JP1_Base_Event
   :
[Jp1Nps]
Name=JP1/Nps
ServiceName=JP1_NPS
Wait=60
Parallel=YES

# Specify the services you want to start after the JP1 services.
[OtherService1]
Name=XYZ
ServiceName=XYZ

# Specify the command to be executed after all services have
stopped.
[Command]
StopReadyCommand=c:\sfiles\stop.exe
```

Service startup delay time / timer monitoring period definition file (Windows only)

Format

```
[StartTimeControl]
DelayTime=delay-time-for-service-start-processing-in-seconds
SurveillanceTime=monitoring-time-in-seconds
```

File name

`Jp1svprm_wait.dat` (service startup delay time / timer monitoring period definition file)

`Jp1svprm_wait.dat.sample` (sample of service startup delay time / timer monitoring period definition file)

Storage destination directory

installation-folder`\conf\boot\`

Description

Sets the specified length of time that the startup of services is delayed and the length of time that the startup of services is monitored in the start sequence definition file (`JP1SVPRM.DAT`).

Application of settings

After Windows or all the services specified in the start sequence definition file (`JP1SVPRM.DAT`) have stopped, restart the JP1/Base Control Service to apply the settings.

Definition details

Service startup delay time

Set the length of time that the startup of the services in the start sequence definition file (`JP1SVPRM.DAT`) will be delayed. Enter a value in the range from `1` to `900` (seconds).

Timer monitoring time

Set the length of time that the startup of the services in the start sequence definition file will be monitored. Enter a value in the range from `60` to `900` (seconds). If any service fails to start within this period, a message is output to the Windows event log and to the integrated trace log.

Notes

- When a startup delay time is set, the setting `Parallel=YES` (allow services to start in parallel) in the start sequence definition file (`JP1SVPRM.DAT`) is ignored.
- Be aware that if any services activated by the startup control are monitored by JP1/PFM/SSO or controlled by JP1/Power Monitor, monitoring or control of the service will be suspended during the specified delay time.
- If a forced termination or planned termination is executed from JP1/Power Monitor on the local machine during the delay time for service startup, system stop processing waits until the delay time has elapsed.

Definition examples

The following shows examples of settings in the service startup delay time / timer monitoring period definition file (`Jp1svprm_wait.dat`).

```
[StartTimeControl]
DelayTime=60
SurveillanceTime=600
```

Event server index file

Format

```
server event-server-name directory-name
```

File name

`index`

Storage destination directory

In Windows:

installation-folder`\conf\event\`

In UNIX:

`/etc/opt/jp1base/conf/event/`

Description

Accessed by the event server. It defines the directories where the other environment setting files, event databases, and work files are stored. There is usually no need to change the default settings in this file.

You can define multiple event servers if you want to specify a large-capacity or high-speed disk other than the one where you have installed JP1/Base or you want to run more than one event server on the local host.

Application of settings

Start the event service to apply the settings.

Definition details

The following conventions apply to entries in the event server index file (`index`):

- Each line of the text file is no more than 1,024 bytes and the file size is no more than 2 GB.
- Separate parameter keywords with a space (code `0x20`) or a tab (code `0x09`).
- Do not insert a space or any other characters in front of the parameter name at the start of a line.
- A hash mark (`#`) (code `0x23`) at the start of a line indicates a comment. You can enter a comment or line space anywhere in a file.
- Letters are case sensitive.

Specify an event server and directory to use. To have multiple event servers on the local host, associate each event server with a corresponding directory.

`server` *event-server-name directory-name*

event-server-name

Specify the name of the event server. For *event-server-name*, specify one of the following names. The default is `*`:

- `*`

  In this case, the local host name (value returned by the `hostname` command) is used. Under normal circumstances, there is no need to change the default asterisk. If you configure the JP1 program to support DNS, you should replace the asterisk with an event server name or an at mark (`@`).

- *event-server-name*

  Specify this parameter if you configured the JP1 program to support DNS or use JP1 programs in a cluster system. For an example of configuring an event server in a system that uses DNS, see *8.1.3 Setting up an event server in a system that uses DNS services*.

  For the event server name, specify the name of the host on which the event server starts as a character string of no more than 255 bytes. Letters are case sensitive. If you want to use a server to distribute and collect event service definitions in an environment that supports the DNS, you should specify an at mark (`@`) for the event server name.

- `@`

  When an at mark (`@`) is specified, the event server supports the DNS. Also, the event server can be used to distribute and collect event service definitions in an environment that supports the DNS.

directory-name

You can change the directory that the event server uses. If the directory has been changed, place the event server settings file and forwarding settings file in this directory.

- When a full path is specified:

  Place the event database and all the work files in the specified directory.

- When a partial path is specified:

  The partial path indicates subdirectories of the directory shown in the following table, so place the event database and all the work files in the specified directories.

Table 14-4: Base directories of the partial paths specified (in Windows)

File name	Directory
Event server settings file or forwarding settings file	*installation-folder*`\conf\event\servers\`
Event database	*installation-folder*`\sys\event\servers\`
Temporary work files	*installation-folder*`\sys\tmp\event\servers\`

Table 14-5: Base directories of the partial paths specified (in UNIX)

File name	Directory
Event server settings file or forwarding settings file	`/etc/opt/jp1base/conf/event/servers/`
Event database	`/var/opt/jp1base/sys/event/servers/`
Temporary work files	`/var/opt/jp1base/sys/tmp/event/servers/`

Notes

- To support the DNS, the DNS must return a FQDN as a local host name. If the DNS fails to return the FQDN as a local host name, the FQDN format event server will not be recognized as an event server of the physical host.
- If you change the server parameter of an active event service, the event service does not stop.

Event server settings file

Format

```
# Comment
ports address receiver-port AP-port
client-bind address
users { * | user-name } ...
eventids {* | basic-code | basic-code:extended-code-card}...
alt-userid alternate-user-ID alternate-group-ID
forward-limit retry-time
after-error forwarding-suspension-period
retry-interval transfer-retry-interval
buffnum SES-event-count
include ses-conf file-name
include ajs-conf
expire event-expiration-time
db-size event-database-capacity
remote-server event-server-name communication-type [address [port]]
forward-timeout amount-of-time-to-wait
options [no-sync | sync] [remote-receive] [conv-off] [v5-unused] [KAJP1037-hntroff]
[KAJP1037-syslogoff] [save-rep]
error-size file-size
trace-size file-size
evtlog-size file-size
fwderr-size file-size
log-keep log-file-count
log-level level
repetition-noncheck-server { * | event-server-name } ...
restart number-of-restart retry-interval reset time
```

File name

`conf`

Storage destination directory

In Windows:

folder-specified-in-event-server-index-file\
shared-folder`\jp1base\event\conf\ (in a cluster system)`

For the default event server index file (`index`), the file name is:
installation-folder`\conf\event\servers\default\`

In UNIX:

directory-specified-in-event-server-index-file/
shared-directory`/event/conf (in a cluster system)`

For the default event server index file (`index`), the file name is: `/etc/opt/jp1base/conf/event/servers/default/`

Description

Defines the operating environment for the event service. In this file, you mainly define the following information:

- The IP address and port number for sending and receiving JP1 events
- Which JP1 events are retrievable and the JP1 users permitted to acquire those events
- Whether to retry upon a failed attempt to forward an event
- The sending and receiving of JP1 events to and from a host running JP1/SES and JP1/AJS
- The expiration time for JP1 events stored in the event database and the maximum size of the event database
- The connection method for forwarding JP1 events to an event server at a remote host, and the procedure for handling transfer errors

Application of settings

Start or restart an event service to apply the settings.

Definition details

The following conventions apply to entries in the event server settings file (`conf`).

- Each line of the text file is no more than 1,024 bytes and the file size is no more than 2 GB.
- Separate parameter keywords with a space (code `0x20`) or a tab (code `0x09`).
- Do not insert a space or any other characters in front of the parameter name at the start of a line.
- A hash mark (`#`) (code `0x23`) at the start of a line indicates a comment. You can enter a comment or line space anywhere in a file.
- Letters are case sensitive.

`ports` *address receiver-port AP-port*

Specify the IP address and port number to be used by the event server when connecting to a remote program. The values specified here do not apply to receiving events from hosts running either of the pre-version 6 programs, JP1/SES or JP1/AJS.

address

Specify the IP address in one of the following forms.

If you omit the `ports` parameter, the event server name is used.

- `0.0.0.0`

  No set address. The system determines the IP address.

  For a system that only runs on physical hosts, specify the IP address.

- *IP-address*

  Specify numbers separated by periods (example: `172.16.50.50`). You can specify multiple IP addresses. Multiple IP addresses are useful when you use event services in an environment with multiple networks. For details on using JP1/Base in an environment with multiple networks, see *4.3 Using JP1/Base in an environment of distinct networks*. When you specify multiple IP addresses, separate them with a colon (example: `172.16.50.50:172.16.50.51:172.16.50.52`). You can assign no more than four IP addresses.

  Note

  If you specified an IP address other than the IP address returned to the primary server by the OS name resolution, you need to specify the IP address in the `server` parameter in the API settings file.

- *host-name*

  Specify a name that is no more than 255 bytes and can be converted into an IP address by the system's `hosts` file or name server.

receiver-port

Specify the port number for receiving JP1 events forwarded from a remote server. Use either of the following:

- *port-number*

  Specify the port number using numbers.

- Service name

  Specify the `tcp` service name defined in the system's `services` file. As a general rule, specify `jp1imevt` for the service name. This value is used when the `ports` parameter is omitted.

AP-port

Specify the port number for receiving requests from an application to issue or acquire JP1 events. Use either of the following:

- *port-number*

Specify the port number using numbers.

- Service name

  Specify the `tcp` service name defined in the system's `services` file. As a general rule, specify `jp1imevtapi` for the service name. This value is used when the `ports` parameter is omitted.

`client-bind` *address*

Specify the IP address the event server uses to send JP1 events to other programs. This parameter is useful when you use event services in an environment with multiple networks. Under normal circumstances, there is no need to specify `client-bind`. When you omit it, JP1 events are sent from the IP address specified in the `ports` parameter. For details on using JP1/Base in an environment with multiple networks, see *4.3 Using JP1/Base in an environment of distinct networks*. Note that this parameter setting is not applicable when transferring events to hosts running either of the pre-version 6 programs, JP1/SES or JP1/AJS.

address

Specify the IP address using either of the following methods:

- `0.0.0.0`

  No specific IP address is set, and the system automatically assigns one. Specify this value as a general rule when you enable multi-LAN connectivity.

- *IP-address*

  Specify numbers separated by periods. This address is used to send events.

`users {* |` *user-name*`}...`

Specify the users permitted to acquire JP1 events.

You can specify this parameter more than once. The permitted users are equivalent to the sum of all the specifications. When the `users` parameter is omitted, no users can acquire JP1 events.

`*`

All users can acquire JP1 events.

user-name

Specify a user name. The specified user can acquire JP1 events.

`eventids {* |` *basic-code* `|` *basic-code*`:`*extended-code*`}...`

Specify which event IDs can be acquired by programs. If a JP1 event is issued whose ID is not specified, an error will not occur, but the event cannot be acquired.

You can specify this parameter more than once. The retrievable event IDs are equivalent to the sum of all the specifications. When the `eventids` parameter is omitted, no JP1 events can be acquired.

`*`

All JP1 events can be acquired.

basic-code

Specify the basic code for each event ID, using no more than 8 hexadecimal digits. The extended code is always 0.

basic-code`:`*extended-code*

Specify the basic and extended code for each event ID, using no more than 8 hexadecimal digits each, using a colon to separate the two codes.

`alt-userid` *alternate-user-ID alternate-group-ID*

Specify a value to be set in the event data, replacing the numerical user ID or group ID which are not recognized in the Windows and Java execution environment.

In *alternate-user-ID* and *alternate-group-ID*, specify a number from -1 to 65,535. If a value is not specified, -1 is used for both values.

`forward-limit` *retry-time*

Specify the retry timeout period for forwarding JP1 events that have failed to be sent. The system resends the JP1 events specified in the forwarding settings file (`forward`) at regular intervals, specified by the `retry-interval` parameter, until the transfer succeeds or the specified time elapses. Specify a number from `0` to `86400` (seconds). When no time limit has been specified, the default is `0` (i.e. no retries). When you specify the `forward-limit` parameter, specify a value greater than the retry interval specified for the `retry-interval` parameter.

`after-error` *forwarding-suspension-period*

Specify the length of time that JP1 event transfer will be suspended after it fails to be forwarded to a remote server. During the specified time, the remote server is assumed to be in an error state and, as a result, no JP1 events will be forwarded to that server. Specify a number from `0` to `2147483647` (seconds). The value must be less than the `retry-interval` parameter. The default is `30`.

`retry-interval` *transfer-retry-interval*

Specify the interval at which the system will attempt to resend JP1 events that failed. Specify a number from `60` to `2147483647` (seconds). The value must be greater than the after-error parameter. The default is `600`.

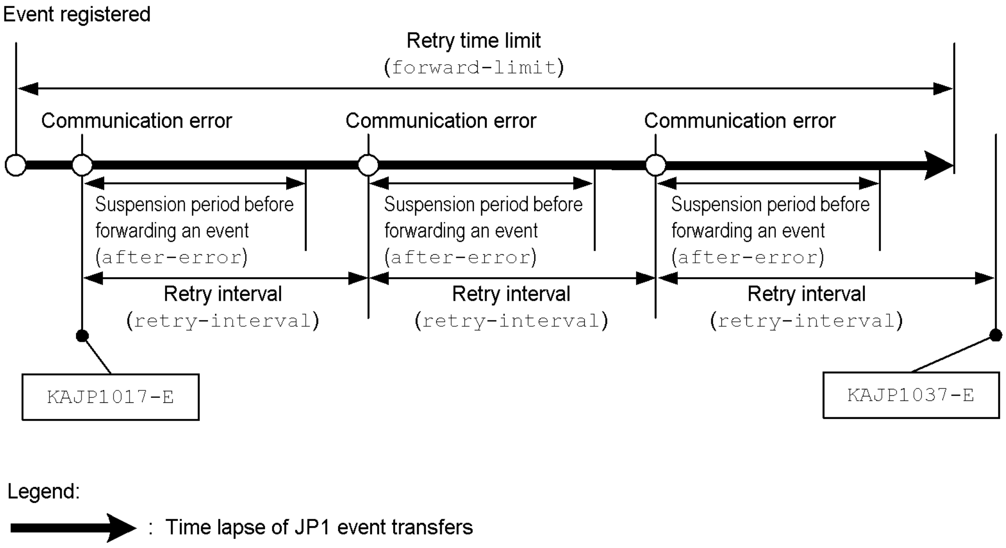
Correlation between the parameters related to retrying

The parameters related to retrying JP1 event transfers are `forward-limit`, `after-error`, and `retry-interval`. By default, if a JP1 event fails to forward, JP1/Base will retry at 600-second intervals for a maximum of 3,600 seconds.

In a cluster system, if a failover occurs on the sending or receiving host while a JP1 event is being transferred, the transfer will fail. In the JP1/Base settings, always enable retries to ensure that JP1 events will be forwarded successfully.

The following figure shows the correlation between the parameters related to retrying JP1 event transfers:

Figure 14-2: Correlation between the parameters related to retrying JP1 event transfers


Event registered
Retry time limit
(forward-limit)
Communication error
Communication error
Communication error
Suspension period before forwarding an event (after-error)
Suspension period before forwarding an event (after-error)
Suspension period before forwarding an event (after-error)
Retry interval (retry-interval)
Retry interval (retry-interval)
Retry interval (retry-interval)
KAJP1017-E
KAJP1037-E
Legend:
: Time lapse of JP1 event transfers

If another JP1 event is transferred within the retry interval not within the `after-error` suspension period, at the same time, JP1/Base will also reattempt to transfer the event that failed to transfer before.

If the event service is restarted or reloaded while JP1/Base is reattempting to transfer a JP1 event, the JP1 event will be resent after the event service is restarted, provided the `forward-limit` time has not elapsed.

`buffnum` *SES-event-count*

This parameter links the JP1/SES event with the product to use. For details on this parameter, see *J. Linking with Products That Use JP1/SES Events*.

`include ses-conf` *file-name*

This parameter links the JP1/SES event with the product to use. For details on this parameter, see *J. Linking with Products That Use JP1/SES Events*.

`include ajs-conf`

This parameter links the JP1/SES event with the product to use. For details on this parameter, see *J. Linking with Products That Use JP1/SES Events*.

`expire` *event-expiration-time*

Specify the length of time for storing issued JP1 events in the event database. JP1 events are stored in the event database for the specified time and while they are in the database, they can be viewed from JP1/IM - View. If the JP1 events stored in the database reach the capacity specified in the `db-size` parameter, events might be deleted even though the expiration time has not yet been reached. Specify a number from `0` to `2147483647` (seconds). If an expiration time is not specified, the default is `31536000` (365 days).

`db-size` *event-database-capacity*

Specify the event database capacity. When the specified size is reached, JP1 events might be deleted, starting from the oldest ones, even though the expiration time specified in the `expire` parameter has not been reached. The JP1/Base event service occupies up to twice the amount of disk space specified in this parameter. Specify a number from `0` to `2147483647` (bytes). The default is `2147483647`.

The following is the formula for calculating the capacity required for the event database in respect to the number of days for which events are stored. Use this formula as a guide for specifying the capacity:

`[a x (b + 64) + (c x 64)}x d]/2` (bytes)

a: Number of events registered per day#

b: Average size per event. (You must actually measure this size.)

c: Number of events transferred per day

d: Number of days for storage

#: The events registered daily include those generated on the local host, JP1/SES events, JP1 events received from other hosts, and transferred events.

`remote-server` *event-server-name communication-type* `[`*address* `[`*port*`]]`

Specify the method for connecting to a remote server for event transfers. You can specify multiple `remote-server` parameters if the value in *event-server-name* is different in each case.

event-server-name

Specify the event server name in either of the following ways:

- *event-server-name*

  Specify a specific event server name that is no more than 255 bytes.

- `*`

  Specify an asterisk to indicate all of the event servers, other than those that have been individually specified.

  When this specification is omitted, events can be forwarded only to event servers that are explicitly specified.

communication-type

Specify the method for connecting to the specified remote server:

- `keep-alive`

  When you need to forward a JP1 event to a remote server, establish a TCP/IP connection from the sending server, and forward the event. After the event transfer, keep the connection open so it can be reused until the remote event server shuts down.

  Note

  When a connection is severed, and then recovered, the first attempt to transfer a JP1 event after the connection is recovered might fail. A connection might be severed, either because the firewall is set up to do so when there is no communication between the servers, or because a temporary communication error occurred.

- `close`

  When you need to forward a JP1 event to a remote server, establish a TCP/IP connection from the sending server, and forward the event. End the connection three seconds after the event transfer.

- `ses`

  This parameter links the JP1/SES event with the product to use. For details on this parameter, see *J. Linking with Products That Use JP1/SES Events*.

address

Specify the IP address using either of the following methods:

- *IP-address*

  Specify numbers separated by periods (example: `172.16.50.50`).

- *host-name*

  Specify a name that is no more than 255 bytes and that can be converted into an IP address by the system's `hosts` file or name server.

The specified address must match the value set in the `ports` parameter for the event server specified in the event server settings file (`conf`).

The default host name is the event server name.

port

Specify the port number using one of the following methods:

- *port-number*

  Use numbers to specify the port number.

- Service name

  Specify the `tcp` service name defined in the system's `services` file.

The specified address must match the value set in the `ports` parameter for the event server specified in the event server settings file (`conf`).

The default is the same value as the transfer port of the local event server.

`forward-timeout` *amount-of-time-to-wait*

Specify the length of time to wait for a response from the destination server when forwarding a JP1 event. If no response is received within the specified time, the system assumes that the transfer failed.

Specify a number from `10` to `600` (seconds). The default is `90`.

`options [no-sync | sync] [remote-receive] [conv-off] [v5-unused] [KAJP1037-hntroff] [KAJP1037-syslogoff] [save-rep]`

Specify option flags. You can specify the parameter and a flag on different lines.

`no-sync | sync`

After the `no-sync` flag is specified, the system is allowed to buffer JP1 events written to the database. Specifying this flag might improve performance when JP1 events are generated. However, issued JP1 events might be lost if the system shuts down unexpectedly due to a failure. The purpose of using JP1/Base in a cluster system is to enhance reliability, so do not specify this option.

Specifying `sync` flag ensures that each JP1 event will be written to disk when the event is issued. You can thus acquire all of the events after restarting the system. Writing each JP1 event to disk at the time it is issued might, however, cause a performance decrease when issuing JP1 events.

If you specify neither the `no-sync` flag nor the `sync` flag, events are written to the disks at regular intervals (every 10 seconds), so only some of the issued JP1 events might be lost.

`remote-receive`

Allows JP1 events to be acquired by a program running on a remote host over a network.

You must specify this flag to search for JP1 events on a remote host using the JP1/IM - View GUI connected to that host, and to view information in the pre-Version 6 program JP1/AOM-EE.

`conv-off`

This flag links the JP1/SES event with the product to use. For details on this flag, see *J. Linking with Products That Use JP1/SES Events*.

`v5-unused`

Suppresses the use of all of the functions related to the compatibility with the pre-Version 6 programs, JP1/SES and JP1/AJS. When you specify this flag, the processes used for the compatibility with JP1/SES and JP1/AJS will not start. Therefore, sending or receiving events to or from JP1/OJE and other products by using the JP1/SES protocol is not possible.

Do not remove this flag unless it is linked with the programs that are compatible to pre-version 6. For details on the linkage with pre-Version 6 products, see *J. Linking with Products That Use JP1/SES Events*.

`KAJP1037-hntroff`

Suppresses output of the `KAJP1037-E` (event transfer failure) message to the integrated trace log.

`KAJP1037-syslogoff`

Suppresses the `KAJP1037-E` (event transfer failure) message being output to the `syslog` (in UNIX) or the event log (in Windows).

`save-rep`

Keeps the event database duplication prevention table in a file. The duplication prevention table prevents JP1 events from being registered twice.

If you specify the `save-rep` flag, make sure that the directory that stores the event database has a minimum capacity of 32 + total number of the source event servers x 288 bytes. For details on the duplication prevention table, see *1.4.2 Event database.*

Note

The KAJP1017-E message informing a transfer error will be output to the integrated trace log and syslog (in UNIX) or the event log (in Windows), even if you have specified KAJP1037-hntroff or KAJP1037-syslogoff. Monitor for transfer errors by checking the KAJP1017-E message.

The KAJP1037-E message can also be checked by the event service transfer error log (fwderr.*).

error-size *file-size*

Specify the maximum size that will be used for the event service error log files (error.*). When a file exceeds the specified size, it is overwritten starting from the beginning. Specify a number from 65536 to 2147483647 (bytes). The default is 500000.

The following shows the formula for calculating the required capacity of an event service error log file in relation to the number of days for which events are stored. Use this formula as a guide for specifying the file size.

a + (b x c) x d (bytes)

a: Basic part (1 KB)

b: Average error message size (approx. 120 bytes)

c: Number of errors per day

d: Number of days for storage

trace-size *file-size*

Specify the maximum size of an event transfer trace log file (trace.*). When a file exceeds the specified size, it is overwritten from the beginning. Specify a number from 65536 to 2147483647 (bytes). The default is 1000000.

The following shows the formula for calculating the required capacity of an event transfer trace log file in relation to the number of days for which you want to store events. When specifying the file size, consider the amount of log data output per day and the number of events acquired per day.

a + (b + c + d) x e (bytes)

a: Basic part (1 KB)

b: Amount of output log data necessary to register one event x Number of events registered per day

c: Amount of output log data necessary to acquire one event x Number of events acquired per day

d: Amount of output log data necessary to transfer one event x Number of events transferred per day *e*: Number of days for storage

The amount of output log data differs according to the operation of the event service; however, the following can be used as a reference value for the amount of output log data.

Table 14-6: Amount of log output (event transfer trace log)

Amount of log output (in bytes)		
Registering an event	**Acquiring an event**#1	**Transferring an event**#2 **(retries if the transfer fails)**
Approx. 150#3	Approx. 150#3	Approx. 1,500

#1: Event acquisition includes JP1 events acquired by other applications. The value above comes from the amount of data output to a log when the 10th JP1 event is acquired from an event database containing ten events. The output amount varies depending on the number of JP1 events registered in an event database and where a JP1 event is registered.

#2: When transferring a JP1 event, the amount of data output to a log is the maximum if the transfer fails and is performed again.

#3: The amount of data output to a log when the communication type is set to `close` in the API settings file (`api`).

The number of events acquired per day represents how often events are acquired via the event acquisition function from the user application or JP1 series programs. You can use the following formula as a guideline for the number of events JP1 series products acquire per day.

```
Number-of-events-acquired#1 x
number-of-events-registered-in-event-database +
number-of-events-registered-per-day#2
```

#1: The number of JP1/IM events acquired from the event database is equivalent to the sum of the following numbers:

- Number of times JP1/IM - View is started
- Number of times JP1/IM - View searches for events

#2: If event reception jobs for JP1/AJS are registered for execution, JP1/AJS acquires events that are newly registered with the event database. JP1/AJS acquires a registered event only once even if multiple event reception jobs are registered.

`evtlog-size` *file-size*

Specify the maximum size (in bytes) of an event service trace log file (`imevterr.*`). When a file exceeds the specified size, it is overwritten from the beginning. Specify a number from `65536` to `2147483647` (bytes). The default is `1000000`.

The following is the formula for calculating the capacity required for an event service trace log in respect to the number of days for which events are stored. When specifying the file size, consider the amount of log output per day and the number of events acquired per day.

`a + (b + c + d) x e` (bytes)

a: Basic part (1 KB)

b: Amount of log output necessary to register one event x Number of events registered per day

c: Amount of log output necessary to acquire one event x Number of events acquired per day

d: Amount of log output necessary to transfer one event x Number of events transferred per day

e: Number of days for storage

The amount of output log data differs according to the operation of the event service; however, the following can be used as a reference value for the amount of output log data. An event service trace log file is not affected by the log level defined in the `log-level` parameter.

Table 14-7: Amount of log output (event service trace log)

Amount of log output (in bytes)		
Registering an event	**Acquiring an event#1**	**Transferring an event#2** **(retries the transfer if it fails)**
Approx. 3,000	Approx. 7,000	Approx. 3,000

#1: Event acquisition includes JP1 events acquired by other applications. The value above comes from the amount of data output to a log when the 10th JP1 event is acquired from an event database containing ten events. The output amount varies depending on the number of JP1 events registered in an event database and where a JP1 event is registered.

#2: When transferring a JP1 event, the amount of data output to a log is the maximum if the transfer fails and is performed again.

The number of events acquired per day represents how often events are acquired via the event acquisition function from the user application or JP1 series programs. You can use the following formula as a guideline for the number of events JP1 series products acquire per day.

`Number-of-events-acquired`[#1] `x number-of-events-registered-in-event-database + number-of-events-registered-per-day`[#2]

#1: The number of JP1/IM events acquired from the event database is equivalent to the sum of the following numbers:

- Number of times JP1/IM - View is started
- Number of times JP1/IM - View searches for events

#2: If event reception jobs for JP1/AJS are registered for execution, JP1/AJS acquires events that are newly registered with the event database. JP1/AJS acquires a registered event only once even if multiple event reception jobs are registered.

`fwderr-size` *file-size*

Specify the maximum size of an event service transfer error log file (`fwderr.*`). When a file exceeds the specified size, it is overwritten starting from the beginning. Specify a number from `65536` to `2147483647` (bytes). The default is `1000000`.

The following shows the formula for calculating the required capacity of an event transfer error log file in relation to the number of transfer failures for which you want to store events.

Number-of event-transfer-failure-to-store `x ( 150 +` *length-of-event-server-name* `+` *length-of-destination-event server-name*`)`

If there are multiple destination servers, the length of the destination event server name is equal to the length of the longest server name among the destination event server names.

`log-keep` *number-of- log-files*.

Specify the maximum number of event service error log files, event transfer trace log files, and event service trace log files that can be created. A log file is created when the event service starts. If the number of log files at event service startup exceeds the specified count, files are deleted, starting from the oldest. Specify a number from `0` to `50`. The default is `5`. When `0` is specified, logs are not kept.

`log-level` *level*

For JP1/Base versions 06-51 and earlier, specify a level for output to `syslog`, the event log, event service error log files, and event transfer trace log files. Specify a number from `1` to `10`. The default is `1`. Specify 1 as a general rule. Specify `2` or a higher level to output more detailed messages in the event of an error or attempting to recover from an error.

For JP1/Base version 06-71 and later, you do not need to specify this value because detailed log data is output regardless of the value.

`repetition-noncheck-server` *{ * | event-server-name } ...*

Specify the name of the event server that suppresses the duplication registration check. The duplication registration check checks whether a JP1 event has already been registered when receiving a JP1 event. A JP1 event is a duplicate of another if its source event server name, source event database serial number, and the time of registration are the same as the other one.

You can use the duplication check to prevent an event from being lost when forwarding a JP1/SES protocol event through several routes.

You can specify this parameter multiple times. The event servers that suppress duplication registration are equivalent to the sum of all the specifications. When this parameter is omitted, the duplication registration check is performed on the JP1 events from all source event servers.

`*`

In this case, the duplication registration checks from all source event servers are suppressed.

event-server-name

Specify the name of each event server that suppresses the duplication registration check. Event server names are case sensitive.

`restart` *number-of-restart retry-interval reset time*

Set the JP1/Base to restart if an error occurs in the event service process on the physical host. To restart JP1/Base, specify the number of restarts, the interval at which the system will attempt to restart, and the restart count reset time. The process will restart only if the number of abnormal terminations during the period specified by the reset time is less than the number of restart times. The recovery message (`KAJP1072-I`) is output when the process restarts. The message is also sent out as a JP1 event (event ID: `00003D04`). Therefore, if you see this JP1 event, then you know that the event service process was restarted. This parameter is valid only in the UNIX version of JP1/Base, not in the Windows version. If you omit this parameter, the process will not restart even after the event service process has been abnormally terminated. Instead, the event service will stop.

Also, when an event service is restarting, the JP1 event transferred from the sending host will not be received. JP1/Base will try to re-send the JP1 event, assuming that JP1/Base is set to do so on the sending host. However, if the retry interval is exceeded, the transfer will fail. To prevent such failures, make sure that the value you set for *number of restarts* x *retry interval* is less than the retry limit for forwarding JP1 events (`forward-limit` parameter) in the `conf` parameter on the sending host.

Number of restarts

Specify how many times the system will attempt to restart. The recommended value is `4`. Specify a number from `0` to `99`. If `0` is specified, the process does not restart. If you specify a number less than `0`, the system uses `0`. If you specify a number greater than `99`, the system uses `99`.

Retry interval

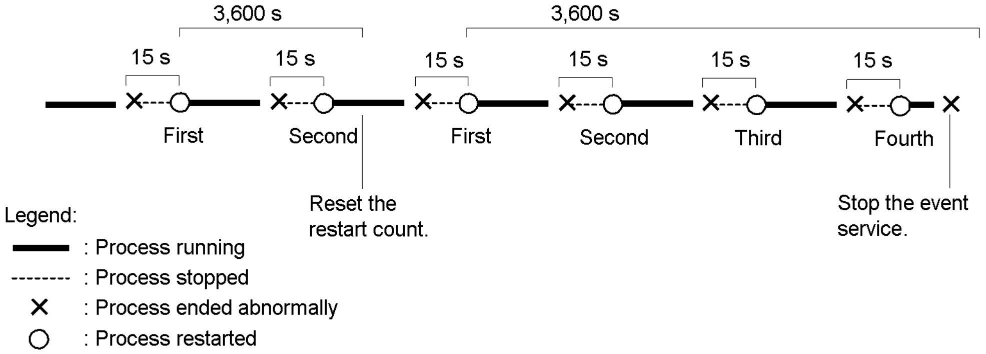
Specify how long an event service process will wait to restart after it ends abnormally. If a restart fails, the process will wait until the specified interval elapsed before another attempt is made to restart the service. The recommended value is `15` (seconds). Specify a number from `0` to `3600`. If you specify a number less than `0`, the system uses `0`. If you specify a number greater than `3600`, the system uses `3600`.

Reset time

Specify the number of seconds that will elapse after the process is restarted, before the number of restarts is reset. The number of restarts is reset the specified time after the process is restarted. The recommended reset time is `3600` (seconds). Specify a number from `3600` to `2147483647` (seconds). If you specify a number less than `3600`, the system uses `3600`. If you specify a number greater than `2147483647`, the system uses `2147483647`.

The following figure illustrates the process action using the recommended values (the number of retries is `4`, the retry interval is `15`, and the reset time is `3600`).

Figure 14-3: Example of action when an event service process ends abnormally



In this example, the number of restarts is reset 3,600 seconds after the process is restarted if the process does not end abnormally within 3,600 seconds. Then, the next time the process ends abnormally, the restart count starts from 1. If the process ends abnormally again within 3,600 seconds after the reset, the restart count is not reset. If the number of restarts reaches the specified value, the system no longer attempts to restart the process.

Notes

- Only the child processes of the `jevservice` process, whose process ID can be confirmed in the `jevstat` command, can be restarted by specifying the `restart` parameter.
- If the parent process ends abnormally, the event service stops.
- A separate retry count is used for each child process.

The `jevservice` process has the following 6 types of child processes.

Table 14-8: Event service process composition

Parent process name	Child process name	Overview
`jevservice`	`jevservice` (LogTrc)	Outputs the messages recorded in syslog or the integrated trace log.
	`jevservice` (DBMngr)	Manages the event database.
	`jevservice` (SESEmu)	This is the SES compatibility function. When the `v5-unused` flag is specified in the options parameter, this function is not used.
	`jevservice` (EvtAPI)	Accepts registration or acquisition requests of JP1 events.
	`jevservice` (FwdRcv)	Receives the forwarded JP1 events.
	`jevservice` (FwdMgr)	Forwards JP1 events.

Definition examples

The following shows examples of settings in the event server settings file (`conf`):

```
# For port number, use jp1imevt and jp1imevtapi defined
# in the system services file.
ports 0.0.0.0 jp1imevt jp1imevtapi
# Programs executed only in user root and adm can acquire
# JP1 events.
users root adm
# Only the JP1 events that have an ID of 2000, 2001, 3000,
# or 3001 can be issued and acquired by API of JP1/SES.
# Programs compatible to JP1/Base can issue and acquire all
# JP1 events.
eventids *
eventids 2000 2001 3000 3001
# If you are using Windows on your local computer, or
# if you are using UNIX on your
# local computer but JP1 events are issued by Java,
# when you forward JP1 events in UNIX environment, user ID
# or Group ID will be interpreted as 1001 and 100.
alt-userid 1001 100
# If forwarding of a JP1 event fails, JP1/Base will retry
# forwarding.
# Retry will continue until either the JP1 event is sent
# successfully or one hour
#(3600 seconds) elapses.
forward-limit 3600
# If forwarding events to a remote host fails, to prevent
# network load from increasing, no events will be sent to
# this host within the next 300 seconds.
after-error 300
# To add settings to the above userids and evendids,
# see JP1/SES environment settings
# file /usr/bin/jp1_ses/jpevent.conf.
include ses-conf /usr/bin/jp1_ses/jpevent.conf
# JP1 events received 31 days (2,678,400 seconds) ago
# will be deleted.
# Also, if data amount of the stored JP1 events reaches
# 1,000,000 bytes, JP1 events will be deleted from
# the oldest ones.
expire 2678400
db-size 1000000
# JP1 events can be acquired from a remote host.
# (Make sure to specify the host if you want to refer to the
# JP1/AOM - EE information from JP1/M-Console View that is
# connected to another computer.)
options remote-receive
# Allows the OS to buffer JP1 events written to the disk.
options no-sync
# Host 1 and host 2 are within the local LAN, so you can
# leaving them connecting to TCP/IP.
# Other computers (except host 3) are connected by phone
# line dial ups, so the connections will be frequently
interrupted.
# Host 3 uses JP1/SES, not JP1/Base.
remote-server host1 keep-alive
remote-server host2 keep-alive
remote-server host3 ses
remote-server *    close
# Set the maximum size of the error log file to 500,000 bytes,
# and the trace log file to 1,000,000 bytes.
# If the capacity exceeds the specified size, data will be
# overwritten starting from the top the file.
# If there are five or more log files, files will be deleted
# from the older ones.
error-size 500000
trace-size 1000000
log-keep 5
```

Forwarding settings file

Format

```
to-upper
event-filter
end-to
or
to event-server-name
event-filter
end-to
```

File name

`forward`

Storage destination directory

In Windows:

folder-specified-in-event-server-index-file`\`
shared-folder`\jp1base\event\ (in a cluster system)`

With the default event server index file (`index`), the file name is:
installation-folder`\conf\event\servers\default\`

In UNIX:

directory-specified-in-event-server-index-file`\`
shared-directory`/event/ (in a cluster system)`

With the default event server index file (`index`), the file name is: `/etc/opt/jp1base/conf/event/servers/default/`

Description

A forwarding settings file (`forward`) is a group of forwarding setting blocks that define which JP1 events will be forwarded to a specific event server.

Application of settings

The settings are applied when the event service starts or restarts, or the forwarding settings file is reloaded by executing the `jevreload` command. For details on the `jevreload` command, see *jevreload* in *13. Commands*.

Definition details

The following conventions apply to entries in the forwarding settings file (`forward`).

- The forwarding settings file (`forward`) is a text file and each line cannot exceed 1,024 bytes.

- Separate parameter keywords with a space (code `0x20`) or a tab (code `0x09`).
- Do not insert a space or any other characters in front of the parameter name at the start of a line.
- A hash mark (#) (code `0x23`) at the start of a line indicates a comment.
- Letters are case sensitive.

In the `to-upper` format, the JP1 events are forwarded to a server at a higher level in the hierarchy defined in JP1/IM - Manager.

In the `to` format, you can choose the destination event server. Specify an event server name defined in the remote-server parameters in the event server settings file (`conf`).

Whichever format you use, you must write filter conditions for forwarding JP1 events to the remote server. For details on the writing format of an event filter, see *Event filter syntax*.

Notes

- In a forwarding settings file (`forward`), you can write comments between the blocks, but not within a block. You can also specify multiple forwarding setting blocks.
- When JP1 events are forwarded through several routes, the destination event server might receive multiple instances of the same JP1 event. In this case, a duplication check is performed for the transferred JP1 event. The check examines the following conditions:
  - Whether the first JP1 event matches the *source event server name*.
  - - Whether the first JP1 event matches the *serial number for the source event server*.
  - - Whether the first JP1 event matches the *registered time*.
  - - Whether the *registered reason* is `4` (a forwarded event)

  If all of these conditions are met, the JP1 event is considered to be a duplicate, and the second and subsequent events are not registered in the event database.
- When multiple transfer blocks (`to` to `end-to`) are specified and have the same destination assigned, the transfer processing is done in the order of event filters set in these blocks. At the end, the forwarding processing is the same as the case when events are transferred with multiple event filters specified and connected with OR.

Definition examples

The setting examples in the figures below refer to forwarding JP1 events in the following system configuration:

Table 14-9: Example of forwarding settings

Host name	Role in configuration
jp1-svs1	Integrated manager
jp1-svs2	Submanager
jp1-sva1	JP1 site host

Conditions

JP1 events are forwarded from jp1-sva1 to jp1-svs2 if any one of the following is true:

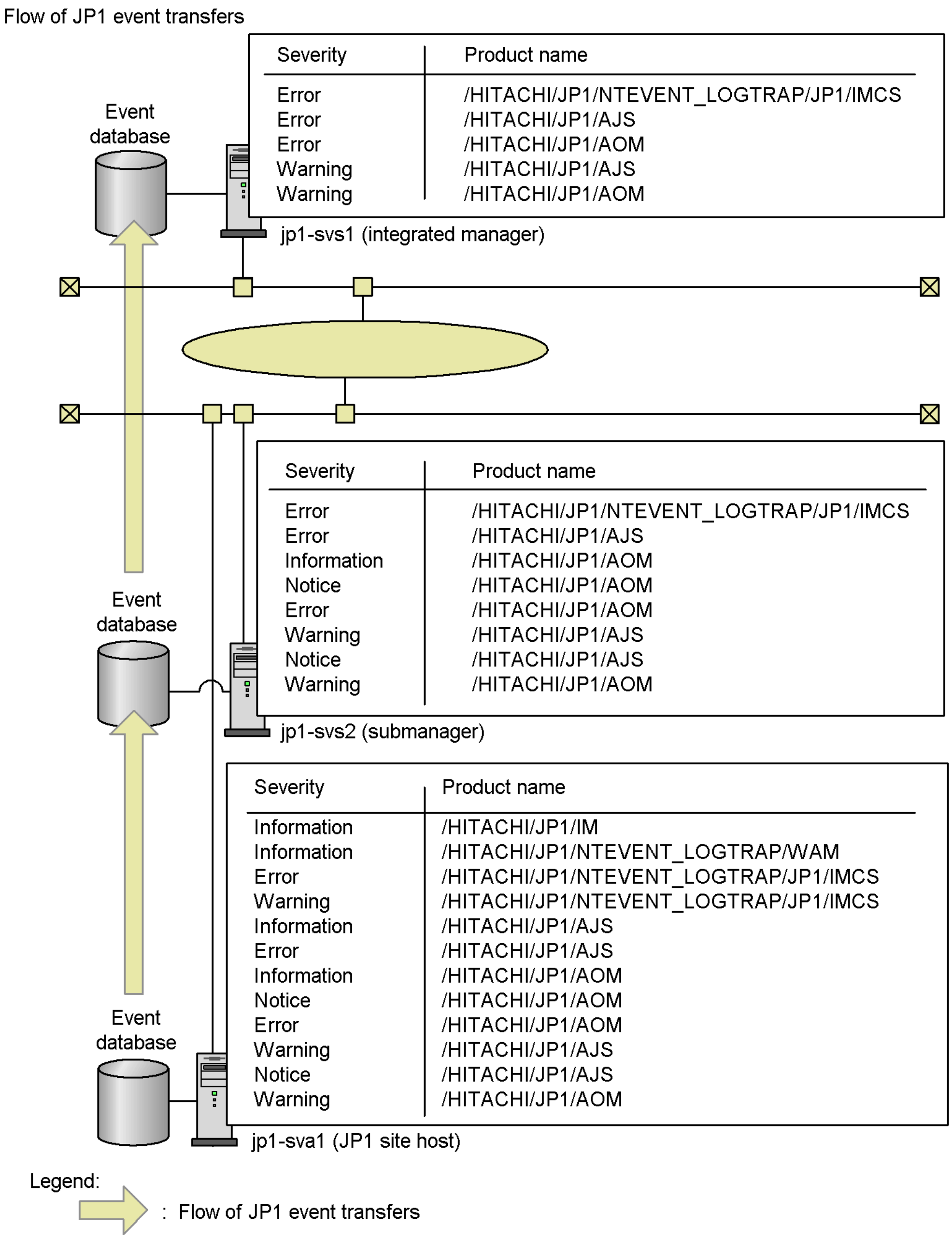
- SEVERITY is set to Error
- PRODUCT_NAME is set to /HITACHI/JP1/AJS, and SEVERITY is set to Warning or Notice
- PRODUCT_NAME is set to /HITACHI/JP1/AOM

JP1 events are forwarded from jp1-svs2 to jp1-svs1 if any one of the following is true:

- SEVERITY is set to Error
- PRODUCT_NAME is set to /HITACHI/JP1/AJS, and SEVERITY is set to Warning
- PRODUCT_NAME is set to /HITACHI/JP1/AOM, and SEVERITY is set to Warning

The flow of JP1 event transfers is shown below.

Figure 14-4: Definition examples and flow of JP1 event transfers



Severity	Product name
Error	/HITACHI/JP1/NTEVENT_LOGTRAP/JP1/IMCS
Error	/HITACHI/JP1/AJS
Error	/HITACHI/JP1/AOM
Warning	/HITACHI/JP1/AJS
Warning	/HITACHI/JP1/AOM

Severity	Product name
Error	/HITACHI/JP1/NTEVENT_LOGTRAP/JP1/IMCS
Error	/HITACHI/JP1/AJS
Information	/HITACHI/JP1/AOM
Notice	/HITACHI/JP1/AOM
Error	/HITACHI/JP1/AOM
Warning	/HITACHI/JP1/AJS
Notice	/HITACHI/JP1/AJS
Warning	/HITACHI/JP1/AOM

Severity	Product name
Information	/HITACHI/JP1/IM
Information	/HITACHI/JP1/NTEVENT_LOGTRAP/WAM
Error	/HITACHI/JP1/NTEVENT_LOGTRAP/JP1/IMCS
Warning	/HITACHI/JP1/NTEVENT_LOGTRAP/JP1/IMCS
Information	/HITACHI/JP1/AJS
Error	/HITACHI/JP1/AJS
Information	/HITACHI/JP1/AOM
Notice	/HITACHI/JP1/AOM
Error	/HITACHI/JP1/AOM
Warning	/HITACHI/JP1/AJS
Notice	/HITACHI/JP1/AJS
Warning	/HITACHI/JP1/AOM

Example of defining the forward file in jp1-svs1

```
#----------------------------------------------------------
# JP1/Base - Event Service Forwarding Setting
#----------------------------------------------------------
# Event Server Name: jp1-svs1
# (Nothing)
```

Example of defining the forward file in jp1-svs2

```
#-----------------------------------------------------------
# JP1/Base - Event Service Forwarding Setting
#-----------------------------------------------------------
# Event Server Name : jp1-svs2
to jp1-svs1
E.SEVERITY IN Error
OR
E.PRODUCT_NAME IN /HITACHI/JP1/AJS
E.SEVERITY IN Warning
OR
E.PRODUCT_NAME IN /HITACHI/JP1/AOM
E.SEVERITY IN Warning
end-to
```

Example of defining the forward file in jp1-sva1

```
#-----------------------------------------------------------
# JP1/Base - Event Service Forwarding Setting
#-----------------------------------------------------------
# Event Server Name : jp1-sva1
to jp1-svs2
E.SEVERITY IN Error
OR
E.PRODUCT_NAME IN /HITACHI/JP1/AJS
E.SEVERITY IN Warning Notice
OR
E.PRODUCT_NAME IN /HITACHI/JP1/AOM
end-to
```

API settings file

Format

```
server event-server-name communication-type [address [port]]
client event-server-name connection-source-address
log-keep number-of-log-files
log-size file-size
```

File name

`api`

Storage destination directory

In Windows:
installation-folder`\conf\event\`

In UNIX:
`/etc/opt/jp1base/conf/event/`

Description

Defines the method for connecting from the application program to the event server and the port to use for the connection. There is usually no need to change the default settings in an API settings file. You can add additional information if you want to execute an application program on the local host that obtains JP1 events from an event server on another host.

If you change the default value of the ports parameter in the event server settings file (`conf`), you must specify the same port number in the API settings file.

Application of settings

The settings are applied when the JP1/Base event converter or programs linked to an event service, such as JP1/IM or JP1/AJS, starts or restarts.

Definition details

The following conventions apply to entries in the API settings file (`api`):

- Each line of the text file is no more than 1,024 bytes and the file size is no more than 2 GB.
- Separate parameter keywords with a space (code `0x20`) or a tab (code `0x09`).
- Do not insert a space or any other characters in front of the parameter name at the start of a line.

- A hash mark (#) (code 0x23) at the start of a line indicates a comment. You can enter a comment or line space anywhere in a file.
- Letters are case sensitive.

`server` *event-server-name communication-type* `[`*address* `[`*port*`]]`

Specify how to connect to the event server. You can specify multiple `server` parameters if the value in *event-server-name* is different in each case.

event-server-name

Specify the event server name in either of the following ways:

- *event-server-name*

  Specify a specific event server name that is no more than 255 bytes.

- `*`

  Specify a value for the event servers that have not been individually specified.

  If this setting is omitted, an application program cannot connect to any event servers that are not individually specified.

communication-type

Specify the method for connecting to the specified remote server:

- `keep-alive`

  Keeps the TCP/IP connection open for reuse unless explicitly disconnected by the application program.

- `close`

  Closes the TCP/IP connection after acquiring each JP1 event. Specify `close` if you are using a telephone line, for example, and you do not want to keep the connection open all of the time. Note that specifying `close` reduces efficiency.

Notes

- Be sure to specify `keep-alive` if you want to link with the event service in JP1/AJS, JP1/IM, or JP1/Power Monitor.
- In the following cases, even if you set `close`, `keep-alive` is used for the setting:

  The IP address resolved from the OS by the physical host name (returned by the `hostname` command) is the same as the IP address of the event service to which a linked program (such as JP1/AJS, JP1/IM, or JP1/Power Monitor) is trying to connect to.

address

Specify the IP address to connect to by using one of the methods below. The specified address must match the value set in the `ports` parameter for the event server specified in the event server settings file (`conf`). The default host name is the event server name.

- *IP-address*

  Specify numbers separated by periods (example: `172.16.50.50`).

- *host-name*

  Specify a name that is no more than 255 bytes and can be converted into an IP address by the system's `hosts` file or name server.

- `0.0.0.0`

  This value prevents application programs from issuing or acquiring events. (This includes JP1 programs, but excludes application programs that use functions or commands from the pre-Version 6 JP1 programs, JP1/SES and JP1/AJS.)

  JP1/AJS and most other programs will still issue events if you specify `0.0.0.0`. But by specifying this value, you can reduce the overhead for processing issued events, and speed up event processing.

port

Specify the port number using one of the methods below. The specified address must match the value set in the `ports` parameter for the event server specified in the event server settings file (`conf`). When no port is specified, the service name is assumed to be `jp1imevtapi`.

- *port-number*

  Use numbers to specify the port number.

- Service name

  Specify the `tcp` service name defined in the system's `services` file.

`client` *event-server-name connection-source-address*

Specify the connection source address to be used when connecting to the event server. By default, the OS automatically assigns the source connection address. However, in an environment where multiple NICs are assigned, you need to define this parameter to explicitly specify which source connection address to use. You can specify multiple values for this parameter.

event-server-name

Specify the destination event server name in one of the following ways:

- *event-server-name*

  Specify a specific event server name that is no more than 255 bytes.

- `*`

  Specify a value for the event servers that have not been individually specified.

  The default connection source address is `0.0.0.0`.

Connection source address

Specify the connection source address using one of the following methods:

- *IP-address*

  Specify numbers separated by periods (example: `172.16.50.50`). The IP address specified here must be the IP address assigned to the local host.

- `0.0.0.0`

  The OS automatically assigns the connection source IP to be used.

`log-keep` *number-of-log-files*

Number of log files

Specify the number of event service API log files (`IMEvapi.*`) to be saved. The current log file is switched when its size reaches the limit specified in `log-size`. When the number of log files reaches the maximum you specify here, the oldest file is deleted. Specify a number from `0` to `50`. The default is `5`. When `0` is specified, logs are not kept.

`log-size` *file-size*

File size

Specify the maximum size (in bytes) of an event service API log file (`IMEvapi.*`). Specify a number from `65536` to `2147483647`. The default is `1000000`. Log information is output only when the API is loaded and when an error occurs.

Action definition file for log file trapping

Format

```
retry-times=number-of-retries (to connect to the event service)
retry-interval=retry-interval (to connect to the event service)
open-retry-times=retry-count (to open a log file)
open-retry-interval=retry-interval (to open a log file)
read-retry-times=retry-sets-threshold (to read a log file)
hold-count=number-of-JP1-events-to-be-held
keep-event={ OLD | NEW }
FILETYPE={ SEQ | SEQ2 | WRAP1 | WRAP2 | HTRACE }
RECTYPE={VAR { '\n ' | 'end-of-line-character' | 'end-of-line-symbol'} | FIX
record-length }
HEADLINE=number-of-header-lines
HEADSIZE=header-size
MARKSTR=[!]"regular-expressions"
      [!]"regular-expression"#
ACTDEF=[{EXIT}][<severity>][event-ID][!]"regular-expressions"
                    [!]"regular-expression"#
```

#: The regular expression *n* represents multiple specifications.

File name

Any

Storage destination directory

Any

If you have created an action definition file for log file trapping with the file name `jevlog.conf` in the following directory, you can omit the `-f` option in the `jevlogstart` command.

In Windows:

installation-folder`\conf\`

In UNIX:

`/etc/opt/jp1base/conf/`

You can create an action definition file for log file trapping in any directory, using any file name. However, you must specify a file name with the directory name added for the `-f` option of the `jevlogstart` command.

Description

Specifies the format of the monitored log file, the retry settings when monitoring fails and other settings. The action definition file for log file trapping is not provided by default. Users can create the file, or the file can be created by using the distribution definition function.

Application of settings

The settings are applied when you execute the `jevlogstart` command or the `jevlogreload` command. For details on the `jevlogstart` and `jevlogreload` commands, see *jevlogstart* and *jevlogreload* in *13. Commands*.

Definition details

The following conventions apply to entries in the action definition file for log file trapping:

- A hash mark (#) (code `0x23`) at the start of a line indicates a comment.
- Start writing from column 1.
- Link parameters and their values with equal signs. You can enter blanks between the parameter and equal sign, but not between the equal sign and the value. For a parameter to which multiple values are specified, enter blanks between the values. A blank is one or more spaces or tab characters. Examples are shown below:

  `FILETYPE△ △=SEQ`

  `ACTDEF=0△message`

  where △ indicates a single space.
- A comment cannot be written between values or at the end of multiple values, or on a new line. Only enter spaces.

`retry-times=`*number-of-retries* (to connect to the event service)

Specify the number of retries to perform when a connection to the event service fails due to a temporary communication error. Specify a number from `0` to `86400`. If you omit this parameter, retry processing is not performed.

Regardless of the settings in `retry-times` and `retry-interval`, an error occurs when 86,400 seconds (24 hours) have elapsed since the retries began.

`retry-interval=`*retry-interval* (to connect to the event service)

Specify the retry interval when a connection to the event service fails due to a temporary communication error. This parameter is valid only when you specify a value of 1 or greater in `retry-times`. The retry interval is the length of time from when the trap fails to connect to the event service until when it next tries to establish a connection. This interval does not include the time required for the connection processing. Specify a number from `1` to `600` (seconds). The default is `10`.

Regardless of the settings in `retry-times` and `retry-interval`, an error occurs when 86,400 seconds (24 hours) have elapsed since the retries began.

`open-retry-times=`*retry-count* (to open a log file)

Specify the number of retries to perform when the log file trapping function is temporarily unable to read a log file for monitoring. Specify a number from `1` to `3600`. The default is `1`.

Regardless of the settings in `retry-times` and `retry-interval`, an error occurs when 3,600 seconds (1 hours) have elapsed since the retries began.

`open-retry-interval=`*retry-interval* (to open a log file)

Specify the retry interval when the log file trapping function is temporarily unable to read a log file for monitoring. The retry interval is the length of time from the open failure until the next time the trap attempts to open the log file. Specify a number from `1` to `600` (seconds). The default is `1`.

Regardless of the settings in `retry-times` and `retry-interval`, an error occurs when 3,600 seconds (1 hours) have elapsed since the retries began.

`read-retry-times=`*retry-sets-threshold* (to read a log file)

Specify for a threshold value the number of continuous retry sets to perform when the log file trapping function is temporarily unable to read a log file. This threshold is the total number of retry sets, where one set is five retries at 10-millisecond intervals. When the specified threshold is exceeded, an error occurs. Specify a number from `1` to `1000`. The default is `100`.

`hold-count=`*number-of-held-JP1-events*

Specify the number of JP1 events that can be held during retry processing. Specify a number from `1` to `1000`. The default is `100`.

The system resources must be utilized to hold JP1 events converted from log data during retry processing. The memory requirement is as follows:

number-of-JP1-events-to-be-held (kilobytes)

`keep-event={ OLD | NEW }`

When the number of JP1 events held during retry processing exceeds the specified hold count, the excess JP1 events will be deleted. Specify whether to keep the older JP1 events or the recent JP1 events once the maximum number that can be held has been exceeded. The default is `OLD`.

`OLD`

Specify this value to keep older JP1 events. JP1 events will be held up to the number specified in the `hold-count` parameter. Any subsequent JP1 events will be deleted.

`NEW`

Specify this value to keep recent JP1 events. When the specified hold count has been exceeded, JP1 events will be deleted, starting from the oldest.

`FILETYPE={ SEQ | SEQ2 | WRAP1 | WRAP2 | HTRACE }`

Specify the data output format of the log file to be read. The default is `SEQ`.

`SEQ`

Specify for a sequential file (a log file that is written to continuously or, when it reaches a certain size, is replaced by a new log file with a different file name).

`SEQ2`

Specify `SEQ2` for the following files:

- In Windows:

  A log file that is renamed, and then replaced by a new log file created with the same name as the original file.

- In UNIX:

  A log file that is renamed or deleted, and then replaced by a new log file created with the same name as the original file.

Note

When `SEQ2` is specified, the system reads the data written to the previous log file since the last read, and then reads the data from the new log file that was swapped in during the monitoring interval. If the log file is switched more than once during the monitoring interval, the system can only read data from the last file. When specifying the `-t` option (monitoring interval) in the `jevlogstart` command, consider how often the log file will be switched.

`WRAP1`

Specify in case of a wrap-around file (data is wrapped around from the end, overwriting the existing data from the top of the file).

To determine the read position of a `WRAP1` file, the log file trapping function makes a copy of the log file to be read and compares it with the current log file. Therefore, the sizes of `WRAP1` and the file to be monitored must be the same.

Note

When a large log file is being monitored with the `WRAP1` setting, it will take a long time for the first JP1 event to be generated if the write data position is near the end of the file.

`WRAP2`

Specify in case of a wrap-around file (when all data is wrapped around from the end, overwriting the existing data from the top of the file).

Specify a `SEQ2` file if you want to delete or rename the full log file and re-create the log file.

Notes

- When `WRAP2` is specified, some data might not be read if data is deleted as a result of wrapping around before the trapping service reads all the data. Remember this when specifying the `-t` option (monitoring interval) in the `jevlogstart` command because a long monitoring interval results in a large amount of data being read at one time.
- JP1/Base detects a wraparound by detecting reduction in the file size. Note that JP1/Base does not assume a wraparound if the file size after a wraparound is equal to or greater than that before a wraparound.

`HTRACE`

Specify in case of a multi-process trace file (a pair of fixed-size trace files that are shared by multiple processes as memory-mapped files).

The write method is the same as `WRAP1`. When the file reaches a certain size, data is wrapped around from the end, overwriting the existing data from the top of the file.

`RECTYPE={ VAR { '\n ' | '`*end-of-line-character*`' | '`*end-of-line-symbol*`'} | FIX` *record-length* `}]`

Specify the record format of the log file to be read. The default is `RECTYPE=VAR'\n '`. In other words, the default format is variable-length records with `\n` at the end for the line separator.

`VAR`

For variable-length record format, specify the end-of-line character or end-of-line symbol. As with the single character specification in the C language, you can enclose the character or symbol with single quotation marks and specify an escape sequence.

`FIX`

For the fixed-length record format, specify the record length as the line separator. Specify the record length as a number in the range from `1` to `9999999` (bytes).

HEADLINE=*number-of-header-lines*]

If the log file has headers, specify the number of header lines as a number from 0 to 99999 (lines). The default is 0.

HEADSIZE=*header-size*]

If the log file has headers, and if the number of header lines cannot be specified, specify the header size as a number from 0 to 9999999 (bytes). Headers that cannot be specified with a header line count include headers in binary data, and headers whose record format differs from the log data. This parameter is invalid if the HEADLINE parameter is specified. The default is 0 bytes.

MARKSTR=[!]"*regular-expressions*"

Using regular expressions, specify any data that you do not want to monitor, for example, data other than log data. Enclose the regular expression with double quotation marks. Data other than log data includes, for example, data output to a log file at regular intervals. An example is shown below.

```
"==== 13:00:00 JP1/Base Event ===="
```

Specify an exclusion condition by writing an exclamation mark in front of the value enclosed with quotation marks. This excludes data that does not match the regular expression from being monitored.

More than one regular expression can be specified in one MARKSTR parameter. When multiple regular expressions are specified, they are interpreted as AND conditions, and only data that matches all the conditions, including the mismatch (!) condition, is not monitored. Separate regular expressions using linefeeds. Specify values only in the second and subsequent lines. In this case, insert one or more spaces before the value you specified. The following is an example of excluding data that contains ==== and MARK from being monitored.

```
MARKSTR="===="(line feed)
     △ △ △ △ △"MARK"
     △: Space
```

You can specify multiple values for this parameter. There is no limit on how many values can be specified. When multiple values are specified for this parameter, they are interpreted as OR conditions, all data that matches any one of the conditions is not monitored.

The check performed on regular expressions that are specified in this parameter applies to the input log data up to the length specified in the -m option of the jevlogstart command. When this parameter is omitted, the log-file trapping service assumes that there is no data other than log data.

ACTDEF=[{EXIT}][<severity>][event-ID][!]"*regular-expressions*"

Specify the conditions for converting specific log messages into JP1 events, and specify the event ID and severity of those JP1 events. When log data matches a regular expression, the JP1 event is issued with the specified event ID. Do not place a space or tab character anywhere between an equal sign, `{EXIT}`, *<severity>*, or *event-ID*. Placing a space or tab character between any of the above results in a syntax error.

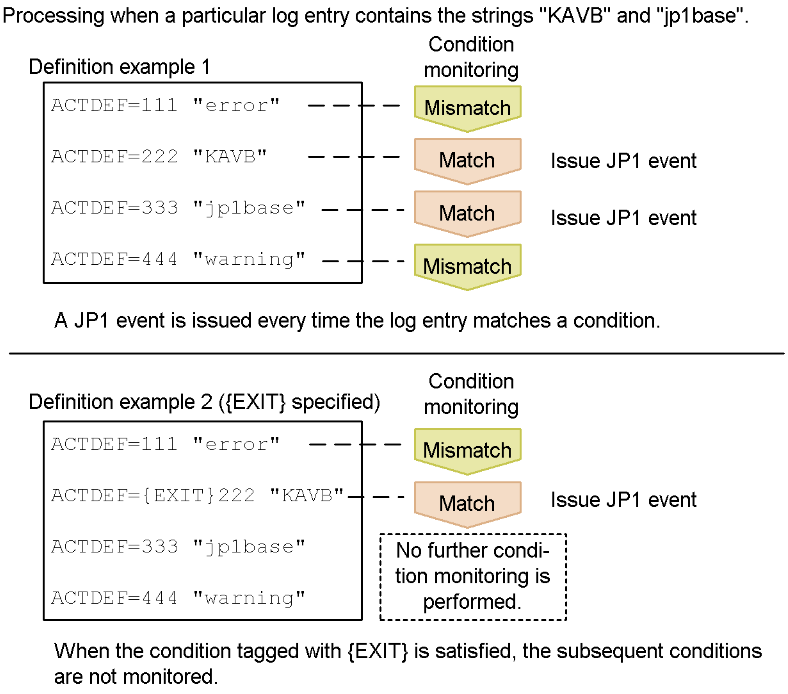
`{EXIT}`

This parameter applies when specifying multiple `ACTDEF` parameters. Specify `{EXIT}` to halt monitoring log data as soon as data matching the condition tagged with `{EXIT}` has been detected.

Normally, when multiple `ACTDEF` parameters are specified and a particular log entry matches more than one of the conditions, the system issues a JP1 event for every such match. When you specify `{EXIT}` for a condition, a JP1 event with the specified event ID is issued if a match is found, and the conditions in the subsequent `ACTDEF` parameters are not monitored.

The following figure shows how the processing differs according to whether `{EXIT}` is specified.

Figure 14-5: Example of specifying an action definition file for log file trapping


Processing when a particular log entry contains the strings "KAVB" and "jp1base".
Definition example 1
Condition monitoring
ACTDEF=111 "error"
Mismatch
ACTDEF=222 "KAVB"
Match
Issue JP1 event
ACTDEF=333 "jp1base"
Match
Issue JP1 event
ACTDEF=444 "warning"
Mismatch
A JP1 event is issued every time the log entry matches a condition.
Definition example 2 ({EXIT} specified)
Condition monitoring
ACTDEF=111 "error"
Mismatch
ACTDEF={EXIT}222 "KAVB"
Match
Issue JP1 event
ACTDEF=333 "jp1base"
ACTDEF=444 "warning"
No further condition monitoring is performed.
When the condition tagged with {EXIT} is satisfied, the subsequent conditions are not monitored.

<severity>

Specify in angle brackets (`<>`) the severity level, an extended JP1 event attribute. Specify the severity level and event ID in pair. You can specify any of the following values.

- `Emergency`
- `Alert`
- `Critical`
- `Error`
- `Warning`
- `Notice`
- `Information`
- `Debug`

The default is `Notice`.

event-ID

Specify an event ID, which is used when registering a JP1 event in an event server. An event ID is a hexadecimal number consisting of the upper four bytes (basic code) and the lower four bytes (extended code), separated by a colon. Write the characters A to F in upper case. The lower four bytes, or both the colon and lower four bytes, can be omitted. The default in this case is `0`. If the upper and lower bytes do not add up to eight digits each, leading zeros are added. The specifiable range of values is `0:0` to `1FFF:0` and `7FFF8000:0` to `7FFFFFFF:0`. Always specify 0 for the extended code. Three examples of event ID expressions are shown below.

Each represents the same event ID.

```
0000011A:00000000
11A:0
11A
```

"*regular-expression*"

Use regular expressions to specify the log data to be converted to JP1 events. Enclose the regular expression with double quotation marks. An exclamation mark before the opening quote specifies exclusion conditions, and data that does *not* match the specified regular expression is set to be converted.

More than one regular expression can be specified in one `ACTDEF` parameter. When multiple regular expressions are specified, they are interpreted as AND conditions, and only data that matches all the conditions, including the mismatch (`!`) condition, is converted into JP1 events. Separate regular expressions using linefeeds. Specify regular expressions only in the second and subsequent lines. In this case, insert one or more spaces before the value you specified. The following is an example of specifying data that contains `jp1base` and `error` to be converted into JP1 events by using event ID `00000333`.

```
ACTDRF=00000333  "jp1base"(line feed)
     △  △  △  △  △"error"
     △: Space
```

You can specify multiple values for this parameter. There is no limit on how many values can be specified. When multiple values are specified for this parameter, they are interpreted as OR conditions, all data that matches any one of the conditions is converted into a JP event.

The check performed on regular expressions that are specified in this parameter applies to the input log data up to the length specified in the `-m` option of the `jevlogstart` command.

This parameter is mandatory.

Notes

- The regular expressions you can specify in the `MARKSTR` and `ACTDEF` parameters differ according to your OS. For details on the syntax of regular expressions, see *F. Syntax of Regular Expressions*.
- Message `KAVA3646-E` is output to the standard error output at execution of the `jevlogstart` command for the following errors:
  - The log file is a multi-process trace, but `HTRACE` is not specified as the file format in the action definition file for log file trapping.
  - The log file is not a multi-process trace, but `HTRACE` is specified as the file format in the action definition file for log file trapping.

  When you specify the `-r` option in the `jevlogstart` command, the log file trap waits for the target file to be created. If the file format is incorrectly specified, after the log file is created, the KAVA3646-E message is output to the syslog, event log, and integrated trace log, and log file trapping stops.

  If this error message appears, correct the file format in the action definition file for log file trapping, and then re-execute the `jevlogstart` command.

  For incorrect file formats in other situations, an error message and JP1 event `00003A22` are issued after log-file trapping starts and the log file reaches a set size and is swapped over. For details on this JP1 event, see *15.3(6) Details about event ID 00003A22*.

  If JP1 event `00003A22` is received, check the status of the log file indicated in the error message, and review the file format specified in the action definition file for log file trapping. The table below describes the possible causes of JP1 event 00003A22 for each log file format.

Table 14-10: JP1 events notified according to file formats

Log file format in the action definition file for log file trapping	Error triggering the JP1 event
SEQ	• The log file is deleted. • The log file size is smaller than before. • The log file is deleted and re-created with the same name.#
SEQ2	• The log file size is smaller than before being re-created under a different name.
WRAP1	• The log file is deleted. • The log file size is smaller than before. • The log file is deleted and re-created with the same name.#
WRAP2	• The log file is deleted. • The log file is deleted and re-created with the same name.#
HTRACE	• The log file is deleted. • The log file is deleted and re-created with the same name.

#: The log file might be a SEQ2 file. Check the file format specified in the action definition file for log file trapping.

Definition examples

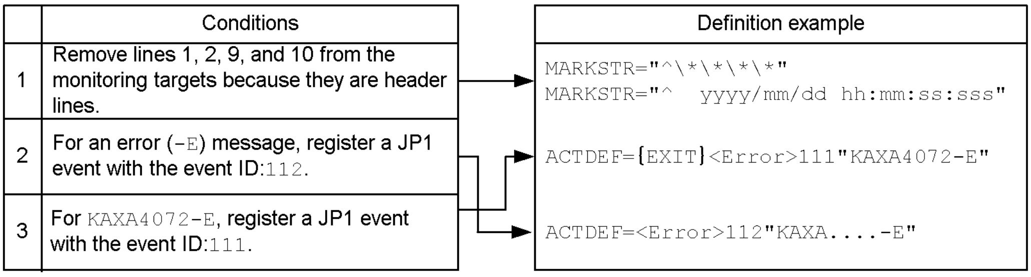
- Examples of defining MARKSTR and ACTDEF parameters

This subsection explains how to define the MARKSTR and ACTDEF parameters based on the following log data.

1	`**** Microsoft WindowsNT5.1(Build:2600)   jp1server TZ=(local)-9:00   2009/01/01 12:00:00.000`
2	`yyyy/mm/dd hh:mm:ss.sss     pid     tid     message-id       message(LANG=0x0411)`
3	`2009/01/01 12:00:00.111    KAXA 4004-E    An attempt to start HostA has failed.`
4	`2009/01/01 12:00:00.111    KAXA 4004-E   An attempt to start HostB has failed.`
5	`2009/01/01 12:00:00.111    KAXA 4072-E   A memory insufficiency occurred in HostC.`
6	`2009/01/01 12:00:00.111    KAXA 4037-W   Startup of HostD is delayed.`
7	`2009/01/01 12:00:00.115    KAXA 4072-E   A memory insufficiency occurred in HostD.`
8	`2009/01/01 12:00:00.116    KAXA 4102-I   JP1Base has started.`
9	`**** Microsoft WindowsNT5.1(Build:2600)   jp1server TZ=(local)-9:00   2009/01/02 12:00:00.000`
10	`yyyy/mm/dd hh:mm:ss.sss     pid     tid     message-id       message(LANG=0x0411)`
11	`2009/01/02 15:00:01.004    KAXA 7226-I   HostD will now stop.`
12	`2009/01/02 15:00:02.108    KAXA 4103-I   JP1Base has stopped.`
13	`2009/01/02 15:10:24.275    KAXA 4037-W   Startup of HostB is delayed.`
14	`2009/01/02 15:10:45.501    KAXA 2178-E ***** An error occurred in communication between HostD and HostA ****`
15	`2009/01/02 15:10:46.149    KAXA 4072-E   A memory insufficiency occurred in HostB.`
16	`2009/01/02 15:12:48.410    KAXA 4037-W   Startup of HostE is delayed.`

Setting example 1:

The left part of the following figure lists conditions for log file trapping, and the right part provides examples of defining the action definition file for log file trapping.



	Conditions
1	Remove lines 1, 2, 9, and 10 from the monitoring targets because they are header lines.
2	For an error (`-E`) message, register a JP1 event with the event ID:`112`.
3	For `KAXA4072-E`, register a JP1 event with the event ID:`111`.

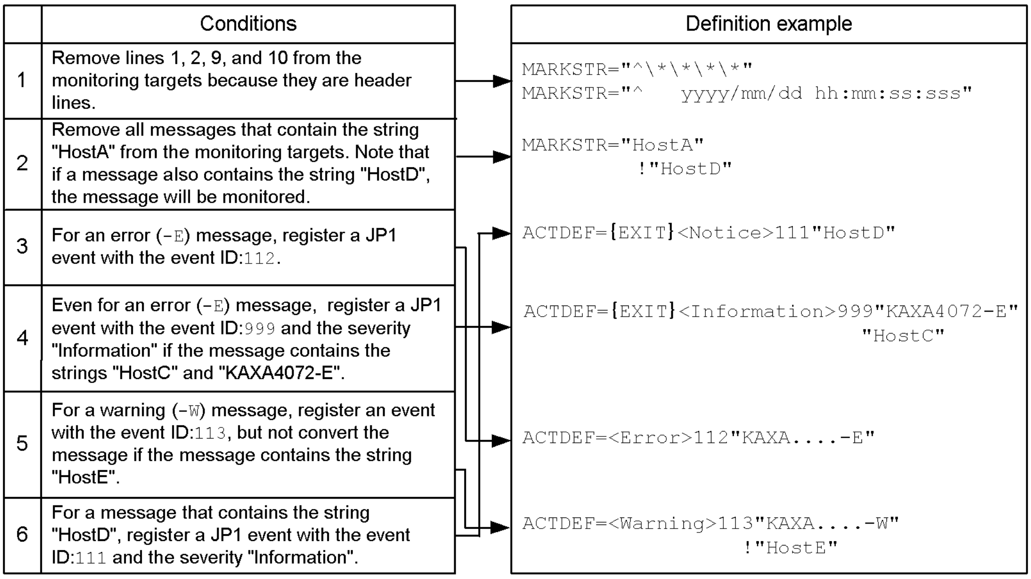
Definition example

```
MARKSTR="^\*\*\*\*"
MARKSTR="^  yyyy/mm/dd hh:mm:ss:sss"

ACTDEF={EXIT}<Error>111"KAXA4072-E"

ACTDEF=<Error>112"KAXA....-E"
```

●Conditions are compared in the defined order. Therefore, if condition 2 and condition 3 are defined in that order, a single message that contains the string "KAXA4072-E" satisfies conditions 2 and 3, and two JP1 events (event IDs are `111` and `112`) will be registered. For this reason, in this case, you need to define condition 3 and condition 2 in that order, and then define `{EXIT}` so that further monitoring will not be performed if condition 3 is satisfied.

Setting example 2:

The left part of the following figure lists conditions for log file trapping other than those of example 1, and the right part provides examples of defining the action definition file for log file trapping.



	Conditions
1	Remove lines 1, 2, 9, and 10 from the monitoring targets because they are header lines.
2	Remove all messages that contain the string "HostA" from the monitoring targets. Note that if a message also contains the string "HostD", the message will be monitored.
3	For an error (-E) message, register a JP1 event with the event ID:112.
4	Even for an error (-E) message, register a JP1 event with the event ID:999 and the severity "Information" if the message contains the strings "HostC" and "KAXA4072-E".
5	For a warning (-W) message, register an event with the event ID:113, but not convert the message if the message contains the string "HostE".
6	For a message that contains the string "HostD", register a JP1 event with the event ID:111 and the severity "Information".

Definition example

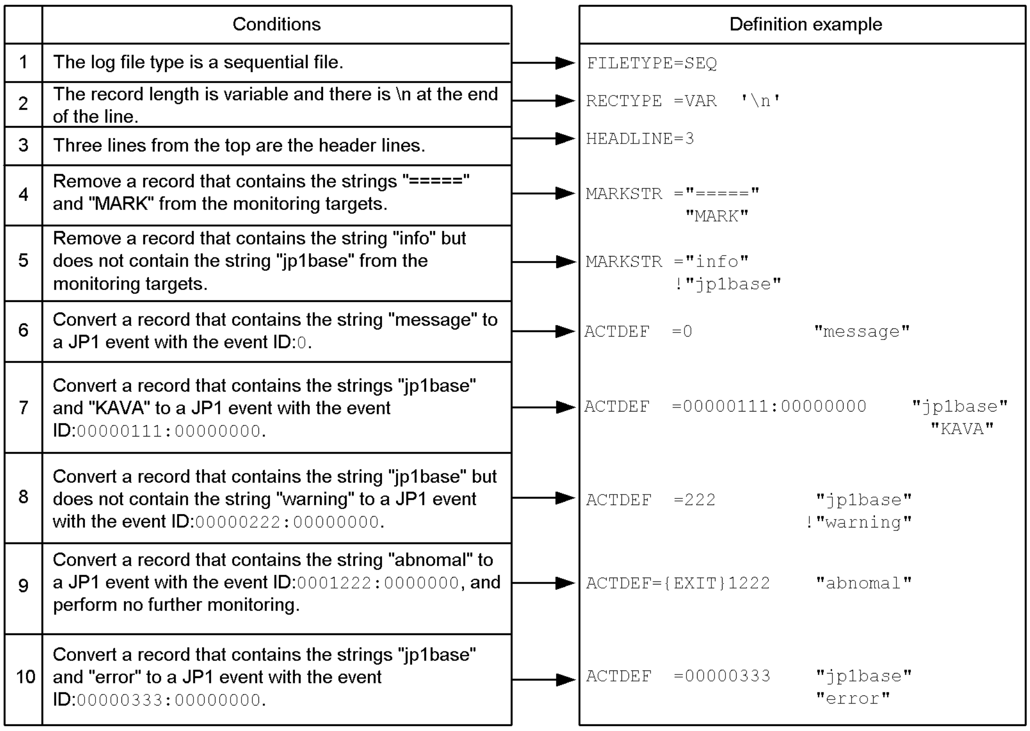
```
MARKSTR="^\*\*\*\*"
MARKSTR="^    yyyy/mm/dd hh:mm:ss:sss"

MARKSTR="HostA"
         !"HostD"

ACTDEF={EXIT}<Notice>111"HostD"

ACTDEF={EXIT}<Information>999"KAXA4072-E"
                                  "HostC"

ACTDEF=<Error>112"KAXA....-E"

ACTDEF=<Warning>113"KAXA....-W"
                  !"HostE"
```

●Conditions are compared in the defined order. Therefore, if condition 3 and condition 4 are defined in that order, JP1 events with the event IDs 112 and 999 will be registered for a message that contains the strings "KAXA4072-E" and "HostC". For this reason, in this case, you need to define condition 4 and condition 3 in that order, and then define {EXIT} so that further monitoring will not be performed if condition 4 is satisfied.

●If there is not {EXIT} for condition 6, JP1 events with the event IDs 111 and 112 will be registered for an error message that contains the string "HostD", and JP1 events with the event IDs 111 and 113 will be registered for a warning message that contains the string "HostD".

Setting example 3:

The left part of the following figure lists conditions for log file trapping, and the right part provides examples of defining the action definition file for log file trapping.



	Conditions
1	The log file type is a sequential file.
2	The record length is variable and there is \n at the end of the line.
3	Three lines from the top are the header lines.
4	Remove a record that contains the strings "=====" and "MARK" from the monitoring targets.
5	Remove a record that contains the string "info" but does not contain the string "jp1base" from the monitoring targets.
6	Convert a record that contains the string "message" to a JP1 event with the event ID:`0`.
7	Convert a record that contains the strings "jp1base" and "KAVA" to a JP1 event with the event ID:`00000111:00000000`.
8	Convert a record that contains the string "jp1base" but does not contain the string "warning" to a JP1 event with the event ID:`00000222:00000000`.
9	Convert a record that contains the string "abnomal" to a JP1 event with the event ID:`0001222:0000000`, and perform no further monitoring.
10	Convert a record that contains the strings "jp1base" and "error" to a JP1 event with the event ID:`00000333:00000000`.

Definition example

```
FILETYPE=SEQ
RECTYPE =VAR  '\n'
HEADLINE=3
MARKSTR ="====="
         "MARK"
MARKSTR ="info"
        !"jp1base"
ACTDEF  =0           "message"
ACTDEF  =00000111:00000000    "jp1base"
                                "KAVA"
ACTDEF  =222         "jp1base"
                    !"warning"
ACTDEF={EXIT}1222    "abnomal"
ACTDEF  =00000333    "jp1base"
                     "error"
```

Log information definition file

Format

```
log-keep number-of-log-files
log-size file-size
```

File name

`jevlogd.conf`

Storage destination directory

In Windows:

installation-folder`\conf\event\`

In UNIX:

`/etc/opt/jp1base/conf/event/`

Output directory for log files

In Windows:

installation-folder`\sys\tmp\event\logtrap\jevtraplog\jevtraplog.{000|001|002|003|004}`#

In UNIX:

`/var/opt/jp1base/sys/tmp/event/logtrap/jevtraplog/jevtraplog.{000|001|002|003|004}`#

#: Use the `log-keep` parameter to change the number of log files.

Description

Specifies the file size and number of log files used for log file trapping. The log information definition file (`jevlogd.conf`) is not provided by default. When this file does not exist, the default number of log files and default file size are assumed. Create and modify the log information definition file (`jevlogd.conf`), if necessary.

Application of settings

Start the log-file trap management service or daemon to apply the settings.

Definition details

The following conventions apply to entries in the log information definition file (`jevlogd.conf`):

- A hash mark (#) (code `0x23`) at the start of a line indicates a comment.
- Use one or more spaces or tab characters to separate parameters and values.
- Define one parameter per line.
- Do not enter a space or tab before the first parameter in a line.
- You cannot write a comment between a value and the following linefeed character.
- If the definition file contains an error, the default will be used.
- Letters are case sensitive.

`log-keep` *number-of-log-files*

Specify how many log files to use for log file trapping (`jevtraplog.*`). The current log file is switched when its size reaches the limit specified in `log-size`. When the number of log files reaches the maximum you specify here, the oldest file is deleted. In *number-of-log-files*, specify a number in the range from `0` to `50`. If this parameter is omitted, the default is used. The default is `5`. When `0` is specified, logs are not kept.

`log-size` *file-size*

Specify the maximum size of a log file used for log file trapping (`jevtraplog.*`). In *file-size*, specify a number in the range from `65536` to `2147483647` bytes. If this parameter is omitted, the default is used. The default is `1000000`.

Log information is output when the log-file trap management service (or daemon) starts and when an error occurs.

Definition examples

The following shows an example of settings in the log information definition file (`jevlogd.conf`).

```
log-keep 5
log-size 65536
```

Action definition file for event log trapping (Windows only)

Format

```
server event-server-name
retry-times retry-count
retry-interval retry-interval
trap-interval monitoring-interval
matching-level comparison-level
filter-check-level filter-check-level
jp1event-send JP1-event-issuance

# filter
filter log-type
  condition-statement-1
  condition-statement-2
 :
  condition-statement-n
end-filter
```

File name

`ntevent.conf`

Storage destination directory

installation-folder`\conf\event\`

Description

Specifies the conditions for converting event log data into JP1 event and the event-log monitoring interval.

Application of settings

To apply the settings, start the event log trapping service or reload the action definition file for event log trapping by executing the `jeveltreload` command. For details on the `jeveltreload` command, see *jeveltreload (Windows only)* in *13. Commands*.

Definition details

An action definition file for event log trapping (`ntevent.conf`) consists of a destination event server name, retry setting, and one or more filters. Comments are marked with hash marks and disregarded.

`server` *event-server-name*

Specify the name of the destination event server for registering JP1 event converted from the event log. Specify a server name that is no more than 255 bytes. Enclose the event server name with double quotation marks. You can only specify an event server that runs on the local host. When no event server is specified, the local host name is assumed.

`retry-times` *retry-count*

Specify the number of retries to perform when a connection to the event service fails due to a temporary communication error. Specify a number from `0` to `86400`. By default, retry processing is not performed.

`retry-interval` *retry-interval*

Specify the retry interval when a connection to the event service fails due to a temporary communication error. This parameter is valid only when you specify a value of 1 or greater in `retry-times`. The retry interval is the length of time from when the trap fails to connect to the event service until when it next tries to establish connection. This interval does not include the time required for the connection processing. Specify a number from `1` to `600` (seconds). The default is `10`.

`trap-interval` *monitoring-interval*

Specify the interval over which to monitor the event log. The event log trapping function monitors the event log in real time and also at set intervals. Specify a number from `1` to `180` (seconds). The default is `10`.

`matching-level [0|1]`

Specify the comparison level for the event log and definitions when the explanation about the log entry cannot be read because you specified the `message` or `category` attribute in a filter condition but the message DLL or category DLL is not properly configured. When `0` is specified, the next filter condition will be compared skipping the current one. When `1` is specified, the current filter condition is compared. The default is 0.

`filter-check-level [0|1]`

Specify a checking level when an invalid log type (log type that does not exist in the system) or invalid regular expression is found in a filter condition. Invalidate the filter condition when `0` is specified and the filter condition contains an invalid log type or invalid regular expression. If there are one or more valid filter conditions, the service will start up and the settings will be reloaded successfully. If there are no valid filter conditions, the service will not startup and the settings will not be reloaded. When `1` is specified and one or more of the filter conditions contains an invalid log type or invalid regular expression, the service will not start up and the settings will not be reloaded. The default is `0`.

`jp1event-send [0|1]`

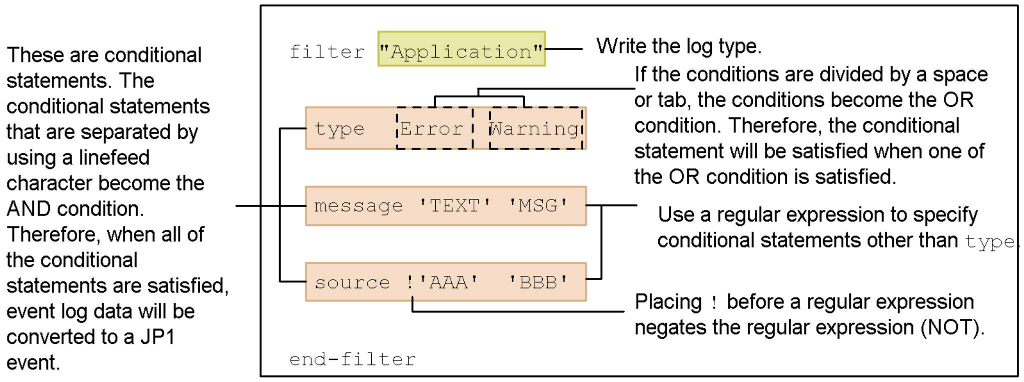
Specify whether to output a message when the event log acquisition fails while monitoring the event log. When `0` is specified, a JP1 event is not output even if the event log acquisition fails. When `1` is specified, a JP1 event (`00003A73`) is output when the event log acquisition fails. Monitoring might be resumed after the JP1 event indicating failure of event log acquisition. In this case, a JP1 event (`00003A74`) is output. The default is `0`.

Note that a message is output to the integrated trace log regardless of the setting of this parameter. For details on JP1 events, see *15.3 JP1 event details*.

Filter syntax

A filter is a set of condition statements for converting event log data into JP1 events. The condition statements within a filter are AND conditions, and those between filters are OR conditions. If you specify multiple filters, conversion is performed when any one of the filters is satisfied. You must specify at least one filter condition. The following figure shows the syntax conventions of a filter.

Figure 14-6: Filter syntax conventions (action definition file for event log trapping)



```
filter "Application"
type Error Warning
message 'TEXT' 'MSG'
source !'AAA' 'BBB'
end-filter
```

These are conditional statements. The conditional statements that are separated by using a linefeed character become the AND condition. Therefore, when all of the conditional statements are satisfied, event log data will be converted to a JP1 event.
Write the log type.
If the conditions are divided by a space or tab, the conditions become the OR condition. Therefore, the conditional statement will be satisfied when one of the OR condition is satisfied.
Use a regular expression to specify conditional statements other than type.
Placing ! before a regular expression negates the regular expression (NOT).

This definition converts event log data that satisfies the following conditions to a JP1 event:
- Event log entries of "Application log"
- Event log entries whose type is Error or Warning
- Event log entries whose messages contain the strings "TEXT" or "MSG"
- Event log entries whose sources contain the strings other than "AAA" or the string "BBB".

■ Log type

Specify the type of event logs to be monitored. The log type is the name of each log listed in the Windows Event Viewer. Enclose the log type with double quotation marks.

Log types specifiable (six types):

```
"Application"
```

```
"Security"
```

```
"System"

"DNS Server"

"Directory Service"

"File Replication Service"
```

When the same log type is specified in multiple filters, the event log will be monitored if any one of the filters succeeds.

- Condition statement format

In *condition-statement*, specify one of the attribute names listed in the table below and the items displayed in the corresponding event viewer.

Table 14-11: Attribute names that can be specified in filter condition statements

Attribute name	**Meaning**
`type`	Log types
`source`	Information about the source displayed in the Event Viewer Details window
`category`#	Information about the category displayed in the Event Viewer Details window
`id`	Information about the event ID displayed in the Event Viewer Details window
`user`	User name displayed in the Event Viewer Details window
`message`#	Explanatory information displayed in the Event Viewer Details window
`computer`	Computer name displayed in the Event Viewer Details window

#:

- Make sure that the message DLL containing the explanation about the event log entry is configured properly according to the Windows event log conventions. If the message DLL is not properly configured, the event log trapping function might not trap those entries because it cannot read the explanation in the event log. If you want to trap messages that do not contain the message DLL or category DLL, specify 1 for the `matching-level` parameter.
- If the message DLL is not properly configured, a warning will appear in the event viewer indicating that the explanation was not found, possibly because the message DLL file does not exist. This warning is output by the event viewer. As such, it is not trapped by the event log trapping function.
- If log data is converted into a JP1 event without the message DLL, the character string output after the above warning is enclosed in double quotation marks, and then registered. A comma (`,`) is used to separate multiple character strings. If log

data is converted without a category DLL, the applicable value is registered as a category enclosed with brackets.

The coding format is shown below.

`type` *log-type-1 log-type-2 log-type-3...*

Specify log types. When multiple types are specified, the condition will be satisfied when a match is found with any one of the specified types. The severity level of a JP1 event after conversion depends on the log type. The following table lists the specifiable log types and the corresponding JP1 event severity.

Table 14-12: Log types specifiable in `type` and the corresponding JP1 event severity

Log type	Contents	JP1 event severity
`Information`	Information	`Information`
`Warning`	Warning	`Warning`
`Error`	Error	`Error`
`Audit_success`	Audit succeeded	`Notice`
`Audit_failure`	Audit failed	`Notice`

Log types not listed in the above table cannot be specified in `type`. In addition, when converting log data to something other that a listed type, the JP1 event severity level is set to `Information`.

Attribution names other than `type`

attribute-name `'`*regular-expression-1*`'` `'`*regular-expression-2*`'` `'`*regular-expression-3*`'` . . .

Using regular expressions, specify an attribute name other than `type`. Enclose the regular expression with single quotation marks. Sets exclusion conditions by writing an exclamation mark in front of the value enclosed with single quotation marks. This specifies data that does not match the regular expression to be converted. The regular expressions that you can use depend on the OS. For details on the syntax of regular expressions, see *F. Syntax of Regular Expressions*.

Notes

- You can specify a combination of values for the retry count and retry interval that causes the system to continue retrying for more than 24 hours. When retry processing exceeds 24 hours, however, the system aborts retrying and stops the event log trapping service.
- The retry functionality can be used to prevent the Windows media sense

functionality from stopping the service.

- When the filter-check-level is set to 0 (or is unspecified) and a filter condition is invalidated, the KAVA3025-W or KAVA3026-W message is output to the event log and integrated trace log. (For file reloading, the message is output only to the standard error output.) Only 10 or fewer messages are output for invalidated filters.
- When the filter-check-level is set to 0 (or is unspecified) and there are no valid filter conditions, the KAVA3027-E or KAVA3028-E message (reloading) is output to the event log and integrated trace log. (For file reloading, the message is output to the event log, integrated trace log, and standard error output.)

Supplied action definition file for event log trapping

According to the setting in the supplied action definition file for event log trapping (ntevent.conf), if a connection to the event service fails, the event log trap will retry three times, once per 10-second interval. As conditions for conversion to JP1 events, the defaults also specify that Warning and Error entries output to the System log or Application log are to be converted into JP1 events. The following table shows the settings of the provided file:

```
retry-times 3
retry-interval 10

filter "System"
    type Warning Error
end-filter

filter "Application"
    type Warning Error
end-filter
```

When the action definition file for event log trapping (ntevent.conf) and forwarding settings file (forward) are used by default, if a JP1 event fails to transfer, the error message KAJP1037-E will be output to the event log and converted into a JP1 event. The converted JP1 event is then resent, and another transfer error will occur.

To prevent the event transfer from looping, change the setting in the action definition file, so that the message KAJP1037-E will not be trapped. A setting example is shown below:

```
retry-times 3
retry-interval 10

filter "System"
type Warning Error
end-filter
```

```
# Trap event log entries with severity level Error or Warning
# that were not output by the JP1/Base Event service.
filter "Application"
    type Warning Error
    source !'JP1/Base Event'
end-filter

# Trap event log entries with severity level Error or Warning
# from the JP1/Base Event service, except entries with ID 1037.
filter "Application"
    type Warning Error
    source 'JP1/Base Event'
    id !'1037'
end-filter
```

Examples of defining a filter

Definition examples1: Using OR and AND conditions

Definition example using an OR condition

Select data entries of the `System` log type containing any one of the strings `TEXT`, `MSG`, or `-W` in the explanatory information.

```
filter "System"
    message 'TEXT' 'MSG' '-W'
end-filter
```

Specify an OR condition by separating conditions using spaces and tag characters.

Definition example using an AND condition

Select data entries of the `System` log type containing all of the strings `TEXT`, `MSG`, and `-W` in the explanatory information.

```
filter "System"
    message 'TEXT'
    message 'MSG'
    message '-W'
end-filter
```

Specify an AND condition by separating conditions using a linefeed character. After inserting a linefeed character, write the condition starting from the attribute names.

Definition example 2: Using multiple filters

Trap event log entries that have the `Application` log type and that satisfy the following conditions.

Filter 1:

- Type: Application log:
- Type: Error
- Explanation: Contains `-E` and `JP1/Base`.

Filter 2:

- Type: Application log:
- Type: Warning
- Explanation: Contains `-W` or `warning`.

```
# Filter 1
filter "Application"
    type Error
    message '-E'
    message 'JP1/Base'
end-filter
# Filter 2
filter "Application"
    type Warning
    message '-W' 'warning'
end-filter
```

Definition example 3: Using regular expressions

Trap event log entries that satisfy the following conditions.

- Type: Application log
- Type: Error
- Event ID: 111
- Explanation: Contains `-E` or `MSG`, and does not contain `TEXT`.

```
filter "Application"
    type Error
    id '^111$'
    message '-E' 'MSG'
    message !'TEXT'
end-filter
```

To specify the event ID 111 condition using a regular expression, specify `id '^111$'`. If you specify `id '111'`, the event ID must *contain* 111, so event IDs 1112 and 0111 will also satisfy the condition. Writing an exclamation mark in front of the value enclosed with quotation marks selects data that does not match the regular expression. For details on regular expressions, see *F. Syntax of Regular Expressions*.

Definition example 4: Excluding specific event log entries

Trap event log entries that have System log type and a Warning severity level, but exclude entries that satisfy the following conditions.

- Source: AAA
- Event ID: 111
- Explanation: Contains `TEXT`.

```
# Do not trap event log entries from source AAA.
filter "System"
    type Warning
    source !'AAA'
end-filter
# Trap all event log entries from source AAA,
# except those with an event ID of 111.
filter "System"
    type Warning
    source 'AAA'
    id !'^111$'
end-filter
# From source AAA, trap all event log entries
# whose event ID is 111 and do not contain TEXT
# in the explanatory information.
filter "System"
    type Warning
    source 'AAA'
    id '^111$'
    message !'TEXT'
end-filter
```

Distribution definition file

Format

```
[destination-host,...]
definitions
[&destination-host,...]
definitions
[destination-host,...]@action-definition-file-name
definitions
  :
```

File name

Table 14-13: Names of distribution definition file

Definition file for distribution destination	Name of distribution definition file
Forwarding settings file	`[jev_forward.conf	`*any file*`]`
Action definition file for log file trapping	`[jev_logtrap.conf	`*any file*`]`
Action definition file for event log trapping	`[jev_ntevent.conf	`*any file*`]`

Storage destination directory

Table 14-14: Storage locations of distribution definition files (in Windows)

Definition file for distribution destination	Storage location
Forwarding settings file	*event-folder*#\
Action definition file for log file trapping	*installation-folder*`\conf\`
Action definition file for event log trapping	*installation-folder*`\conf\event\`

#: Replace *event-folder* with the following folder:

- *installation-folder*`\conf\event\servers\default`
- *shared-folder*`\jp1base\event` (in a cluster system)

Table 14-15: Storage locations of distribution definition files (in Unix)

Definition file for distribution destination	**Storage location**
Forwarding settings file	*event-directory*#`/`
Action definition file for log file trapping	`/etc/opt/jp1base/conf/`
Action definition file for event log trapping	`/etc/opt/jp1base/conf/event/`

#: Replace *event-directory* with the following directory:

- `/etc/opt/jp1base/conf/event/servers/default`
- *shared-directory*`/event` (in a cluster system)

Description

Specifies the definition information to distribute and the destination host. You must prepare a distribution definition file for each definition file for which you want to distribute the definitions of. Create the file in the storage location, using the default name or any other name.

Application of settings

Execute the `jevdef_distrib` command to distribute definitions and apply the settings. For details on the `jevdef_distrib` command, see *jevdef_distrib* in *13. Commands*.

Definition details

The following conventions apply to entries in the distribution definition file.

- Any characters preceding the left square bracket (`[`) are assumed to be comments. Characters following square brackets (`[ ]`) are assumed to be definitions.
- If you specify a hash mark for a comment line, the comment line is also distributed.
- Each line must end with a linefeed character.

`[`*destination-host*`]`

- Specify a host name for a host that is defined in the JP1/IM - Manager system configuration and running JP1/Base 07-00 or a later version.
- To distribute the same definitions to multiple hosts, specify the hosts within `[ ]`, using commas to separate the hosts.
- Host names can be no more than 255 bytes.

- The maximum length of a line is 1,023 bytes.

`&`

You can add `&` to the beginning of a host name to distribute definitions to all of the hosts that are defined one layer below the specified host in the configuration definition information. If you specify an `&` for a host defined in the lowest layer in the configuration definition information, the specification is ignored. A single pair of square brackets can simultaneously contain a host prefixed with an ampersand (`&`) and a host without an ampersand (`&`).

`@`*action-definition-file-name*

You can use an arbitrary name for the definition file only when you distribute definitions in the action definition file for log file trapping. The file name cannot use the following symbols: `\ / : , ; * ? " < > |`, tags or spaces. If you specify `@`*action-definition-file-name* following square brackets, definitions are distributed to the following folder on the host specified in the square brackets:

In Windows: *installation-folder*`\conf\`

In UNIX: `/etc/opt/jp1base/conf/`

definitions

Specify definitions you want to distribute to each host. The file format is the same as that of each definition file. For details, see the following sections:

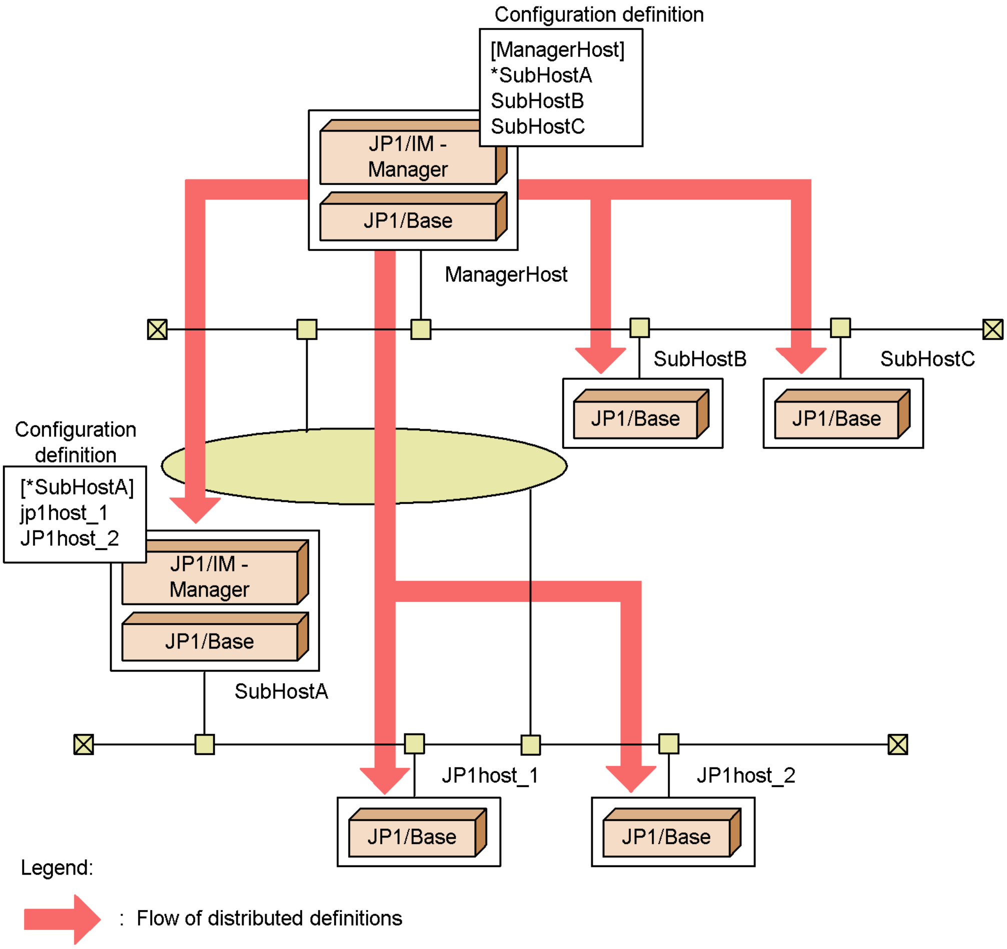
- File format of *Forwarding settings file*
- File format of *Action definition file for log file trapping*

  Note: Do not modify parameters related to file attributes (`FILETYPE`, `HEADLINE`, `HEADSIZE`, and `RECTYPE`).
- File format of *Action definition file for event log trapping (Windows only)*

Definition examples

This subsection shows an example of configuring a distribution definition file for distributing definitions in the following system:

Figure 14-7: Example system configuration



In the above example system configuration, `ManagerHost` is the integrated manager. SubHostA, SubHostB, and SubHostC are managed hosts for ManagerHost, and JP1host_1 and JP1host_2 are managed hosts for SubHostA, as defined in the system configuration for JP1/IM - Manager. For details on how to define the system configuration, see the *Job Management Partner 1/Integrated Management - Manager Configuration Guide*.

The following shows an example distribution definition file for distributing definitions in the forwarding settings file (forward) from ManagerHost to managed hosts.

```
#------------------------------------------
# JP1/Base - Event Server jev_forward.conf
#------------------------------------------
```

```
[SubHostA, SubHostB, SubHostC]
#-----------------------------------------
# JP1/Base - Event Server Forwarding Setting
#-----------------------------------------
to ManagerHost
E.SEVERITY IN Error
OR
E.PRODUCT_NAME IN /HITACHI/JP1/AOM
end-to

[JP1host_1, JP1host_2]
#-----------------------------------------
# JP1/Base - Event Server Forwarding Setting
#-----------------------------------------
to SubHostA
E.SEVERITY IN Error Warning
OR
E.PRODUCT_NAME IN /HITACHI/JP1/AOM
end-to
```

The following is an example for distributing definitions in the action definition file for log file trapping. In the example, ManagerHost distributes definitions as a file named ACTDEF1 to SubHostA and SubHostB, and as a file named ACTDEF2 to SubHostC.

The following shows an example distribution definition file (jev_logtrap.conf) for distributing definitions in the action definition file for log file trapping.

```
#-----------------------------------------
# JP1/Base - Event Server jev_logtrap.conf
#-----------------------------------------

[SubHostA,SubHostB]@ACTDEF1
FILETYPE=SEQ
RECTYPE =VAR '\n'
HEADLINE=3
MARKSTR ="====="
         "MARK"
ACTDEF  =00000111:00000000  "message"
[SubHostC]@ACTDEF2
FILETYPE=SEQ
RECTYPE =VAR '\n'
HEADLINE=3
MARKSTR ="====="
         "MARK"
ACTDEF  =00000222:00000000  "error"
```

Password definition file (Windows only)

Format

```
; Comment
OS-user-name:password
```

File name

Any

Storage destination directory

Any

Description

Sets password management information for multiple OS users in one operation.

Application of settings

Execute the `jbsmkpass` command to apply the settings. For details on the `jbsmkpass` command, see *jbsmkpass (Windows only)* in *13. Commands*.

Definition details

Write one entry per line. The characters you enter must be no more than 4,096 bytes per line. The characters following the semicolon (`;`) and up to the next linefeed constitute a comment. Each entry consists of two fields delimited with a colon (`:`). Specify each field as explained below.

OS-user-name

Specify one or more OS user names registered on each host.

As the OS user name to be registered, you can specify not only a user name but also the name of the domain to which the local host belongs or the local host name. To specify a domain name or local host name, use a backslash (\) as a separator between the domain or local host name and user name (for example, `domain\user1` or `server\user1`). If you specify a domain name, JP1/Base checks if the specified OS user is a user who belongs to that domain. If the specified OS user name is not a user of the domain, you cannot register the user under the OS user name. If you specify a local host name, JP1/Base checks whether the OS user name you entered is a local user. If the specified OS user name is a local user, you cannot register the user under the OS user name.

If you do not specify a domain name or local host name, JP1/Base checks whether the specified OS user is a local user. If the entered OS user is not a local user, JP1/Base checks whether it is a user in a domain containing a trusted domain. If the specified OS user name is not a local user or a user of the domain, you cannot register the user under the OS user name.

To register an OS user name with the Windows domain controller, use the format *domain-name\user-name*. As the domain controller does not differentiate between a domain user and local user, the user name will be treated as a domain user.

password

Specify the password for the *OS-user-name*. If you omit the password, the OS user is registered in the password information as an OS user without a password.

Note

Take care when selecting **The logon check is not done to Windows, when OS user is set** in the **User Mapping** page of the JP1/Base Environment Settings dialog box. When this check box is selected, the OS users can still be registered even if an OS user name or password is incorrect. However, if the mapped JP1 user tries to execute a job or remote command, an insufficient rights error occurs.

Definition examples

The format of the password definition file is shown below:

```
jp1user1:passwd000
```

User permission level file

Format

```
; Comment
JP1-user:JP1-resource-group=JP1-permission-level:JP1-resource-group=JP1-permission-level:...
```

File name

`JP1_UserLevel`

Storage destination directory

In Windows:

installation-folder`\conf\user_acl\`
shared-folder`\jp1base\conf\user_acl\ (in a cluster system)`

In UNIX:

`/etc/opt/jp1base/conf/user_acl/`
shared-directory`/jp1base/conf/user_acl/ (in a cluster system)`

Description

Sets operating permissions for JP1 resource groups that JP1 users access.

Application of settings

Execute the `jbsaclreload` command to apply the settings. For details on the `jbsaclreload` command, see *jbsaclreload* in *13. Commands*.

Definition details

A JP1 user permission level file (`JP1_UserLevel`) assigns a JP1 permission level to each user for operating on JP1 resource groups. Each line contains a single entry. The characters you enter must be no more than 4,096 bytes per line. The characters following the semicolon (`;`) and up to the next linefeed constitute a comment. Each entry consists of two or more fields delimited with a colon (`:`). Specify each field as explained below.

JP1-user-name

Specify a JP1 user name registered on the authentication server. You can use alphanumeric characters to specify a JP1 user name but the characters must be lower case. You can enter a character string that is from 1 to 31 bytes.

JP1-resource-group=JP1-permission-level

Specify a JP1 resource group and JP1 permission level (JP1 user operating permission). Use no more than 64 bytes for characters in each parameter.

You can specify multiple JP1 permission levels for a JP1 resource group, using commas to delimit the permission levels as in the following example: `JP1_AJS_Admin,JP1_JPQ_Admin,JP1_Console_Admin`.

For details on the JP1 resource groups and JP1 permission levels to be specified, see the manual for the JP1 program that uses JP1/Base user authentication.

The *JP1-resource-group* and *JP1-permission-level* parameters are described below.

JP1 resource group

A JP1 resource group is a set of entities (resources) such as jobs, jobnets, or events, that are managed together. For details on the JP1 resource group to specify, see *Job Management Partner 1/Integrated Management - Manager Configuration Guide*, *Job Management Partner 1/Automatic Job Management System 2 Planning and Administration Guide*, *Job Management Partner 1/Automatic Job Management System 3 System Design (Configuration) Guide*, *Job Management Partner 1/Automatic Job Management System 3 System Design (Work Tasks*) *Guide,* and the *JP1/Automatic Job Management System 3 Administration Guide*. For details on other products, see the product manuals. An asterisk (`*`) specified in this parameter allows the JP1 user to access all JP1 resource groups. However, you cannot specify any other JP1 resource group for a JP1 user for whom you have already specified an asterisk (`*`).

JP1-permission-level

A JP1 permission level indicates the types of operating permissions that a JP1 user holds for a management target (resource). Permissible operations depend on whether the management targets (the resources) are jobs, jobnets, events, or other entities. Operating permissions are managed as combinations of different permissions set for specific types of resources.

JP1 permission levels include `JP1_AJS_Admin`, `JP1_JPQ_Admin` and `JP1_Console_Admin`. For details on the JP1 permission level to specify, see *Job Management Partner 1/Integrated Management - Manager Configuration Guide*, *Job Management Partner 1/Automatic Job Management System 2 Planning and Administration Guide*, *Job Management Partner 1/Automatic Job Management System 3 System Design (Configuration) Guide*, *Job Management Partner 1/Automatic Job Management System 3 System Design (Work Tasks*) *Guide,* and the *JP1/Automatic Job Management System 3 Administration Guide*. For details on other products, see the manuals for those products.

Note

The user permission level file (`JP1_UserLevel`) is also used for the GUI. Any information you enter in the GUI will be applied to this file.

Definition examples

The following shows an example of settings in the user permission level file (`JP1_UserLevel`):

```
jp1admin:*=JP1_AJS_Admin,JP1_JPQ_Admin,JP1_Console_Admin
```

Directory server modification file (Windows only)

Format

```
"SERVER"=directory-server-name
"PORT"=destination-port-number
"BASE_DN"=container-object-ID
"ATTR_NAME"=relative-ID
"SSL"=dword:{00000000 | 00000001}
```

File name

Any

Storage destination directory

Any

Description

Sets the common definition information in order to temporarily change the directory server when the linked directory server cannot be used due to a failure.

Application of settings

Execute the `jbschgds` command to apply the settings of the directory server modification file to the common definition information. The `jbschgds` command can also be used to remove temporary changes. For details on the `jbschgds` command, see *jbschgds (Windows only)* in *13. Commands*.

Definition details

For details on the directory server modification file, see the definition examples in *Directory server linkage definition file (Windows only)*. However, do not specify `ENABLE`.

Definition examples

The following shows an example of settings in the directory server modification file.

```
"SERVER"="host-B.domain.local"
"PORT"=dword:0000027C
"BASE_DN"="OU=JP1,DC=domain,DC=local"
"ATTR_NAME"="CN"
"SSL"=dword:00000001
```

Directory server linkage definition file (Windows only)

Format

```
"ENABLE"=dword:{00000000 | 00000001}
"SERVER"=directory-server-name
"PORT"=Destination-port-number
"BASE_DN"=container-object-ID
"ATTR_NAME"=relative-ID
"SSL"=dword:{00000000 | 00000001}
```

File name

`jp1bs_ds_setup.conf` (Directory server linkage definition file)

`jp1bs_ds_setup.conf.model` (Model file of the directory server linkage definition file)

Storage destination directory

installation-folder`\conf\ds\`
shared-folder`\jp1base\conf\ds\ (in a cluster system)`

Description

Specifies the common definition information on the authentication server in order to perform login authentication linking with the directory server. If you use a secondary authentication server, set up the function on both primary and secondary authentication servers.

Application of settings

Execute the `jbssetcnf` command to apply the settings of directory server linkage definition file (`jp1bs_ds_setup.conf`) to the common definition information. For details on the `jbssetcnf` command, see *jbssetcnf* in *13. Commands*.

Definition details

Define the following parameters in the directory server linkage definition file (`jp1bs_ds_setup.conf`).

ENABLE (Can be omitted)

Specify whether to link with the directory server. If you do not want to link with the directory server, specify as `00000000`. If you want to link with the directory server, specify as `00000001`. The default is `00000000`.

`SERVER`

Specify the directory server for normal use. To use SSL, specify the directory server name in the FQDN format. You can enter a character string that is from 1 to 255 bytes.

`PORT` (Can be omitted)

Specify the destination port number of the directory server that is normally used in hexadecimal numbers. The specifiable range is `00000001` to `0000ffff`. The default is `00000185`, when SSL is not used (port number: `389`), and `0000027C` when SSL is used (port number: `636`).

`BASE_DN`

Specify the ID of the container object where JP1 users exist. You can enter a character string that is from 1 to 4,095 bytes.

`ATTR_NAME`

Specify attribute names of the relative ID that is used as a JP1 user name. You can enter a character string that is from 1 to 255 bytes.

`SSL` (Can be omitted)

Specify whether to use SSL. Specify as `00000000` if you do not want to use SSL. Specify as `00000001` if you want to use SSL. The default is `00000001`.

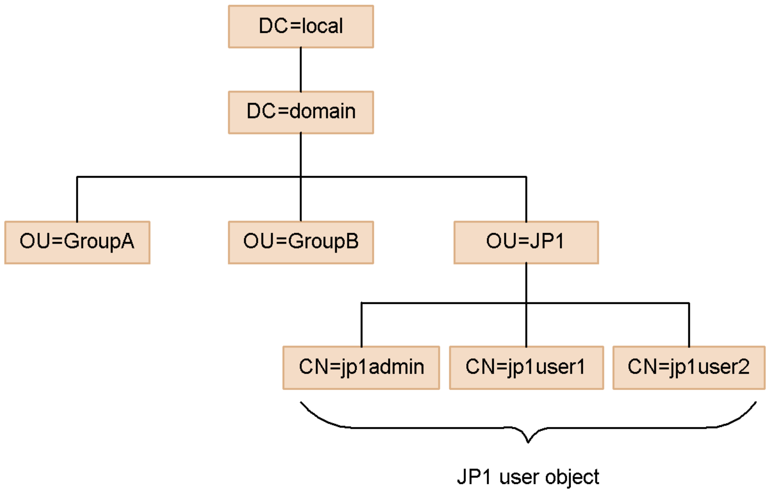
Note

If you want to configure this file on a logical host, configure it on both the primary and secondary nodes. Replace `JP1_DEFAULT` in `JP1_DEFAULT\JP1BASE` with *logical-host-name*.

Definition examples

The following shows the configuration of the directory server.

Figure 14-8: Example of directory server configuration



The following shows an example of settings in the directory server linkage file (`jp1bs_ds_setup.conf`).

```
[JP1_DEFAULT\JP1BASE\DIRSRV]
"ENABLE"=dword:00000001
"SERVER"="host-A.domain.local"
"PORT"=dword:0000027C
"BASE_DN"="OU=JP1,DC=domain,DC=local"
"ATTR_NAME"="CN"
"SSL"=dword:00000001
```

User mapping definition file

Format

```
; Comment
JP1-user-name:server-host-name:user-list
```

File name

`jp1BsUmap.conf`

Storage destination directory

In Windows:

installation-folder`\conf\user_acl\`
shared-folder`\jp1base\conf\user_acl\ (in a cluster system)`

In UNIX:

`/etc/opt/jp1base/conf/user_acl/`
shared-directory`/jp1base/conf/user_acl/ (in a cluster system)`

Description

Sets user mapping information for multiple JP1 users in one operation.

Application of settings

Execute the `jbsmkumap` command or the `jbssetumap` command to apply the settings. For details on the `jbsmkumap` and `jbssetumap` commands, see *jbsmkumap* and *jbssetumap* in *13. Commands*.

Definition details

Write one entry per line. The characters you enter must be no more than 4,096 bytes per line. The characters following the semicolon (`;`) and up to the next linefeed constitute a comment. Each entry consists of three fields delimited with a colon (`:`). Specify each field as explained below.

JP1-user-name

Specify a JP1 user name registered on the authentication server. You can use alphanumeric characters to specify a JP1 user name but the characters must be lower case. You can enter a character string that is from 1 to 31 bytes. Alternatively, enter an asterisk (`*`) to grant the rights of the users specified in *user-list* to all JP1 users. When writing multiple entries for the same server host, you can use both an asterisk and a specific JP1 user name registered on the authentication server to specify the same JP1 user name. An asterisk can only be specified once.

server-host-name

Specify the name of the server host that issues operating instructions. Enter a character string that is no more than 255 bytes. Specify an asterisk (`*`) to validate operations from any server host.

Specifying a physical host in **Server host**

Specify the host name displayed by the `hostname` command. If you are using domain names with the DNS service, specify the host name in FQDN format.

Specifying a logical host in **Server host**

Specify the logical host name whether or not you are using the DNS service.

To enable users to log into the system from JP1/AJS - View or to execute JP1/AJS commands on the local host, you must specify the local host name as the server host name. For details see the *Job Management Partner 1/Automatic Job Management System 2 Planning and Administration Guide*, *Job Management Partner 1/Automatic Job Management System 3 System Design (Configuration) Guide*, *Job Management Partner 1/Automatic Job Management System 3 System Design (Work Tasks) Guide*, and the *Job Management Partner 1/Automatic Job Management System 3 Administration Guide*.

user-list

Specify one or more OS user names registered on each host. Use commas to separate multiple names. When multiple OS user names are specified, the name written first in the list is taken as the primary OS user when no user is specified at job execution or at command execution. You can enter a character string that is no more than 64 bytes for each OS user name.

Note that in *user-list*, you can specify only OS users for whom you entered password information by executing the `jbspassmgr`, `jbsumappass`, or `jbsmkpass` command. If you want to specify the OS users to be mapped in *user-list*, be sure to register their information in the password management information. If you register OS user information containing the name of the domain to which the local host belongs, you must also enter the domain name with the OS user name in the user list.

Note

The GUI also uses the user mapping definition file (`jp1BsUmap.conf`). Any information you enter in the GUI will be reflected in this file.

Definition examples

The following shows an example of settings in the user mapping definition file (`jp1BsUmap.conf`):

```
jp1admin:*:Administrator
```

Health check definition file

Format

```
[JP1_EVENT]
OUTPUT={YES | NO}
RECOVER={YES | NO}
[SYSLOG]
OUTPUT={YES | NO}
RECOVER={YES | NO}
[OTHER_HOSTS]
INTERVAL=remote-host-monitoring-interval (seconds)
HOST=host-name1,host-name2,...
```

File name

`jbshc.conf`

Storage destination directory

In Windows:

installation-folder`\conf\jbshc\`
shared-folder`\jp1base\conf\jbshc\ (in a cluster system)`

In UNIX:

`/etc/opt/jp1base/conf/jbshc/`
shared-directory`/jp1base/conf/jbshc/ (in a cluster system)`

Description

Specifies the host to be monitored and the process-monitoring interval as the behavior of the health check function.

Application of settings

When you start the process management function, the settings are read from the health check definition file (`jbshc.conf`) and process monitoring begins.

Definition details

The following conventions apply to entries in the health check definition file (`jbshc.conf`).

- A hash mark (`#`) (code `0x23`) at the start of a line indicates a comment.
- Do not enter a space or tab before or after an equal sign (`=`) or comma (`,`) or at the beginning or end of a line. If you enter either of these, the line will be ignored.
- Lines containing only a linefeed character are ignored.

[JP1_EVENT]

This section is about issuing JP1 events.

OUTPUT={YES | NO}

Specify whether to issue a JP1 event when a process is in an abnormal state. Specify YES or NO. The default is YES.

RECOVER={YES | NO}

Specify whether to issue a JP1 event when a process has recovered. Specify YES or NO. The default is YES.

RECOVER=YES is invalid if you have specified OUTPUT=NO.

[SYSLOG]

This section is about message output to the syslog or event log.

OUTPUT={YES | NO}

Specify whether to output a message to the syslog or event log when a process is in an abnormal state. Specify YES or NO. The default is YES.

RECOVER={YES | NO}

Specify whether to output a message to the syslog or event log when a process has recovered. Specify YES or NO. The default is YES.

RECOVER=YES is invalid if you have specified OUTPUT=NO.

[OTHER_HOSTS]

This section is about remote host monitoring.

INTERVAL=*remote-host-monitoring-interval* (seconds)

Specify the interval over which to monitor a remote host. The specifiable range is 60 to 7200 (seconds).

Estimate the monitoring interval as follows:

(*number-of hosts-specified-in- the-HOST-parameter*) x 3 (seconds)

Allow 3 seconds per host as the time required to monitor processes. The time might vary depending on the state of the network and the status of the monitored hosts.

If you set a monitoring interval that is shorter than this guideline, errors will be detected more quickly, but the health check function might not finish monitoring a remote host within the specified interval. In this case, the function waits until the previous monitoring round ends.

If you set a monitoring interval that is longer than this guideline, you can save network and OS resources, but error detection might be delayed.

The default is `300` (seconds).

If the message `KAVA7219-W` is output to the integrated trace log during a health check

> The specified monitoring interval might be too short. Estimate the required monitoring interval using the following equation:
>
> (*current-interval*) + ((*KAVA7227-I-output-time* - *KAVA7219-W output-time*) x 1.1)

`HOST=`*host-name1*`,`*host-name2*`, . . .`

Specify the target remote hosts to be monitored. There is no need to specify this keyword if you want to monitor the local host only.

Delimit the host names with commas. You can specify multiple values for the `HOST` parameter. A maximum of 1,024 remote hosts can be specified. Hosts in excess of this maximum are not monitored.

Common definition settings file (health check function)

Format

```
[JP1_DEFAULT\JP1BASE\JBSHC]
"ENABLE"=dword:{00000000 | 00000001}
"FAILOVER"=dword:{00000000 | 00000001}
```

File name

Any

`jbshc_setup.conf.model` (Model file for the common definition settings file (health check function))

Storage destination directory

The model file for the common definition settings file (health check function) is located in the following directory. Copy this file to create a new file with any file name.

In Windows:
installation-folder`\conf\jbshc\`
shared-folder`\jp1base\conf\jbshc\ (in a cluster system)`

In UNIX:
`/etc/opt/jp1base/conf/jbshc/`
shared-directory`/jp1base/conf/jbshc/ (in a cluster system)`

Description

The health check function is disabled by default. This file specifies the common definition information to enable the health check function, so that this function can be used.

Application of settings

Execute the `jbssetcnf` command, to register the health check function information into the common definition information. For details on the `jbssetcnf` command, see *jbssetcnf* in *13. Commands*.

Definition details

The following conventions apply to entries in the common definition settings file (health check function).

- A hash mark (#) (code `0x23`) at the start of a line indicates a comment.
- Do not enter a space or tab before or after an equal sign (`=`) or comma (`,`) or at the beginning or end of a line. If a space or tab character appears in these locations,

an error occurs at `jbssetcnf` command execution.

- Lines containing only a linefeed character are ignored.

`[JP1_DEFAULT\JP1BASE\JBSHC]`

This section is for enabling or disabling the health check function and failover at error detection. To set a logical host, change `JP1_DEFAULT` to the logical host name.

`"ENABLE"=dword:{00000000 | 00000001}`

Specify whether to enable or disable the health check function. Specify `dword:00000001` to enable the function. Specify `dword:00000000` to disable the function. The default is `00000000`.

`"FAILOVER"=dword:{00000000 | 00000001}`

Specify whether to enable or disable failovers in a cluster system when the health check function monitoring the local host detects a process error. Specify `dword:00000001` to perform failovers#. Specify `dword:00000000` to disable failovers. The default is `00000000`.

#: This will stop all JP1/Base services in Windows, and the health check function process (`jbshcd`) in UNIX. If the system detects such a stop, it will try to initiate a failover by using the cluster software.

JP1/Base parameter definition file

Format

```
[JP1_DEFAULT\JP1BASE]
"SEND_PROCESS_TERMINATED_ABNORMALLY_EVENT"=dword:{0 | 1}
"SEND_PROCESS_RESTART_EVENT"=dword:{0 | 1}
"SEND_AUTHSRV_EVENT"=dword:{0 | 1}
```

File name

`jp1bs_param_V7.conf`

Storage destination directory

In Windows:

installation-folder`\conf\`
shared-folder`\jp1base\conf\ (in a cluster system)`

In UNIX:

`/etc/opt/jp1base/conf/`
shared-directory`/jp1base/conf/ (in a cluster system)`

Description

When a process ends abnormally or the authentication server is swapped over automatically in a system with two authentication servers, JP1/Base outputs an error message to the integrated trace log. This file is preset so that these messages can be issued as JP1 events.

Application of settings

Execute the `jbssetcnf` command to apply the settings of the JP1/Base parameter definition file (`jp1bs_param_V7.conf`) to the common definition information. Restart JP1/Base and the programs that require JP1/Base to apply the settings. For details on the `jbssetcnf` command, see *jbssetcnf* in *13. Commands*.

Definition details

Locate the following lines in this file:

`SEND_PROCESS_TERMINATED_ABNORMALLY_EVENT`

Specifies whether to issue a JP1 event when a process ends abnormally or when a timeout occurs at process startup. The default is `dword:0`.

`SEND_PROCESS_RESTART_EVENT`

Specifies whether to issue a JP1 event when the process is restarted. The default is `dword:0`.

`SEND_AUTHSRV_EVENT`

Specifies whether to issue a JP1 event when the authentication server is swapped. The default is `dword:0`.

To enable issuing of a JP1 event at error detection, change `dword:0` in both parameters to `dword:1`. To disable issuing of a JP1 event at error detection, change `dword:1` in both parameters to `dword:0`.

Note

If you want to configure this file on the logical host, configure it on both the primary and secondary nodes. Replace `JP1_DEFAULT` in `JP1_DEFAULT\JP1BASE` with *logical-host-name*.

Extended startup process definition file

Format

```
process-name|path|startup-options|restart-or-not|number-of-restarts|retry-interval|restart-count-reset-time|
```

File name

`jp1bs_service_0700.conf`

Storage destination directory

In Windows:

installation-folder`\conf\`
shared-folder`\jp1base\conf\ (in a cluster system)`

In UNIX:

`/etc/opt/jp1base/conf/`
shared-directory`/jp1base/conf/ (in a cluster system)`

Description

This file contains information on what processes to automatically restart, should a process abnormally stop, regardless the reason.

Application of settings

Execute the `jbs_spmd_reload` command or restart JP1/Base to apply the settings. For details on the `jbs_spmd_reload` command, see *jbs_spmd_reload* in *13. Commands*.

Definition details

The definition file contains initial definitions when you open it first. Do not modify the parameters for the process name, path, and startup options. Also note that you cannot omit the parameter delimiter (|). To insert a comment line, prefix the line with `#`. The characters following `#` and up to the next linefeed constitute a comment.

Restart or not

Specify whether to restart a process when it ends abnormally. To restart a process, specify `1`. Otherwise, specify `0`. The default is `0`.

Number of restarts

Specify how many times the system will attempt to restart a process. The specifiable range is 0 to 99. An optimum number is already set for each process. You can change the number as required. This parameter is valid only when the *restart-or-not* parameter is set to `1`.

Retry interval

Specify the interval (in seconds) at which the system will attempt to restart a process. The specifiable range is 0 to 3,600. An optimum number is already set for each process. You can change the number as required. This parameter is valid only when the *restart-or-not* parameter is set to `1`.

Restart count reset time

Specify the number of seconds that will elapse after the process is restarted, before the number of restarts is reset. The number of restarts is reset the specified time after the process is restarted. Then, the next time the process ends abnormally, the restart count starts from 1.

If the restarted process ends abnormally before the specified time elapses after the restart, however, the previous restart count remains. The specifiable range is `3600` to `2147483647` (seconds). An optimum number is already set for each process. You can change the number as required. This parameter is valid only when the *restart-or-not* parameter is set to `1`.

Notes

- If you omit a field or specify an invalid value, the process will fail with an error. If you execute the `jbs_spmd_reload` command with a field omitted or an invalid value specified, an error is returned without reflecting the settings.
- In a cluster system, when you start the process management process for the logical host without an extended startup process definition file (`jp1bs_service_0700.conf`) in the `conf` folder on the logical host, the extended startup process definition file (`jp1bs_service_0700.conf`) is copied from the physical host.

Definition examples

The following shows an example of settings in the extended startup process definition file (`jp1bs_service_0700.conf`) and the action taken when a process ends abnormally.

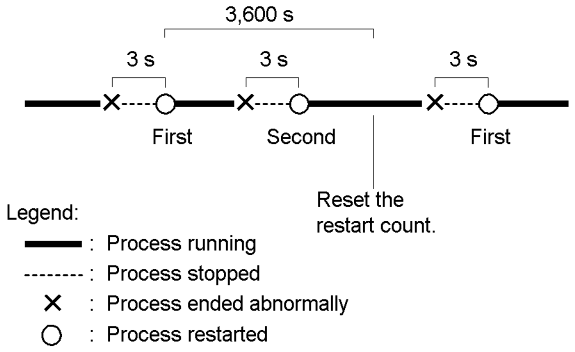
The following conditions are set for JP1/Base processes:

- Restart or not: Restart
- Number of restarts: 4
- Retry interval: 3 seconds
- Restart count reset time:3,600 seconds

```
jcocmd|C:\ProgramFiles\HITACHI\JP1Base\bin\jcocmd.exe||1|4|3|3
600|
jbsroute|C:\ProgramFiles\HITACHI\JP1Base\bin\jbsroute.exe|-o,6
```

```
00|1|4|3|3600|
jbssessionmgr|C:\ProgramFiles\HITACHI\JP1Base\bin\jbssessionmg
r.exe||1|4|3|3600|
jbsplugin|C:\ProgramFiles\HITACHI\JP1Base\bin\jbsplugind.exe||
1|4|3|3600|
```

Figure 14-9: Example of action when a process ends abnormally



In this example, the number of restarts is reset 3,600 seconds after the process is restarted if the process does not end abnormally within 3,600 seconds. Then, the next time the process ends abnormally, the restart count starts from 1. If the process ends abnormally again no more than 3,600 seconds after a restart, the restart count is not reset. If the number of restarts reaches the specified value, the system no longer attempts to restart the process.

jp1hosts definition file

Format

```
# Comment
host-name IP-address, IP-address, IP-address
```

File name

`jp1hosts` or any other file name

Storage destination directory

In Windows:

installation-folder`\conf\`
shared-folder`\jp1base\conf\ (in a cluster system)`

In UNIX:

`/etc/opt/jp1base/conf/`
shared-directory`/jp1base/conf/ (in a cluster system)`

Description

This file specifies the `hosts` information specific for JP1/Base. The `jp1hosts` definition file is provided by default. This default `jp1hosts` definition file cannot be used without editing it. When you use the default `jp1hosts` definition file, you must first edit it according to the use in JP1/Base. When you create your own `jp1hosts` definition file, store it in the same folder as the default `jp1hosts` file is stored.

Application of settings

Execute the `jbshostsimport` command to apply the `jp1hosts` information to the common definition information. For details on the `jbshostsimport` command, see *jbshostsimport* in *13. Commands*.

Definition details

The following conventions apply to entries in the `jp1hosts` definition file:

- A `jp1hosts` definition file consists of one entry per line. The characters you enter must be no more than 255 bytes per line.
- A hash mark (`#`) (code `0x23`) at the start of a line indicates a comment.

host-name IP-address, *IP-address*, *IP-address*

- This line indicates the correspondence between the host name and IP addresses. For *host-name* and *IP-address*, you can use ASCII characters only. Also, `" / \ [ ] ; : | = , + ? <`, and `>` are not allowed. *host-name* and *IP-address* must be separated by one or more spaces or tab characters. *host-name* cannot be a string that is recognized as an IP address.

- Use a comma (`,`) to delimit multiple *IP-addresses*. The spaces and tab characters before and after the comma are ignored. Each IP address must be specified in the format of `W.X.Y.Z` (`W`, `X`, `Y`, and `Z` are numeric numbers from 0 to 255).
- No more than four *IP-addresses* can be specified for one *host-name*. You cannot specify the same host name twice. If you do this, an error will occur when you execute the `jbshostsimport` command.

Host access control definition file

Format

```
AllowHost {
upper-host
all-host
host host-name-1
host host-name-2
...
host host-name-n
}
```

File name

`jbsdfts_srv.conf`

Storage destination directory

In Windows:
installation-folder`\conf\jbsdfts`

In UNIX:
`/etc/opt/jp1base/conf/jbsdfts`

Description

This file specifies which host has access permissions when linking with the IM configuration management function of JP1/IM. All access attempts from any other hosts will be rejected. However, all access attempts from a local host will be permitted.

Application of settings

Execute the `jbs_spmd_reload` command or restart JP1/Base to apply the settings. For details on the `jbs_spmd_reload` command, see *jbs_spmd_reload* in *13. Commands*.

Definition details

`upper-host`

All higher-level hosts in the JP1/IM configuration management are given permission. Hosts not configured by using IM configuration management are assumed to not be higher-level hosts. The default is `upper-host`.

`all-host`

Allows all hosts to have permission.

`host` *host-name*

Grants permission to the host specified in *host-name*.

Note

You need to specify permissions individually to the hosts not configured by using IM configuration management.

Local action environment variable file

Format

```
Environment variable name 1=variable-value-1
[Environment variable name 2=variable-value-2]
  :
```

File name

Any file name that is no more than 255 bytes.

Storage destination directory

Any file name and directory. Specify both in the `var` option in the local action execution definition file.

Description

This file defines the environment variables used to execute the command specified by the local action function. By preparing multiple local action environment variable files, you can specify environment variables for each execution command. In Windows, if the local action environment variable file is not specified, you can use the system environment variables to execute a command.

Application of settings

The settings are referenced when the environment variables execute a command.

Definition details

Environment variable name

Specify an environment variable name. A linefeed character cannot be used in an environment variable name.

Variable value

Specify the value of the environment variable.

The name and value of an environment variable can be replaced by the name and value of the system environment. For example, by enclosing the name of a system environment variable with the symbols `<-` and `->`, you can specify the environment variable name, just like you can enclose a variable name with percentage signs `%` in Windows or start one with a dollar sign `$` in UNIX. However, you can only perform one replacement per line.

Local action execution definition file

Format

```
# Common block
 [cmn
  [usr JP1-user-name]
  [var environment-variable-file-name]
  [evt [{yes|no}]/[{yes|no}]]
  [cnt-opt [queue=number-of-actions-in-queue] , [exec=number-of-actions-simultaneously-execute]]
end-cmn]

# Action block
act action-name
 cnd
   Event filter
 end-cnd
  [det same-action-suppress-time]
  [usr JP1-user-name]
  [var environment-variable-file-name]
 cmd command-to-execute
  [evt [{yes|no}]/[{yes|no}]]
  [cmd-opt usrprofile={0|1}]
end-act
  :
```

File name

`jbslcact.conf`

Storage destination directory

In Windows:

installation-folder`\conf\lcact`
shared-folder`\jp1base\conf\lcact (in a cluster system)`

In UNIX:

`/etc/opt/jp1base/conf/lcact/`
shared-directory`/jp1base/conf/lcact/ (in a cluster system)`

Description

This file defines the commands and their execution conditions for the local action function. The file consists of a common block and an action block. The common block defines the parameters commonly set in all actions blocks. The action block defines, in pairs, the JP1 event conditions for actions and the actions to execute when the JP1 event conditions are satisfied.

The local action function checks the execution conditions from the higher-level action block, and execute the action once the conditions are satisfied. If an action blocks on a level lower than the action block satisfies the conditions, the action block is ignored without being checked. Therefore, define conditions in the sequence according to their priority.

Application of settings

Start or reload JP1/Base to apply the settings.

Definition details

The following conventions apply to entries in the local action execution definition file:

- A hash mark (#) (code `0x23`) at the start of a line indicates a comment.
- The maximum length of a line is 4,200 bytes.
- Separate parameter with a space (code `0x20`) or a tab (code `0x09`).
- Letters are case sensitive.

Only one common block can be specified before an action block. When a parameter is specified in both the common block and the action block, specification in the action block takes effect. The coding conventions for the common block are as follows:

`cmn` to `end-cmn`

Indicates the start and end of the common block.

`usr` *JP1-user-name*

Specifies the JP1 user maps to the OS user who executes the action. If this parameter is omitted, the same parameter is required in the action block.

`var` *environment-variable-file-name*

Specifies the environment variable file names to refer to when executing an action. Enter a file name that is no more than 255 bytes.

`evt [{yes|no}]/[{yes|no}]`

Specifies whether to issue JP1 events indicating action start and action end. The event before the forward slash (/) is the action start event, and the event after is the action end event. When `yes` is specified, the system will issue a JP1 event. When `no` is specified or this parameter is omitted, the system will not issue a JP1 event.

`cnt-opt [queue=`*number-of-action-in-queue*`] ,`
`[exec=`*number-of-action-simultaneously-execute*`]`

Specifies the number of actions in the queue and the number of actions to be executed simultaneously. Separate the `queue` option and the `exec` option with a comma.

`queue=`*number-of-action-in-queue*

Specifies the maximum number of actions to be in the queue after the action conditions are satisfied. If the actions exceed the maximum number specified in this parameter, the actions will not be executed. As a result, specify a sufficient number. The specifiable range is from `0` to `65535`. The default is `1024`.

`exec=`*number-of-action-simultaneously-execute*

Specifies the maximum number of actions to be executed simultaneously. When the number of actions in execution has reached the maximum, other actions will wait in the queue. The specifiable range is from `1` to `48`. The default is `1`.

You can specify no more than 1,000 action blocks. Action blocks cannot be omitted. When a parameter is specified in both the common block and the action block, the specification in the action block takes effect. The coding format for the action block is shown below.

`act` *action-name* to *end-act*

Indicates start and end of the action block. Specify any action name that is 50 bytes or less after the `act` parameter. Action names are output to the local action execution log.

`cnd` to `end-cnd`

This parameter indicates the start and end of the block that specifies the JP1 event conditions for executing an action. Specify this block right after the `act` parameter. Specify the action conditions in the format of an event filter. For details on the writing format of an event filter, see *Event filter syntax*.

[`det` *same-action-suppress-time*]

Specifies in seconds the length of time during which same action is not executed. The specifiable range is 1 to 3,600 (seconds). If this parameter is omitted, the same action will not be suppressed.

usr *JP1-user-name*

Specifies the JP1 user who maps to the OS user who executes the action. You can specify an attribute variable name to JP1 users. If this parameter is omitted, the same parameter is required in the common block.

`var` *environment-variable-file-name*

Specifies the environment variable file names to refer to when executing an action. Enter a file name that is no more than 255 bytes. You can specify an attribute variable name in the environment variable file.

`cmd` *Command-to-execute*

Specifies the command to be executed for an action. Enter a name that is no more than 4,096 bytes. You can specify an attribute variable name in the command to be executed. For details on the format of the commands to be executed, see *1.8.2 Commands for local actions*.

`evt [{yes|no}]/[{yes|no}]`

Specifies whether to issue JP1 events indicating action start and action end. The event before the forward slash (`/`) is the action start event, and after is the action end event. When `yes` is specified, the system will issue a JP1 event. When `no` is specified or this parameter is omitted, the system will not issue a JP1 event.

`cmd-opt usrprofile={0|1}`

Specifies whether to load the user profile when executing a command.

The default is `0`.

`0`: Do not load the profile of the user who maps to the OS user.

`1`: Load the profile of the user who maps to the OS user.

Attribute variable name

You can specify an attribute variable name in specific items of the action block. You can specify an attribute variable name in three items: *JP1-user-name*, *environment-variable-file-name*, and *command-to-execute*. Before the execution of an action, the JP1 event that satisfies the action requirements acquires and expands the attribute value corresponding to the attribute variable name. The acquired information will be expanded in multiple locations, but the character string after the expansion is not expanded. Names of the specifiable attribute variables are shown in the following table.

Table 14-16: Attribute variables that can be specified in a local action

Type of information	Attribute variable name	Contents
Information contained in the basic attributes of JP1 events	EVID	Event ID (*basic-code*:*extended-code*)
	EVPID	Source process ID
	EVUSRID	User ID of the source process
	EVGRPID	Group ID of the source process
	EVUSR	Source user name
	EVGRP	Source group name
	EVHOST	Host name of the source name
	EVIPADDR	Source IP address
	EVMSG	Entire message text
Information contained in the basic attributes of JP1 events	EVSEV	Severity of the event extended information (Emergency, Alert, Critical, Error, Warning, Notice, Information, Debug)
	EV"Extended attribute name"	Any extended attribute

The following provides some examples of specifying an attribute variable name.

```
cmd  abcd.bat $EVUSR
```

This example specifies the attribute variable name `EVUSR` (attribute value: *USER01*) in the `cmd` parameter. In this example, attribute value is expanded to `abcd.bat USER01`.

Note the following points when specifying an attribute variable name:

- The character code of a JP1 event is expanded as is, even if it differs from that of the operating environment. Make sure you use the same character code.
- An action cannot be executed when the length of the character string after an expansion exceeds the limit.
- Irrelevant attribute variable values are `NULL`. Depending on the type of JP1 events, some items might not have an attribute variable name, and other might contain unrecognizable character codes (codes excluded from the character set of ASCII code) in attribute information. In such a case, actions cannot be executed, or the result might be incorrect even if an action is executed. Refer to the manual of the product that issues JP1 events when you specify an attribute variable.

- Do not write alphanumeric characters or underscores (_) right after an attribute variable name. Otherwise, the variable cannot be properly converted. If you want to write characters after the attribute variable name, enclose the name with { and }. The following shows an example, whereas the event ID (`$EVID`) is assumed to be `100:0`, and the extended attribute is EX (`$EV"EX"`) ABC.

```
Action definition -> Information converted
$EVID abc -> 100:0 abc
$EVIDabc -> $EVIDabc (in Windows), None (in UNIX)
${EVID}abc -> 100:0abc
$EVID_abc -> $EVID_abc (in Windows), None (in UNIX)
${EVID}_abc -> 100:0_abc
$EV"EX" abc -> ABC abc
$EV"EX"abc -> ABCabc
```

- If the characters to be converted include any of the following prohibited characters, the prohibited character is converted into a space (`0x20`) before proceeding.

  Prohibited characters to be converted into a space: `0x01` to `0x1F` (except tab characters: `0x09`) and `0x7F`.

  For example, depending on the setting of `$EVMSG`, if the acquired message contains a linefeed code (`0x0A`), the linefeed code will be converted into a space (`0x20`) before being proceeded.

  Example: For action `echo $EVMSG`, assume that the received event message contains a linefeed character: line 1 `0x0A` line 2, the command executed as an action is: `echo` line 1 △ line2, whereas △ represents a space

- In UNIX, the final expansion depends on the shell interpretation. If the expanded data contains a character that has specific meaning in a shell, for example, an asterisk `*`, will be replaced by the pre-defined meaning. To disable the replacement, enclose the entire variable with double quotation marks ("), for example, "$EVMSG".

Common definition settings file (local action function)

Format

```
[JP1_DEFAULT\JP1BASE\LCACT]
"LOGSIZE"=size-of-local-action-execution-log-file
"LOGFILENUM"=number-of-local-action-execution-log-files-to-be-saved
"PAUSE"=dword:{00000000 | 00000001}
```

File name

Any

`jp1bs_lcact_setup.conf.model` (Model file for the common definition settings file (local action function))

Storage destination directory

The model file for the common definition settings file (local action function) is located in the following directory. Copy this file to create a new file with any file name.

In Windows:

installation-folder`\conf\lcact\`
shared-folder`\jp1base\conf\lcact\ (in a cluster system)`

In UNIX:

`/etc/opt/jp1base/conf/lcact/`
shared-directory`/jp1base/conf/lcact/ (in a cluster system)`

Description

This file specifies the local action function to pause or unpause in order to perform maintenance. This file also specifies log information of the local action execution log file to the common definitions.

Application of settings

Execute the `jbssetcnf` command to register information of the common definition settings file (local action function) into the common definition information. For details on the `jbssetcnf` command, see *jbssetcnf* in *13. Commands*.

Next, either execute the `jbs_spmd_reload` command or restart JP1/Base to apply the common definition information settings. For details on the `jbs_spmd_reload` command, see *jbs_spmd_reload* in *13. Commands*.

Definition details

The following conventions apply to entries in the common definition settings file (local action function).

- A hash mark (#) (code 0x23) at the start of a line indicates a comment.
- Do not enter a space or tab before or after an equal sign (=) or comma (,) or at the beginning or end of a line. If a space or tab character appears in these locations, an error occurs at `jbssetcnf` command execution.
- Lines containing only a linefeed character are ignored.

`[JP1_DEFAULT\JP1BASE\LCACT]`

This section specifies whether to enable the local action function and the log information of the local action execution log. To set a logical host, change JP1_DEFAULT to the logical host name.

`"LOGSIZE"=`*size-of-local-action-execution-log-file*

Specify, in bytes, the size of the local action execution log file with hexadecimal numbers. The specifiable range is `00002000` (8 KB) to `00400000` (4,096 KB). When a size smaller than the lower limit of the range is specified, the lower limit will be used. When a size larger than the upper limit of the range, the upper limit will be used. The default is `00100000` (1,024 KB).

`"LOGFILENUM"=`*number-of-local-action-execution-log-files-to-be-saved*

Specify, with hexadecimal numbers, how many of the local action execution log files you want to save. The specifiable range is `00000001` (one file) to `00000010` (16 files). When a size smaller than the lower limit of the range is specified, the lower limit will be used. When a size larger than the upper limit of the range, the upper limit will be used. The default is `00000004` (four files).

`"PAUSE"=dword:{00000000 | 00000001}`

Specifies whether to start the local action function or to pause the function. To start the function, specify as `dword:00000000`. To pause the function, specify `dword:00000001`. If a number out of the specifiable range is specified, the default will be used. The default is `00000000`.

Chapter
15. JP1 Events

This chapter describes the types of JP1 events output by JP1/Base, and the occurrences that lead to event generation. Details about each JP1 event are also provided.

15.1 JP1 event attributes

This section lists and describes the attributes of JP1 events. JP1 events have two types of attributes: *basic attributes* and *extended attributes*.

Basic attributes are held by all JP1 events. Extended attributes are assigned separately by the specific program that issued the JP1 event.

15.1.1 Basic attributes

The following table lists and describes the basic attributes of JP1 events.

Table 15-1: Basic attributes of JP1 events

Attribute	**Format**#1	**Contents**	**JP1/SES support**
Serial number	Numeric value (32 bits)	Order in which events (including local events) arrive at this event server, regardless of the source. This attribute is not preserved for JP1 event transfers between event servers. This attribute is mainly used to prevent delays or duplication when events are forwarded to a pseudo-operator or to another event server.	No
Event ID	Two numeric values (32 bits)#2	An 8-byte value indicating the application program that issued the event and the event contents.	Yes
Registered reason	Numeric value (32 bits)	Reason for registration of the JP1 event on this event server. This attribute is not preserved for JP1 event transfers between event servers. One of the following codes is set: `1`: Event issued by the local event server to the local event server `2`: Event issued by the local event server to the remote event server (this value cannot be obtained from an application) `3`: Event issued by the remote event server to the local event server `4`: Event forwarded from the remote event server to the local event server because of the environment settings	No
Source process ID	Numeric value (32 bits)	Process ID of the application program that issued the event.	Yes
Registered time	Numeric value (32 bits)	Time of event registration on the source event server (number of seconds since UTC 1970-01-01 00:00:00, based on the source host clock).	Yes
Arrived time	Numeric value (32 bits)	Time of event registration on the local event server (number of seconds since UTC 1970-01-01 00:00:00). This attribute is not preserved for JP1 event transfers between event servers.	No

Attribute	Format[#1]	Contents	JP1/SES support
Source user ID	Numeric value (32 bits)	User ID (number) of the source process. In Windows and Java, set to a fixed value according to the environment settings (-1 to 65,535).	Yes
Source group ID	Numeric value (32 bits)	Group ID (number) of the source process. In Windows and Java, set to a fixed value according to the environment settings (-1 to 65,535).	Yes
Source user name	Character string (0 to 20 bytes)	User name of the source process.	Yes
Source group name	Character string (0 to 20 bytes)	Group name of the source process. Null string in Windows and Java.	Yes
Source event server name[#3]	Character string (0 to 255 bytes)	Name of the source event server. Set to the event server name of the first agent host, even if the JP1 event is forwarded from that agent host to a submanager host, and then to a manager host.	Yes
Destination event server name[#3]	Character string (0 to 255 bytes)	Name of the remote event server, if the application program explicitly specifies forwarding to a remote event server.	Yes
Source IP address	Byte string (0 to 16 bytes)	IP address corresponding to the source event server. (Not an accurate value if the JP1 event is sent through network address translation (NAT) or a proxy server, or is forwarded according to the environment settings.)	Yes
Destination IP address	Byte string (0 to 16 bytes)	IP address corresponding to the destination event server. (Not an accurate value if the JP1 event is sent through network address translation (NAT) or a proxy server, or is forwarded according to the environment settings.)	Yes
Source serial number	Numeric value (32 bits)	Serial number in the event database on the source host (unchanged at event transfer).[#4]	No
Code set	Character string (0 to 255 bytes)	Name of the character code-set in which the message, detailed information, and extended attributes are written.[#5]	No
Message	Character string (0 to 1,023 bytes) [#6]	Message text indicating the JP1 event contents.	Yes

Attribute	Format#1	Contents	JP1/SES support
Detailed information	Character string or byte string (0 to 1,024 bytes) #6	Any data.	Yes

Legend:

Yes: Attribute supported in JP1/SES

No: Attribute not supported in JP1/SES

#1: A character string is any non-zero byte string. Zeros can be included within the string.

#2: Represented as a hexadecimal with a colon separating the upper four bytes (basic code) and lower four bytes (extended code). For example, an event ID can be expressed as `00000111:00000000` or as `111:0`. For the range of values, see the manual for the specific JP1 program. The range of event IDs that can be specified by the user is `0:0` to `1FFF:0`, and `7FFF8000:0` to `7FFFFFFF:0`. The extended code is always 0.

#3: The event server name is normally the host name.

#4: JP1/SES protocol events are assigned a number based on the time in milliseconds at which the event server receives them.

#5: The values include:

- 8859_1 (ISO-8859-1)
- SJIS (shift JIS)
- EUCJIS (EUC Japanese)
- UTF-8 (Japanese UTF-8)

#6: The total maximum length of the message plus detailed information is 1,024 bytes. The relationships between these two items are shown below.

Detailed information format	Without message	With message (character string)
None	--	1,023 bytes
Character string	1,023 bytes	1,022 bytes total
Byte string	1,024 bytes	1,023 bytes total

15.1.2 Extended attributes

An extended attribute is an attribute optionally set by a program when issuing a JP1 event. An extended attribute consists of common information and program-specific information. The common information is information shared among all of the JP1 programs. The program-specific information is extended information that is not common information.

The following table lists common information.

Table 15-2: Common information in extended attributes

Item	Attribute name	Contents
Event level	SEVERITY	Indicates the urgency of a JP1 event. The following levels are used, starting from the most severe: Emergency, Alert, Critical, Error, Warning, Notice, Information, and Debug
User name	USER_NAME	Name of the user who executed the job.
Product name	PRODUCT_NAME	Name of the program that issued the JP1 event. The program names set in this attribute include: /HITACHI/JP1/AJS /HITACHI/JP1/AOM /HITACHI/JP1/IM /HITACHI/JP1/NBQ /HITACHI/JP1/NETMDM /HITACHI/JP1/NPS /HITACHI/JP1/NQSEXEC /HITACHI/JP1/SES /HITACHI/JP1/BASE
Object type	OBJECT_TYPE	Object type: JOB, JOBNET, BATCHJOB, ACTION, LIST, EVENTDB, COMMAND, LOGFILE, SNMP_TRAP, SESSION, or SPMD
Object name	OBJECT_NAME	Object name (job, jobnet, and so on). For a hierarchy of objects such as a jobnet, the lowest element is set.
Root object type	ROOT_OBJECT_TYPE	Object type. Normally the same as OBJECT_TYPE, but when there is a hierarchy of objects as in a jobnet, the type of the top-level object is set. The range of values is the same as for OBJECT_TYPE.
Root object name	ROOT_OBJECT_NAME	Name of the unit for execution instructions during user operation. Normally the same as OBJECT_NAME, but when there is a hierarchy of objects as in a jobnet, the name of the top-level object is set.
Object ID	OBJECT_ID	Object ID. When paired with PRODUCT_NAME, the OBJECT_ID uniquely identifies an instance of the object within the JP1 system. (The format is product-dependent. This information is used when a user launches the monitor screen for a JP1 program from the Tool Launcher in JP1/IM - View.)

Item	Attribute name	Contents
Occurrence	OCCURRENCE	The event that occurred in relation to the object shown in OBJECT_NAME. The values set in this attribute include: END, LATEEND, LATESTART, NOTICE, PAUSE, START, SWITCH, and RECEIVE
Start time	START_TIME	Time at which execution started or restarted, as the number of seconds since UTC 1970-01-01 00:00:00. This item is not always set.
End time	END_TIME	Time at which execution completed, as the number of seconds since UTC 1970-01-01 00:00:00. This item is not always set.
Result code	RESULT_CODE	Result code represented as a character string of decimal (base 10) numbers. This item is not always set.

15.2 List of JP1 events output by JP1/Base

The following table lists the events output by JP1/Base.

Table 15-3: JP1 events output by JP1/Base

Event ID	Occurrence	Message
00003D00	When the event database is switched	`Event DB was switched from` *old-database-number* `to` *new-database-number*`.`
00003D04	When the event service restart function restarts an abnormally stopped process	`The event service was recovered by restarting an internal function.`
00003A10#4	When a log file trap successfully connects to the event service at retry	`Event issuance was delayed because the system retried the log file trap.`
00003A20#4	When a log file trap cannot start log file monitoring	`Monitoring of the relevant log file cannot start.`
00003A21#4	When the retry count for reading application log files reaches the threshold and monitoring of the affected log file stops	`Monitoring will now stop because the specified number of retries was performed, but the relevant log file cannot be read.`
00003A22#4	When an application log file is in error status	`Monitoring of the relevant log file cannot continue.`
00003A71	When a log message for a Windows event is detected	Windows event-log message
00003A73	When a Windows event log failed to be acquired	`Acquisition of event log data failed.`
00003A74	When it is possible to monitor a Windows event log	`An event log can now be monitored.`
Event ID set in the `ACTDEF` parameter in the action definition file#4	When a record of an AP log file is detected	Contents of one line of log file data
00003A80	When an SNMP trap is detected	NNM messages (For details, see *I.5 JP1 events for SNMP trap conversion*).
00003FA0#1	When the command execution control receives an command execution request from the Execute Command window	`[`*host-name*`:`*JP1-user-name*`] Command execution started.`

Event ID	Occurrence	Message
00003FA1[#1]	When the command execution requested from the Execute Command window completes	`[`*host-name*`:`*JP1-user-name*`] Command execution ended normally.`
00003FA2[#1]	When command execution from the Execute Command window is not performed for some reason	`[`*host-name*`:`*JP1-user-name*`] Command execution ended abnormally.`
00003FA3[#1]	When the interval for issuing elapsed time events has been specified by the `jcocmddef` command. When the command execution requested from the Execute Command window or automated action is performed after the issuance interval of the elapse time event has been exceeded.	`[`*host-name*`] The execution time of command execution exceeded the regulation value (`*number*` sec)`
00003FA5[#1]	When a threshold of queued commands is specified in the `jcocmddef` command. When the number of queued commands has reached the threshold of the automated action	`In `*target-host-name*`, the number of queued commands requested from `*source-host-name*` has exceeded the threshold (xx).`
00003FA6[#1]	When a threshold of queued commands is specified in the `jcocmddef` command. When the threshold of queued commands for the automated action is specified as `0`	`In `*target-host-name*`, the number of queued commands requested from `*source-host-name*` has become 0.`
00004700[#2]	When an authentication server is blocked	*connection-sequence*`: `*authentication-server-name*` was successfully blocked.`
00004701[#2]	When an authentication server is unblocked	*connection-sequence*`: `*authentication-server-name*` was successfully unblocked.`
00004702[#2]	When all authentication servers are blocked	`All authentication servers are blocked.`
00004720[#2]	When the process ends abnormally	*component-name management-target-process-name* `has ended abnormally.`
00004721[#2]	When an attempt to start a process results in a timeout	`A `*component-name*` timeout occurred in `*management-target-process-name*` Processing continues.`

Event ID	Occurrence	Message
00004722[#2]	When an abnormally ended process is restarted	`Restart of the` *component-name management-target-process-name* `has finished.`
00004740	When a monitored process ends abnormally	*function-name* `ended abnormally.`
00004741	When a monitored process has been unable to access (update) shared memory for a set time (`SEVERITY:Error`)	*function-name* `has been processing for` *nn* `seconds.`
00004742	When a monitored process has been unable to access (update) shared memory for a set time (`SEVERITY:Warning`)	*function-name* `has been processing for nn seconds. After passes of` *mm* `seconds, becomes error condition.`
00004743	When a monitored process that was unable to access (update) shared memory for a set time has recovered	*function-name* `has a normal status.`
00004747	When the health check function ends abnormally	`The health check function stopped because an error occurred.`
00004748	When an error (service inactivity) is detected during monitoring of a remote host	`Monitoring notification cannot be performed at` *host-name* `because` *service-name* `is not functioning.`
00004749	When an error (host unreachable) is detected during monitoring of a remote host	`Monitoring cannot be performed because a connection with` *host-name* `cannot be established.`
0000474A	When remote host monitoring can be resumed	*host-name* `can now be monitored.`
0000474B	When the shared memory is inaccessible	`The shared memory is locked.`
00002102[#3]	In UNIX, a JP1 event is output in one of the following cases: • When the event service starts while the JP1/SES compatibility function is enabled • When connected from the JP1/SES or JP1/AJS event service on a remote host	None

Event ID	Occurrence	Message
00002103#3	In UNIX, a JP1 event is output in one of the following cases: • When the event service starts while the JP1/SES compatibility function is enabled • When connected from the JP1/SES or JP1/AJS event service on a remote host • When connected to the JP1/SES or JP1/AJS event service on a remote host In Windows, a JP1 event is output in one of the following cases: • When connected from the JP1/SES or JP1/AJS event service on a remote host • When connected to the JP1/SES or JP1/AJS event service on a remote host	None
00002104#3	In UNIX, a JP1 event is output in one of the following cases: • When the event service stops while the JP1/SES compatibility function is enabled • When the JP1/SES or JP1/AJS event service stops on the remote host that is connected to	Function name of the process
00010B7F#3	In Windows or UNIX, when connected from the JP1/SES or JP1/AJS event service on a remote host	None
00004780	When a request to start execution of the action is accepted, or when the JP1 event (action start event) is registered	`An action execution start request was accepted.` (*action-execution-information*)
00004781	When command execution completed and the JP1 event (action end event) is registered	`An action has completed.` (*action-execution-information*)

Event ID	Occurrence	Message
00004782	When command execution is not completed and the JP1 event (action end event (not executable) is registered	`An action ended without being executed.` (*action-execution-information*)
00004783	When command execution is canceled and the JP1 event (action end event (cancellation)) is registered	`An action ended because it was cancelled.` (*action-execution-information*)

#1: This JP1 event is issued only when the `jcocmddef` command was used when specifying JP1/IM - Manager. For details on the settings, see *jcocmddef* in *13. Commands*.

#2: Issued only when you have configured JP1 events to be issued upon a change in the blocked status of an authentication server or upon the abnormal end of a process. For details on how to issue a JP1 event indicating the blocked status of the authentication server or abnormal process status, see *2.4.2(2) Detecting process termination and authentication server switching*.

#3: JP1 events for the JP1/SES compatibility function have no severity specified. However, you do not need to take action for these indications, because they are equivalent to the Information severity level.

#4: The log file trap or JP1/AJS log monitoring job issues the event.

15.3 JP1 event details

This section lists JP1 event details by event ID.

(1) Details about event ID 00003D00

Attribute type		Item	Attribute name	Contents
Basic attribute		Message	--	`Event DB was switched from` *old-database-number* `to` *new-database-number*`.`
		Detailed information	--	Old event database number
Extended attribute	Common information	Event level	`SEVERITY`	`Notice`
		Product name	`PRODUCT_NAME`	`/HITACHI/JP1/IM`
		Object type	`OBJECT_TYPE`	`EVENTDB`
		Object name	`OBJECT_NAME`	Old event database number
		Object ID	`OBJECT_ID`	*event-server-name*`:`*old-database-number*
		Occurrence	`OCCURRENCE`	`SWITCH`
	Program-specific information	Old event database number	`E0`	Old event database number

Legend:

--: None

(2) Details about event ID 00003D04

Attribute type		Item	Attribute name	Contents
Basic attribute		Event ID	--	00003D04
		Message	--	`The event service was recovered by restarting an internal function.`

Attribute type		Item	Attribute name	Contents
Extended attribute	Common information	Event level	`SEVERITY`	`Notice`
		Product name	`PRODUCT_NAME`	`/HITACHI/JP1/IM`
		Object type	`OBJECT_TYPE`	`EVENT`
		Object name	`OBJECT_NAME`	`jevservice`
		Occurrence	`OCCURRENCE`	`NOTICE`

Legend:

--: None

(3) Details about event ID 00003A10

Attribute type		Item	Attribute name	Contents
Basic attribute		Event ID	--	00003A10
		Message	--	`KAVA3640-W Event issuance was delayed because the system retried the log file trap. (ID =` *process-ID*`/`*thread-ID*`[`*monitoring-target-name*`])`
Extended attribute	Common information	Event level	`SEVERITY`	`Warning`

Attribute type		Item	Attribute name	Contents
		Product name	`PRODUCT_NAME`	In Windows: • `jevlogstart` command with `-p` option specified `/HITACHI/JP1/NT_LOGTRAP/`*program-name* *program-name* is the name of the source program that output the log data, as specified in the `-p` option. • `jevlogstart` command with `-p` option unspecified `/HITACHI/JP1/NT_LOGTRAP` In UNIX: • `jevlogstart` command with `-p` option specified `/HITACHI/JP1/UX_LOGTRAP/`*program-name* *program-name* is the name of the source program that output the log data, as specified in the `-p` option. • `jevlogstart` command with `-p` option unspecified `/HITACHI/JP1/UX_LOGTRAP`
		Object type	`OBJECT_TYPE`	`LOGFILE`
		Object name	`OBJECT_NAME`	`jevlogstart`
		Object ID	`OBJECT_ID`	ID of the log file trap that executed the retry processing
		Occurrence	`OCCURRENCE`	`RECONNECT`
	Program-specific information	Retry start time	`RETRY_START_TIME`	Time at which retry processing started (number of seconds since UTC 1970-01-01 00:00:00)
		Reconnect time	`RECONNECT_TIME`	Time at which reconnection to the event service was confirmed (number of seconds since UTC 1970-01-01 00:00:00)
		Number of held events	`HOLD_EVENT`	Number of JP1 events held during retry processing
		Number of deleted events	`DELETE_EVENT`	Number of JP1 events deleted during retry processing

Legend:

--: None

(4) Details about event ID 00003A20

Attribute type		Item	Attribute name	Contents
Basic attribute		Event ID	--	00003A20
		Message	--	`KAVA3643-E Monitoring of the relevant log file cannot start. (code=`*error-number*`, file name=`*log-file-name*`)`
Extended attribute	Common information	Event level	`SEVERITY`	`Error`
		Product name	`PRODUCT_NAME`	In Windows: • `jevlogstart` command with `-p` option specified `/HITACHI/JP1/NT_LOGTRAP/`*program-name* *program-name* is the name of the source program that output the log data, as specified in the `-p` option. • `jevlogstart` command with `-p` option unspecified `/HITACHI/JP1/NT_LOGTRAP` In UNIX: • `jevlogstart` command with `-p` option specified `/HITACHI/JP1/UX_LOGTRAP/`*program-name* *program-name* is the name of the source program that output the log data, as specified in the `-p` option. • `jevlogstart` command with `-p` option unspecified `/HITACHI/JP1/UX_LOGTRAP`
		Object type	`OBJECT_TYPE`	`LOGFILE`
		Object name	`OBJECT_NAME`	Name (path) of the monitored log file
		Object ID	`OBJECT_ID`	ID of the log file trap
		Occurrence	`OCCURRENCE`	`NOTICE`

Attribute type		Item	Attribute name	Contents
	Program-specific information	Monitoring stop time	`WATCH_STOP_TIME`	Time at which log file monitoring stopped (number of seconds since UTC 1970-01-01 00:00:00)

Legend:

--: None

(5) Details about event ID 00003A21

Attribute type		Item	Attribute name	Contents
Basic attribute		Event ID	--	00003A21
		Message	--	`KAVA3644-E Monitoring will now stop because the specified number of retries was performed, but the relevant log file cannot be read. (code=`*error-number*`, file name=`*log-file-name*`)`
Extended attribute	Common information	Event level	`SEVERITY`	`Error`

		Product name	`PRODUCT_NAME`	In Windows:
				• `jevlogstart` command with `-p` option specified
				`/HITACHI/JP1/NT_LOGTRAP/`*program-name*
				program-name is the name of the source program that output the log data, as specified in the `-p` option.
				• `jevlogstart` command with `-p` option unspecified
				`/HITACHI/JP1/NT_LOGTRAP`
				
				In UNIX:
				• `jevlogstart` command with `-p` option specified
				`/HITACHI/JP1/UX_LOGTRAP/`*program-name*
				program-name is the name of the source program that output the log data, as specified in the `-p` option.
				• `jevlogstart` command with `-p` option unspecified
				`/HITACHI/JP1/UX_LOGTRAP`

Attribute type		Item	Attribute name	Contents
		Object type	`OBJECT_TYPE`	`LOGFILE`
		Object name	`OBJECT_NAME`	Name (path) of the monitored log file
		Object ID	`OBJECT_ID`	ID of the log file trap
		Occurrence	`OCCURRENCE`	`NOTICE`
	Program-specific information	Monitoring stop time	`WATCH_STOP_TIME`	Time at which log file monitoring stopped (number of seconds since UTC 1970-01-01 00:00:00)

Legend:

--: None

(6) Details about event ID 00003A22

Attribute type		Item	Attribute name	Contents
Basic attribute		Event ID	--	00003A22
		Message	--	`KAVA3645-E Monitoring of the relevant log file cannot continue. (code=`*error-number*`, file name=`*log-file-name*`)`
Extended attribute	Common information	Event level	`SEVERITY`	`Error`

Attribute type		Item	Attribute name	Contents

		Product name	`PRODUCT_NAME`	In Windows:
				• `jevlogstart` command with `-p` option specified
				`/HITACHI/JP1/NT_LOGTRAP/`*program-name*
				program-name is the name of the source program that output the log data, as specified in the `-p` option.
				• `jevlogstart` command with `-p` option unspecified
				`/HITACHI/JP1/NT_LOGTRAP`
				In UNIX:
				• `jevlogstart` command with `-p` option specified
				`/HITACHI/JP1/UX_LOGTRAP/`*program-name*
				program-name is the name of the source program that output the log data, as specified in the `-p` option.
				• `jevlogstart` command with `-p` option unspecified
				`/HITACHI/JP1/UX_LOGTRAP`

		Object type	`OBJECT_TYPE`	`LOGFILE`
		Object name	`OBJECT_NAME`	Name (path) of the monitored log file
		Object ID	`OBJECT_ID`	ID of the log file trap
		Occurrence	`OCCURRENCE`	`NOTICE`
	Program-specific information	Error detection time	`WATCH_CHECK_TIME`	Time at which the log file error was detected (number of seconds since UTC 1970-01-01 00:00:00)

Legend:

--: None

(7) Details about event ID 00003A71

Attribute type		Item	Attribute name	Contents
Basic attribute		Message	--	Windows event-log message[#]. Maximum 1,023 bytes. Any excess is truncated.
Extended attribute	Common information	Event level	`SEVERITY`	Registered according to severity levels of Windows event log. Value: Severity levels `Error`: Error `Warning`: Warning `Information`: Information, Other `Notice`: Audit_success, Audit_failure
		Product name	`PRODUCT_NAME`	`/HITACHI/JP1/NTEVENT_LOGTRAP/`*source*
		Object type	`OBJECT_TYPE`	`LOGFILE`
		Object name	`OBJECT_NAME`	`NTEVENTLOG`
		Root object type	`ROOT_OBJECT_TYPE`	`LOGFILE`
		Root object name	`ROOT_OBJECT_NAME`	`NTEVENTLOG`
	Program-specific information	Windows log registration date/time	`A0`	time_t form (number of seconds since UTC 1970-01-01 00:00:00)
		Computer name	`A1`	Computer name
		NT log type	`A2`	`System/Security/Application/Directory Service/DNS Server/File Replication Service`
		NT log type	`A3`	`Error/Warning/Information/Audit_Success/Audit_Failure` Other type: `None` In Windows Vista or Windows Server 2008, the information displayed in **Level** in the Event Viewer window For the security log, the information displayed in **Keyword** in the Event Viewer window

Attribute type		Item	Attribute name	Contents
		NT log category	A4	Category None if unidentifiable. In Windows Vista or Windows Server 2008, the information displayed in **Category**, under **Task**, in the Event Viewer window
		NT event ID	A5	Windows event ID
		NT user name	A6	Windows user name. N/A if unidentifiable.
		Platform	PLATFORM	NT
		Program name	PPNAME	/HITACHI/JP1/ NTEVENT_LOGTRAP

Legend:

--: None

#: If the message DLL containing the explanatory information about the event log entry is not set correctly, the inserted strings and detail code are enclosed with double quotation marks in the output JP1 message.

(8) Details about event ID 00003A73

Attribute type		Item	Attribute name	Contents
Basic attribute		Event ID	--	00003A73
		Message	--	KAVA3030-W Acquisition of event log data failed. (function=*function*, code=*cause-code*, log=*log-type*)
Extended attribute	Common information	Event level	SEVERITY	Warning
		Product name	PRODUCT_NAME	/HITACHI/JP1/ NTEVENT_LOGTRAP
		Object type	OBJECT_TYPE	LOGFILE
		Object name	OBJECT_NAME	NTEVENTLOG
	Program-specific information	Error detected time	ERROR_TIME	Time at which the error occurred, registered as the number of seconds since UTC 1970-01-01 00:00:00.

Attribute type		Item	Attribute name	Contents
		Log type	`LOG_TYPE`	Windows log type of the error that occurred `System/Security/ Application/Directory Service/DNS Server/File Replication Service`
		API name that error occurred	`ERROR_FUNCTION`	Windows API name of the error that occurred
		Cause of error	`ERROR_CAUSE_ID`	Error cause code

Legend:

--: None

(9) Details about event ID 00003A74

Attribute type		Item	Attribute name	Contents
Basic attribute		Event ID	--	00003A74
		Message	--	`KAVA3031-I An event log can now be monitored. (log=`*log-type*`)`
Extended attribute	Common information	Event level	`SEVERITY`	`Information`
		Product name	`PRODUCT_NAME`	`/HITACHI/JP1/ NTEVENT_LOGTRAP`
		Object type	`OBJECT_TYPE`	`LOGFILE`
		Object name	`OBJECT_NAME`	`NTEVENTLOG`
	Program-specific information	Recover time	`RECOVER_TIME`	Length of time to recover from the error, registered as the number of seconds since UTC 1970-01-01 00:00:00.
		Log type	`LOG_TYPE`	Windows log type of the error that occurred `System/Security/ Application/Directory Service/DNS Server/File Replication Service`

Legend:

--: None

(10) Details about event IDs specified in the ACTDEF parameter in the action definition file

Attribute type		Item	Attribute name	Contents
Basic attribute		Message	--	Contents of one line of log file data
Extended attribute	Common information	Event level	`SEVERITY`	Severity set in the `ACTDEF` parameter in the action definition file
		Product name	`PRODUCT_NAME`	In Windows: • `jevlogstart` command with `-p` option specified `/HITACHI/JP1/NT_LOGTRAP/`*program-name* *program-name* is the name of the source program that output the log data, as specified in the `-p` option. • `jevlogstart` command with `-p` option unspecified `/HITACHI/JP1/NT_LOGTRAP` In UNIX: • `jevlogstart` command with `-p` option specified `/HITACHI/JP1/UX_LOGTRAP/`*program-name* *program-name* is the name of the source program that output the log data, as specified in the `-p` option. • `jevlogstart` command with `-p` option unspecified `/HITACHI/JP1/UX_LOGTRAP`
		Object type	`OBJECT_TYPE`	`LOGFILE`
		Object name	`OBJECT_NAME`	Log file name set in the start command option
		Root object type	`ROOT_OBJECT_TYPE`	`LOGFILE`
		Root object name	`ROOT_OBJECT_NAME`	Log file name set in the start command option
	Program-specific information	Platform	`PLATFORM`	In Windows: `NT` In UNIX: `UNIX`

Attribute type		Item	Attribute name	Contents
		Program name	`PPNAME`	In Windows: `/HITACHI/JP1/NT_LOGTRAP` In UNIX: `/HITACHI/JP1/UX_LOGTRAP`

Legend:

--: None

(11) Details about event ID 00003FA0

Attribute type		Item	Attribute name	Contents
Basic attribute		Message	--	`KAVB2100-I [`*host-name:JP1-user-name*`] Command execution started.`
Extended attribute	Common information	Event level	`SEVERITY`	`Information`
		Product name	`PRODUCT_NAME`	`/HITACHI/JP1/IM`
		Object type	`OBJECT_TYPE`	`COMMAND`
		Object name	`OBJECT_NAME`	`JCOCMD`
		Occurrence	`OCCURRENCE`	`NOTICE`
		User name	`USER_NAME`	JP1 user who executes the command
		Start time	`START_TIME`	Time at which the request for command execution is received
	Program-specific information	Destination host	`EXECHOST`	Destination host that executes the command
		Command execution	`EXECCMD`	Execution command-name
		Environment variable file name	`EXECENV`	Environment variable file used in execution

Legend:

--: None

(12) Details about event ID 00003FA1

Attribute type		Item	Attribute name	Contents
Basic attribute		Message	--	`KAVB2101-I [`*host-name:JP-user-name*`] Command execution ended normally.`
Extended attribute	Common information	Event level	`SEVERITY`	`Information`
		Product name	`PRODUCT_NAME`	`/HITACHI/JP1/IM/JCOCMD`
		Object type	`OBJECT_TYPE`	`COMMAND`
		Object name	`OBJECT_NAME`	`JCOCMD`
		Occurrence	`OCCURRENCE`	`NOTICE`
		User name	`USER_NAME`	JP1 user who executes the command
		End time	`END_TIME`	Command end time
		Result code	`RESULT_CODE`	Return code of the command executed
	Program-specific information	Destination host	`EXECHOST`	Destination host that executes the command
		Command execution	`EXECCMD`	Command executed

Legend:

--: None

(13) Details about event ID 00003FA2

Attribute type		Item	Attribute name	Contents
Basic attribute		Message	--	`KAVB2102-E [`*host-name*`:`*JP1-user-name*`] Command execution ended abnormally.`
Extended attribute	Common information	Event level	`SEVERITY`	`Error`
		Product name	`PRODUCT_NAME`	`/HITACHI/JP1/IM/JCOCMD`
		Object type	`OBJECT_TYPE`	`COMMAND`

Attribute type		Item	Attribute name	Contents
		Object name	`OBJECT_NAME`	`JCOCMD`
		Occurrence	`OCCURRENCE`	`NOTICE`
		User name	`USER_NAME`	JP1 user who executes the command
		End time	`END_TIME`	The time when the command ended abnormally.

Legend:

--: None

(14) Details about event ID 00003FA3

Attribute type		Item	Attribute name	Contents
Basic attribute		Message	--	`KAVB2402-W [`*host-name*`] The execution time of command execution exceeded the regulation value (`*number*` sec)`
Extended attribute	Common information	Event level	`SEVERITY`	`Warning`
		Product name	`PRODUCT_NAME`	`/HITACHI/JP1/IM/JCOCMD`
		Object type	`OBJECT_TYPE`	• `COMMAND` (in the Execute Command window) • `Action` (automated action)
		Object name	`OBJECT_NAME`	`JCOCMD`
		Occurrence	`OCCURRENCE`	`NOTICE`
		User name	`USER_NAME`	JP1 user who executes the command
		Start time	`START_TIME`	Time at which the request for command execution is received
	Program-specific information	Destination host	`EXECHOST`	Destination host that executes the command
		Command execution	`EXECCMD`	Execution command name
		Request host	`REQUESTHOST`	Host that issued the command

Attribute type		Item	Attribute name	Contents
		Command ID	COMMANDID	Command ID
		Execution time	EXEC_TIME	Time when the command was executed

Legend:

--: None

(15) Details about event ID 00003FA5

Attribute type		Item	Attribute name	Contents
Basic attribute		Message	--	KAVB2071-W In *destination-host*, the number of queued commands requested from *source-host-name* has exceeded the threshold (*xx*).
Extended attribute	Common information	Event level	SEVERITY	Warning
		Product name	PRODUCT_NAME	/HITACHI/JP1/IM/JCOCMD
		Object type	OBJECT_TYPE	ACTION
		Object name	OBJECT_NAME	JCOCMD
		Occurrence	OCCURRENCE	NOTICE
		User name	USER_NAME	JP1 user who executes the command
		Start time	START_TIME	Time at which the request for command execution is received
	Program-specific information	Destination host	EXECHOST	Destination-host that executes the command
		Request host	REQUESTHOST	Host that issued the command

Legend:

--: None

(16) Details about event ID 00003FA6

Attribute type		Item	Attribute name	Contents
Basic attribute		Message	--	`KAVB2072-I In the` *target-host*`, the number of queued commands requested from the` *source-host* `has become 0.`
Extended attribute	Common information	Event level	`SEVERITY`	`Information`
		Product name	`PRODUCT_NAME`	`/HITACHI/JP1/IM/JCOCMD`
		Object type	`OBJECT_TYPE`	`ACTION`
		Object name	`OBJECT_NAME`	`JCOCMD`
		Occurrence	`OCCURRENCE`	`NOTICE`
		User name	`USER_NAME`	JP1 user who executes the command
		Start time	`START_TIME`	Time at which the request for command execution is received
	Program-specific information	Destination host	`EXECHOST`	Destination host that executes the command
		Request host	`REQUESTHOST`	Host that issued the command

Legend:

--: None

(17) Details about event ID 00004700

Attribute type	Item	Attribute name	Contents
Basic attribute	Event ID	--	00004700
	Message	--	`KAVA1524-W` *connection-sequence*`:` *authentication-server-name* `was successfully blocked.`

Attribute type		Item	Attribute name	Contents
Extended attribute	Common information	Event level	`SEVERITY`	`Warning`
		Product name	`PRODUCT_NAME`	`/HITACHI/JP1/BASE/JBSSESS`
		Object type	`OBJECT_TYPE`	`SESSION`
		Object name	`OBJECT_NAME`	Name of the host that has blocked the authentication server
		Occurrence	`OCCURRENCE`	`NOTICE`
	Program-specific information	Target host name for failed connection	`AUTHSRV_NAME`	Name of the authentication server which has been blocked

Legend:

--: None

(18) Details about event ID 00004701

Attribute type		Item	Attribute name	Contents
Basic attribute		Event ID	--	00004701
		Message	--	`KAVA1525-I` *connection-sequence*`:` *authentication-server-name* `was successfully unblocked.`
Extended attribute	Common information	Event level	`SEVERITY`	`Information`
		Product name	`PRODUCT_NAME`	`/HITACHI/JP1/BASE/JBSSESS`
		Object type	`OBJECT_TYPE`	`SESSION`
		Object name	`OBJECT_NAME`	Name of the host that unblocked the authentication server
		Occurrence	`OCCURRENCE`	`NOTICE`
	Program-specific information	Target host name for failed connection	`AUTHSRV_NAME`	Name of the authentication server which has been unblocked

Legend:

--: None

(19) Details about event ID 00004702

Attribute type		Item	Attribute name	Contents
Basic attribute		Event ID	--	00004702
		Message	--	`KAVA1396-E All authentication servers were blocked.`
Extended attribute	Common information	Event level	`SEVERITY`	`Error`
		Product name	`PRODUCT_NAME`	`/HITACHI/JP1/BASE/JBSSESS`
		Object type	`OBJECT_TYPE`	`SESSION`
		Object name	`OBJECT_NAME`	Name of the host which has blocked connection to all authentication servers
		Occurrence	`OCCURRENCE`	`NOTICE`

Legend:

--: None

(20) Details about event ID 00004720

Attribute type		Item	Attribute name	Contents
Basic attribute		Event ID	--	00004720
		Message	--	`KAVB3737-E The` *component-name management-target-process-name* `terminated abnormally.`
Extended attribute	Common information	Event level	`SEVERITY`	`Error`
		Product name	`PRODUCT_NAME`	`/HITACHI/JP1/BASE/SPMD`
		Object type	`OBJECT_TYPE`	`SPMD`
		Object name	`OBJECT_NAME`	Name of the abnormally ended process
		Occurrence	`OCCURRENCE`	`NOTICE`

Legend:

--: None

(21) Details about event ID 00004721

Attribute type		Item	Attribute name	Contents
Basic attribute		Event ID	--	00004721
		Message	--	`KAVB3613-W` *component-name* `timeout occurred in` *management-target-process-name*`. Processing continues.`
Extended attribute	Common information	Event level	`SEVERITY`	`Warning`
		Product name	`PRODUCT_NAME`	`/HITACHI/JP1/BASE/SPMD`
		Object type	`OBJECT_TYPE`	`SPMD`
		Object name	`OBJECT_NAME`	Name of the process for which an attempt to start it resulted in a timeout
		Occurrence	`OCCURRENCE`	`NOTICE`

Legend:

--: None

(22) Details about event ID 00004722

Attribute type		Item	Attribute name	Contents
Basic attribute		Event ID	--	00004722
		Message	--	`KAVB3616-I Restart of the` *component-name management-target-process-name* `has finished.`
Extended attribute	Common information	Event level	`SEVERITY`	`Information`
		Product name	`PRODUCT_NAME`	`/HITACHI/JP1/BASE/SPMD`
		Object type	`OBJECT_TYPE`	`SPMD`
		Object name	`OBJECT_NAME`	Name of the restarted process
		Occurrence	`OCCURRENCE`	`NOTICE`

Legend:

--: None

(23) Details about event ID 00004740

Attribute type		Item	Attribute name	Contents
Basic attribute		Event ID	--	00004740
		Message	--	`KAVA7017-E` *function-name* `ended abnormally. (host name =` *host-name*`, process name =` *process-name*`, internal function name =` *internal-function-name*`, pid =` *process-ID*`, tid =` *thread-ID*`)`
Extended attribute	Common information	Event level	`SEVERITY`	`Error`
		Product name	`PRODUCT_NAME`	`/HITACHI/JP1/BASE/JBSHC`
		Object type	`OBJECT_TYPE`	`JBSHC`
		Object name	`OBJECT_NAME`	Name of the function that ended abnormally
		Occurrence	`OCCURRENCE`	`NOTICE`
	Program-specific information	Host name	`HOST_NAME`	Host name
		Process name	`PROCESS_NAME`	Process name
		Internal function name	`SFUNCTION_NAME`	Internal function name
		Process ID	`PROCESS_ID`	Process ID
		Thread ID	`THREAD_ID`	Thread ID

Legend:

--: None

(24) Details about event ID 00004741

Attribute type	Item	Attribute name	Contents
Basic attribute	Event ID	--	00004741
	Message	--	`KAVA7014-E` *function-name* `has been processing for nn seconds. (host name =` *host-name*`, process name =` *process-name*`, internal function name =` *internal-function-name*`, pid =` *process-ID*`, tid =` *thread-ID*`)`

Attribute type		Item	Attribute name	Contents
Extended attribute	Common information	Event level	`SEVERITY`	`Error`
		Product name	`PRODUCT_NAME`	`/HITACHI/JP1/BASE/JBSHC`
		Object type	`OBJECT_TYPE`	`JBSHC`
		Object name	`OBJECT_NAME`	Function name
		Occurrence	`OCCURRENCE`	`NOTICE`
	Program-specific information	Host name	`HOST_NAME`	Host name
		Process name	`PROCESS_NAME`	Process name
		Internal function name	`SFUNCTION_NAME`	Internal function name
		Process ID	`PROCESS_ID`	Process ID
		Thread ID	`THREAD_ID`	Thread ID

Legend:

--: None

(25) Details about event ID 00004742

Attribute type	Item	Attribute name	Contents
Basic attribute	Event ID	--	00004742
	Message	--	`KAVA7013-W` *function-name* `has been processing for nn seconds. After passes of mm seconds, becomes error condition. (host name =` *host-name*`, process name =` *process-name*`, internal function name =` *internal-function-name*`, pid =` *process-ID*`, tid =` *thread-ID*`)`

Attribute type		Item	Attribute name	Contents
Extended attribute	Common information	Event level	`SEVERITY`	`Warning`
		Product name	`PRODUCT_NAME`	`/HITACHI/JP1/BASE/JBSHC`
		Object type	`OBJECT_TYPE`	`JBSHC`
		Object name	`OBJECT_NAME`	Function name
		Occurrence	`OCCURRENCE`	`NOTICE`
	Program-specific information	Host name	`HOST_NAME`	Host name
		Process name	`PROCESS_NAME`	Process name
		Internal function name	`SFUNCTION_NAME`	Internal function name
		Process ID	`PROCESS_ID`	Process ID
		Thread ID	`THREAD_ID`	Thread ID

Legend:

--: None

(26) Details about event ID 00004743

Attribute type	Item	Attribute name	Contents
Basic attribute	Event ID	--	00004743
	Message	--	`KAVA7016-I` *function-name* `has a normal status. (host name =` *host-name*`, process name =` *process-name*`, internal function name =` *internal-function-name*`, pid =` *process-ID*`, tid =` *thread-ID*`)`

Attribute type		Item	Attribute name	Contents
Extended attribute	Common information	Event level	`SEVERITY`	`Information`
		Product name	`PRODUCT_NAME`	`/HITACHI/JP1/BASE/JBSHC`
		Object type	`OBJECT_TYPE`	`JBSHC`
		Object name	`OBJECT_NAME`	Function name
		Occurrence	`OCCURRENCE`	`NOTICE`
	Program-specific information	Host name	`HOST_NAME`	Host name
		Process name	`PROCESS_NAME`	Process name
		Internal function name	`SFUNCTION_NAME`	Internal function name
		Process ID	`PROCESS_ID`	Process ID
		Thread ID	`THREAD_ID`	Thread ID

Legend:

--: None

(27) Details about event ID 00004747

Attribute type		Item	Attribute name	Contents
Basic attribute		Event ID	--	00004747
		Message	--	`KAVA7003-E The health check function stopped because an error occurred. (host name=`*host-name*`)`
Extended attribute	Common information	Event level	`SEVERITY`	`Error`
		Product name	`PRODUCT_NAME`	`/HITACHI/JP1/BASE/JBSHC`
		Object type	`OBJECT_TYPE`	`JBSHC`
		Object name	`OBJECT_NAME`	Host name
		Occurrence	`OCCURRENCE`	`NOTICE`

Legend:

--: None

(28) Details about event ID 00004748

Attribute type		Item	Attribute name	Contents
Basic attribute		Event ID	--	00004748
		Message	--	`KAVA7222-E Monitoring notification cannot be performed at` *host-name* `because` *service-name* `is not functioning.`
Extended attribute	Common information	Event level	`SEVERITY`	`Error`
		Product name	`PRODUCT_NAME`	`/HITACHI/JP1/BASE/JBSHC`
		Object type	`OBJECT_TYPE`	`JBSHC`
		Object name	`OBJECT_NAME`	Host name
		Occurrence	`OCCURRENCE`	`NOTICE`
	Program-specific information	Service name	`SERVICE_NAME`	Service name

Legend:

--: None

(29) Details about event ID 00004749

Attribute type		Item	Attribute name	Contents
Basic attribute		Event ID	--	00004749
		Message	--	`KAVA7223-E Monitoring cannot be performed because a connection with` *host-name* `cannot be established.`
Extended attribute	Common information	Event level	`SEVERITY`	`Error`
		Product name	`PRODUCT_NAME`	`/HITACHI/JP1/BASE/JBSHC`
		Object type	`OBJECT_TYPE`	`JBSHC`
		Object name	`OBJECT_NAME`	Host name
		Occurrence	`OCCURRENCE`	`NOTICE`

Legend:

--: None

(30) Details about event ID 0000474A

Attribute type		Item	Attribute name	Contents
Basic attribute		Event ID	--	0000474A
		Message	--	`KAVA7224-I` *host-name* `can now be monitored.`
Extended attribute	Common information	Event level	`SEVERITY`	`Information`
		Product name	`PRODUCT_NAME`	`/HITACHI/JP1/BASE/JBSHC`
		Object type	`OBJECT_TYPE`	`JBSHC`
		Object name	`OBJECT_NAME`	Host name
		Occurrence	`OCCURRENCE`	`NOTICE`

Legend:

--: None

(31) Details about event ID 0000474B

Attribute type	Item	Attribute name	Contents
Basic attribute	Event ID	--	0000474B
	Message	--	`KAVA7030-E The shared memory is locked. (host name =` *host-name*`, process name =` *process-name*`, internal function name =` *internal-function-name*`, pid =` *process-ID*`, tid =` *thread-ID*`)`

Attribute type		Item	Attribute name	Contents
Extended attribute	Common information	Event level	`SEVERITY`	`Error`
		Product name	`PRODUCT_NAME`	`/HITACHI/JP1/BASE/JBSHC`
		Object type	`OBJECT_TYPE`	`JBSHC`
		Object name	`OBJECT_NAME`	Function name
		Occurrence	`OCCURRENCE`	`NOTICE`
	Program-specific information	Host name	`HOST_NAME`	Host name
		Process name	`PROCESS_NAME`	Process name
		Internal function name	`SFUNCTION_NAME`	Internal function name
		Process ID	`PROCESS_ID`	Process ID
		Thread-ID	`THREAD_ID`	Thread ID

Legend:

--: None

(32) Details about event ID 00002102

Attribute type	Item	Attribute name	Contents
Basic attribute	Message	--	--
	Detailed information	--	--

Legend:

--: None

(33) Details about event ID 00002103

Attribute type	Item	Attribute name	Contents
Basic attribute	Message	--	--
	Detailed information	--	--

Legend:

--: None

(34) Details about event ID 00002104

Attribute type	Item	Attribute name	Contents
Basic attribute	Message	--	Function name of the process
	Detailed information	--	--

Legend:

--: None

(35) Details about event ID 00010B7F

Attribute type	Item	Attribute name	Contents
Basic attribute	Message	--	--
	Detailed information	--	--

Legend:

--: None

(36) Details about event ID 00004780

Attribute type	Item	Attribute name	Contents
Basic attribute	Event ID	--	00004780
	Message	--	`KNAM3203-I An action execution start request was accepted. (actno=`*action-number*`, actnm=`*action-name*`, host=`*execution-host-name*`, eventid=`*event-ID*`, eventseq=`*serial-number*`)`

Attribute type		Item	Attribute name	Contents
Extended attribute	Common information	Event level	`SEVERITY`	`Information`
		Product name	`PRODUCT_NAME`	`/HITACHI/JP1/BASE/LOCAL_ACTION`
		Object type	`OBJECT_TYPE`	`ACTION`
		Object name	`OBJECT_NAME`	`LOCAL ACTION`
		Object ID	`OBJECT_ID`	Action name
		User name	`USER_NAME`	JP1 user name
		Start time	`START_TIME`	Start time of action execution
		Occurrence	`OCCURRENCE`	`NOTICE`
	Program-specific information	Action event serial number	`ACT_EVENT_SEQ`	JP1 event serial number that initiated the action
		Action event ID	`ACT_EVENT_ID`	JP1 event ID that initiated the action
		Environment variable file name	`EXECENV`	Environment-variable file used for execution#
		Command execution	`EXECCMD`	Execution command name (after the attribute variable expanded)

Legend:

--: None

#: A null character is used if not executed.

(37) Details about event ID 00004781

Attribute type	Item	Attribute name	Contents
Basic attribute	Event ID	--	00004781
	Message	--	`KNAM3210-I An action has completed. (actno=`*action-number*`, actnm=`*action-name* `host=`*execution-host-name*`, JP1 user=`*JP1-user-name*`, OS user=`*OS-user-name*`, proc-ID=`*process-ID*`, code=`*command-result-code*`)`

Attribute type		Item	Attribute name	Contents
Extended attribute	Common information	Event level	SEVERITY	Information
		Product name	PRODUCT_NAME	/HITACHI/JP1/BASE/ LOCAL_ACTION
		Object type	OBJECT_TYPE	ACTION
		Object name	OBJECT_NAME	LOCAL ACTION
		Object ID	OBJECT_ID	Action name
		User name	USER_NAME	JP1 user name
		Start time	START_TIME	Start time of action execution
		End time	END_TIME	End time of action execution
		Result code	RESULT_CODE	End code of the command that has been executed by the action.
		Occurrence	OCCURRENCE	NOTICE
	Program-specific information	Action event serial number	ACT_EVENT_SEQ	JP1 event serial number that initiated the action
		Action event ID	ACT_EVENT_ID	JP1 event ID that initiated the action
		Process ID	EXEC_PID	Process ID/thread ID being executed#
		OS-user-name	EXEC_USER	Executed OS user name#
		Environment variable file name	EXECENV	Environment variable file used for execution#
		Command execution	EXECCMD	Execution command name (after the attribute variable expands)

Legend:

--: None

#: A null character is used if not executed.

(38) Details about event ID 00004782

Attribute type		Item	Attribute name	Contents
Basic attribute		Event ID	--	00004782
		Message	--	`KNAM3211-E An action ended without being executed. (actno=`*action-number*`, actnm=`*action-name*`, host=`*execution-host-name*`, JP1 user=`*JP1-user-name*`, OS user=`*OS-user-name*`, proc-ID=`*Process-ID*`, cmd=`*command-line*`)`
Extended attribute	Common information	Event level	`SEVERITY`	`Error`
		Product name	`PRODUCT_NAME`	`/HITACHI/JP1/BASE/LOCAL_ACTION`
		Object type	`OBJECT_TYPE`	`ACTION`
		Object name	`OBJECT_NAME`	`LOCAL ACTION`
		Object ID	`OBJECT_ID`	Action name
		User name	`USER_NAME`	JP1 user name
		Start time	`START_TIME`	Start time of action execution
		End time	`END_TIME`	End time of action execution
		Occurrence	`OCCURRENCE`	`NOTICE`
	Program-specific information	Action event serial number	`ACT_EVENT_SEQ`	JP1 event serial number that initiated the action
		Action event ID	`ACT_EVENT_ID`	JP1 event ID that initiated the action
		Process ID	`EXEC_PID`	Process ID/thread ID being executed#
		OS-user-name	`EXEC_USER`	Executed OS user name#
		Environment variable file name	`EXECENV`	Environment variable file used for execution#
		Command execution	`EXECCMD`	Execution command name (after the attribute variable expanded)
		Error code	`ERR_CODE`	Error number of the cause of execution failure

Legend:

--: None

#: A null character is used if the attribute is not used or is undefined.

(39) Details about event ID 00004783

Attribute type		Item	Attribute name	Contents
Basic attribute		Event ID	--	00004783
		Message	--	`KNAM3212-W An action ended because it was cancelled. (actno=`*action-number*`, actnm=`*action-name*`, host=`*execution-host-name*`, JP1 user=`*JP1-user-name*`, OS user=`*OS-user-name*`, proc-ID=`*Process-ID*`, cmd=`*command-line*`)`
Extended attribute	Common information	Event level	`SEVERITY`	`Warning`
		Product name	`PRODUCT_NAME`	`/HITACHI/JP1/BASE/LOCAL_ACTION`
		Object type	`OBJECT_TYPE`	`ACTION`
		Object name	`OBJECT_NAME`	`LOCAL ACTION`
		Object ID	`OBJECT_ID`	Action name
		User name	`USER_NAME`	JP1 user name
		Start time	`START_TIME`	Start time of action execution
		End time	`END_TIME`	End time of action execution
		Occurrence	`OCCURRENCE`	`NOTICE`

Attribute type		Item	Attribute name	Contents
	Program-specific information	Action event serial number	`ACT_EVENT_SEQ`	JP1 event serial number that initiated the action
		Action event ID	`ACT_EVENT_ID`	JP1 event ID that initiated the action
		Process ID	`EXEC_PID`	Process ID/thread ID being executed#
		OS-user-name	`EXEC_USER`	Executed OS- user name#
		Environment variable file name	`EXECENV`	Environment variable file used for execution#
		Command execution	`EXECCMD`	Execution command name (after the attribute variable expanded)

Legend:

--: None

#: A null character is used if the attribute is not used or is undefined.

Chapter

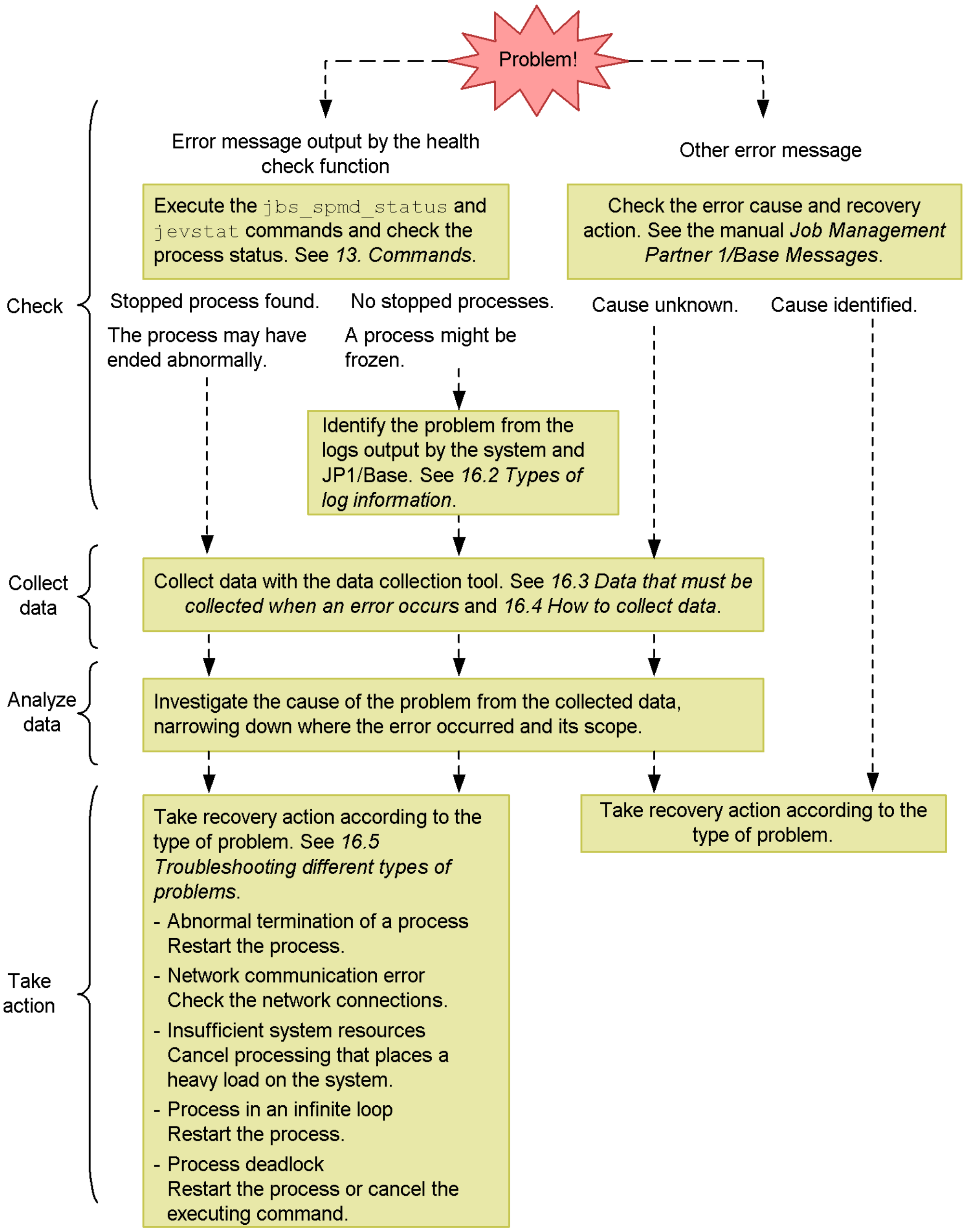
16. Troubleshooting

This chapter explains the type of problems that might occur in JP1/Base and how to recover from such problems.

16.1 Troubleshooting procedure

The figure below shows the recovery procedure if a problem occurs in JP1/Base.

Figure 16-1: Recovery procedure when a problem occurs


Problem!
Error message output by the health check function
Other error message
Check
Execute the jbs_spmd_status and jevstat commands and check the process status. See *13. Commands*.
Check the error cause and recovery action. See the manual *Job Management Partner 1/Base Messages*.
Stopped process found.
The process may have ended abnormally.
No stopped processes.
A process might be frozen.
Cause unknown.
Cause identified.
Identify the problem from the logs output by the system and JP1/Base. See *16.2 Types of log information*.
Collect data
Collect data with the data collection tool. See *16.3 Data that must be collected when an error occurs* and *16.4 How to collect data*.
Analyze data
Investigate the cause of the problem from the collected data, narrowing down where the error occurred and its scope.
Take action
Take recovery action according to the type of problem. See *16.5 Troubleshooting different types of problems*.
- Abnormal termination of a process
Restart the process.
- Network communication error
Check the network connections.
- Insufficient system resources
Cancel processing that places a heavy load on the system.
- Process in an infinite loop
Restart the process.
- Process deadlock
Restart the process or cancel the executing command.
Take recovery action according to the type of problem.

16.2 Types of log information

The following four types of log information are output when JP1/Base is used:

- Common message log information
- Integrated trace log
- Log information of each process
- Operation log

This section explains these types of log information.

16.2.1 Common message log information

The common message log information reports the errors in the system for system administrators. This log information reports the minimum information about an error.

The common message log information is output to syslog for UNIX and to the Windows event log for Windows.

16.2.2 Integrated trace log information

The integrated trace log is created using Hitachi Network Objectplaza Trace Library (HNTRLib2) by collecting the trace information output by each program into a single output destination file. The integrated trace log contains messages with data that is more detailed than the data in the common message log information.

The default destination for the integrated trace log is as follows:

In Windows:

system-drive`\Program Files\Hitachi\HNTRLib2\spool\hntr2{1|2|3|4}.log`

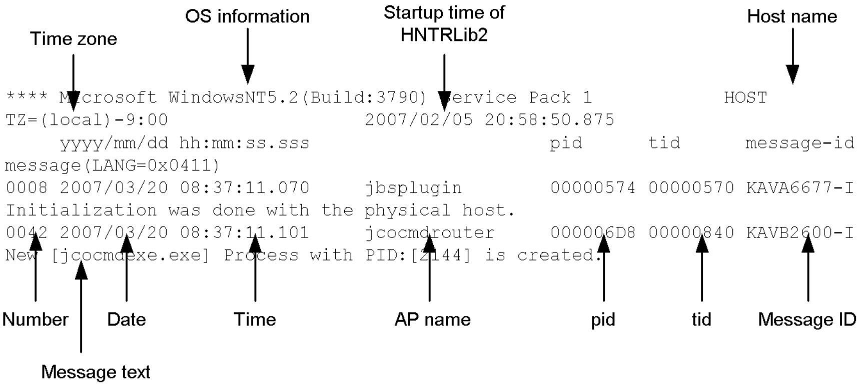
In UNIX:

```
/var/opt/hitachi/HNTRLib2/spool/hntr2{1|2|3|4}.log
```

You can use either the `hntr2util`, `hntr2conf`, or `hntr2getconf` command to view or change the log file destination or size. For details, see *hntr2util (Windows only)*, *hntr2util (UNIX only)*, *hntr2conf*, or *hntr2getconf*in *13 Commands*.

You can use a text editor to view the integrated trace log file. The following figure shows an example of the integrated trace log.

Figure 16-2: Output example of integrated trace log file



```
**** Microsoft WindowsNT5.2(Build:3790) Service Pack 1           HOST
TZ=(local)-9:00                   2007/02/05 20:58:50.875
     yyyy/mm/dd hh:mm:ss.sss                         pid      tid      message-id
message(LANG=0x0411)
0008 2007/03/20 08:37:11.070     jbsplugin         00000574 00000570 KAVA6677-I
Initialization was done with the physical host.
0042 2007/03/20 08:37:11.101     jcocmdrouter      000006D8 00000840 KAVB2600-I
New [jcocmdexe.exe] Process with PID:[2144] is created.
```

The following tables describe headers and items output to the integrated trace log file.

Table 16-1: Headers for the integrated trace log file

Header	Description
OS information	Information on the OS on which Hitachi Network Objectplaza Trace Library (HNTRLib2) is running
host-name	Name of the host on which Hitachi Network Objectplaza Trace Library (HNTRLib2) is running
Time zone	In Windows: OS time zone In UNIX: Value of the environment variable `TZ` for the integrated trace process If the environment variable `TZ` is not set, `Unknown` is displayed.
Start time of Hitachi Network Objectplaza Trace Library (HNTRLib2)	Time at which Hitachi Network Objectplaza Trace Library (HNTRLib2) started

Table 16-2: Output items for the integrated trace log file

Output item	Description
Number (4 digits)	Trace record sequence number. Records are individually numbered for each process that outputs log information.
Date (10 bytes)	Trace acquisition date: *yyyy*/*mm*/*dd* (year/month/day)

Output item	Description
Time (12 bytes)	Trace acquisition time (local time): *hh*:*mm*:*ss*.*sss* (hour: minute: second. millisecond)
AP name (maximum of 16 bytes)	Application identification name. • Process management `JBS_SPMD` • Startup control `JP1ControlSvc` • Authentication access control `jp1BsSess` • Operation access control `jp1BsAcl` • Authentication server `jbssessionmgr` • Configuration management `jbsroute` • Command execution (control process) `jcocmdrouter` • Command execution (Inter-JP1/Base communication process) `jcocmdcom` • Command execution (JP1/IM-M-JP1/Base communication process) `jcocmdapi` • Command execution (execution control process) `jcocmdexe` • Command execution (execution process) `jcocmdcmc` • Plug-in service `jbsplugin` • Plug-in (manager command) `jbsrmtcmd` • Plug-in (agent command) `plAdapter_Event` • Health check (for local host monitoring) `jbshcd` • Health check (for other host monitoring) `jbshchostd`

Output item	Description

	• Event service
	`jevservice`
	• JP1/AJS-compatible process
	`jevsessvc`
	• Log file trap (Windows)
	`jevtraplog`
	• Log file trap (UNIX)
	`jevlogd`
	• Event log trap
	`jevtrapevt`
	• SNMP trap converter
	`jp1co_evtgw`
	• Other command names
	Command name

pid	Process ID. Process ID assigned by the OS.
tid	Thread ID. ID used to differentiate threads.
Message ID	Message ID described in the message output format. Message ID used for this product.
Message text	Message text output to the integrated trace log. Message text output by this product.

Note:

The log time is output to the integrated trace log. The output log time is in a time zone format used by the output process.

For this reason, if you have changed the value of the environment variable `TZ` before you start a service or execute a command, a time value different from the value of the time zone set on the OS might be output.

16.2.3 Log information of each process

The log of each process contains information that is output by the functionality of JP1/Base. Each function outputs information to a different log file. For details on the log files, see *16.2.5 Log files and directories*.

16.2.4 Operation log

The operation log provides a history of output log information about what operation was performed on the authentication server, and when and who performed it. For details on the operation log, see *K. Operation Log Output*.

16.2.5 Log files and directories

(1) In Windows

For details on the type of log information output by JP1/Base for Windows and the list of default log files, see *A.1(2) List of log files (in Windows)*.

(2) In UNIX

For details on the type of log information output by JP1/Base for UNIX and the list of default log files, see *A.2(2) List of log files (in UNIX)*.

16.3 Data that must be collected when an error occurs

This section describes the data you need to collect when an error occurs. JP1/Base provides a *data collection tool* for collecting the required data. The data collection tool is provided as a batch file (`jbs_log.bat`) for Windows, and as a shell script (`jbs_log.sh`) for UNIX. For details on the data collection tool, see *jbs_log.bat (Windows only)* and *jbs_log.sh (UNIX only)* in *13. Commands*.

In the following tables, the data that can be collected using the initial settings of the data collection tool is indicated as such.

16.3.1 In Windows

(1) OS system information

You need to collect the following log information about the OS. You can use the data collection tool to collect this information.

Type of information	Required data	File name#1
Date and time collected	Execution result of `date /t` Execution result of `time /t`	`date.log`
Windows event log	Application log: *system-folder*`\system32\config\AppEvent.Evt` System log: *system-folder*`\system32\config\SysEvent.Evt`	• `SysEvent(Backup).evt` • `AppEvent(Backup).evt`
Host names set on the machine	*system-folder*`\system32\drivers\etc\hosts`	`hosts`
Service ports set on the machine	*system-folder*`\system32\drivers\etc\services`	`services`
NICs installed	Execution result of `ipconfig /all`	`ipconfig.log`
List of services started	Execution result of `net start`	`netstart.log`
Machine environment variable	Execution result of `set`	`set.log`
Dr. Watson log file#2	*user-specified-folder*`\drwtsn32.log`	`drwtsn32.log`
Crash dump#2	*user-specified-folder*`\user.dmp`	`user.dmp`
Machine system information	Execution result of `msinfo32 /report` *file-name*	`msinfo32.log`

#1: Name of the file under which the information collected by the data collection tool is stored.

#2: Output only if specified in advance. For details on the setting, see *2.4.2(6) Preparing to collect information when a problem occurs (Windows only)*.

(2) JP1/Base information

You need to collect the following information about JP1/Base. You can use the data collection tool to collect this information. If a problem occurs while the machine is connected to the network, you also need to collect the files on the remote machine.

Type of informatio n	Required data	File name#1
Environment settings	All files in *installation-folder*`\conf`	Same as the name of the file from which the data is collected.
	All files in *installation-folder*`\conf\default\`	Same as the name of the file from which the data is collected.
	All files in *installation-folder*`\plugin\conf\`	Same as the name of the file from which the data is collected.
	All files in *shared-folder*`\jp1base\conf`#2	Same as the name of the file from which the data is collected.
Common definition information	Execution result of `jbsgetcnf` command	File specified in the `jbsgetcnf` command
	Execution result of `jbsgetcnf -h` *logical-host-name*#2	
Log information	All files in *installation-folder*`\log\`	Same as the name of the file from which the data is collected.
	All files in *shared-folder*`\jp1base\log\`#2	Same as the name of the file from which the data is collected.
	All files in `%ALLUSERSPROFILE%\Hitachi\jp1\jp1_default\JP1Base\log\`#4, #5	Same as the name of the file from which the data is collected.
	All files in `%ALLUSERSPROFILE%\Hitachi\jp1\`*logical-host-name*`\JP1Base\log\`#4, #5	Same as the name of the file from which the data is collected.

Type of informatio n	Required data	File name#1
Log of installation	*Windows-installation-folder*`\Temp\HITACHI_JP1_INST_LOG\jp1base_inst{1|2|3|4|5}.log`	Same as the name of the file from which the data is collected.
Service operating information	All files in *installation-folder*`\sys\OPI\`	Same as the name of the file from which the data is collected.
	All files in *shared-folder*`\jp1base\sys\OPI\`	Same as the name of the file from which the data is collected.
Event service settings	All files in *installation-folder*`\sys\tmp\event\`	Same as the name of the file from which the data is collected.
	All files in *shared-folder*`\jp1base\event\`#2	Same as the name of the file from which the data is collected.
Event database	All files in *installation-folder*`\sys\event\`#3	Same as the name of the file from which the data is collected.
	All files in *shared-folder*`\jp1base\event\`#2, #3	Same as the name of the file from which the data is collected.
Command execution log	All files in *installation-folder*`\log\COMMAND`#3	Same as the name of the file from which the data is collected.
	All files in *shared-folder*`\jp1base\log\Command\`#2, #3	Same as the name of the file from which the data is collected.
Integrated trace log	*system-drive*`\Program Files\Hitachi\HNTRLib2\spool\hntr2*.log`	Same as the name of the file from which the data is collected.
ISAM maintenance information	Execution result of `Jischk` command#6 Physical host specified: *installation-folder*`\log\Command\*` Logical host specified: *shared-folder*`\jp1base\log\Command\*`	`isamchk.log`
File list	Execution result of `dir /s` *installation-folder*	`dir_jp1base.log`
	Execution result of `dir /s` *shared-folder*`\jp1base`	`dir_jp1base.log`

Type of information	Required data	File name#1
Version information	*system-drive*\Program Files \InstallShield Installation Information \{F8C71F7C-E5DE-11D3-A21E-006097C00EBC}\setup.ilg , setup.ini	base_setup.ilg, base_setup.ini
Patch log	*installation-folder*\Patchlog.txt	Patchlog_jp1base.txt
JP1/Base binding status	Execution result of netstat -na	netstat.log
Host name for resolving the network address	Execution result of jbsgethostbyname	jbsgethostbyname.log
Access permissions for folders	Execution result of *cacls-installation-folder*	cacls_jp1base.log
	Execution result of *cacls-shared-folder*\jp1base	
	Execution result of *cacls-installation-folder*\log	cacls_jp1base_log.log
	Execution result of *cacls-shared-folder*\jp1base\log	
	Execution result of *cacls-installation-folder*\log\COMMAND	cacls_jp1base_log_COMMAND.log
	Execution result of *cacls-shared-folder*\jp1base\log\COMMAND	
	Execution result of *cacls-installation-folder*\sys	cacls_jp1base_sys.log
	Execution result of *cacls-installation-folder*\sys\event	cacls_jp1base_sys_event.log
	Execution result of *cacls-installation-folder*\sys\event\servers	cacls_jp1base_sys_event_servers.log
	Execution result of *cacls-installation-folder*\sys\event\servers\default	cacls_jp1base_sys_event_servers_default.log
	Execution result of *cacls-shared-folder*\jp1base\event	cacls_jp1base_event.log
Hitachi Integrated Installer log files	All files in *Windows-installation-folder*\Temp\HCDINST\	Copies of the files that are shown in the left column

Note: When you specify a different path in the event server index file (`index`), or change the destination for the integrated trace log, directly collect information from either the specified path or the changed destination.

#1: Name of the file under which the information collected by the data collection tool is stored.

#2: Output when data about the logical host (cluster environment) is collected.

#3: Extra disk space might be required to collect large files of data from the event database and command execution log. Make sure that you check the file size before you collect data.

#4: The value set in the environment variable `%ALLUSERSPROFILE%` at installation is used.

#5: For Windows Vista or Windows Server 2008.

#6: For OSs other than Windows Vista and Windows Server 2008.

(3) JP1/Base processes

Use the Windows task manager to check the operation status of processes.

(4) Operation data

If an error occurs, you need to collect the following operational information:

- Details of the operation
- Time the error occurred
- Machine configuration (version of each OS, host name, configuration of JP1/IM - Manager)
- Whether the error occurs repeatedly under the same conditions
- User name used to log in from JP1/IM - View

(5) Error information on the screen

Collect hard copies of the following:

- The error dialog boxes (In addition, copy the contents of the details if the dialog box contains a **Details** button.)

(6) Collecting user dumps (for Windows Vista and Windows Server 2008)

If an application error causes the JP1/Base process to stop, collect the user dumps.

(7) Collecting problem reports (for Windows Vista and Windows Server 2008)

If an application error causes the JP1/Base process to stop, collect the problem reports.

16.3.2 In UNIX

(1) OS system information

You need to collect the following log information about the OS. You can use the data collection tool to collect this information.

Type of information	Required data	File name#1
Date and time collected	Execution result of date	jp1_default_base_1st.tar.Z, date.log
System log (syslog)	/var/adm/syslog/syslog.log (HP-UX)#2 /var/adm/messages (Solaris)#2 /var/adm/messages (AIX)#2	jp1_default_base_1st.tar.Z, syslog.log
Host names set on the machine	/etc/hosts	jp1_default_base_1st.tar.Z, hosts
Service ports set on the machine	/etc/services	jp1_default_base_1st.tar.Z, services
List of users registered on the machine	/etc/passwd	jp1_default_base_1st.tar.Z, passwd
NICs installed	Execution result of netstat -in	jp1_default_base_1st.tar.Z, netstat_in.log
List of processes	Execution result of ps -elfa	jp1_default_base_1st.tar.Z, ps.log
Machine environment variable	Execution result of env	jp1_default_base_1st.tar.Z, env.log
Kernel parameter information	HP-UX: Execution result of sysdef /usr/sbin/kmtune Execution result of ulimit -a Solaris: Execution result of /usr/sbin/sysdef -i Execution result of ulimit -a AIX: Execution result of lsattr -E -l sys0 Execution result of ulimit -a /etc/security/limits	jp1_default_base_1st.tar.Z HP-UX: sysdef.log kmtune.log ulimit.log Solaris: sysdef.log ulimit.log AIX: lsatt.log ulimit.log limits

Type of information	Required data	File name#1
Page size information	Execution result of dmesg (HP-UX) Execution result of pagesize (Solaris and AIX)	jp1_default_base_1st.tar.Z, pagesize.log
Shared memory information	Execution result of ipcs -a	jp1_default_base_1st.tar.Z, ipcs.log
Memory information	Execution result of swapinfo -t (HP-UX) Execution result of swap -l (Solaris) Execution result of lsps -s (AIX)	jp1_default_base_1st.tar.Z, swapinfo.log
Disk information	Execution result of bdf (HP-UX) Execution result of df -k (OS other than HP-UX)	jp1_default_base_1st.tar.Z, df.log
System diagnostics	Execution result of /etc/dmesg (HP-UX) Execution result of /usr/sbin/dmesg (Solaris) Execution result of /usr/bin/alog -o -t boot (AIX)	jp1_default_base_1st.tar.Z, sys_info.log
OS patches implemented	HP-UX: /usr/sbin/swlist -l product /usr/sbin/swlist /usr/sbin/swlist -l fileset -a patch_state *.*,c=patch Solaris: showrev -a AIX: lslpp -l -a /usr/bin/instfix -a -icv	jp1_default_base_1st.tar.Z, patch_info.log
OS version information	Execution result of uname -a	jp1_default_base_1st.tar.Z, uname_a.log
Installed Hitachi products	/etc/.hitachi/pplistd/pplistd	jp1_default_base_1st.tar.Z, pplistd
Host name for resolving the network address	Execution result of jbsgethostbyname	jp1_default_base_1st.tar.Z, jbsgethostbyname.log
Name service settings file	/etc/nsswitch.conf	jp1_default_base_1st.tar.Z, nsswitch.conf
DNS server settings file	/etc/resolv.conf	jp1_default_base_1st.tar.Z, resolv.conf

Type of information	Required data	File name[#1]
Network interface settings	Execution result of `ifconfig -a`	`jp1_default_base_1st.tar.Z`, `ifconfig.log`

#1: Names of the compressed file and expanded file after execution of the data collection tool (listed in that order).

#2: The name of a `syslog` file might be different from the default file name.

(2) JP1/Base information

You need to collect the following information about JP1/Base. You can use the data collection tool to collect this information. If a problem occurs while the machine is connected to the network, you also need to collect the files on the remote machine.

Type of information	Default file name	File name
Environment settings	All files in `/etc/opt/jp1base/conf/`	`jp1_default_base_1st.tar.Z`, same as the name of the file from which data is collected
	All files in `/etc/opt/jp1base/default/`	`jp1_default_base_1st.tar.Z`, same as the name of the file from which data is collected
	All files in `/opt/jp1base/plugin/conf/`	`jp1_default_base_1st.tar.Z`, same as the name of the file from which data is collected
	All files in *shared-directory*`/jp1base/conf`[#1]	*logical-host-name*`_1st.tar.Z`, same as the name of the file from which data is collected
Common definition information	`/opt/jp1/hcclibcnf/` (can also be checked from the `jbsgetcnf` command execution result)	`jp1_default_base_1st.tar.Z`, same as the name of the file from which data is collected
	All files in `/etc/opt/jp1base/default/`	`jp1_default_base_1st.tar.Z`, same as the name of the file from which data is collected
Log information	All files in `/var/opt/jp1base/log/`	`jp1_default_base_1st.tar.Z`, same as the name of the file from which data is collected
	shared-directory`/jp1base/log`[#1#2]	*logical-host-name*`_base_1st.tar.Z`, same as the name of the file from which data is collected

Type of information	Default file name	File name
Log of installation	/tmp/HITACHI_JP1_INST_LOG/jp1base_inst{1|2|3|4|5}.log	jp1_default_base_1st.tar.Z, same as the name of the file from which data is collected
Service operating information	All files in /var/opt/jp1base/sys/OPI/	jp1_default_base_1st.tar.Z, same as the name of the file from which data is collected
	All files in *shared-directory*/jp1base/sys/OPI/	*logical-host-name*_base_1st.tar.Z, same as the name of the file from which data is collected
Event service settings	All files in /var/opt/jp1base/sys/tmp/event/	jp1_default_base_1st.tar.Z, same as the name of the file from which data is collected
	All files in *shared-directory*/event/#1	*logical-host-name*_base_1st.tar.Z, same as the name of the file from which data is collected
Event database	All files in /var/opt/jp1base/sys/event/	jp1_default_base_2nd.tar.Z, same as the name of the file from which data is collected
	All files in *shared-directory*/event/#1	*logical-host-name*_base_2nd.tar.Z, same as the name of the file from which data is collected
JP1/SES-related log data	All files in /var/tmp/jp1_ses/	jp1_default_base_2nd.tar.Z, same as the name of the file from which data is collected
	All files in /var/opt/jp1_ses/log/ (or under HP-UX symbolic link /usr/lib/jp1_ses/log/)	jp1_default_base_2nd.tar.Z, same as the name of the file from which data is collected
	All files in /usr/lib/jp1_ses/log/ (for OS other than HP-UX)	jp1_default_base_2nd.tar.Z, same as the name of the file from which data is collected
	All files in /usr/lib/jp1_ses/sys/	jp1_default_base_2nd.tar.Z, same as the name of the file from which data is collected
	All files in /usr/tmp/jp1_ses/	jp1_default_base_2nd.tar.Z, same as the name of the file from which data is collected
	/usr/bin/jp1_ses/jp*	jp1_default_base_2nd.tar.Z, same as the name of the file from which data is collected

Type of information	Default file name	File name
	`/tmp/.JP1_SES*`	`jp1_default_base_2nd.tar.Z`, same as the name of the file from which data is collected
Command execution log	All files in `/var/opt/jp1base/log/COMMAND`	`jp1_default_base_2nd.tar.Z`, same as the name of the file from which data is collected
	All files in *shared-directory*`/jp1base/log/COMMAND`	`jp1_default_base_2nd.tar.Z`, same as the name of the file from which data is collected
Process operating status (except event service)	Execution result of `jbs_spmd_status`	`jp1_default_base_1st.tar.Z`, `jbs_spmd_status.log`
	Execution result of `jbs_spmd_status -h` *logical-host-name*#1	`jp1_default_base_1st.tar.Z`, `jbs_spmd_status_`*logical-host-name*`.log`
Process operating status of event service	Execution result of `jevstat` command	`jp1_default_base_1st.tar.Z`, `jevstat.log`
	Execution result of `jevstat` *logical-host-name*#1	`jp1_default_base_1st.tar.Z`, `jevstat_`*logical-host-name*`.log`
Integrated trace log file	`/var/opt/hitachi/HNTRLib2/spool/hntr2*.log`	`jp1_default_base_1st.tar.Z`, same as the name of the file from which data is collected

ISAM maintenance information	Execution result of `Jischk` command
	Physical host specified:
	`/var/opt/jp1base/log/COMMAND`
	Logical host specified:
	shared-directory`/jp1base/log/COMMAND`
		Physical host specified:
		`jp1_default_base_1st.tar.Z`, `com.jischk`, `log`
		Logical host specified:
		`jp1_default_base_1st.tar.Z`, `com.jischk_`*logical-host-name*`.log`

Core file diagnostics	Execution result of `car` command (results of analyzing core files in `/var/opt/jp1base/` and `/opt/jp1base/`)	`jp1_default_base_2nd.tar.Z`, `core_`*module-name*`.log`
		`jp1_default_base_2nd.tar.Z`, `core_`*module-name*`_cat.tar.Z`

File list	Execution result of `ls` command
	`ls -lRa /opt/jp1base`
	`ls -lRa /etc/opt/jp1base`
	`ls -lRa /var/opt/jp1base`
		`jp1_default_base_1st.tar.Z`, `inst_dir.log`

	Execution result of `ls` command#1
	`ls -lRa` *shared-directory*`/jp1base`
	`ls -lRa` *shared-directory*`/event`
		`jp1_default_base_1st.tar.Z`, `share_dir.log`

Type of information	Default file name	File name
Patch log	`/opt/jp1base/PatchInfo`	`jp1_default_base_1st.tar.Z`, `PatchInfo`
Patch log information	`/opt/jp1base/PatchLog`	`jp1_default_base_1st.tar.Z`, `PatchLog`
JP1/Base binding status	Execution result of `netstat -na`	`jp1_default_base_1st.tar.Z`, `netstat_na.log`

Note: When you specify a different path in the event server index file (`index`), or change the destination for the integrated trace log, you must specify the following option in the data collection tool in order to collect information from either the specified path or the changed destination.

`jbs_log.sh` (*any-option*) [*directory-specified-in-the-index-file*]

`jbs_log.sh` (*any-option*) [*destination-directory-for-the-integrated-trace-log*]

#1: Output when data about the logical host (cluster environment) is collected.

#2: Extra disk space might be required to collect large files of data from the event database and command execution log. Make sure that you check the file size before you collect data.

(3) Operation data

If an error occurs, you need to collect the following operational information:

- Details of the operation
- Time the error occurred
- Machine configuration (version of each OS, host name, configuration of JP1/IM - Manager)
- Whether the error occurs repeatedly under the same conditions
- User name used to log in from JP1/IM - View

(4) Error information on the screen

Collect hard copies of the following:

- The error dialog boxes (In addition, copy the contents of the details if the dialog box contains a **Details** button.)

16.4 How to collect data

This section describes how to collect data when an error occurs.

16.4.1 In Windows

(1) Execute the data collection tool

Execute the data collection tool (`jbs_log.bat`).

By executing `jbs_log.bat`, you can collect the data needed for investigating a JP1/Base error on that host.

The amount of data collected varies greatly depending on your operating environment. Before executing the data collection tool, estimate the amount of data as follows, and make sure you have sufficient disk space.

Data size when a physical host is specified in `jbs_log.bat`

If you specify a physical host (by omitting the `-h` option) in the `jbs_log.bat` command, use the following equation to estimate how much data will be collected about JP1/Base and the computer environment:

Data size = 5 + *a* + *b* + *c* + *d* (MB)

a

Size of all the files in *installation-folder*`\log\` (maximum 45 MB#1)

b

Size of all the files in *installation-folder*`\sys\` (maximum 55 MB#2)

c

Data size of the Dr. Watson log and crash dump

d

Total size of the following files

- *system-drive* (such as `C:\WINNT`) `\system32\config\AppEvent.evt`
- *system-drive* (such as `C:\WINNT`) `\system32\config\SysEvent.evt`

#1: An extra 142 MB is required if you are running JP1/IM - Manager on the same host.

#2: This is the default. This value increases if you change the size of the event database.

Data size when a logical host is specified in `jbs_log.bat`

If you specify a logical host in the `jbs_log.bat` command, use the following equation to estimate how much data will be collected about JP1/Base and the computer environment:

Data size = 5 + a + b + c + d + e + f (MB)

a

Size of all the files in *installation-folder*`\log\` (maximum 45 MB$^{\#1}$)

b

Size of all the files in *installation-folder*`\sys\` (maximum 55 MB$^{\#2}$)

c

Data size of the Dr. Watson log and crash dump

d

Total size of the following files

- *system-drive* (such as `C:\WINNT`) `\system32\config\AppEvent.evt`
- *system-drive* (such as `C:\WINNT`) `\system32\config\SysEvent.evt`

e

Data size of *shared-folder*`\jp1base\log\` (maximum 45 MB$^{\#1}$)

f

Data size of *shared-folder*`\jp1base\event\` (maximum 55 MB$^{\#2}$)

#1: An extra 142 MB is required if you are running JP1/IM - Manager on the same host.

#2: This is the default. This value increases if you change the size of the event database. For details on estimating the maximum size, see the *Release Notes*.

To check the size of each folder in Internet Explorer, right-click the folder, and then display the Properties window.

For details on estimating the maximum disk space requirements of each folder, see the *Release Notes*.

An example of `jbs_log.bat` execution is shown below.

```
c:\>c:\usertools\jbs_log.bat data-folder
```

Specify a full path for *data-folder*. If the path contains a space, enclose the path in double quotation marks (").

When you execute the tool, a jp1default folder is created in the directory you specified in *data-folder*. If you specify the -h option, in addition to the jp1default folder, a folder with the name of the logical host is created. Two further folders, base_1st and base_2nd are created in each of these folders, and the data collected by jbs_log.bat is copied under them. If necessary, you can compress the collected data by using an archiving tool.

The jbs_log.bat command provides options for excluding specific files, such as command execution logs (ISAM) and event database files. For details, see *jbs_log.bat (Windows only)* in *13. Commands*.

Notes on data collection with JP1/IM, JP1/AJS, and other pre-version 07-00 programs

In JP1/Base version 07-00 or later, the data collection tool cannot be customized for collecting JP1/IM and JP1/AJS data. To collect data from these programs, execute the program-specific data collection tool.

(2) Check the status of the process

Use the Windows task manager to check the operating status of a desired process. The system displays the following process names when the processes are operating normally. The value in parentheses in the table indicates the number of processes that can be executed simultaneously.

Parent process name	Function	Child process name	Function
hntr2srv.exe (1)	Starts the Hitachi Network Objectplaza Trace Library (HNTRLib2)	--	--
hntr2mon.exe (1)	Hitachi Network Objectplaza Trace Library (HNTRLib2)	--	--
jbs_service.exe (1)	Starts the JP1/Base process management	--	--
jbs_spmd.exe (1)	JP1/Base process management#1	jbssessionmgr.exe (1)	Authentication server#1, #3 This process exists only on the host that is set as the authentication server. The displayed name is jbssessionmgr when the jbs_spmd_status command is executed.

Parent process name	Function	Child process name	Function
		jbsroute.exe (1)	Configuration management[#1, #3] The displayed name is jbsroute when the jbs_spmd_status command is executed.
		jcocmd.exe (1) jcocmdexe.exe (1) jcocmdapi.exe (number of screens where commands are executed [#2] + 1 (when JP1/IM - Manager has been installed))	Command execution[#1, #3] The displayed name is jcocmd when the jbs_spmd_status command is executed.
		jbsplugind.exe	Plug-in service[#1, #3] The displayed name is jbsplugin when the jbs_spmd_status command is executed.
		jbshcd.exe (1)	Health check (for local host monitoring)[#1, #3] The displayed name is jbshcd when the jbs_spmd_status command is executed.
		jbshchostd.exe (1)	Health check (for remote host monitoring)[#1, #3] The displayed name is jbshchostd when the jbs_spmd_status command is executed.
		jbssrvmgr.exe (1)	Service management control function[#1,#3] The displayed name is jbssrvmgr when the jbs_spmd_status command is executed.
		jbslcact.exe (1)	Local action function[#1,#3] The displayed name is jbslcact when the jbs_spmd_status command is executed.

Parent process name	Function	Child process name	Function
		jbscomd.exe (1) jbscomd_api.exe (1 to 9999) jbscomd_ses.exe (1) jbscomd_snd.exe (1) jbscomd_rcv.exe (1)	Inter-process communication[#1,#3] The displayed name is jbscomd when the jbs_spmd_status command is executed.
jbapmsrvcecon.exe (1)	Startup control	powendar.exe (1)	Power control This process is generated when JP1/Power Monitor is installed.
jevservice.exe (1)	Event service[#1, #4]	jevsessvc.exe (1)	Event service This process is generated only on physical hosts.
jevtraplog.exe (1)	Log file trap	--	This process is generated only when the log file trapping function is used.
jevtrapevt.exe (1)	Event log trap	--	This process is generated only when the event log trapping function is used.
imevtgw.exe (1)	SNMP trap converter	--	This process is generated only when the SNMP trap converter is used.

Legend:

--: None

#1: The maximum number of processes that can be executed simultaneously with the indicated process is the calculation result of the following format when multiple logical hosts operate on one physical host in the cluster system or when one logical host and one physical host are started at the same time: (*number-of-logical-hosts* + 1) x *number-of-processes*

#2: The number of Execute Command windows opened by the connected JP1/IM - View. The number of processes increases as the number of open windows increases. When you close an Execute Command window, the corresponding process disappears.

#3: You can use the jbs_spmd_status command to check the status of these processes. If the processes are running normally, the jbs_spmd_status command returns the following information.

- If an authentication server has been set:

```
jbssessionmgr
```

`jbsroute`

`jcocmd`

`jbsplugin`

`jbshcd`

`jbshchostd`

`jbssrvmgr`

`jbslcact`

`jbscomd`

- If an authentication server has not been set:

  `jbsroute`

  `jcocmd`

  `jbsplugin`

  `jbshcd`

  `jbshchostd`

  `jbssrvmgr`

  `jbslcact`

  `jbscomd`

#4: The status of these processes can be checked with the `jevstat` command. Executing the `jevstat` command when the processes are running normally displays the following string:

`jevservice`

(3) Check the operation data

If an error occurs, check the operation data and record it. You need to check the following information:

- Details of the operation
- Time the error occurred
- Machine configuration (version of each OS, host name, configuration of JP1/IM - Manager)
- Whether the error occurs repeatedly under the same conditions
- User name used to log in from JP1/IM - View

(4) Collect the error information on the screen

If an error is displayed on the screen, also collect that information. Collect hard copies of the following:

- The error dialog boxes

In addition, copy the contents of the details if the dialog box contains a **Details** button.

(5) Collect user dumps (for Windows Vista and Windows Server 2008)

When an application error causes the JP1/Base process to stop, an error dialog box appears. After the dialog box appears, perform the following actions to collect the user dumps:

Note

> If you close the error dialog box, normal dumping does not occur, thus making it impossible to collect user dumps. If you accidentally close the error dialog box before collection (for example, by clicking the **OK** button accidentally), reproduce the error and then collect the user dumps.

1. Start Task Manager.

   You can start Task Manager by performing one of the following actions:

   - Right-click an empty area on the taskbar, and then select **Task Manager**.
   - Press the **CTRL**+**SHIFT**+**ESC** keys.

2. Click the **Processes** tab.
3. Right-click the process name of JP1/Base that was stopped by an application error, and then select **Create Dump File**.
4. When a dialog box appears indicating the destination path for user dumps, open the destination and collect the user dumps from there.

(6) Collect problem reports (for Windows Vista and Windows Server 2008)

When an application error causes the JP1/Base process to stop, perform the following actions to collect a problem report:

1. Enter `wercon` in the Run dialog box and click the **OK** button.

   The Problem Reports and Solutions dialog box appears.

2. On the left side of the dialog box, click **View problem history**.
3. Double-click the appropriate problem.

   The full problem report then appears.

4. Select **Copy to Clipboard**.
5. Paste the copied report into a text file, and then save the file.

You can now use the saved report for problem investigation.

16.4.2 In UNIX

(1) Execute the data collection tool

Execute the data collection tool (`jbs_log.sh`).

By executing `jbs_log.sh`, you can collect the data needed for looking into a JP1/Base error on that host.

The amount of data collected varies greatly depending on your operating environment. Before executing the data collection tool, estimate the amount of data as follows, and make sure you have sufficient disk space.

Data size when a physical host is specified in `jbs_log.sh`

If you specify a physical host (by omitting the `-h` option) in the `jbs_log.sh` command, use the following equation to estimate how much data will be collected about JP1/Base and the computer environment:

Data size = 3 + *a* + *b* + (60 x *c*) MB

a

Size of all the files in `/var/opt/jp1base/` (maximum 83 MB$^{\#1, \#2}$)

b

Size of the core files under `/` (only if output)

c

Number of core files under `/`, and in the `/var/opt/jp1base/` or `/opt/jp1base/` directory

#1: An extra 142 MB is required if you are running JP1/IM - Manager on the same host.

#2: This is the default. This value increases if you change the size of the event database. For details on estimating the maximum size, see the *Release Notes*.

Data size when a logical host is specified in `jbs_log.sh`

If you specify a logical host in the `jbs_log.sh` command, use the following equation to estimate how much data will be collected about JP1/Base and the computer environment:

Data size = 3 + *a* + *b* + (60 x c) + *d* + *e* (MB)

a

Size of all the files in `/var/opt/jp1base/` (maximum 83 MB$^{\#1, \#2}$)

b

Size of the core files under `/` (only if output)

c

Number of core files under `/`, and in the `/var/opt/jp1base/` or `/opt/jp1base/` directory

d

Data size of *shared-directory*`/jp1base/log/` (maximum 45 MB#1)

e

Data size of *shared-directory*`/event/` (maximum 55 MB#2)

#1: An extra 142 MB is required if you are running JP1/IM - Manager on the same host.

#2: This is the default. This value increases if you change the size of the event database. For details on estimating the maximum size, see the *Release Notes*.

You can check the size of each folder by executing the `du` command.

For details on estimating the maximum disk space requirements of each folder, see the *Release Notes*.

An example of `jbs_log.sh` execution is shown below.

```
jbs_log.sh -f output-file-name
```

The `jbs_log.sh` command provides options for excluding specific files, such as command execution logs (ISAM) and event database files. For details, see *jbs_log.sh (UNIX only)* in *13. Commands*.

Notes on data collection with JP1/IM, JP1/AJS, and other pre-version 07-00 programs

In JP1/Base version 07-00 or later, the data collection tool cannot be customized for collecting JP1/IM and JP1/AJS data. To collect data from these programs, execute the program-specific data collection tool.

(2) Check the status of the process

The following table lists the processes displayed when you execute the `ps` command. In UNIX, by executing the data collection tool (`jbs_log.sh`), you can collect `ps` command execution results in addition to the other data.

The value in parentheses in the table indicates the number of processes that can be executed simultaneously.

Parent process name	Function	Child process name	Function
hntr2mon (1)	Hitachi Network Objectplaza Trace Library (HNTRLib2)	--	--
jbs_spmd (1)	Process management#1	jbssessionmgr (1)	Authentication server#1, #4 This process exists only on the host that is set as the authentication server. The displayed name is jbssessionmgr when the jbs_spmd_status command is executed.
		jbsroute (1 to 9)	Configuration management#1, #4 The displayed name is jbsroute when the jbs_spmd_status command is executed.
		jcocmd (1) jcocmdexe (1) jcocmdapi (number of windows where commands are executed #2 + 1 (when JP1/IM - Manager has been installed)) jcocmdcmc (0 to the number of commands#3)	Command execution#1, #4 The displayed name is jcocmd when the jbs_spmd_status command is executed.
		jbsplugind#5	Plug-in service#1, #4 The displayed name is jbsplugin when the jbs_spmd_status command is executed.
		jbshcd (1)	Health check (for local host monitoring)#1, #4 The displayed name is jbshcd when the jbs_spmd_status command is executed.
		jbshchostd (1)	Health check (for remote host monitoring)#1, #4 The displayed name is jbshchostd when the jbs_spmd_status command is executed.

Parent process name	Function	Child process name	Function
		jbssrvmgr (1)	Service management control function#1,#4 The displayed name is jbssrvmgr when the jbs_spmd_status command is executed.
		jbslcact (1)	Local action function#1,#4 The displayed name is jbslcact when the jbs_spmd_status command is executed.
		jbscomd.exe (1) jbscomd_api.exe (1 to 9999) jbscomd_ses.exe (1) jbscomd_snd.exe (1) jbscomd_rcv.exe (1)	Inter-process communication#1,#4 The displayed name is jbscomd when the jbs_spmd_status command is executed.
jevservice (1)	Event service#1, #6	jevservice (6 to 9,999)	Event service
		jesdmain (1)#7	For compatibility with JP1/SES This process is generated only on physical hosts.
		jesrd (4 to 9,999)	For compatibility with JP1/SES This process is generated only on physical hosts.
jevlogd (1 to 2)	Log file trap	jelparentim (0 to the number of times the jevlogstart command is executed)	Log file trap The jelchildim process is generated for each file to be monitored for each jelparentim. When the jevlogstop command is executed, the jelparentim process disappears.
imevtgw (1)	SNMP trap converter	--	This process is generated only when the SNMP trap converter is used.

Legend:

--: None

#1: The maximum number of processes that can be executed simultaneously with the indicated process is the calculation result of the following format when multiple logical hosts operate on one physical host in the cluster system or when one logical host and one physical host are started at the same time: (*number-of-logical-hosts* + 1) x *number-of-processes*

#2: The number of Execute Command windows opened by the connected JP1/IM - View. The number of processes increases as the number of open windows increases. When you close an Execute Command window, the corresponding process disappears.

#3: The number of the remote commands and automated actions executed using JP1/IM - Manager. A process is generated for each command. When processing finishes, the process disappears. If you execute commands successively, multiple processes might be generated.

#4: You can use the `jbs_spmd_status` command to check the status of these processes. If the processes are running normally, the `jbs_spmd_status` command returns the following information.

- If an authentication server has been set:

  ```
  jbssessionmgr
  
  jbsroute
  
  jcocmd
  
  jbsplugin
  
  jbshcd
  
  jbshchostd
  
  jbssrvmgr
  
  jbslcact
  
  jbscomd
  ```

- If an authentication server has not been set:

  ```
  jbsroute
  
  jcocmd
  
  jbsplugin
  
  jbshcd
  
  jbshchostd
  
  jbssrvmgr
  
  jbslcact
  
  jbscomd
  ```

#5: The process name displayed by the `ps-el` command is `jbsplugin`.

#6: The status of these processes can be checked with the `jevstat` command. Executing the `jevstat` command when the processes are running normally displays the following string:

`jevservice`

#7: The process name displayed when you execute the `ps` command is `/var/opt/jp1base/sys/tmp/event/servers/default/jpevent.conf`.

(3) Check the operation data

If an error occurs, check the operation data and record it. You need to check the following information:

- Details of the operation
- Time the error occurred
- Machine configuration (version of each OS, host name, configuration of JP1/IM - Manager)
- Whether the error occurs repeatedly under the same conditions
- User name used to log in from JP1/IM - View

(4) Collect the error information on the screen

If an error is displayed on the screen, also collect that information. Collect hard copies of the following:

- The error dialog boxes

In addition, copy the contents of the details if the dialog box contains a **Details** button.

16.5 Troubleshooting different types of problems

This section describes how to troubleshoot different types of problems.

16.5.1 Problems in Windows or UNIX

The following problems might occur in Windows or UNIX.

Table 16-3: Problems common to both Windows and UNIX

No.	Problem
1	Multiple JP1 events occur within a short period of time, causing a delay in registration and transfer.
2	The event database is corrupt.
3	When JP1/Base starts, the message `The port ID for the SES emulator is not defined` appears.
4	JP1/Base does not function as defined in a definition file.

(1) Multiple JP1 events occur within a short period of time, causing a delay in registration and transfer.

When an error generates a large number of JP1 events in quick succession, the JP1 event reporting the error might take a long time to appear in JP1/IM - View. This might delay the execution of any JP1/AJS jobs triggered by these JP1 events. Forwarding of the JP1 events being processed when the error occurs resumes when the failed host is restored and the event service restarts.

If it is essential to stop the delayed JP1 events from being sent, because of the load on the system or the effect on job processing, initialize the event database on the issuing host. If you want to save the JP1 events already registered in the event database, use the `jevexport` command to output the event database in CSV format before you initialize the database.

For details on the procedure to initialize the event database, see *8.2 Initializing the event database*.

To prevent the generation of large numbers of JP1 events, adjust the JP1 event forwarding conditions in the forwarding setting file (`forward`).

(2) The event database is corrupt.

The event database might be corrupt due to the following reasons:

- Sudden loss of power because of a power outage or some other reason
- Backing up or restoring the event database by an OS command or backup software while the event service is active

- Editing the event database in a text editor
- Redirecting command output results or other information to the event database
- A hard disk error

Even if the event database is damaged, the event service will still start or continue running, and new JP1 events can still be registered or acquired as normal. However, damaged records will not be retrieved or acquired. Damaged records in the event database might also affect the performance of event searches from JP1/IM - View.

The KAJP1057-W, KAJP1058-W, or KAJP1059-E message is output to the event log, syslog, and integrated trace log when the event database is damaged. Initialize the event database if any of these messages appears.

For details on the procedure to initialize the event database, see *8.2 Initializing the event database*.

(3) When JP1/Base starts, the message "The port ID for the SES emulator is not defined" appears.

The reason this message displays, and the necessary action to correct the error, are described below:

Causes

No port ID for SES compatibility is specified in the `services` file. This is not a problem if no events in JP1/SES format will be sent or received.

Action

If events will be forwarded to or from JP1/SES, JP1/AJS, or a program that uses the JP1/SES protocol (JP1/OJE, for example), add the `JP1AutoJob` specification (in Windows) or `jesrd` specification (in UNIX) to the `services` file. You can specify any port number.

(4) JP1/Base does not function as defined in a definition file.

Because some of the settings for a service running on a host do not reflect the settings in the service's definition file, the service might not function as expected. In order to determine the source of the problem, you must compare the operating information of the service that is currently running and the contents of the service's definition file.

You can use the `jbsgetopinfo` command to view the operating information of a service that is currently running. This command provides operating information defined in the forwarding settings file for the event service, the action definition file for the log file trap, and the action definition file for the event log trap (Windows only) for the service. Compare the operating information with the contents of each respective definition file. If there is a difference, take the necessary action to correctly incorporate the contents of the definition files. For details on the `jbsgetopinfo` command, see *jbsgetopinfo* in *13. Commands*.

16.5.2 Problems in Windows

The following problems might occur in Windows:

Table 16-4: Problems in Windows

No.	Problem
1	The JP1/Base event service fails to start.
2	The Event Console window for JP1/IM - View displays incorrect times for JP1 events.
3	The authentication server fails to start.
4	The message `Service specific error 3004.` appears and the JP1/Base EventlogTrap service does not start.
5	The startup control function (JP1/Base Control Service) could not start or stop a service normally.
6	The startup control function (JP1/Base Control Service) could not stop a system when the system terminated.
7	To start the services in a specific order, you used the startup control to define the sequence of each service to start after the previous service had finished starting. However, the service started before the previous service finished starting, and an error message was displayed.
8	When you used the startup control (JP1/Base Control Service) to start a service, the following warning was displayed: `The service indicated in` *XXXX* `has already started.`
9	When you used the startup control (JP1/Base Control Service) to start a service, the following message is output to the event viewer's application log: `Could not verify that the` *XXXX* `service has started within the specified time.`
10	When you used the startup control (JP1/Base Control Service) to start a service, the message `KAVA4003-E The` *XXXX* `service could not start because an unexpected error occurred.` is output and the service does not start.
11	Cannot log in when the directory server linkage function is enabled.

(1) The JP1/Base event service fails to start.

The following describes why the JP1/Base event service does not start on a Windows host, and the action you should take.

Causes

You might have installed JP1/Base on a computer that is using an existing instance of JP1/IM. In this case, selecting **Auto** (in the Services dialog box that opens from the Control Panel) for the JP1/IM Control Service or JP1/IM Event service might prevent the JP1/Base Event service from starting.

Action

Change the settings for the JP1/IM Control Service and JP1/IM Event service to the manual mode. In addition, set the other JP1/Base-related services to the manual mode.

(2) The Event Console window for JP1/IM - View displays incorrect times for JP1 events.

The following describes why the time for JP1 events displayed on the Event Console window for JP1/IM - View is incorrect, and the action you should take.

Causes

The system is using an old version of `msvcrt.dll`.

Action

When installing JP1/Base, be sure to choose **Restart** in the dialog box that asks whether you want to replace `msvcrt.dll`. After replacing the file, restart the system.

If a malfunction such as incorrect event time occurs after installing other products, re-install JP1/Base.

(3) The authentication server fails to start.

The following describes why the authentication server does not start, and the action you should take.

Causes

The authentication server will not start unless you select the local host under **Order of authentication server** in the **Authentication Server** page of the JP1/Base Environment Settings window. By default, the authentication server does not start if you do not select automatic setup when installing JP1/Base for the first time.

Action

Specify the local host under **Order of authentication server** in the **Authentication Server** page of the JP1/Base Environment Settings window.

(4) The JP1/Base EventlogTrap service fails to start, and the following message is displayed: "Service specific error 3004."

The reason this message displays and the JP1/Base EventlogTrap service does not start, and the necessary action to correct the error, are described below:

Causes

This error occurred because the event log trapping service (JP1/Base EventlogTrap) started before the event service (JP1/Base Event) starts. This might occur if you select **Auto** as the startup method for the event log trapping service (JP1/Base EventlogTrap) in the Services dialog box that opens from the Control Panel.

Action

To automatically start the event log trapping service (JP1/Base EventlogTrap), use the startup control (JP1/Base Control Service) and set the event log trapping service (JP1/Base EventlogTrap) to start after the event service (JP1/Base Event) starts. For details on the startup control (JP1/Base Control Service), see *7. Setting the Service Start and Stop Sequences (Windows Only)*.

(5) The startup control function (JP1/Base Control Service) could not start or stop a service normally.

The following describes why you might not be able to start or stop a service normally using the JP1/Base Control Service, and the action you should take.

Causes

The possible causes are as follows:

1. An interactive command or a command that displays a dialog box is registered in the start sequence definition file (`JP1SVPRM.DAT`).
2. The path for a command in the start sequence definition file (`JP1SVPRM.DAT`) includes spaces, but has not been enclosed in double quotation marks (`"`).

Action

To correct the problem, perform one of the following actions. Each number corresponds to the respective number of the causes described above:

1. Check whether there is any interactive command or a command that displays a dialog box. Do not register these commands.
2. Enclose the path in double quotation marks or register a reference path in the `PATH` environment variable. Write only the executable file name in the start sequence definition file (`JP1SVPRM.DAT`).

(6) The startup control function (JP1/Base Control Service) could not stop a system when the system terminated.

The following describes why you might not be able to stop a service using the JP1/Base Control Service when the system terminates, and the action you should take.

Causes

The possible causes are as follows:

1. JP1/Power Monitor is not installed.
2. You have shut down from the **Start** menu.
3. Although you executed a forced shutdown from JP1/Power Monitor, the `[Control Value]` section is not registered in the definition file.

4. The shutdown command for the OS was executed by a program other than JP1/Power Monitor.
5. The startup method for the service is set to **Auto** in the Services dialog box that opens from the Control Panel.
6. You have stopped the JP1/Base Control Service manually.

Action

To correct the problem, perform one of the following actions. Each number corresponds to the respective number of the causes described above:

1. Install JP1/Power Monitor.
2. Use JP1/Power Monitor to perform planned shutdown or forced shutdown.
3. Register the `[Control Value]` section in the definition file.
4. Use JP1/Power Monitor to perform planned shutdown or forced shutdown.
5. Change the startup method for the service to **Manual** in the Services dialog box that opens from the Control Panel.
6. Use JP1/Power Monitor to perform planned shutdown or forced shutdown.

(7) To start the services in a specific order, you used the startup control to define the sequence of each service to start after the previous service had finished starting. However, the service started before the previous service finished starting, and an error message was displayed.

The following describes why a service might start before the previous service has finished starting, and the action you should take. An error message is output when this happens. This might occur even though the start sequence has been defined for each service.

Causes

The possible causes are as follows:

1. The startup control (JP1/Base Control Service) tried to complete the previous service's startup processing before starting the next service's startup processing. However, it did not finish before the specified maximum timeout, and the startup control started the startup processing of the service defined as the next one.
2. The start sequence definition file (`JP1SVPRM.DAT`) specifies that the next service's startup processing is to start without waiting for the previous service's startup processing to finish.

Action

To correct the problem, perform one of the following actions. Each number corresponds to the respective number of the causes described above:

1. Check the time necessary to start the service that caused the timeout. Then, in the start sequence definition file (`JP1SVPRM.DAT`), increase the value of the `Wait=` parameter for the service so that there will be no timeout.
2. In the start sequence definition file (`JP1SVPRM.DAT`), consider changing the value of the `Parallel=` parameter for the service. For details, see *Start sequence definition file (Windows only)* in *14. Definition Files*.

(8) When you used the startup control (JP1/Base Control Service) to start a service, the following warning was displayed: "The service indicated in XXXX has already started."

The following describes why, when you start a service using the startup control (JP1/Base Control Service), the warning `The service indicated in` *XXXX* `has already started` is displayed, and the action you should take.

Causes

This warning message is displayed when the service to be started using the startup control has already started. A possible cause of this warning message is that the service's startup settings have been set to start the service automatically.

Action

If you use the startup control to start the services, set the services' startup settings so that you can start the services manually.

(9) When you used the startup control (JP1/Base Control Service) to start a service, the message "Could not verify that the XXXX service has started within the specified time." is output to the event viewer's application log.

When you start a service using the startup control (JP1/Base Control Service), the following message might be output to the application log of the event viewer: `Could not verify that the` *XXXX* `service has started within the specified time.` If the specified service has already started, check the settings described below. If this message is displayed while the specified service has not started, consult the developer of the service about the possible cause of the startup failure.

If the `Wait=` parameter is not set in the section applicable to the service:

The service needs more than 60 seconds (the default timeout) to complete startup. Place the `Wait=` parameter in the service's section, and set its value to more than 60 seconds.

If the `Wait=` parameter is set in the section applicable to the service:

The service needs a period longer than the specified timeout to complete startup. Set the service's `Wait=` parameter to a value larger than the current one.

(10) When you used the startup control (JP1/Base Control Service) to start a service, the message "KAVA4003-E The XXXX service could not start because an unexpected error occurred." is output and the service does not start.

The following describes why, when you start a service using the startup control (JP1/ Base Control Service), the service fails to start and the following message is displayed, and the action you should take: `KAVA4003-E The` *service-name* `service could not start because an unexpected error occurred`

Causes

This error might occur when startup of the service controlled by the JP1/Base startup control coincides with automatic startup of the same service by the Windows Service Control Manager.

Action

Set a slightly later time for the service to start under the startup control. This will prevent startup failure due to overloading at service startup.

For details, see *7.3 Setting the timing for starting services*.

(11) Cannot log in when the directory server linkage function is enabled.

If the directory server linkage function has been enabled and a login attempt fails, refer to the integrated trace log to find the source of the error. If any of the following error messages is included, see the manual *Job Management Partner 1/Base Messages* to check the cause and action. After you check the cause and the necessary action to correct the problem, contact your directory server administrator:

- KAVA1677-W
- KAVA1678-W
- KAVA1679-W
- KAVA1687-W
- KAVA1688-W
- KAVA1690-W
- KAVA1691-W

16.5.3 Errors in UNIX

The following error might occur in UNIX:

Table 16-5: Problems in UNIX

No.	Problem
1	Failure to start the authentication server

No.	Problem
2	Failure to start the event service because an error such as KAJP1005-E or KAJP1852-E occurred

(1) Failure to start the authentication server

The following describes why the authentication server does not start, and the action you should take.

Causes

If you changed the setting so that the authentication server stops, you cannot start the authentication server by specifying the local host in *authentication-server* in the `jbssetusrsrv` command.

Action

Use the `jbssetusrsrv` command to specify the local host in *authentication-server*, and then perform the following:

```
cd /etc/opt/jp1base/conf
cp -p jp1bs_spmd.conf.session.model jp1bs_spmd.conf
```

(2) Failure to start the event service because an error such as KAJP1005-E or KAJP1852-E occurred

The following describes why you might not be able start the event service if an error message occurs, and the action you should take.

Causes

The possible causes are as follows:

1. The values of kernel parameters are set without taking JP1/Base and other products into consideration.
2. Although the directory specified in the event server index file (`index`) has a symbolic link, there is no directory at the destination of the symbolic link.
3. The directory to be created when the event service starts cannot be created because of inappropriate permissions or other reasons.

Action

To correct the problem, perform one of the following actions. Each number corresponds to the respective number of the causes described above:

1. Re-set the values of kernel parameters. For details on the values of kernel parameters, see *G. List of Kernel Parameters*.
2. Create the directory and re-create the symbolic link.
3. Change the user privileges to superuser privileges, and then re-execute the

event service.

16.5.4 Errors detected by the health check function

The health check function can detect errors in the JP1/Base processes. The following describes the causes and recovery actions for errors detected by the health check function.

(1) There is a large number of system resources (CPU, disk, and other resources) being consumed. Or, the number of process requests exceeds the performance limit.

Cancel any processing that places a high load on the system.

(2) The command process does not end as expected. Or, the command process does not end and still retains system resources.

Using an OS function such as the `kill` command, forcibly end the command process.

(3) A process is in a deadlock or infinite loop

If a process goes into a deadlock or infinite loop and fails to end in a timely manner, take the recovery action described in the following table.

No.	Function	Process name		Recovery action
1	Process management	`jbs_spmd`		Restart JP1/Base. In Windows: Restart the JP1/Base services (process management including user management). In UNIX: Restart JP1/Base.#
2	Authentication server	`jbssessionmgr`		
3	Configuration management	`jbsroute`		
4	Command execution	`jcocmd`		
5	Plugin service	`jbsplugind`		
6	Event service	`jevservice`		Restart the event service. In Windows: Restart the JP1/Base Event service. In UNIX: Restart the event service.#
7	Log file trap	`jevtraplog`	`jevtraplog` `jevlogd`	Restart the log-file trap management service (daemon). In Windows: Restart the JP1/Base LogTrap service. In UNIX: Restart the log-file trap management daemon.#

No.	Function	Process name		Recovery action
			jelparentim	Using the jevlogstart command, restart the log file trap that has the ID indicated in the error message.
			jelchildim	
8	Event log trap	jevtrapevt		Restart the event log trapping service (JP1/Base EventlogTrap).
9	SNMP trap converter	imevtgw		Restart NNM.
10	Health check	jbshcd jbshchostd		Restart JP1/Base. In Windows: Restart the JP1/Base services (process management including user management). In UNIX: Restart JP1/Base.#

#: After terminating the processes with the stop command, use the `ps -el` command to make sure all the processes have ended. If any processes are still active, end them with the `kill` command. Then restart the processes using the start command.

(4) Unable to connect to the host to be monitored

- Check whether the host has started.
- Check whether JP1/Base has started.
- Check whether there is a problem on the network.
- Make sure that JP1/Base installed on the host to be monitored is version 07-51 or later.

16.6 Notes on using JP1/Base

This section gives some notes on using JP1/Base.

(1) Notes on starting the system

- If you execute the following commands at the same time, JP1/Base might not start normally. Do not execute them at the same time.
  - `jbs_start`
  - `jbs_start.cluster`
  - `jbs_spmd`

(2) Notes on starting the system operation

- Do not use the following commands when JP1/Base is active:
  - `jbshostsimport`
  - `jbsunsetcnf`
  - `jevdbinit`
  - `jevdbmkrep`
  - `jp1base_setup` (UNIX)
  - `jp1base_setup_cluster` (UNIX)
  - `jp1bshasetup` (Windows)
  - `Jischk`
  - `Jiscond`
  - `Jisconv`
  - `Jiscpy`
  - `Jisext`
  - `Jiskeymnt`
  - `Jislckext`
  - `Jisprt`
  - `Jislckreg` (UNIX)
  - `Jisrsdel` (UNIX)
- You can change the following environment settings while JP1/Base is active if you are not currently executing commands using JP1/IM and JP1/AJS, or jobs or

automated actions:

- JP1 user settings
- Authority level for JP1 resource groups (for Windows)
- JP1 user operating permission settings (for UNIX)
- Authentication server change

You should be careful when you change the above environment settings while JP1/IM or JP1/AJS is operating.

(3) Notes on user authentication

- When workloads for login are concentrated on a single authentication server, the system might display the KAVB0109-E message (indicating a communication error between the connecting host and authentication host) or the KAVB0105, KAVB0106, or KAVB0108 message, disabling further login. If this error occurs, wait a while and then retry the login.
- When you log in from JP1/IM - View or JP1/AJS - View, spaces after a password are ignored.

(4) Notes on controlling the start sequence

- The **Log On As** setting in the Service dialog box of JP1/Base Control Service must be **System Account**. Do not select the **Allow Service to Interact with Desktop** option.
- Do not register interactive commands and commands that display dialog boxes in the `JP1SVPRM.DAT` file.

(5) Notes on the files and directories used by JP1/Base

- When you use JP1/Base on UNIX, do not create any file or directory under `/var/opt/jp1base/tmp`. If created, the file or directory might be deleted.
- In Windows, the command execution process uses *installation-folder*`\COMMAND` as the current folder. Therefore, the OS users mapped to JP1 users require read permission for the current folder. Write permission is required if you are creating a file and redirecting the command result to it, or if you are creating temporary files, in the current folder.

Appendixes

A. List of Files and Directories

This appendix lists the names of the files and directories for JP1/Base.

A.1 In Windows

In the following tables, the *Base_Path* indicates the *installation-folder* in this manual. By default, *Base_Path* is C:\Program Files\Hitachi\jp1base. *SystemDrive* in the table is the same as *system-drive* used in the body of this manual.

Table A-1: List of files and folders of JP1/Base (in Windows)

Contents	File name/folder name
Command storage folder	*Base_Path*\bin\
Environment settings folder[#1]	*Base_Path*\conf\ *shared-folder*\jp1base\conf\
Language type settings file	*Base_Path*\conf\jp1bs_param.conf *shared-folder*\jp1base\conf\jp1bs_param.conf
Configuration definition file	*Base_Path*\conf\route\jbs_route.conf *shared-folder*\jp1base\conf\route\jbs_route.conf
JP1/IM function header file	*Base_Path*\include\JevApi.h
Log folder[#2]	*Base_Path*\log\ *shared-folder*\jp1base\log\
Folder for plug-in	*Base_Path*\plugin\
Operating information storage folder	*Base_Path*\sys\OPI\ *shared-folder*\jp1base\sys\OPI\
Readme file	*Base_Path*\readme.txt
Event database storage folder[#3]	*Base_Path*\sys\event\servers\[#4] *shared-folder*\jp1base\event\[#4]
Log and temporary folder[#2]	*Base_Path*\sys\tmp\event\servers\[#4]
	Event ID save file for JP1/AJS compatibility • *Base_Pat*h\sys\tmp\event\servers\default\ereb.backup[#4] • *shared-folder*\jp1base\event\ereb.backup[#4]
	Internal action file for the log file trapping function • *Base_Path*\sys\tmp\event\logtrap\conftbl.*ID-number*

Contents	File name/folder name
Tool folder	*Base_Path*`\tools\`
	Data collection tool sample batch file - *Base_Path*`\tools\jbs_log.bat`
	Function sample source file that issues and collects JP1 events - *Base_Path*`\tools\event\receiver.c` - *Base_Path*`\tools\event\sender.c`
	AR System linkage sample batch file - *Base_Path*`\tools\helpdesk\register_ars.bat`
Integrated trace log folder	*SystemDrive*`\Program Files\Hitachi\HNTRLib2\spool\`

#1: For details on definition files, see *A.1(1) List of definition files (in Windows)*.

#2: For details on log files, see *A.1(2) List of log files (in Windows)*.

#3: For details on event database file names, see *1.4.2 Event database*.

#4: This file or folder is stored in a different folder if you specify another path in the event server index file (`index`).

(1) List of definition files (in Windows)

The definition files used in JP1/Base are listed below.

Table A-2: List of definition files (in Windows)

Function	File name/folder name
Startup control	Start sequence definition file - *Base_Path*`\conf\boot\JP1SVPRM.DAT` - *Base_Path*`\conf\boot\JP1SVPRM.DAT.MODEL`
	Service startup delay time / timer monitoring period definition file - *Base_Path*`\conf\boot\jp1svprm_wait.dat` - *Base_Path*`\conf\boot\jp1svprm_wait.dat.sample`
Event service	Event server index file - *Base_Path*`\conf\event\index`
	Event server settings file - *Base_Path*`\conf\event\servers\default\conf`#1 - *shared-folder*`\jp1base\event\conf`#1
	Forwarding settings file - *Base_Path*`\conf\event\servers\default\forward`#1 - *shared-folder*`\jp1base\event\forward`#1

Function	File name/folder name
	API settings file - *Base_Path*`\conf\event\api`
	Configuration definition file for JP1/AJS compatibility - *Base_Path*`\sys\tmp\event\servers\default\ajses.def`
Event conversion	Log file trap definition file You can specify any folder and any file.
	Log information definition file - *Base_Path*`\conf\event\jevlogd.conf`
	Event log trap definition file - *Base_Path*`\conf\event\ntevent.conf`
	Action definition file for converting the SNMP traps - *Base_Path*`\conf\evtgwt\imevtgw.conf` - *shared-folder*`\jp1base\conf\evtgwt\imevtgw.conf`#2
	Filter file for converting SNMP traps - *Base_Path*`\conf\evtgwt\snmpfilter.conf` - *shared-folder*`\jp1base\conf\evtgwt\snmpfilter.conf`#2
Event service definition information collection and distribution	Distribution definition file (forward setting file) - *Base_Path*`\conf\event\servers\default\[jev_forward.conf |` *any-file*`]` #3 - *shared-folder*`\jp1base\event\[jev_forward.conf |` *any-file*`]` #3
	Distribution definition file (log file trap definition file) - *Base_Path*`\conf\[jev_logtrap.conf |` *any-file*`]` #3
	Distribution definition file (event log trap definition file) - *Base_Path*`\conf\event\[jev_ntevent.conf |` *any-file*`]` #3
User management	Password definition file You can specify any folder and any file.
	User permission level file - *Base_Path*`\conf\user_acl\JP1_UserLevel` - *shared-folder*`\jp1base\conf\user_acl\JP1_UserLevel`
	Directory server modification file You can specify any folder and any file.

Function	File name/folder name
	Directory server linkage definition file • *Base_Path*\conf\ds\jp1bs_ds_setup.conf • *Base_Path*\conf\ds\jp1bs_ds_setup.conf.model • *shared-folder*\jp1base\conf\ds\jp1bs_ds_setup.conf • *shared-folder*\jp1base\conf\ds\jp1bs_ds_setup.conf.model
	User mapping definition file • *Base_Path*\conf\user_acl\jp1BsUmap.conf • *shared-folder*\jp1base\conf\user_acl\jp1BsUmap.conf
Health check function	Health check definition file • *Base_Path*\conf\jbshc\jbshc.conf • *shared-folder*\jp1base\conf\jbshc\jbshc.conf
	Model file for the common definition settings file (health check function) • *Base_Path*\conf\jbshc\jbshc_setup.conf.model • *shared-folder*\jp1base\conf\jbshc\jbshc_setup.conf.model
	Model file for the common definition settings file (health check function) (for upgrade from version 07-00 or earlier) • *Base_Path*\default\jbshc_com.conf.model • *shared-folder*\jp1base\default\jbshc_com.conf.model
Plugin service	Request transmission settings file • *Base_Path*\conf\plugin\reqforward.conf • *shared-folder*\jp1base\conf\plugin\reqforward.conf
Operation log output function	Operation log definition file • *Base_Path*\conf\jp1bs_baselog_setup.conf • *Base_Path*\conf\jp1bs_baselog_setup.conf.model
Process management	JP1/Base parameter definition file • *Base_Path*\conf\jp1bs_param_V7.conf • *shared-folder*\jp1base\conf\jp1bs_param_V7.conf
	Extended startup process definition file • *Base_Path*\conf\jp1bs_service_0700.conf • *shared-folder*\jp1base\conf\jp1bs_service_0700.conf
Communication settings	jp1hosts definition file • *Base_Path*\conf\jp1hosts • *shared-folder*\jp1base\conf\jp1hosts

Function	File name/folder name
	Communication protocol settings file • *Base_Path*`\conf\physical_ipany.conf` • *Base_Path*`\conf\logical_ipany.conf` • *Base_Path*`\conf\physical_recovery_0651.conf` • *Base_Path*`\conf\logical_recovery_0651.conf` • *Base_Path*`\conf\physical_anyany.conf` • *Base_Path*`\conf\physical_ipip.conf` • *Base_Path*`\conf\logical_ipip.conf` • *shared-folder*`\jp1base\conf\physical_ipany.conf` • *shared-folder*`\jp1base\conf\logical_ipany.conf` • *shared-folder*`\jp1base\conf\physical_recovery_0651.conf` • *shared-folder*`\jp1base\conf\logical_recovery_0651.conf` • *shared-folder*`\jp1base\conf\physical_anyany.conf` • *shared-folder*`\jp1base\conf\physical_ipip.conf` • *shared-folder*`\jp1base\conf\logical_ipip.conf`
	Host access control definition file • *Base_Path*`\conf\jbsdfts\jbsdfts_srv.conf`
Local action function	Local action environment variable file You can specify any folder and any file.
	Local action execution definition file • *Base_Path*`\conf\lcact\jbslcact.conf` • *shared-folder*`\jp1base\conf\lcact\jbslcact.conf`
	Common definition settings file (local action function) • *Base_Path*`\conf\lcact\jp1bs_lcact_setup.conf.model` • *shared-folder*`\jp1base\conf\lcact\jp1bs_lcact_setup.conf.model`

#1: This file or folder is stored in a different folder if you specify another path in the event server index file (`index`).

#2: These files are not used.

#3: This file does not exist unless definition information distribution is used.

(2) List of log files (in Windows)

The table below lists the default log files output by JP1/Base.

Note:

JP1/Base also outputs some internal log files required for program maintenance. There is no need for users to reference or modify these internal log files. You might need to keep these files temporarily for data collection purposes if a system error occurs.

Log type indicates the type of log to which JP1/Base outputs data.

The *File name/folder name* column in the following table indicates the full pathname of the log file when JP1/Base is installed in the default location and the full pathname of the log file when a cluster system is operated.

Max. disk space indicates the maximum space the log file uses on a disk. If there are multiple log files, this column indicates the total.

File changing timing indicates when JP1/Base switches the output log files. Output destinations are changed when the indicated file size is reached or when the indicated event occurs. If there is only one log file, file changing causes that log file to be overwritten. If there are multiple log files and the maximum disk space has been reached, the file with the oldest update date is overwritten.

Table A-3: List of log files (in Windows)

<table>
<tr><th>Log type</th><th>File name/folder name</th><th>Max. disk space</th><th>File changing timing</th></tr>
<tr><td>Process management log</td><td>• <i>Base_Path</i>\log\JBS_SPMD{1|2|3}.log
• <i>shared-folder</i>\jp1base\log\JBS_SPMD{1|2|3}.log</td><td>384 KB</td><td>128 KB</td></tr>
<tr><td></td><td>• <i>Base_Path</i>\log\JBS_SPMD_COMMAND{1|2|3}.log
• <i>shared-folder</i>\jp1base\log\JBS_SPMD_COMMAND{1|2|3}.log</td><td>384 KB</td><td>128 KB</td></tr>
<tr><td></td><td>• <i>Base_Path</i>\log\JBS_SERVICE{1|2|3}.log
• <i>shared-folder</i>\jp1base\log\JBS_SERVICE{1|2|3}.log</td><td>384 KB</td><td>128 KB</td></tr>
<tr><td>Authentication server log</td><td>• <i>Base_Path</i>\log\jbssessionapi.log{1|2|3|4|5|6|7|8}.log#1
• <i>shared-folder</i>\jp1base\log\jbssessionapi.log{1|2|3|4|5|6|7|8}.log#1</td><td>2 MB</td><td>256 KB</td></tr>
<tr><td></td><td>• %ALLUSERSPROFILE%\Hitachi\JP1\jp1_default\JP1Base\log\jbssessionapi.log{1|2|3|4|5|6|7|8}.log#2#3
• %ALLUSERSPROFILE%\Hitachi\JP1\<i>logical-host-name</i>\JP1Base\log\jbssessionapi.log{1|2|3|4|5|6|7|8}.log#2#3</td><td>2 MB</td><td>256 KB</td></tr>
<tr><td></td><td>• <i>Base_Path</i>\log\jbssessionmgr{1|2|3|4|5|6|7|8}.log
• <i>shared-folder</i>\jp1base\log\jbssessionmgr{1|2|3|4|5|6|7|8}.log</td><td>2 MB</td><td>256 KB</td></tr>
<tr><td></td><td>• <i>Base_Path</i>\log\jbssessionmgr_trace{1|2|3|4|5|6|7|8}.log
• <i>shared-folder</i>\jp1base\log\jbssessionmgr_trace{1|2|3|4|5|6|7|8}.log</td><td>2 MB</td><td>256 KB</td></tr>
</table>

Log type	File name/folder name	Max. disk space	File changing timing
Log of the authentication server setting command	• *Base_Path*`\log\JBSSESS{1|2|3|4|5|6|7|8}.log` • *shared-folder*`\jp1base\log\JBSSESS{1|2|3|4|5|6|7|8}.log`	2 MB	256 KB
Log of the environment settings program	• *Base_Path*`\log\jp1bssetup{1|2}.log` • *shared-folder*`\jp1base\log\jp1bssetup{1|2}.log`	128 KB	64 KB
Log of the logical host setting program	• *Base_Path*`\log\jp1hasetup.{log|log.old}`	2,000 KB	1,000 KB
SNMP trap converter log (for definitions)	• *Base_Path*`\log\imevtgw.conf{1|2|3}.log`	3 MB	1 MB
SNMP trap converter log (for monitoring)	• *Base_Path*`\log\imevtgw.log{1|2|3}.log`	15 MB	5 MB
Command execution log (ISAM)#4	• *Base_Path*`\log\COMMAND\ACTISAMLOGV8.DRF` • *shared-folder*`\jp1base\log\COMMAND\ACTISAMLOGV8.DRF`	125 MB#5	125 MB#5
	• *Base_Path*`\log\COMMAND\ACTISAMLOGV8.K01` • *shared-folder*`\jp1base\log\COMMAND\ACTISAMLOGV8.K01`	200 KB#5	None
	• *Base_Path*`\log\COMMAND\ACTISAMLOGV8.KDF` • *shared-folder*`\jp1base\log\COMMAND\ACTISAMLOGV8.KDF`	1 KB	When the command is executed
	• *Base_Path*`\log\COMMAND\CMDISAMLOGV8.DRF` • *shared-folder*`\jp1base\log\COMMAND\CMDISAMLOGV8.DRF`	125 MB#5	125 MB#5
	• *Base_Path*`\log\COMMAND\CMDISAMLOGV8.K01` • *shared-folder*`\jp1base\log\COMMAND\CMDISAMLOGV8.K01`	200 KB#5	None
	• *Base_Path*`\log\COMMAND\CMDISAMLOGV8.KDF` • *shared-folder*`\jp1base\log\COMMAND\CMDISAMLOGV8.KDF`	1 KB	When the command is executed
Common definition information log	• *Base_Path*`\log\JBSCNFCMD\JBSCNFCMD{1|2}.log` • *shared-folder*`\jp1base\log\JBSCNFCMD\JBSCNFCMD{1|2}.log`	128 KB	64 KB

Log type	File name/folder name	Max. disk space	File changing timing
Log of jp1hosts information command	• *Base_Path*`\log\JBSCNFCMD\JBSCOMMCMD{1|2}.log` • *shared-folder*`\jp1base\log\JBSCNFCMD\JBSCOMMCMD{1|2}.log`	128 KB	64 KB
User mapping command log	• *Base_Path*`\log\JBSUMAPCMD\JBSUMAPCMD{1|2}.log` • *shared-folder*`\jp1base\log\JBSUMAPCMD\JBSUMAPCMD{1|2}.log`	128 KB	64 KB
Remote command log[#4]	• *Base_Path*`\log\JCOCMD\jcocmd_result{1|2|3}.log` • *shared-folder*`\jp1base\log\JCOCMD\jcocmd_result{1|2|3}.log`	2,304 KB	768 KB
	• *Base_Path*`\log\JCOCMD\jcocmdapi{1|2|3}.log` • *shared-folder*`\jp1base\log\JCOCMD\jcocmdapi{1|2|3}.log`	2,304 KB	768 KB
	• *Base_Path*`\log\JCOCMD\jcocmdapi_trace{1|2|3}.log` • *shared-folder*`\jp1base\log\JCOCMD\jcocmdapi_trace{1|2|3}.log`	2,304 KB	768 KB
	• *Base_Path*`\log\JCOCMD\jcocmdcom{1|2|3}.log` • *shared-folder*`\jp1base\log\JCOCMD\jcocmdcom{1|2|3}.log`	2,304 KB	768 KB
	• *Base_Path*`\log\JCOCMD\jcocmdcom_trace{1|2|3}.log` • *shared-folder*`\jp1base\log\JCOCMD\jcocmdcom_trace{1|2|3}.log`	2,304 KB	768 KB
	• *Base_Path*`\log\JCOCMD\jcocmdexe{1|2|3}.log` • *shared-folder*`\jp1base\log\JCOCMD\jcocmdexe{1|2|3}.log`	2,304 KB	768 KB
	• *Base_Path*`\log\JCOCMD\jcocmdexe_trace{1|2|3}.log` • *shared-folder*`\jp1base\log\JCOCMD\jcocmdexe_trace{1|2|3}.log`	2,304 KB	768 KB
	• *Base_Path*`\log\JCOCMD\jcocmdrouter{1|2|3}.log` • *shared-folder*`\jp1base\log\JCOCMD\jcocmdrouter{1|2|3}.log`	2,304 KB	768 KB
	• *Base_Path*`\log\JCOCMD\jcocmdrouter_trace{1|2|3}.log` • *shared-folder*`\jp1base\log\JCOCMD\jcocmdrouter_trace{1|2|3}.log`	2,304 KB	768 KB

Log type	File name/folder name	Max. disk space	File changing timing
	• *Base_Path*`\log\JCOCMD\JCOCMDCMD{1|2|3}.log` • *shared-folder*`\jp1base\log\JCOCMD\JCOCMDCMD{1|2|3}.log`	2,304 KB	768 KB
Plug-in service log	• *Base_Path*`\log\plugin\jbsplugin{1|2|3|4|5|6|7|8}.log` • *shared-folder*`\jp1base\log\plugin\jbsplugin{1|2|3|4|5|6|7|8}.log`	2,048 KB	256 KB
	• *Base_Path*`\log\plugin\jbsplugincom_{0|1|2|3|4|5|6|7|8|9}`#6`_{1|2|3|4|5|6|7|8}.log` • *shared-folder*`\jp1base\log\plugin\jbsplugincom_{0|1|2|3|4|5|6|7|8|9}`#6`_{1|2|3|4|5|6|7|8}.log`	20 MB	256 KB
	• *Base_Path*`\log\plugin\jbsplugincmd{1|2|3|4|5|6|7|8}.log` • *shared-folder*`\jp1base\log\plugin\jbsplugincmd{1|2|3|4|5|6|7|8}.log`	2,048 KB	256 KB
	• *Base_Path*`\log\plugin\jbspluginmgrapi{1|2|3|4|5|6|7|8}.log`#1 • *shared-folder*`\jp1base\log\plugin\jbspluginmgrapi{1|2|3|4|5|6|7|8}.log`#1	2,048 KB	256 KB
	• *Base_Path*`\log\plugin\jbsplugincomapi{1|2|3|4|5|6|7|8}.log`#1 • *shared-folder*`\jp1base\log\plugin\jbsplugincomapi{1|2|3|4|5|6|7|8}.log`#1	2,048 KB	256 KB
	• *Base_Path*`\log\plugin\jbsplugincmdapi{1|2|3|4|5|6|7|8}.log` • *shared-folder*`\jp1base\log\plugin\jbsplugincmdapi{1|2|3|4|5|6|7|8}.log`	2,048 KB	256 KB
	• *Base_Path*`\log\plugin\jbspluginhcshm{1|2|3|4|5|6|7|8}.log` • *shared-folder*`\jp1base\log\plugin\jbspluginhcshm{1|2|3|4|5|6|7|8}.log`	2,048 KB	256 KB
	• *Base_Path*`\log\plugin\jbsrmtcmd{1|2|3|4|5|6|7|8}.log`#1 • `%ALLUSERSPROFILE%\Hitachi\JP1\jp1_default\JP1Base\log\plugin\jbsrmtcmd{1|2|3|4|5|6|7|8}.log`#2#3	2,048 KB	256 KB

Log type	File name/folder name	Max. disk space	File changing timing
	• *Base_Path*\log\plugin\jjbspluginremotecmd{1|2|3|4|5|6|7|8}.log • *shared-folder*\jp1base\log\plugin\jbspluginremotecmd{1|2|3|4|5|6|7|8}.log	2,048 KB	256 KB
	• *Base_Path*\log\plugin\jbsrmtapi{1|2|3|4|5|6|7|8}.log[#1] • %ALLUSERSPROFILE%\Hitachi\JP1\jp1_default\JP1Base\log\plugin\jbsrmtapi{1|2|3|4|5|6|7|8}.log[#2][#3]	2,048 KB	256 KB
	• %ALLUSERSPROFILE%\Hitachi\JP1\jp1_default\JP1Base\log\plugin\jbspluginmgrapi{1|2|3|4|5|6|7|8}.log[#2][#3] • %ALLUSERSPROFILE%\Hitachi\JP1\logical-host-name\JP1Base\log\jbspluginmgrapi{1|2|3|4|5|6|7|8}.log[#2][#3]	2,048 KB	256 KB
	• %ALLUSERSPROFILE%\Hitachi\JP1\jp1_default\JP1Base\log\plugin\jbsplugincomapi{1|2|3|4|5|6|7|8}.log[#2][#3] • %ALLUSERSPROFILE%\Hitachi\JP1\logical-host-name\JP1Base\log\jbsplugincomapi{1|2|3|4|5|6|7|8}.log[#2][#3]	2,048 KB	256 KB
Configuration management log[#4]	• *Base_Path*\log\route\JBSRT{1|2|3}.log • *shared-folder*\jp1base\log\route\JBSRT{1|2|3}.log	384 KB	128 KB
Start sequence control log	• *Base_Path*\log\boot\ContServ{1|2}.log	128 KB	64 KB
Event log trap trace log	• *Base_Path*\log\ntevtrap\trace{1|2}.log	1,024 KB	512 KB
Log of the health check function (local host monitoring)	• *Base_Path*\log\jbshc\jbshc{1|2|3|4|5|6|7|8}.log • *shared-folder*\jp1base\log\jbshc\jbshc{1|2|3|4|5|6|7|8}.log	2,048 KB	256 KB
Log of the health check function (remote host monitoring)	• *Base_Path*\log\jbshc\jbshchost{1|2|3|4|5|6|7|8}.log • *shared-folder*\jp1base\log\jbshc\jbshchost{1|2|3|4|5|6|7|8}.log	2,048 KB	256 KB

Log type	File name/folder name	Max. disk space	File changing timing
Health check command log	• *Base_Path*\log\jbshc\jbshcstatus{1|2|3|4|5|6|7|8}.log • *shared-folder*\jp1base\log\jbshc\jbshcstatus{1|2|3|4|5|6|7|8}.log	2,048 KB	256 KB
Log of the health check API	• *Base_Path*\log\jbshc\jbshcapi{1|2|3|4|5|6|7|8}.log • *shared-folder*\jp1base\log\jbshc\jbshcapi{1|2|3|4|5|6|7|8}.log	2,048 KB	256 KB
Log of the command for deleting shared memory used by the health check function	• *Base_Path*\log\jbshc\jbshcshmctl{1|2|3|4|5|6|7|8}.log • *shared-folder*\jp1base\log\jbshc\jbshcshmctl{1|2|3|4|5|6|7|8}.log	2,048 KB	256 KB
Application error log	• *Base_Path*\log\jbsdump.log	5 MB	5 MB
Operation log	• *Base_Path*\log\BASE\base_log[{1|2|3|4|5|6|7|8|9|10|11|12|13|14|15|16}].log	68 MB#7	1,024 KB#7#8
Trace log for the event setting, centralized management, and acquisition command	• *Base_Path*\sys\tmp\event\servers\default\jevdef_get.{000|001|002}#9 • *shared-folder*\jp1base\event\jevdef_get.{000|001|002}#9	64 KB	When the command is executed
Trace log for event setting, centralized management, and distribution command	• *Base_Path*\sys\tmp\event\servers\default\jevdef_distrib.{000|001|002}#9 • *shared-folder*\jp1base\event\jevdef_distrib.{000|001|002}#9	64 KB	When the command is executed
Trace log of the event service	• *Base_Path*\sys\tmp\event\servers\default\trace.{000|001|002|003|004}#9, #10 • *shared-folder*\jp1base\event\trace.{000|001|002|003|004}#9, #10	5 MB#10	When the event service starts
	• *Base_Path*\sys\tmp\event\servers\default\imevterr.{000|001|002|003|004}#9, #10 • *shared-folder*\jp1base\event\imevterr.{000|001|002|003|004}#9, #10	5 MB#10	When the event service starts

Log type	File name/folder name	Max. disk space	File changing timing
Transfer error log of the event service	• *Base_Path*\sys\tmp\event\servers\default\fwderr.{000|001|002|003|004}[#9, #10] • *shared-folder*\jp1base\event\fwderr.{000|001|002|003|004} [#9, #10]	5 MB[#10]	When the event service starts
Error log of the event service	• *Base_Path*\sys\tmp\event\servers\default\error.{000|001|002|003|004}[#9, #10] • *shared-folder*\jp1base\event\error.{000|001|002|003|004} [#9, #10]	2,500 KB[#10]	When the event service starts
Log of the event service API.	• *Base_Path*\sys\tmp\event\IMEvapi.{000|001|002|003|004}[#1, #11] • %ALLUSERSPROFILE%\Hitachi\JP1\jp1_default\JP1Base\log\event\IMEvapi.{000|001|002|003|004}[#3, #11, #12]	5 MB[#11]	1 MB[#11]
Socket communication connection log for compatibility with JP1/AJS	• *Base_Path*\sys\tmp\event\servers\default\evtrace.dir\{ajevconn.csv|ajevconn.bak}[#9]	2,000 lines[#13]	1,000 lines
Log of JP1/SES-format event transmission and reception for compatibility with JP1/AJS	• *Base_Path*\sys\tmp\event\servers\default\evtrace.dir\{ajevtrap.csv|ajevtrap.bak}[#9]	2,000 lines[#13]	1,000 lines
Error log of the log file trap	• *Base_Path*\sys\tmp\event\logtrap\.errorfile.*ID-number*	A few hundred bytes[#14]	When the log file trap starts
Log of the log file trap	• *Base_Path*\sys\tmp\event\logtrap\jevtraplog\jevtraplog.{000|001|002|003|004}	5 MB[#15]	1 MB[#15]
Installation log	• *Windows-installation-folder*\Temp\HITACHI_JP1_INST_LOG\jp1base_inst{1|2|3|4|5}.log	128 KB	At installation
Trace log for inter-process communication	• *Base_Path*\log\JBSCOM\jbscomd {1|2|3|4}.log • *shared-folder*\jp1base\log\JBSCOM\jbscomd{1|2|3|4}.log	4 MB	1 MB
	• *Base_Path*\log\JBSCOM\jbscomd_api {1|2|3|4}.log • *shared-folder*\jp1base\log\JBSCOM\jbscomd_api{1|2|3|4}.log	4 MB	1 MB

Log type	File name/folder name	Max. disk space	File changing timing
	• *Base_Path*\log\JBSCOM\jbscomd_ses{1|2|3|4}.log • *shared-folder*\jp1base\log\JBSCOM\jbscomd_ses{1|2|3|4}.log	4 MB	1 MB
	• *Base_Path*\log\JBSCOM\jbscomd_snd{1|2|3|4}.log • *shared-folder*\jp1base\log\JBSCOM\jbscomd_snd{1|2|3|4}.log	4 MB	1 MB
	• *Base_Path*\log\JBSCOM\jbscomd_rcv{1|2|3|4}.log • *shared-folder*\jp1base\log\JBSCOM\jbscomd_rcv{1|2|3|4}.log	4 MB	1 MB
	• *Base_Path*\log\JBSCOM\command {1|2|3|4}.log • *shared-folder*\jp1base\log\JBSCOM\command{1|2|3|4}.log	4 MB	1 MB
Error log of the command for collecting operating information	• *Base_Path*\log\jbsopi\jbsopi_cmd{1|2|3|4|5}.log	5 MB	1 MB
Log for the operating information API	• *Base_Path*\log\jbsopi\jbsopi_api{1|2|3|4|5}.log • *shared-folder*\jp1base\log\jbsopi\jbsopi_api{1|2|3|4|5}.log	5 MB	1 MB
Service management control log	• *Base_Path*\log\jbssrvmgr\jbssrvmgr{1|2|3|4}.log • *shared-folder*\jp1base\log\jbssrvmgr\jbssrvmgr{1|2|3|4}.log	4 MB	1 MB
Trace log of the service management control	• *Base_Path*\log\jbssrvmgr\jbssrvmgr_trace{1|2|3|4}.log • *shared-folder*\jp1base\log\jbssrvmgr\jbssrvmgr_trace{1|2|3|4}.log	4 MB	1 MB
Log of the service management control API	• *Base_Path*\log\jbssrvmgr\jbssrvmgr_api{1|2|3|4}.log • *shared-folder*\jp1base\log\jbssrvmgr\jbssrvmgr_api{1|2|3|4}.log	4 MB	1 MB

Log type	File name/folder name	Max. disk space	File changing timing
Local action execution log	• *Base_Path*`\log\lcact\localact{1-n}`#16`.log` • *shared-folder*`\jp1base\log\lcact\localact{1-n}`#16`.log`	1,024 KB#16	256 KB#16
Local action log	• *Base_Path*`\log\jbslcact\jbslcact{1|2|3|4|5|6|7|8}.log` • *shared-folder*`\jp1base\log\jbslcact\jbslcact{1|2|3|4|5|6|7|8}.log`	2,048 KB	256 KB
	• *Base_Path*`\log\jbslcact\jbslcact_list{1|2|3|4|5|6|7|8}.log` • *shared-folder*`\jp1base\log\jbslcact\jbslcact_list{1|2|3|4|5|6|7|8}.log`	2,048 KB	256 KB
	• *Base_Path*`\log\jbslcact\jbslcact_cancel{1|2|3|4|5|6|7|8}.log` • *shared-folder*`\jp1base\log\jbslcact\jbslcact_cancel{1|2|3|4|5|6|7|8}.log`	2,048 KB	256 KB

#1: For Windows XP Professional or Windows Server 2003.

#2: The value set in the environment variable `%ALLUSERSPROFILE%` at installation is used.

#3: For Windows Vista or Windows Server 2008

#4: Log file for JP1/IM - Manager

#5: You can use the `jcocmddef` command of JP1/IM - Manager with the `-record` option specified to change this to a value within the range below.

- If the number of the records is 1 (`-record 1`)

  DRF file: 7 KB, K01 file: 4 KB

- If the number of the records is 20,000 (default value)

  DRF file: 125 MB, K01 file: 200 KB

- If the number of the records is 196,600 (`-record 196600`)

  DRF file: 1.2 GB, K01 file: 2 MB

#6: Indicates a `jbsplugincom` process identification number.

#7: You can use the operation log definition file (`jp1bs_baselog_setup.conf`) to change the number of files and the maximum disk space. For details on the range of specifiable values, see *K.5 Settings for outputting operation logs*.

#8: You can specify whether to automatically switch files at JP1/Base startup in the operation log definition file (`jp1bs_baselog_setup.conf`).

#9: This file or folder is stored in a different folder if you specify another path in the event server index file (index).

#10: You can change the number of files and the maximum disk space using the event server settings file (conf). For details on the range of specifiable values, see *Event server settings file* in *14. Definition Files*.

#11: You can use the API settings (api) file to change the number of files and the maximum disk space. For details on the range of specifiable values, see *API settings file* in *14. Definition Files*.

#12: The value set in the environment variable %ALLUSERSPROFILE% at execution is used.

#13: One line equals approximately 100 bytes.

#14: A file is created when the log file trap starts, and is deleted when the log file trap terminates normally. If an error occurs, the file remains when the log file trap terminates. If the log file trap generates frequent errors, there will be a large number of error files. Therefore, you need to delete unnecessary error files.

#15: You can change the number of files and the maximum disk space they occupy in the log information definition file (jevlogd.conf). For details on the range of specifiable values, see *Log information definition file* in *14. Definition Files*.

#16: You can use the common definition settings file (local action function) to change the number of files and the maximum disk space. For details on the range of specifiable values, see *Common definition settings file (local action function)* in *14. Definition Files*.

A.2 In UNIX

Table A-4: List of files and directories of JP1/Base (in UNIX)

Contents	File name/directory name
Command storage directory	/opt/jp1base/bin/
Environment setting directory#1	/etc/opt/jp1base/conf/ *shared-directory*/jp1base/conf/
Language type settings file	/etc/opt/jp1base/conf/jp1bs_param.conf *shared-directory*/jp1base/conf/jp1bs_param.conf
Configuration definition file	/etc/opt/jp1base/conf/route/jbs_route.conf *shared-directory*/jp1base/conf/route/jbs_route.conf
JP1/IM function header file	/opt/jp1base/include/JevApi.h
Log directory#2	/var/opt/jp1base/log/ *shared-directory*/jp1base/log/
Directory for plug-in	/opt/jp1base/plugin/

Contents	File name/directory name
Directory for storing operating information	`/var/opt/jp1base/sys/OPI/` *shared-directory*`/jp1base/sys/OPI/`
Event DB storage directory#3	`/var/opt/jp1base/sys/event/servers/`#4 *shared-directory*`/event/`#4
Log and temporary directory#2	`/var/opt/jp1base/sys/tmp/event/servers/`#4
	Event ID save file for JP1/SES compatibility • `/var/opt/jp1base/sys/tmp/event/servers/default/ereb.backup`#4
	Internal action file for the log file trapping function • `/var/opt/jp1base/sys/tmp/event/logtrap/conftbl.`*ID-number*
Tool directory	`/opt/jp1base/tools/`
	Data collection tool sample script file • `/opt/jp1base/tools/jbs_log.sh`
	Function sample source file that issues and collects JP1 events • `/opt/jp1base/tools/event/receiver.c` • `/opt/jp1base/tools/event/sender.c`
	AR System linkage sample script file • `/opt/jp1base/tools/helpdesk/register_ars.sh`
Integrated trace log directory	`/var/opt/hitachi/HNTRLib2/spool/`
Directory for compatibility with JP1/SES	`/usr/bin/jp1_ses/`, `/usr/lib/jp1_ses/` and `/usr/lib/jp1_ses/sys/`
Temporary directory for compatibility with JP1/SES	`/usr/tmp/jp1_ses/`
Message catalog directory for compatibility with JP1/SES	`/usr/lib/jp1_ses/nls/`
Log directory for compatibility with JP1/SES	`/usr/lib/jp1_ses/log/` and `/tmp/` (*file-beginning-with-.JP1_SES*)

#1: For details on definition files, see *A.2(1) List of definition files (in UNIX)*.

#2: For details on log files, see *A.2(2) List of log files (in UNIX)*.

#3: For details on event database file name, see *1.4.2 Event database*.

#4: If you specify a different path in the event server index file (`index`), the log will be stored in a different directory.

(1) List of definition files (in UNIX)

The definition files used in JP1/Base are listed below.

Table A-5: List of definition files (in UNIX)

Function	File name/directory name
Event service	Event server index file • `/etc/opt/jp1base/conf/event/index`
	Event server settings file • `/etc/opt/jp1base/conf/event/servers/default/conf`#1 • *shared-directory*`/event/conf`#1
	Forwarding settings file • `/etc/opt/jp1base/conf/event/servers/default/forward`#1 • *shared-directory*`/event/forward`#1
	API settings file • `/etc/opt/jp1base/conf/event/api`
	Configuration definition file for JP1/SES compatibility • `/var/opt/jp1base/sys/tmp/event/servers/default/jpevent.conf`
Event conversion	Log file trap definition file You can specify any directory and any file.
	Log information definition file • `/etc/opt/jp1base/conf/event/jevlogd.conf`
	Action definition file for converting the SNMP traps • `/etc/opt/jp1base/conf/evtgw/imevtgw.conf` • *shared-directory*`/jp1base/conf/evtgw/imevtgw.conf`#2
	Filter file for converting SNMP traps • `/etc/opt/jp1base/conf/evtgw/snmpfilter.conf` • *shared-directory*`/jp1base/conf/evtgw/snmpfilter.conf`#2
Event service definition information collection and distribution	Distribution definition file (forward setting file) • `/etc/opt/jp1base/conf/event/servers/default/[jev_forward.conf` | *any-file*`]`#3 • *shared-directory*`/event/[jev_forward.conf` | *any-file*`]`#3
	Distribution definition file (log file trap definition file) • `/etc/opt/jp1base/conf/[jev_logtrap.conf` | *any-file*`]`#3
	Distribution definition file (event log trap definition file) • `/etc/opt/jp1base/conf/event/[jev_ntevent.conf` | *any-file*`]`#3

Function	File name/directory name
User management	User permission level file • `/etc/opt/jp1base/conf/user_acl/JP1_UserLevel` • *shared-directory*`/jp1base/conf/user_acl/JP1_UserLevel`
	User mapping definition file • `/etc/opt/jp1base/conf/user_acl/jp1BsUmap.conf` • *shared-directory/*`jp1base/conf/user_acl/jp1BsUmap.conf`
Health check function	Health check definition file • `/etc/opt/jp1base/conf/jbshc/jbshc.conf` • *shared-directory*`/jp1base/conf/jbshc/jbshc.conf`
	Model file for the common definition settings file (health check function) • `/etc/opt/jp1base/conf/jbshc/jbshc_setup.conf.model` • *shared-directory*`/jp1base/conf/jbshc/jbshc_setup.conf.model`
	Model file for the common definition settings file (health check function) (for upgrade from version 07-00 or earlier) • `/etc/opt/jp1base/default/jbshc_com.conf.model` • *shared-directory*`/jp1base/default/jbshc_com.conf.model`
Plugin service	Request transmission settings file • `/etc/opt/jp1base/conf/plugin/reqforward.conf` • *shared-directory*`/jp1base/conf/plugin/reqforward.conf`
Operation log output function	Operation log definition file • `/etc/opt/jp1base/conf/jp1bs_baselog_setup.conf` • `/etc/opt/jp1base/conf/jp1bs_baselog_setup.conf.model`
Process management	JP1/Base parameter definition file • `/etc/opt/jp1base/conf/jp1bs_param_V7.conf` • *shared-directory*`/jp1base/conf/jp1bs_param_V7.conf`
	Extended startup process definition file • `/etc/opt/jp1base/conf/jp1bs_service_0700.conf` • *shared-directory*`/jp1base/conf/jp1bs_service_0700.conf`
Communication settings	`jp1hosts` definition file • `/etc/opt/jp1base/conf/jp1hosts` • *shared-directory*`/jp1base/conf/jp1hosts`

Function	File name/directory name
	Communication protocol settings file • `/etc/opt/jp1base/conf/physical_ipany.conf` • `/etc/opt/jp1base/conf/logical_ipany.conf` • `/etc/opt/jp1base/conf/physical_recovery_0651.conf` • `/etc/opt/jp1base/conf/logical_recovery_0651.conf` • `/etc/opt/jp1base/conf/physical_anyany.conf` • `/etc/opt/jp1base/conf/physical_ipip.conf` • `/etc/opt/jp1base/conf/logical_ipip.conf` • *shared-directory*`/jp1base/conf/physical_ipany.conf` • *shared-directory*`/jp1base/conf/logical_ipany.conf` • *shared-directory*`/jp1base/conf/physical_recovery_0651.conf` • *shared-directory*`/jp1base/conf/logical_recovery_0651.conf` • *shared-directory*`/jp1base/conf/physical_anyany.conf` • *shared-directory*`/jp1base/conf/physical_ipip.conf` • *shared-directory*`/jp1base/conf/logical_ipip.conf`
	Host access control definition file • `/etc/opt/jp1base/conf/jbsdfts/jbsdfts_srv.conf`
Local action function	Local action environment variable file You can specify any folder and any file.
	Local action execution definition file • `/etc/opt/jp1base/conf/lcact/jbslcact.conf` • *shared-directory*`/jp1base/conf/lcact/jbslcact.conf`
	Common definition settings file (local action function) • `/etc/opt/jp1base/conf/lcact/jp1bs_lcact_setup.conf.model` • *shared-directory*`/jp1base/conf/lcact/jp1bs_lcact_setup.conf.model`

#1: If you specify a different path in the event server index file (`index`), the log will be stored in a different directory.

#2: These files are not used.

#3: This file does not exist unless definition information distribution is used.

(2) List of log files (in UNIX)

The table below lists the default log files output by JP1/Base.

Note:

JP1/Base also outputs some internal log files required for program maintenance. There is no need for users to reference or modify these internal log files. You might need to keep these files temporarily for data collection purposes if a system error occurs.

Log type indicates the type of log to which JP1/Base outputs data.

The *File name/folder name* column in the following table indicates the full pathname of the log file when JP1/Base is installed in the default location and the full pathname of the log file when a cluster system is operated.

Max. disk space indicates the maximum space the log file uses on a disk. If there are multiple log files, this column indicates the total.

File changing timing indicates when JP1/Base switches the output log files. Output destinations are changed when the indicated file size is reached or when the indicated event occurs. If there is only one log file, file changing causes that log file to be overwritten. If there are multiple log files and the maximum disk space has been reached, the file with the oldest update date is overwritten.

Table A-6: List of log files (in UNIX)

Log type	File name/directory name	Max. disk space	File changing timing
JP1/Base startup log	• `/var/opt/jp1base/log/JBS_START/jbs_start.log[.old]` • *shared-directory*`/jp1base/log/JBS_START/jbs_start.log[.old]`	128 KB	When the command is executed
JP1/Base shutdown log	• `/var/opt/jp1base/log/JBS_STOP/jbs_stop.log[.old]` • *shared-directory*`/jp1base/log/JBS_STOP/jbs_stop.log[.old]`	128 KB	When the command is executed
Process management log	• `/var/opt/jp1base/log/JBS_SPMD{1|2|3}.log` • *shared-directory*`/jp1base/log/JBS_SPMD{1|2|3}.log`	384 KB	128 KB
	• `/var/opt/jp1base/log/JBS_SPMD_COMMAND{1|2|3}.log` • *shared-directory*`/jp1base/log/JBS_SPMD_COMMAND{1|2|3}.log`	384 KB	128 KB
Authentication server log	• `/var/opt/jp1base/log/jbssessionapi.log{1|2|3|4|5|6|7|8}.log` • *shared-directory*`/jp1base/log /jbssessionapi.log{1|2|3|4|5|6|7|8}.log`	2 MB	256 KB
	• `/var/opt/jp1base/log/jbssessionmgr{1|2|3|4|5|6|7|8}.log` • *shared-directory*`/jp1base/log/jbssessionmgr{1|2|3|4|5|6|7|8}.log`	2 MB	256 KB

Log type	File name/directory name	Max. disk space	File changing timing
	• /var/opt/jp1base/log/jbssessionmgr_trace{1|2|3|4|5|6|7|8}.log • *shared-directory*/jp1base/log/jbssessionmgr_trace{1|2|3|4|5|6|7|8}.log	2 MB	256 KB
Log of the authentication server setting command	• /var/opt/jp1base/log/JBSSESS{1|2|3|4|5|6|7|8}.log • *shared-directory*/jp1base/log/JBSSESS{1|2|3|4|5|6|7|8}.log	2 MB	256 KB
SNMP trap converter log (for definitions)	• /var/opt/jp1base/log/imevtgw.conf{1|2|3}.log	3 MB	1 MB
SNMP trap converter log (for monitoring)	• /var/opt/jp1base/log/imevtgw.log{1|2|3}.log	15 MB	5 MB
Command execution log (ISAM)#1	• /var/opt/jp1base/log/COMMAND/actisamlogv8.DAT • *shared-directory*/jp1base/log/COMMAND/actisamlogv8.DAT	125 MB#2	125 MB#2
	• /var/opt/jp1base/log/COMMAND/actisamlogv8.K01 • *shared-directory*/jp1base/log/COMMAND/actisamlogv8.K01	200 KB#2	None
	• /var/opt/jp1base/log/COMMAND/actisamlogv8.DEF • *shared-directory*/jp1base/log/COMMAND/actisamlogv8.DEF	1 KB	When the command is executed
	• /var/opt/jp1base/log/COMMAND/cmdisamlogv8.DAT • *shared-directory*/jp1base/log/COMMAND/cmdisamlogv8.DAT	125 MB#2	125 MB#2
	• /var/opt/jp1base/log/COMMAND/cmdisamlogv8.K01 • *shared-directory*/jp1base/log/COMMAND/cmdisamlogv8.K01	200 KB#2	None
	• /var/opt/jp1base/log/COMMAND/cmdisamlogv8.DEF • *shared-directory*/jp1base/log/COMMAND/cmdisamlogv8.DEF	1 KB	When the command is executed

Log type	File name/directory name	Max. disk space	File changing timing
Common definition information log	• `/var/opt/jp1base/log/JBSCNFCMD/JBSCNFCMD{1|2}.log` • *shared-directory*`/jp1base/log/JBSCNFCMD/JBSCNFCMD{1|2}.log`	128 KB	64 KB
Log of jp1hosts information command	• `/var/opt/jp1base/log/JBSCNFCMD/JBSCOMMCMD{1|2}.log` • *shared-directory*`/jp1base/log/JBSCNFCMD/JBSCOMMCMD{1|2}.log`	128 KB	64 KB
User mapping command log	• `/var/opt/jp1base/log/JBSUMAPCMD/JBSUMAPCMD{1|2}.log` • *shared-directory*`/jp1base/log/JBSUMAPCMD/JBSUMAPCMD{1|2}.log`	128 KB	64 KB
Remote command log[#1]	• `/var/opt/jp1base/log/JCOCMD/jcocmd_result{1|2|3}.log` • *shared-directory*`/jp1base/log/JCOCMD/jcocmd_result{1|2|3}.log`	2,304 KB	768 KB
	• `/var/opt/jp1base/log/JCOCMD/jcocmdapi{1|2|3}.log` • *shared-directory*`/jp1base/log/JCOCMD/jcocmdapi{1|2|3}.log`	2,304 KB	768 KB
	• `/var/opt/jp1base/log/JCOCMD/jcocmdapi_trace{1|2|3}.log` • *shared-directory*`/jp1base/log/JCOCMD/jcocmdapi_trace{1|2|3}.log`	2,304 KB	768 KB
	• `/var/opt/jp1base/log/JCOCMD/jcocmdcmc{1|2|3}.log` • *shared-directory*`/jp1base/log/JCOCMD/jcocmdcmc{1|2|3}.log`	2,304 KB	768 KB
	• `/var/opt/jp1base/log/JCOCMD/jcocmdcmc_trace{1|2|3}.log` • *shared-directory*`/jp1base/log/JCOCMD/jcocmdcmc_trace{1|2|3}.log`	2,304 KB	768 KB
	• `/var/opt/jp1base/log/JCOCMD/jcocmdcom{1|2|3}.log` • *shared-directory*`/jp1base/log/JCOCMD/jcocmdcom{1|2|3}.log`	2,304 KB	768 KB

Log type	File name/directory name	Max. disk space	File changing timing
	• `/var/opt/jp1base/log/JCOCMD/jcocmdcom_trace{1|2|3}.log` • *shared-directory*`/jp1base/log/JCOCMD/jcocmdcom_trace{1|2|3}.log`	2,304 KB	768 KB
	• `/var/opt/jp1base/log/JCOCMD/jcocmdexe{1|2|3}.log` • *shared-directory*`/jp1base/log/JCOCMD/jcocmdexe{1|2|3}.log`	2,304 KB	768 KB
	• `/var/opt/jp1base/log/JCOCMD/jcocmdexe_trace{1|2|3}.log` • *shared-directory*`/jp1base/log/JCOCMD/jcocmdexe_trace{1|2|3}.log`	2,304 KB	768 KB
	• `/var/opt/jp1base/log/JCOCMD/jcocmdrouter{1|2|3}.log` • *shared-directory*`/jp1base/log/JCOCMD/jcocmdrouter{1|2|3}.log`	2,304 KB	768 KB
	• `/var/opt/jp1base/log/JCOCMD/jcocmdrouter_trace{1|2|3}.log` • *shared-directory*`/jp1base/log/JCOCMD/jcocmdrouter_trace{1|2|3}.log`	2,304 KB	768 KB
	• `/var/opt/jp1base/log/JCOCMD/JCOCMDCMD{1|2|3}.log` • *shared-directory*`/jp1base/log/JCOCMD/JCOCMDCMD{1|2|3}.log`	2,304 KB	768 KB
Plug-in service log	• `var/opt/jp1base/log/plugin/jbsplugin{1|2|3|4|5|6|7|8}.log` • *shared-directory*`/jp1base/log/plugin/jbsplugin{1|2|3|4|5|6|7|8}.log`	2,048 KB	256 KB
	• `/var/opt/jp1base/log/plugin/jbsplugincom_{0|1|2|3|4|5|6|7|8|9}`#3`_{1|2|3|4|5|6|7|8}.log` • *shared-directory*`/jp1base/log/plugin/jbsplugincom_{0|1|2|3|4|5|6|7|8|9}`#3`_{1|2|3|4|5|6|7|8}.log`	20 MB	256 KB
	• `/var/opt/jp1base/log/plugin/jbsplugincmd{1|2|3|4|5|6|7|8}.log` • *shared-directory*`/jp1base/log/plugin/jbsplugincmd{1|2|3|4|5|6|7|8}.log`	2,048 KB	256 KB

Log type	File name/directory name	Max. disk space	File changing timing
	• `/var/opt/jp1base/log/plugin/jbspluginmgrapi{1|2|3|4|5|6|7|8}.log` • *shared-directory*`/jp1base/log/plugin/jbspluginmgrapi{1|2|3|4|5|6|7|8}.log`	2,048 KB	256 KB
	• `/var/opt/jp1base/log/plugin/jbsplugincomapi{1|2|3|4|5|6|7|8}.log` • *shared-directory*`/jp1base/log/plugin/jbsplugincomapi{1|2|3|4|5|6|7|8}.log`	2,048 KB	256 KB
	• `/var/opt/jp1base/log/plugin/jbsplugincmdapi{1|2|3|4|5|6|7|8}.log` • *shared-directory*`/jp1base/log/plugin/jbsplugincmdapi{1|2|3|4|5|6|7|8}.log`	2,048 KB	256 KB
	• `/var/opt/jp1base/log/plugin/jbspluginhcshm{1|2|3|4|5|6|7|8}.log` • *shared-directory*`/jp1base/log/plugin/jbspluginhcshm{1|2|3|4|5|6|7|8}.log`	2,048 KB	256 KB
	• `/var/opt/jp1base/log/plugin/jbsrmtcmd{1|2|3|4|5|6|7|8}.log`	2,048 KB	256 KB
	• `/var/opt/jp1base/log/plugin/jbspluginremotecmd{1|2|3|4|5|6|7|8}.log` • *shared-directory*`/jp1base/log/plugin/jbspluginremotecmd{1|2|3|4|5|6|7|8}.log`	2,048 KB	256 KB
	• `/var/opt/jp1base/log/plugin/jbsrmtapi{1|2|3|4|5|6|7|8}.log`	2,048 KB	256 KB
Installation log	• `/tmp/HITACHI_JP1_INST_LOG/jp1base_inst{1|2|3|4|5}.log`	128 KB	At installation
Setup log	• `/var/opt/jp1base/log/JBS_SETUP/jbs_setup.log`	128 KB	At setup
Configuration management log#1	• `/var/opt/jp1base/log/route/JBSRT{1|2|3}.log` • *shared-directory*`/jp1base/log/route/JBSRT{1|2|3}.log`	384 KB	128 KB
Log of the health check function (local host monitoring)	• `/var/opt/jp1base/log/jbshc/jbshc{1|2|3|4|5|6|7|8}.log` • *shared-directory*`/jp1base/log/jbshc/jbshc{1|2|3|4|5|6|7|8}.log`	2,048 KB	256 KB

Log type	File name/directory name	Max. disk space	File changing timing
Log of the health check function (remote host monitoring)	• `/var/opt/jp1base/log/jbshc/jbshchost{1|2|3|4|5|6|7|8}.log` • *shared-directory*`/jp1base/log/jbshc/jbshchost{1|2|3|4|5|6|7|8}.log`	2,048 KB	256 KB
Log of the health check commands	• `/var/opt/jp1base/log/jbshc/jbshcstatus{1|2|3|4|5|6|7|8}.log` • *shared-directory*`/jp1base/log/jbshc/jbshcstatus{1|2|3|4|5|6|7|8}.log`	2,048 KB	256 KB
Log of the health check API	• `/var/opt/jp1base/log/jbshc/jbshcapi{1|2|3|4|5|6|7|8}.log` • *shared-directory*`/jp1base/log/jbshc/jbshcapi{1|2|3|4|5|6|7|8}.log`	2,048 KB	256 KB
Log of the command for deleting shared memory used by the health check function	• `/var/opt/jp1base/log/jbshc/jbshcshmctl{1|2|3|4|5|6|7|8}.log` • *shared-directory*`/jp1base/log/jbshc/jbshcshmctl{1|2|3|4|5|6|7|8}.log`	2,048 KB	256 KB
Operation log	• `/var/opt/jp1base/log/BASE/base_log[{1|2|3|4|5|6|7|8|9|10|11|12|13|14|15|16}].log`	68 MB#4	1,024 KB#4#5
Trace log for the event setting, centralized management, and acquisition command	• `/var/opt/jp1base/sys/tmp/event/servers/default/jevdef_get.{000|001|002}`#6 • *shared-directory*`/event/jevdef_get.{000|001|002}`#6	64 KB	When the command is executed
Trace log for event setting, centralized management, and distribution command	• `/var/opt/jp1base/sys/tmp/event/servers/default/jevdef_distrib.{000|001|002}`#6 • *shared-directory*`/event/jevdef_distrib.{000|001|002}`#6	64 KB	When the command is executed
Trace log of the event service	• `/var/opt/jp1base/sys/tmp/event/servers/default/trace.{000|001|002|003|004}`#6, #7 • *shared-directory*`/event/trace.{000|001|002|003|004}`#6, #7	5 MB#7	When the event service starts
	• `/var/opt/jp1base/sys/tmp/event/servers/default/imevterr.{000|001|002|003|004}`#6, #7 • *shared-directory*`/event/imevterr.{000|001|002|003|004}`#6, #7	5 MB#7	When the event service starts

Log type	File name/directory name	Max. disk space	File changing timing
	• `/var/opt/jp1base/sys/tmp/event/servers/default/imses.{log|old}`[#6] • *shared-directory*`/event/imses.{log|old}` [#6]	2 MB	When the event service starts
Transfer error log of the event service	• `/var/opt/jp1base/sys/tmp/event/servers/default/fwderr.{000|001|002|003|004}`[#6, #7] • *shared-directory*`/event/fwderr.{000|001|002|003|004}`[#6, #7]	5 MB[#7]	When the event service starts
Error log of the event service	• `/var/opt/jp1base/sys/tmp/event/servers/default/error.{000|001|002|003|004}`[#6, #7] • *shared-directory*`/event/error.{000|001|002|003|004}`[#6, #7]	2,500 KB[#7]	When the event service starts
Log of the event service API.	• `/var/opt/jp1base/sys/tmp/event/IMEvapi.{000|001|002|003|004}`[#8]	5 MB[#8]	1 MB[#8]
JP1/SES compatible process startup log	• `/var/opt/jp1base/sys/tmp/event/servers/default/result.txt`	A few dozen bytes	When the event service starts
Error information generated during connection from the event registration/ reception process to the event service	• `/var/opt/jp1base/sys/tmp/event/refuse.txt`	A few hundred bytes	When an error occurs during event service connection
Error information generated during communication between the event registration/ reception process and the event service	• `/var/opt/jp1base/sys/tmp/event/sock.log`	1 KB	1 KB
Local server error log for compatibility with JP1/SES	• `/usr/lib/jp1_ses/log/.JP1_SES_dmain.log` (for other than HP-UX) • `/var/opt/jp1_ses/log/.JP1_SES_dmain.log` (for HP-UX)	1 KB	When the event service starts
Manager log for compatibility with JP1/SES	• `/usr/lib/jp1_ses/log/.JP1_SES_MNG.log` (for other than HP-UX) • `/var/opt/jp1_ses/log/.JP1_SES_MNG.log` (for HP-UX)	16 KB	When the event service starts

Log type	File name/directory name	Max. disk space	File changing timing
Reception process error log for compatibility with JP1/SES	• `/usr/lib/jp1_ses/log/.JP1_SES_RVC.log` (for other than HP-UX) • `/var/opt/jp1_ses/log/.JP1_SES_RVC.log` (for HP-UX)	16 KB	When the event service starts
Error log of the reception process manager for compatibility with JP1/SES	• `/usr/lib/jp1_ses/log/.JP1_SES_RVM.log` (for other than HP-UX) • `/var/opt/jp1_ses/log/.JP1_SES_RVM.log` (for HP-UX)	16 KB	When the event service starts
Transmission process error log for compatibility with JP1/SES	• `/usr/lib/jp1_ses/log/.JP1_SES_SND.log` (for other than HP-UX) • `/var/opt/jp1_ses/log/.JP1_SES_SND.log` (for HP-UX)	16 KB	When the event service starts
Monitoring process error log for compatibility with JP1/SES	• `/usr/lib/jp1_ses/log/.JP1_SES_WAC.log` (for other than HP-UX) • `/var/opt/jp1_ses/log/.JP1_SES_WAC.log` (for HP-UX)	16 KB	When the event service starts
Start command error log for compatibility with JP1/SES	• `/tmp/.JP1_SES_startlog` *process-ID*	A few hundred bytes#9	When the subsystem for JP1/SES compatibilit y starts
Stop command error log for compatibility with JP1/SES	• `/tmp/.JP1_SES_stoperr` *process-ID*	A few hundred bytes#10	When the subsystem for JP1/SES compatibilit y stops
Error log of the log file trap	• `/var/opt/jp1base/sys/tmp/event/logtrap/.errorfile.`*ID-number*	A few hundred bytes#11	When the log file trap starts
Log of the log file trap	• `/var/opt/jp1base/sys/tmp/event/logtrap/jevtraplog/jevtraplog.{000|001|002|003|004}`	5 MB#12	1 MB#12
Trace log of the `jbs_killall.cluster` command#13	• *shared-directory*`/jp1base/log/jbs_killall.cluster[.{1|2|3|4}].log`	256 KB	When the command is executed

Log type	File name/directory name	Max. disk space	File changing timing
Trace log for inter-process communication	• `/var/opt/jp1base/log/JBSCOM/jbscomd{1|2|3|4}.log` • *shared-directory*`/jp1base/log/JBSCOM/jbscomd{1|2|3|4}.log`	4 MB	1 MB
	• `/var/opt/jp1base/log/JBSCOM/jbscomd_api{1|2|3|4}.log` • *shared-directory*`/jp1base/log/JBSCOM/jbscomd_api{1|2|3|4}.log`	4 MB	1 MB
	• `/var/opt/jp1base/log/JBSCOM/jbscomd_ses{1|2|3|4}.log` • *shared-directory*`/jp1base/log/JBSCOM/jbscomd_ses{1|2|3|4}.log`	4 MB	1 MB
	• `/var/opt/jp1base/log/JBSCOM/jbscomd_snd{1|2|3|4}.log` • *shared-directory*`/jp1base/log/JBSCOM/jbscomd_snd{1|2|3|4}.log`	4 MB	1 MB
	• `/var/opt/jp1base/log/JBSCOM/jbscomd_rcv{1|2|3|4}.log` • *shared-directory*`/jp1base/log/JBSCOM/jbscomd_rcv{1|2|3|4}.log`	4 MB	1 MB
	• `/var/opt/jp1base/log/JBSCOM/command{1|2|3|4}.log` • *shared-directory*`/jp1base/log/JBSCOM/command{1|2|3|4}.log`	4 MB	1 MB
Error log of the command for collecting operating information	• `/var/opt/jp1base/log/jbsopi/jbsopi_cmd{1|2|3|4|5}.log`	5 MB	1 MB
Log for the operating information API	• `/var/opt/jp1base/log/jbsopi/jbsopi_api{1|2|3|4|5}.log` • *shared-directory*`/jp1base/log/jbsopi/jbsopi_api{1|2|3|4|5}.log`	5 MB	1 MB
Log of the service management control	• `/var/opt/jp1base/log/jbssrvmgr/jbssrvmgr{1|2|3|4}.log` • *shared-directory*`/jp1base/log/jbssrvmgr/jbssrvmgr{1|2|3|4}.log`	4 MB	1 MB

Log type	File name/directory name	Max. disk space	File changing timing
Trace log of the service management control	• `/var/opt/jp1base/log/jbssrvmgr/jbssrvmgr_trace{1|2|3|4}.log` • *shared-directory*`/jp1base/log/jbssrvmgr/jbssrvmgr_trace{1|2|3|4}.log`	4 MB	1 MB
Log of the service management control API	• `/var/opt/jp1base/log/jbssrvmgr/jbssrvmgr_api{1|2|3|4}.log` • *shared-directory*`/jp1base/log/jbssrvmgr/jbssrvmgr_api{1|2|3|4}.log`	4 MB	1 MB
Local action execution log	• `/var/opt/jp1base/log/lcact/localact{1-n}`#14`.log` • *shared-directory*`/jp1base/log/lcact/localact{1-n}`#14`.log`	1,024 KB#14	256 KB#14
Local action log	• `/var/opt/jp1base/log/jbslcact/jbslcact{1|2|3|4|5|6|7|8}.log` • *shared-directory*`/jp1base/log/jbslcact/jbslcact{1|2|3|4|5|6|7|8}.log`	2,048 KB	256 KB
	• `/var/opt/jp1base/log/jbslcact/jbslcact_list{1|2|3|4|5|6|7|8}.log` • *shared-directory*`/jp1base/log/jbslcact/jbslcact_list{1|2|3|4|5|6|7|8}.log`	2,048 KB	256 KB
	• `/var/opt/jp1base/log/jbslcact/jbslcact_cancel{1|2|3|4|5|6|7|8}.log` • *shared-directory*`/jp1base/log/jbslcact/jbslcact_cancel{1|2|3|4|5|6|7|8}.log`	2,048 KB	256 KB

#1: Log file for JP1/IM - Manager

#2: You can use the `jcocmddef` command of JP1/IM - Manager with the `-record` option specified to change this to a value within the range below.

- If the number of the records is 1 (`-record 1`)

  `DAT` file: 7 KB, K01 file: 4 KB

- If the number of the records is 20,000 (default value)

  `DAT` file: 125 MB, K01 file: 200 KB

- If the number of the records is 196,600 (`-record 196600`)

  `DAT` file: 1.2 GB, K01 file: 2 MB

#3: Indicates a `jbsplugincom` process identification number.

#4: You can use the operation log definition file (`jp1bs_baselog_setup.conf`) to change the number of files and the maximum disk space. For details on the range of specifiable values, see *K.5 Settings for outputting operation logs*.

#5: You can use the operation log definition file (`jp1bs_baselog_setup.conf`) to specify whether to automatically change files at JP1/Base startup.

#6: If you specify a different path in the event server index file (`index`), the log will be stored in a different directory.

#7: You can change the number of files and the maximum disk space using the event server settings file (`conf`). For details on the range of specifiable values, see *Event server settings file* in *14. Definition Files*.

#8: You can use the API settings (`api`) file to change the number of files and the maximum disk space. For details on the range of specifiable values, see *API settings file* in *14. Definition Files*.

#9: Because a file is created every time an error occurs when the subsystem for JP1/SES compatibility starts, you need to delete unnecessary files.

#10: Because a file is created every time an error occurs when the subsystem for JP1/SES compatibility stops, you need to delete unnecessary files.

#11: A file is created when the log file trapping function starts, and is deleted when the function terminates normally. If an error occurs, the file remains when the function terminates. If the log file trapping function generates frequent errors, there will be a large number of error files. Therefore, you need to delete unnecessary error files.

#12: You can change the number of files and the maximum disk space they occupy in the log information definition file (`jevlogd.conf`). For details on the range of specifiable values, see *Log information definition file* in *14. Definition Files*.

#13: A log file output when the `jbs_killall.cluster` command executes in a cluster system.

#14: You can use the common definition settings file (local action function) to change the number of files and the maximum disk space. For details on the range of specifiable values, see *Common definition settings file (local action function)* in *14. Definition Files*.

B. List of Processes

This appendix describes the processes for JP1/Base.

B.1 Windows processes

Use the Windows task manager to check the operating status of a desired process. The system displays the following process names when the processes are operating normally. The value in parentheses in the table indicates the number of processes that can be executed simultaneously.

Parent process name	Function	Child process name	Function
`hntr2srv.exe` (1)	Starts the Hitachi Network Objectplaza Trace Library (HNTRLib2)	--	--
`hntr2mon.exe` (1)	Hitachi Network Objectplaza Trace Library (HNTRLib2)	--	--
`jbs_service.exe` (1)	Starts the JP1/Base process management	--	--
`jbs_spmd.exe` (1)	JP1/Base process management#1	`jbssessionmgr.exe` (1)#2, #3	Authentication server#1#5 This process exists only on the host that is set as the authentication server. The displayed name is `jbssessionmgr` when the `jbs_spmd_status` command is executed.
		`jbsroute.exe` (1)#2	Configuration management#1#5 The displayed name is `jbsroute` when the `jbs_spmd_status` command is executed.
		`jcocmd.exe` (1)#2 `jcocmdexe.exe` (1) `jcocmdapi.exe` (Execute Command windows count#4 + `1` (when JP1/IM - Manager is installed))	Command execution#1#5 The displayed name is `jcocmd` when the `jbs_spmd_status` command is executed.

Parent process name	Function	Child process name	Function
		`jbsplugind.exe` (1)#2	Plug-in service#1#5 The displayed name is `jbsplugin` when the `jbs_spmd_status` command is executed.
		`jbshcd.exe` (1)	Health check (for local host monitoring)#1#5 The displayed name is `jbshcd` when the `jbs_spmd_status` command is executed.
		`jbshchostd.exe` (1)	Health check (for remote host monitoring)#1#5 The displayed name is `jbshchostd` when the `jbs_spmd_status` command is executed.
		`jbssrvmgr.exe` (1)	Service management control function#1 #5 The displayed name is `jbssrvmgr` when the `jbs_spmd_status` command is executed.
		`jbslcact.exe` (1)	Local action function#1#5 The displayed name is `jbslcact` when the `jbs_spmd_status` command is executed.
		`jbscomd.exe` (1) `jbscomd_api.exe` (1 to 9999) `jbscomd_ses.exe` (1) `jbscomd_snd.exe` (1) `jbscomd_rcv.exe` (1)	Inter-process communication#1#5 The displayed name is `jbscomd` when the `jbs_spmd_status` command is executed.
`jbapmsrvcecon.exe` (1)#3	Startup control	`powendar.exe` (1)	Power control This sub-process is generated when JP1/Power Monitor is installed.

Parent process name	Function	Child process name	Function
jevservice.exe (1)	Event service#1#6	jevsessvc.exe (1)	Event service This process is generated only on physical hosts.#6
jevtraplog.exe (1)	Log file trap	--	Log file trap This process is generated only when the log file function is used.
jevtrapevt.exe (1)	Event log trap	--	Event log trap This process is generated only when an event log trap is used.
imevtgw.exe (1)	SNMP trap converter	--	SNMP trap converter This process is generated only when the SNMP trap converter is used.

Legend:

--: None

#1: The maximum number of processes that can be executed simultaneously with the indicated process is the calculation result of the following format when multiple logical hosts operate on one physical host in the cluster system or when one logical host and one physical host are started at the same time: `(`*number-of-logical-hosts* `+ 1) x` *number-of-processes*

#2: These processes are important and are the core of JP1/Base. For abnormal termination of these processes, JP1/Base has functionality that automatically restarts the processes if they end abnormally. JP1/Base has other functionality that issues a JP1 event if it detects that a process is abnormal. We recommend that you set up this functionality to minimize the effect on your work if a process stops. For details, see *2.4.2 Setup for handling possible errors in JP1/Base*.

#3: The process names are not displayed in full in the Windows Task Manager.

#4: The number of Execute Command windows opened by the connected JP1/IM - View. The number of processes increases as the number of open windows increases. When you close an Execute Command window, the corresponding process disappears.

#5: You can use the `jbs_spmd_status` command to check the status of these processes. If the processes have started normally, the `jbs_spmd_status` command returns the following information.

- If an authentication server has been set:

  `jbssessionmgr`

jbsroute

jcocmd

jbsplugin

jbshcd

jbshchostd

jbssrvmgr

jbslcact

jbscomd

- If an authentication server has not been set:

  jbsroute

  jcocmd

  jbsplugin

  jbshcd

  jbshchostd

  jbssrvmgr

  jbslcact

  jbscomd

#6: The status of these processes can be checked with the `jevstat` command. Executing the `jevstat` command when the processes are running normally displays the following string:

`jevservice`

B.2 UNIX processes

Use the `ps` command in UNIX to check the operation status of a desired process. The system displays the following process names when the processes are operating normally. The value in parentheses in the table indicates the number of processes that can be executed simultaneously.

Parent process name	Function	Child process name	Function
`hntr2mon` (1)	Hitachi Network Objectplaza Trace Library (HNTRLib2)	--	--

Parent process name	Function	Child process name	Function
jbs_spmd (1)	Process management#1	jbssessionmgr (1)#2	Authentication server#1#5 This process exists only on the host that is set as the authentication server. The displayed name is jbssessionmgr when the jbs_spmd_status command is executed.
		jbsroute (1 to 9)#2	Configuration management#1#5 The displayed name is jbsroute when the jbs_spmd_status command is executed.
		jcocmd (1)#2 jcocmdexe (1) jcocmdapi (Execute Command window count#3 + 1 (when JP1/IM - Manager is installed)) jcocmdcmc (0 to the command count#4) jcocmdcom (1)#10	Command execution#1#5 The displayed name is jcocmd when the jbs_spmd_status command is executed.
		jbsplugind (1)#2, #7	Plug-in service#1#5 The displayed name is jbsplugin when the jbs_spmd_status command is executed.
		jbshcd (1)	Health check (for local host monitoring)#1#5 The displayed name is jbshcd when the jbs_spmd_status command is executed.
		jbshchostd (1)	Health check (for remote host monitoring)#1#5 The displayed name is jbshchostd when the jbs_spmd_status command is executed.
		jbssrvmgr (1)	Service management control function#1#5 The displayed name is jbssrvmgr when the jbs_spmd_status command is executed.

Parent process name	Function	Child process name	Function
		`jbslcact` (1)	Local action function#1#5 The displayed name is `jbslcact` when the `jbs_spmd_status` command is executed.
		`jbscomd.exe` (1) `jbscomd_api.exe` (1 to 9,999) `jbscomd_ses.exe` (1) `jbscomd_snd.exe` (1) `jbscomd_rcv.exe` (1)	Inter-process communication#1#5 The displayed name is `jbscomd` when the `jbs_spmd_status` command is executed.
`jevservice` (1)	Event service#1#6	`jevservice` (6 to 9,999)#11	Event service#6
		`jesdmain` (1)#8, #9	For compatibility with JP1/SES#6 This process is generated only on physical hosts.
		`jesrd` (6 to 9,999)#9	For compatibility with JP1/SES#6 This process is generated only on physical hosts.
`jevlogd` (1)	Log file trap	`jelparentim` (0 to the number of times the `jevlogstart` command is executed)	Log file trapping The `jelchildim` process is generated for each file to be monitored for each `jelparentim`. When the `jevlogstop` command is executed, the `jelparentim` process disappears.
`imevtgw` (1)	SNMP trap converter	--	SNMP trap converter This process is generated only when the SNMP trap converter is used.

Legend:

--: None

#1: The maximum number of processes that can be executed simultaneously with the indicated process is the calculation result of the following format when multiple logical hosts operate on one physical host in the cluster system or when one logical host and one physical host are started at the same time: (*number-of-logical-hosts* + 1) x *number-of-processes*

#2: These processes are important and are the core of JP1/Base. For abnormal termination of these processes, JP1/Base has functionality that automatically restarts the processes if they end abnormally. JP1/Base has other functionality that issues a JP1 event when it detects that a process is abnormal. We recommend that you set up this functionality to minimize the effect on your work if a process stops. For details, see *2.4.2 Setup for handling possible errors in JP1/Base*.

#3: The number of Execute Command windows opened by the connected JP1/IM - View. The number of processes increases as the number of open windows increases. When you close an Execute Command window, the corresponding process disappears.

#4: This value is the number of remote commands or automated actions that are executed by JP1/IM. A process is generated for each command. When processing finishes, the process disappears. If you execute commands successively, multiple processes might be generated.

#5: You can use the `jbs_spmd_status` command to check the status of these processes. If the processes have started normally, the `jbs_spmd_status` command returns the following information.

- If an authentication server has been set:

  ```
  jbssessionmgr
  jbsroute
  jcocmd
  jbsplugin
  jbshcd
  jbshchostd
  jbssrvmgr
  jbslcact
  jbscomd
  ```

- If an authentication server has not been set:

  ```
  jbsroute
  jcocmd
  jbsplugin
  jbshcd
  jbshchostd
  jbssrvmgr
  jbslcact
  jbscomd
  ```

#6: The status of these processes can be checked with the `jevstat` command. Executing the `jevstat` command when the processes are running normally displays the following string:

`jevservice`

#7: The process name displayed by the `ps-el` command is `jbsplugin`.

#8: The process name displayed when you execute the `ps` command is `/var/opt/jp1base/sys/tmp/event/servers/default/jpevent.conf`.

#9: This process is started from `jevservice`, but there is no parent-child relationship between the processes.

#10: This process was added in version 07-51.

#11: If `v5-unused` is specified for the `options` parameter in the environment settings file (conf) of the event server, the value is from 5 to 9,999. If `v5-unused` is not specified, the value is from 6 to 9,999.

C. List of Port Numbers

This appendix describes the port numbers that JP1/Base uses. The protocol is TCP/IP. These port numbers, except for those compatible with JP1/SES, are set as defaults at shipment.

C.1 Port numbers for JP1/Base

The following table lists the port numbers used for JP1/Base.

Table C-1: Port numbers for JP1/Base

Service name	Port number	Purpose
`jp1imevt`	20098/tcp	Transferring JP1 events to another host
`jp1imevtapi`	20099/tcp	All the products that register and obtain JP1 events, and functions for issuing and acquiring JP1 events
`jp1imrt`	20237/tcp	Configuration management (when using JP1/IM - Manager)
`jp1imcmda`	20238/tcp	Command execution (when using JP1/IM - Manager)
`jp1imcmdc`	20239/tcp	Command execution (when using JP1/IM - Manager)
`jp1bsuser`	20240/tcp	User authentication server
`JP1AutoJob`#1 (for Windows) `jesrd`#1 (for UNIX)	*user-definable-value*/tcp	Sending and receiving events with a product using the JP1/SES protocol
`jp1bsplugin`	20306/tcp	Used to collect and distribute JP1/IM definition information and used by the JP1/Base health check function.
`jp1bscom`	20600/tcp	Used for communication between JP1/IM configuration management and service management control
`ldap`	389/tcp#2	Used for linkage with a directory server
`ldaps`	636/tcp#2	

#1: For compatibility with JP1/SES. These services are not set in the `services` file when you install JP1/Base. If you want to send and receive events with either of the pre-Version 6 programs JP1/SES and JP1/AJS2, or with a program such as JP1/OJE that uses JP1/SES protocol, set these services in the `services` file.

#2: The port number depends on whether SSL is used for communication between JP1/Base (authentication server) and a directory server. If SSL is used, 636/tcp is used.

C.2 Direction in which data passes through the firewall

The following table describes the direction in which data passes through the firewall. JP1/Base supports address conversion of the packet filtering type and the NAT (static mode) type.

Table C-2: Direction in which data passes through the firewall

Service name	Port number	Direction in which data passes through the firewall
`jp1imevt`	20098/tcp	JP1/Base that transfers JP1 events -> JP1/Base that receives JP1 events
`jp1imevtapi`	20099/tcp	A program such as JP1/IM - Manager that obtains JP1 events -> JP1/Base
`jp1imrt`	20237/tcp	JP1/IM - Manager -> JP1/Base Upper-layer JP1/IM - Manager -> lower-layer JP1/IM - Manager
`jp1imcmda`	20238/tcp	JP1/IM - View -> JP1/Base on the host where JP1/IM - Manager is installed JP1/IM - Manager -> JP1/Base
`jp1imcmdc`	20239/tcp	JP1/Base on the host running JP1/IM - Manager <--> JP1/Base on the host that executes the command
`jp1bsuser`	20240/tcp	JP1/IM - Manager -> JP1/Base JP1/AJS - Manager -> JP1/Base JP1/AJS - Agent -> JP1/Base
`JP1AutoJob` (in Windows) `jesrd` (in UNIX)	*user-definable-value*/tcp	JP1/Base <--> A product using the JP1/SES protocol
`jp1bsplugin`	20306/tcp	Upper-layer program using services such as JP1/IM - Manager -> JP1/Base When using the JP1/Base health check function: JP1/Base on the monitoring host -> JP1/Base on the monitored host
`jp1bscom`	20600/tcp	JP1/Base <--> JP1/Base on a different host
`ldap`	389/tcp#	JP1/Base (authentication server) -> Directory server
`ldaps`	636/tcp#	

Legend:

->: Communication data goes in one direction (from left to right).

<-->: Communication data goes in both directions (from left to right, and from right to left).

#: The port number depends on whether SSL is used for communication between JP1/Base (authentication server) and a directory server. If SSL is used, 636/tcp is used.

To use the port numbers listed in Table C-2 to establish a connection, you must set the firewall that lets the *service-name* port pass through it. You must also set the firewall that allows `ANY` to pass through it in response to the session established for the port number for *service-name*. The response must be `ANY` because the OS performs automatic numbering.

When you install JP1/Base on a firewall server machine, communications within that machine might also be prohibited by the firewall functionality. Therefore, set the firewall server machine to allow communications within the same machine.

C.3 Connection status

The following table describes the connection status at each port number.

Table C-3: Connection status

Service name	Port number	Connection status
`jp1imevt`	20098/tcp	When `keep-alive` is specified in the `remote-server` parameter in the event server settings file (`conf`), the connection is maintained. If you want to forcibly terminate the connection, specify `close` in this parameter.
`jp1imevtapi`	20099/tcp	When `keep-alive` is specified in the `server` parameter in the API settings file (`api`), the connection is maintained. If you want to forcibly terminate the connection, specify `close` in this parameter.
`jp1imrt`	20237/tcp	A connection is established only when required.
`jp1imcmda`	20238/tcp	The connection is maintained. If the connection is forcibly terminated, you must re-execute the command.
`jp1imcmdc`	20239/tcp	The connection is maintained.#1 If the connection is forcibly terminated, the service is automatically reconnected.
`jp1bsuser`	20240/tcp	A connection is established only when required.
`JP1AutoJob` (in Windows) `jesrd` (in UNIX)	*user-definable-value*/tcp	A connection is established only when required.
`jp1bsplugin`	20306/tcp	A connection is established only when required.
`jp1bscom`	20600/tcp	A connection is established only when required.

Service name	Port number	Connection status
`ldap`	389/tcp[#2]	A connection is established only when required.
`ldaps`	636/tcp[#2]	

#1: If there is no communication for more than 30 minutes, the connection is disconnected.

#2: The port number depends on whether SSL is used for communication between JP1/Base (authentication server) and a directory server. If SSL is used, 636/tcp is used.

D. List of Limits

This appendix describes the limits of JP1/Base.

Table D-1: List of limits

Item	Limits
Maximum length of a line in the event service environment settings (event server settings file, forward setting file, and distribution definition file)	1,023 bytes
Maximum length of a filter for a forward setting file	64 kilobytes
Maximum length of an event server name	255 bytes (However, you can specify no more than 240 bytes for a Windows `jevregsvc` command.)
JP1 user name	1 to 31 bytes
JP1 user password	6 to 32 bytes
OS-user-name	1 to 64 bytes (including a domain name. However, the maximum length varies depending on the OS.)
Maximum length of a server host name	255 bytes
Maximum length of a logical host name	196 bytes (63 bytes recommended) for Windows# 255 bytes (63 bytes recommended) for UNIX#
Maximum length of a line in a user-permission level file	4,096 bytes
Maximum length of a line in a user mapping definition file	4,096 bytes
Number of JP1 users that can log into the authentication server simultaneously	10,000 users
Number of JP1 users that can be registered	3,000 users
Number of JP1 users that can be registered in the user permission level file	3,000 users
Maximum length of a line in a health check definition file	1,023 bytes

#: The limits above are those for JP1/Base. Some of these limits do not apply to the items for the cluster software. When specifying a logical host name with JP1/Base, note that the name must not exceed the limit for the cluster software. We recommend 63 bytes or less for actual operation.

E. Performance and Estimation

This appendix describes memory and disk space requirements for JP1/Base.

E.1 Memory requirements

For details on JP1/Base memory requirements, see the *Release Notes*.

E.2 Disk space requirements (in Windows)

For details on JP1/Base disk space requirements in Windows, see the *Release Notes*.

E.3 Disk space requirements (in UNIX)

For details on JP1/Base disk space requirements in UNIX, see the *Release Notes*.

E.4 Disk space requirements for the shared disk in a cluster system

For details on JP1/Base disk space requirements, see the *Release Notes.*

F. Syntax of Regular Expressions

The regular expressions given below can be used with JP1 products. When using a regular expression to select data, specify the search conditions in accordance with the coding conventions explained on the next pages.

F.1 Regular expressions that can be used by default

This section explains the regular expressions that can be used by default under Windows. Under UNIX, the regular expressions provided by the OS are applied, so the syntax is different from that explained below. For details on the regular expressions that can be used under UNIX, see the syntax (`regexp` or `regex`).

(1) Ordinary characters

An *ordinary character* is one that matches itself when specified as the search target in a regular expression. The only characters not handled as ordinary characters are the linefeed character and special characters. Ordinary characters are case sensitive.

(2) Special characters

Special characters are the caret (`^`), dollar sign (`$`), period (`.`), asterisk (`*`), and backslash (\).

These special characters are explained below.

`^`

The caret (`^`) signifies the beginning characters (match the start). The caret is a special character only when used as the first character in a regular expression. When specified elsewhere, the caret is handled as an ordinary character.

When written as a special character, matches are found for lines beginning with the same character string that starts the line (that is, that comes after the caret).

`$`

The dollar sign (`$`) signifies the last characters (match the end). The dollar sign is a special character only when used as the last character in a regular expression. When specified elsewhere, the dollar sign is handled as an ordinary character.

When written as a special character, matches are found for lines ending with the same character string that ends the line (that is, that comes before the dollar sign). When used with the caret, matches are found for the exact character string written between the caret and dollar sign.

(period)

The period (`.`) signifies any single character other than a linefeed character.

When written as a special character, matches are found for any single character other than a linefeed character.

`*`

The asterisk (`*`) signifies zero or more repetitions of the preceding regular expression.

`\`

The backslash (`\`) removes the special meaning of the special characters (`* . ^ $ \`).

When a backslash is written in front of a special character, the special character is handled as an ordinary character. Preceding a lower-case character with a backslash will produce an error, with the following exceptions:

`\n`

Linefeed code

`\t`

Tab character

F.2 Extended regular expressions that can be used when regular expressions are extended

In JP1 products, common regular expressions can be used under Windows and UNIX by extending regular expressions. To extend regular expressions, see *2.4.1 Extending regular expressions to be used*. Under UNIX OSs, the extended regular expressions that are applied differ by OS. For HP-UX, Solaris, and AIX, the extended regular expressions applied are XPG4-compliant. Under Windows, the syntax of the XPG4 regular expressions is applied. This section explains regular expressions that seem to be used frequently.

Regular expressions that can be used when extension has been performed are listed below.

Character string

Signifies the line with the specified string.

`^`*string*

Signifies that the specified string is at the beginning of a line. When specified elsewhere, the caret is handled as an ordinary character.

string`$`

Signifies that the specified string is at the end of a line. When used in a place other than the end of a line, *string*`$` is handled as ordinary characters. When used with the caret, matches are found for the exact character string written between the caret and dollar sign.

^*string*$

Signifies a line that contains the specified string only.

^$

Signifies a blank line.

(period)

The period signifies any single character other than a linefeed character.

[*string*]

Signifies any of the characters specified in the string enclosed by [and].

[*character-character*]

Signifies any single character within the range, in the ascending order of the character codes.

[^*character-character*]

Signifies any single character out of the range, in the ascending order of the character codes.

*character**

Signifies a string in which the immediately preceding character is repeated at least zero times.

regular-expression | *regular-expression*

Signifies either the right or left regular expressions.

\special-character

Handles a special character as an ordinary character.

(*regular-expression*)

Groups regular expressions.

F.3 Comparison between regular expressions supported in Version 06-71 and earlier, and Version 07-00 and later

The following table lists the regular expressions that can be used by default in version 06-71 and earlier versions and those supported from version 07-00. The table also lists the main extended regular expressions available from version 07-00.

Method	Meaning	Version 06-71 and earlier versions		Version 07-00 and later versions	
		In Windows: (JP1-specific regular expression)	In UNIX: (basic regular expression)#1	In Windows: (extended regular expression)#3	In UNIX: (extended regular expression)#2
Character string	Signifies the line with the specified string.	Y	Y	Y	Y
^*string*	Signifies that the specified string is at the beginning of a line.	Y	Y	Y	Y
string$	Signifies that the specified string is at the end of a line.	Y	Y	Y	Y
^*string*$	Signifies the line that contains the specified string only.	Y	Y	Y	Y
^$	Signifies a blank line.	Y	Y	Y	Y
(period)	Signifies any single character.	Y	Y	Y	Y
`.*`	A period (.) combined with an asterisk (*) signifies a single character.	Y	Y	Y	Y
[*string*]	Signifies any of the characters specified in the string enclosed by [and].	N	Y	Y	Y
[^*string*]	Signifies characters other than those specified in the string enclosed by [and].	N	Y	Y	Y

Method	Meaning	Version 06-71 and earlier versions		Version 07-00 and later versions	
		In Windows: (JP1-specific regular expression)	In UNIX: (basic regular expression)#1	In Windows: (extended regular expression)#3	In UNIX: (extended regular expression)#2
[*character*-*character*]	Signifies a single character within the range, in the ascending order of character codes.	N	Y	Y	Y
[^*character*-*character*]	Signifies a single character out of the range, in the ascending order of character codes.	N	Y	Y	Y
*character**	Signifies the string in which the immediately preceding character is repeated at least zero times.	Y	Y	Y	Y
character+	Signifies the string in which the immediately preceding character is repeated at least one time.	N	N	Y	Y
character?	Signifies the string in which the immediately preceding character is not repeated or only one time.	N	N	Y	Y
Character{*n*}	Signifies the string in which the immediately preceding character is repeated at least n times.	N	N	Y	Y

Method	Meaning	Version 06-71 and earlier versions		Version 07-00 and later versions	
		In Windows: (JP1-specific regular expression)	In UNIX: (basic regular expression)#1	In Windows: (extended regular expression)#3	In UNIX: (extended regular expression)#2
Character{*n*,}	Signifies the string in which the immediately preceding character is repeated at least n times.	N	N	Y	Y
Character{*n*,*m*}	Signifies the string in which the immediately preceding character is repeated at least n times, but m times or less.	N	N	Y	Y
regular-expression | *regular-expression*	Signifies either the right or left regular expressions.	N	N	Y	Y
\special-character	Handles a special character as an ordinary character.	Y	Y	Y	Y
(*regular-expression*)	Groups regular expressions.	N	N	Y	Y

Legend:

Y: Can be used

N: Cannot be used

#1: Only JP1/Base uses basic regular expressions by default. Other JP1 products use different regular expressions. So, for details on the regular expressions used by default, see the manual of each product.

#2: If regular expressions are extended, the extended regular expressions that are applied differ by OS. For HP-UX, Solaris, and AIX, the extended regular expressions applied are XPG4-compliant. For details, see the syntax (`regexp` or `regex`).

#3: If regular expressions are extended, the syntax of the XPG4 extended regular expressions is applied. Items that are undefined in the regular expression standard might act differently from the corresponding items for UNIX.

F.4 Tips on using regular expressions

Some tips on using regular expressions are given below. Bear these in mind when specifying regular expressions.

- When specified as a regular expression, a period followed by an asterisk (`.*`) will match any characters. If you use this combination frequently, it might take a long time to find the matches. When you are searching for a long message, for example, use the period and asterisk combination only where required in the search string.
- To find matches with non-null characters in UNIX, you can reduce the search time by using the combination `[^ ]*`. This expression matches repetitions of non-null characters.

F.5 Examples of using regular expressions

The following table gives some examples of using regular expressions.

Specification	Meaning	String specified as a regular expression	Example character string	Match
character-string	Match lines containing the specified string.	spring	**spring** has come.	Yes
			winter-summer-autumn-**spring**	Yes
			---- **spring** -----	Yes
^ *character-string*	Match lines beginning with the specified string.	^spring	**spring** has come.	Yes
			winter-summer-autumn-spring	--
			-----spring-----	--
character-string $	Match lines ending with the specified string.	spring$	spring has come.	--
			winter-summer-autumn-**spring**	Yes

Specification	Meaning	String specified as a regular expression	Example character string	Match
			-----spring-----	--
^ *character-string* $	Match lines consisting of the specified string only.	^spring$	spring has come.	--
			winter-summer-autumn-spring	--
			spring	Yes
			spring	--
^$	Match null lines.	^$		Yes
			spring	--
. (period)	Match any character.	in.e	w**inte**r has come.	Yes
			mother of **inve**ntion	Yes
			life is **in e**verything	Yes
			eight nine ten	--
			increasing population	--
		s..ing	picnic in **spring**	Yes
			skiing in winter	Yes
[*character-string*]	Signifies any of the characters specified in the string enclosed by [and].	[pr]	s**pr**ing has come.	Yes
			today is Monday.	--
[*character-character*]	Signifies a single character within the range, in the ascending order of character codes.	[a-i]	spr**ing** **ha**s **come**.	Yes

Specification	Meaning	String specified as a regular expression	Example character string	Match
[*character-character*]	Signifies a single character out of the range, in the ascending order of character codes.	[^a-i]	**spr**i**n**g ha**s** c**om**e.	Yes
character *	Match strings containing zero or more repetitions of the preceding characters.	ro*m	te**rm**inal	Yes
			cd-**rom**	Yes
			living **room**	Yes
		h.*n	**This is a pen**.	Yes
			That is an apple.	Yes
regular-expression | *regular-expression*	Signifies either of the right and left regular expressions.	[0-9]+|apple	That is an **apple**.	Yes
			spring in **2003**	Yes
\ *special-character*	Handles a special character as an ordinary character.	o\.h	<stdi**o.h**>	Yes
			another man	--
(*regular-expression*)	Groups regular expressions.	i(n.e|ng)	w**inte**r has come.	Yes
			interest**ing** book	Yes

Legend:

Bold type: Character string matching the specified regular expression.

Blank: Null line.

Yes: The example character string is a match.

--: The example character string is not a match.

G. List of Kernel Parameters

When you use JP1/Base in a UNIX environment, adjust the kernel parameters of the OS to allocate the resources required for executing JP1/Base. For details on how to do this, see the *Release Notes*.

H. Handling Changes in Communication Settings

In JP1/Base 06-71 or later, the communication settings can be changed according to the various network configurations. To change the communication settings, use the `jp1hosts` definition file and communication protocol settings file. (To change them for the event service, use the event server settings file (`conf`).) For details on the communication settings, see *4. JP1/Base Communication Settings According to Network Configurations*.

The table below describes the communication settings available for the functionality offered by JP1/Base.

Table H-1: Supported functionality in communication settings

Function		Communication settings	
		jp1hosts definition file	Communication protocol settings file
User management	User authentication function	Yes	Yes
	User mapping function	--	--
Startup control	Start sequence control	--	--
	Stop sequence control	--	--
Event service		No	Yes#
Event conversion	Log file trap	--	--
	Event log trap	--	--
	SNMP trap converter	--	--
Collecting and distributing definitions for the event service		Yes	Yes
Process management		--	--
ISAM utility commands		--	--
Hitachi Network Objectplaza Trace Library (HNTRLib2)		--	--

Legend:

Yes: Supported.

No: Not supported.

--: Not communicated.

#: Changed by the event server settings file (conf). (Events in JP1/SES format are not supported.)

I. Converting SNMP traps

This feature converts SNMP traps, which are managed by NNM, into JP1 events. You can use this feature for integrated control over information about network failures, and the configuration and performance of the system.

The SNMP trap converter for JP1/Base supports the NNM version shown in the following tables.

Table I-1: In Windows or Solaris (SPARC)

NNM supported by the SNMP trap converter	Versions
HP Network Node Manager Starter Edition Software	7.5

Table I-2: In HP-UX (IPF)

NNM supported by the SNMP trap converter	Versions
HP Network Node Manager Starter Edition Software	7.5

To convert SNMP traps into JP1 events, the following requirements must be met:

- The OS used is one of the following:
    - Windows XP Professional
    - Windows Server 2003 (excluding Windows Server 2003 (x64))
    - HP-UX (IPF)
    - Solaris (Solaris (SPARC) global zone)

  The converter cannot be used on Windows Server 2008 and other OSs that NNM does not support.

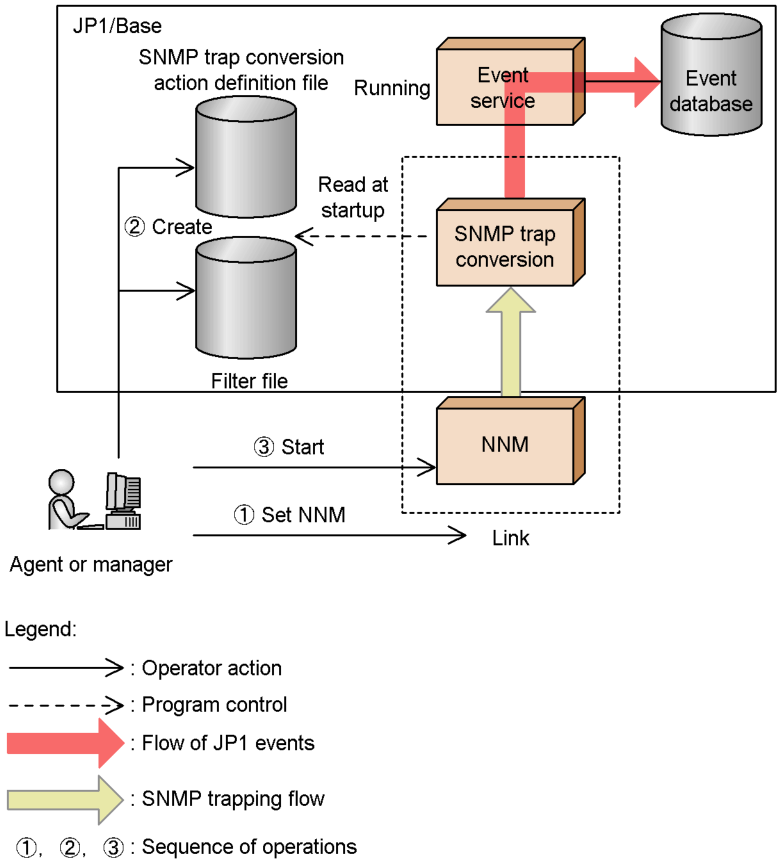
- The value of the LANG environment variable for `ovw` (NNM GUI) matches the value for the environment where the `ovstart` command of NNM is executed.

  If the values do not match, SNMP traps might not be converted into JP1 events, or the traps might be converted into JP1 events different from those shown in the NNM alarms browser. For details, see the NNM documentation.

I.1 Using the SNMP trap converter to convert SNMP traps into events

The following figure shows how SNMP traps are converted into JP1 events and registered in an event database.

Figure I-1: Overview of SNMP trap conversion to JP1 event registration



To use the SNMP trap converter, you need to create the SNMP trap conversion action definition file (`imevtgw.conf`) and SNMP trap conversion filter file (`snmpfilter.conf`). These two files are used to specify the conditions for converting SNMP traps into JP1 events, and the severity levels for JP1 events. The SNMP trap converter begins when NNM starts.

While it is running, the SNMP trap converter obtains SNMP traps that satisfy the conditions specified in the SNMP trap conversion filter file (`snmpfilter.conf`), and then converts these traps into JP1 events. The acquired information consists of the event message, severity level, enterprise name, enterprise ID, object name, object ID, and source list. If the SNMP trap converter is not running, output SNMP traps are not converted into JP1 events. Trapped SNMP messages can be registered as JP1 events using a maximum of 1,023 bytes. If a message exceeds this maximum, the message is truncated from the 1,024th byte when the message is converted into a JP1 event.

All JP1 events converted from SNMP traps are assigned an event ID of 00003A80. For details on attributes of JP1 events, see *I.5 JP1 events for SNMP trap conversion*.

The SNMP trap converter checks for syntax errors when reading the action definition file and the filter file for converting SNMP traps (`snmpfilter.conf`). If a syntax error is found, a message appears.

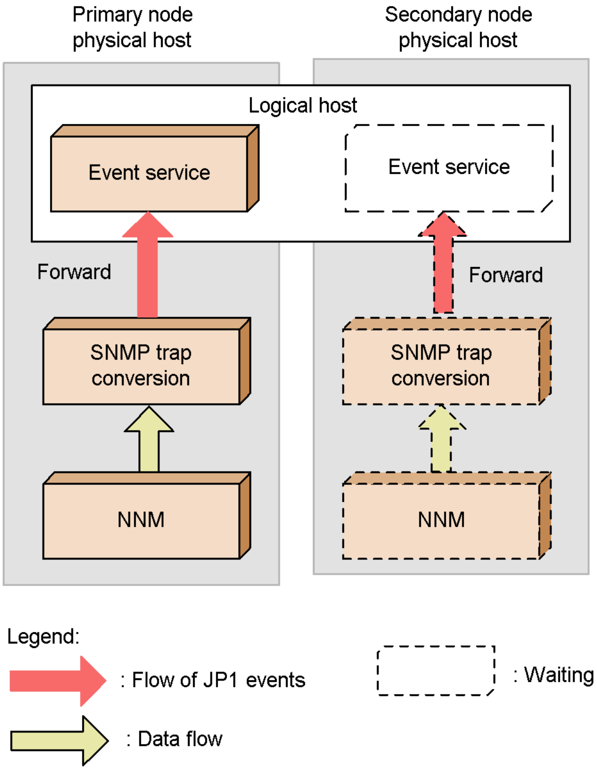
(1) SNMP trapping in a cluster system

The SNMP trap converter operates only on a physical host. Also, it operates by using the NNM function linked with the starting up and shutting down of NNM. It therefore operates independently of JP1/Base failovers.

By default, JP1 events are registered in the event service on the physical host. To register JP1 events in the event service on a logical host, specify the event server name on the logical host for the `imevt_server` parameter, and specify the registration trigger to the event server for the `imevt_regkind` parameter in the SNMP trap conversion action definition file. However, if NNM is used in a non-cluster system, and that system is configured to directly register converted JP1 events to the logical host, the standby node cannot monitor the SNMP traps it receives.

The following figure illustrates how to configure a cluster system (where NNM is used) to directly register JP1 events to a logical host.

Figure I-2: Configuration example for directly registering JP1 events to a logical host



To use NNM in a cluster system, set up NNM on both the primary and secondary nodes, referring to *I.2 Setting the SNMP trap converter*. Register NNM and JP1/Base in the same cluster group.

If you are using NNM in a cluster system and JP1/Base in a non-cluster system (that is, these programs are being used on the physical hosts only), you must start JP1/Base on the physical host at both the primary and secondary nodes.

(2) Types of SNMP traps that can be converted

The following criteria apply to SNMP trap conversion:

- Maximum line length in the definition files

  The length of each line in the definition files (`imevtgw.conf`, `snmpfilter.conf`, and `trapd.conf`) must not exceed 1,023 bytes.

- Enterprise name

  The enterprise name defined in the `trapd.conf` file must not begin with a hash mark, exclamation mark, or plus sign.

- Event name

  The event name defined in the `trapd.conf` file must not begin with an asterisk.

- Object ID

  The object ID defined in the `trapd.conf` file must not include an asterisk. Only SNMP traps whose object IDs completely match those defined in the `trapd.conf` file will be converted into JP1 events.

- Source list

  If you specify particular sources (nodes) in NNM by selecting **Only specified sources** in the Sources page of the Modify Events dialog box, which opens from the Event Configuration window, only the SNMP traps generated by those sources will be converted into JP1 events.

  You can also specify a file containing source names. If you use a file, you cannot use the hash mark to enter comment lines. Each source (node) must not exceed 511 bytes in length. Sources (nodes) do not support regular expressions.

- Message

  If the message acquired from the `trapd.conf` file contains any special "`$` variables", the SNMP trap converter expands the `$` variables to present the information contained in the SNMP trap. The `$` variables supported by the SNMP trap converter are listed below. All other variables are output without being expanded when an SNMP trap is converted.

- $ variables expanded by default

```
$#          $number    $-number   $+number   $>number   $>-number
$>+number   $x         $X         $@         $O         $o
$G          $S         $e         $E         $A         $*
```

- $ variables not expanded by default

```
$r          $ar        $c         $s         $N         $$
$C          $aA        $T
```

To expand a `$` variable that is not expanded by default, specify the variable in the SNMP trap conversion action definition file (`imevtgw.conf`). For details on how to do this, see *I.4(1) Action definition file for converting SNMP traps (imevtgw.conf)*.

The KAVA2108-E message is output if an error occurs when information is expanded from a `$` variable. If you want to detect errors as JP1 events, monitor such errors using the log file trap, and make the KAVA2108-E message (output to the integrated trace log) the SNMP trap condition.

The output message after expansion of the $ variables might differ from the message output by NNM. You can check the output messages in either of the following ways:

- In JP1/IM - View, from the Tool Launcher double-click **Network Management** to launch the NNM window.
- In JP1/IM - View, open the Event Details window, click the **Monitor** button to launch the NNM window, and examine the NNM alarm browser.

■ Generic traps

Generic traps can be converted by the SNMP trap converter.

If generic traps are defined for JP1 event conversion in the filter file for converting SNMP traps (`snmpfilter.conf`), enterprise-specific generic traps are also converted as generic traps. If both generic traps and enterprise-specific generic traps are defined in the `trapd.conf` file, enterprise-specific generic traps will be converted as such in NNM, but as generic traps by the SNMP trap converter. As a result, the information displayed in JP1/IM - View might sometimes differ from the information displayed in NNM. To avoid this problem, add a definition for enterprise-specific generic traps to the filter file for converting SNMP traps (`snmpfilter.conf`). Examples of a generic trap and of an enterprise-specific generic trap are shown below.

Example: Generic trap

Enterprise name: `snmpTraps`

Event name: `SNMP_Link_Down`

Object ID: `.1.3.6.1.6.3.1.1.5.3`

Example: Enterprise-specific generic trap

Enterprise ID: `hitachi`

Event name: `HI_Link_Down`

Object ID: `.1.3.6.1.6.3.1.1.5.3.1.3.6.1.4.1.116`

Note that the following SNMP traps used internally in NNM cannot be converted into JP1 events:

- `OpenView.OV_Ack_Alarm`
- `OpenView.OV_Delete_Alarm`
- `OpenView.OV_Unack_Alarm`
- `OpenView.OV_ChgSev_Alarm`
- `OpenView.OV_ChgCat_Alarm`

- Events generated by the ECS engine (`OpenView.OV_Corr_Indic`, and so on)

For details, see the NNM documentation.

(3) Note

Note the following points when using the SNMP trap converter:

- An error message is displayed and the event data is discarded if a connection to the event service fails when the SNMP trap converter attempts to convert an SNMP trap to a JP1 event.

I.2 Setting the SNMP trap converter

The following explains the procedures for starting the SNMP trap converter, changing the settings, and stopping the SNMP trap converter.

(1) Setup

Set up the SNMP trap converter before using it. Setup is also required if you re-install JP1/Base over a previous installation.

To set up the SNMP trap converter:

1. Execute the `imevtgw_setup` command to register the SNMP trap converter in NNM.

    - In Windows:

      At the command prompt, execute the following command:

```
cd installation-folder\bin
imevtgw_setup.exe
```

    - In UNIX:

      Execute the command as follows:

```
/opt/jp1base/bin/imevtgw_setup
```

   The SNMP trap converter is registered in the NNM process management.

2. Make sure that the SNMP trap converter is registered correctly.

   Check the NNM process as follows.

    - In Windows:

      From the Windows **Start** menu, choose **Programs**, **Network Node Manager**, **Network Node Manager Admin**, **NNM Services - Status**.

    - In UNIX:

      Execute the command as follows:

```
/opt/OV/bin/ovstatus
```

If the `IMEvtgw` process appears under the `ovw` process, the SNMP trap converter has been registered correctly.

(2) Starting the SNMP trap converter

To start the SNMP trap converter:

1. Edit the action definition file for converting SNMP traps (`imevtgw.conf`).

   For details on the action definition file, see *I.4(1) Action definition file for converting SNMP traps (imevtgw.conf)*.

2. Edit the SNMP trap conversion filter file (`snmpfilter.conf`).

Specify the conditions for all SNMP traps to be converted into JP1 events, using the appropriate enterprise and event names listed in `trapd.conf`. For details on how to do this, see *I.4(2) SNMP trap conversion filter file (snmpfilter.conf)*.

1. Start NNM.

   SNMP trap converter begins when NNM starts.

   - In Windows:

     From the Windows **Start** menu, choose **Programs**, **Network Node Manager**, **Network Node Manager Admin**, and then **NNM Services - Start**.

   - In UNIX:

     To start the NNM background process, execute the following command: `/opt/OV/bin/ovstart`

2. Confirm that the converter functions normally.

   Generate an SNMP trap that can be converted, and then confirm that the trap was successfully converted into a JP1 event.

(3) Changing a setting while a trap is active

If you change the settings in the action definition file for converting (`imevtgw.conf`) SNMP traps or filter file for converting SNMP traps (`snmpfilter.conf`), apply the new settings as follows.

If you edit the SNMP trap conversion action definition file

After editing the definition file, restart the SNMP trap converter.

If you edit the SNMP trap conversion filter file

You can apply the new settings without stopping the SNMP trap converter by executing the `xnmevents` command (provided by NNM) with the `-event` option.

(4) Stopping the SNMP trap converter

To stop the SNMP trap converter:

- In Windows:

  From the Windows **Start** menu, choose **Programs**, **Network Node Manager**, **Network Node Manager Admin**, and then **NNM Services - Stop**.

- In UNIX:

  Execute the command as follows:
  `/opt/OV/bin/ovstop`

(5) Clearing the SNMP trap converter

Before you uninstall JP1/Base, clear the SNMP trap converter registered in the NNM process management.

To clear the SNMP trap converter:

In Windows:

1. From the Windows **Start** menu, choose **Programs**, **Network Node Manage**r, **Network Node Manager Admin**, and then **NNM Services - Status**. Check whether IMEvtgw (the SNMP trap converter) is inactive.

   If IMEvtgw is running, from the **Start** menu choose **Programs**, **Network Node Manager**, **Network Node Manager Admin**, and then **NNM Services - Stop** to end the service.

2. At the command prompt, execute the following command:

   `cd` *installation-folder*`\bin`

   ```
   imevtgw_setup.exe -d
   ```

   This command deletes the `imevtgw.exe` file from the NNM folder, and clears the setting for starting the SNMP trap converter from the NNM process management.

In UNIX:

1. Execute the `/opt/OV/bin/ovstatus` command and make sure that IMEvtgw (the SNMP trap converter) is inactive.

   If IMEvtgw is running, execute the `/opt/OV/bin/ovstop` command to end the NNM daemon processes.

2. Execute the following command:

   ```
   /opt/jp1base/bin/imevtgw_setup -d
   ```

   This command deletes the `imevtgw.exe` file and `imevtgw` file from the

NNM directory, and clears the setting for starting the SNMP trap converter from the NNM process management.

I.3 SNMP trap conversion command syntax

This section describes the command syntax used to execute the SNMP trap converter.

(1) imevtgw_setup (Windows, HP-UX, and Solaris only)

Function

Register the SNMP trap converter in the NNM process management.

Format

```
imevtgw_setup { -d }
```

Required execution permission

In Windows: Administrators

In UNIX: Superuser

Storage destination directory

In Windows:

installation-folder`\bin\`

In UNIX:

`/opt/jp1base/bin`

Arguments

`-d`

Specifies the SNMP trap converter to be disabled.

Notes

- If you want to uninstall JP1/Base, execute this command to disable the SNMP trap converter registered in the NNM process management before uninstallation.
- Execute this command if a patch has been applied or if an upgrade has been performed.
- Execute this command after you stop the SNMP trap converter.
- If NNM is used in a cluster environment, execute this command on both the executing and standby nodes. If the NNM cluster operation method used in Windows is "direct data sharing", only execute this command on the active nodes.

I.4 Definition files for SNMP trap conversion

This section describes the format and syntax of the definition files used for SNMP trap conversion.

(1) Action definition file for converting SNMP traps (imevtgw.conf)

Format

```
nnm_url_base  http://host-name:port-number /OvCgi/jovw.exe?MapName=default
severity SNMP-trap-severity to JP1-event-severity
snmp-filter
source  host-name1  host-name2  host-name3...
end-filter
var_expand    0 | 1
var_option $variable...
imevt_server event-server-name
imevt_regkind 0 | 1
```

Storage destination directory

In Windows:

installation-folder`\conf\evtgw\imevtgw.conf`

In UNIX:

`/etc/opt/jp1base/conf/evtgw/imevtgw.conf`

Description

The action definition file for SNMP trap conversion specifies the following items: the URL of NNM, the severity mapping between SNMP traps and JP1 events, and the actions to be performed when converting SNMP traps.

Application of settings

When the SNMP trap converter is started, the settings take effect.

Definition statement

- Separate the parameters using spaces or tab characters.
- A hash mark (#) at the start of a line indicates a comment.

Definition details

`nnm_url_base`

In JP1/IM-View, to launch NNM from the Event Details window, specify the URL of NNM in the following format:

```
http://host-name:port-number /OvCgi/
jovw.exe?MapName=default
```

This parameter specifies the name of the host on which the action definition file for SNMP trap conversion (imevtgw.conf) is set. You do not need to specify a port number if you specified a Windows host in *host-name*. If you specify a UNIX host, you must also specify the appropriate port number. Write 8880 if you are using NNM 6.2 (NNM 07-01) or an earlier version. Write 3443 if you are using NNM 6.4 (NNM 07-10) or a later version. Note that the port number might differ, depending on the port number set in NNM. Check the NNM port number setting.

severity

Associate the severity level of the SNMP trap with the severity level of the resulting JP1 event. You can specify any of the following values for the SNMP trap severity:

- normal
- warning
- minor
- major
- critical
- unknown

unknown indicates that there is no data identifying the SNMP trap severity, or the data does not match normal, warning, minor, major, or critical.

You can specify any of the following values for the JP1 event severity:

- Information
- Notice
- Warning
- Error
- Emergency
- Critical
- Alert
- Debug

By default, or if no severity parameter is specified, the severity levels are mapped as shown below.

SNMP trap severity	JP1 event display after conversion (severity level)
`normal`	`Information`
`warning`	`Warning`
`minor`	`Error`
`major`	`Critical`
`critical`	`Alert`

`snmp-filter`

`source` *host-name1 host-name2 host-name3*...

`end-filter`

Specify the names of SNMP agent hosts from which SNMP traps are to be converted into JP1 events. Specify the sources (host names) shown in the NNM alarms browser. Event server names are case sensitive.

For SNMP traps issued by the specified hosts, only SNMP traps that satisfy the conditions specified in the SNMP trap conversion filter file (`snmpfilter.conf`) are converted into JP1 events. The condition will be satisfied when a match is found with any one of the specified host names.

Note the following points when specifying the `source` condition statement.

- The `source` condition statement must be enclosed within `snmp-filter` and `end-filter`.
- Separate the `source` and *host-name* specification using spaces or tab characters.
- The length of each line must not exceed 1,023 bytes. Host names will be deleted from the 1,024th byte and on.
- Specify only one `source` condition statement in one `snmp-filter`. If it is impossible to include all the target host names in a source attribute condition statement, use an additional `snmp-filter` statement to specify an additional `source` condition statement.

When this parameter is unspecified, all SNMP traps that match the conditions specified in the filter file for converting SNMP traps (`snmpfilter.conf`) will be converted into JP1 events.

`var_expand 0|1`

Specify whether to expand `$` variables (`$r`, `$ar`, `$c`, `$s`, `$N`, `$$`, `$C`, `$aA`, and `$T`) contained in the messages acquired from the `trapd.conf` file to present the information contained in the SNMP traps.

When you specify 0, the following 18 $ variables will be expanded: $#, $*number*, $-*number*, $+*number*, $>*number*, $>-*number*, $>+*number*, $x, $X, $@, $O, $o, $G, $S, $e, $E, $A, and $*.

When you specify 1, in addition to $#, $*number*, $-*number*, $+*number*, $>*number*, $>-*number*, $>+*number*, $x, $X, $@, $O, $o, $G, $S, $e, $E, $A, $*, .$r, $ar, $c, $s, $N, $$, $C, $aA, and $T, 27 $ variables in total will be expanded.

The default is 0.

var_option $*variable...*

If a message obtained from trapd.conf contains a $ variable specified with this parameter, the same information is expanded as displayed by NNM. You can specify two $ variables: $E and $e.

If this parameter is omitted, or if no information is specified for a $ variable, the $ variable option for the SNMP trap converter is used to expand information. In this case, the information expanded differs from that displayed by NNM.

imevt_server *event-server-name*

Specify the name of the event server to register converted JP1 events on a logical host when using a cluster system. Only an event server running on the local host can be specified. The event server name you specify in this parameter must be set in the remote-server parameter of the event server settings file (conf). For JP1/Base version 09-00 or later, if the imevt_regkind parameter is set to 0, you must also set the remote-server parameter. For details on the event server settings file (conf), see *Event server settings file* in *14. Definition Files*.

The local host is the default location for the destination for registering JP1 events.

imevt_regkind 0|1

This parameter specifies the registration trigger for JP1 events on the event server specified with the imevt_server parameter. If 0 is specified, the registration trigger is assumed to be 3#. If 1 is specified, the registration trigger is assumed to be 1#.

If no imevt_server parameter is specified, you do not need to set this parameter.

If this parameter is omitted, the registration trigger is assumed to 1.

#: JP1 event registration trigger

1: Event issued by the local event server to the local event server

3: Event issued by the remote event server to the local event server

Notes

For the conventional SNMP trap converter, if the imevt_server parameter was specified and the remote-server parameter in the event server settings file (conf) was set to a value other than the default, the event server name set in the imevt_server parameter must be specified in the remote-server parameter. In such a case, if any of the following actions is performed, the SNMP trap converter changes the JP1 event registered reason from 3 to 1:

- Perform an overwrite upgrade to version 9.
- Migrate the definition file for the previous version to version 9.
- Because the above actions cause the registration trigger to change, the system might be affected if any of the following is performed:
- The B.REASON attribute is set in the forwarding settings file (forward).
- A B.REASON attribute is set with the -f option of the jevexport command in the filter file.
- A B.REASON attribute is specified as the third argument (lpszFilter) for the JevGetOpen function that obtains a JP1 event.
- The JevGetRegistFactor function (that obtains a JP1 event) is used to obtain the registration trigger.

To prevent the old value of registration trigger from changing, the imevt_regkind parameter needs to be set to 0. However, if the parameter is set to 0, JP1 event registration might cause an error. If an error occurs, the SNMP event to be registered is lost.

For JP1/Base version 09-00 or later, the remote-server parameter only needs to be set if the imevt_regkind parameter is set to 0.

Definition examples

To create an SNMP action definition file, this example assumes the following:

- NNM URL: Local host (HostA)
- Port number: 8080
- Severity mapping between SNMP traps and JP1 events: In addition to the default ones, the following mapping is added:
- A SNMP trap with an unknown severity level is mapped to a JP1 event with an Information severity level.
- SNMP agent host names: hostA, hostB, hostC, and 10.208.aa.bbb

- `$` variable expansion parameter: `$` variables (`$r`, `$ar`, `$c`, `$s`, `$N`, `$$`, `$C`, `$aA`, and `$T`) are expanded as information contained in the SNMP traps when converting JP1 events.
- `$` variables option parameters: If a `$E` or `$e` is included, the same information as displayed by NNM will be expanded.

```
# NNM URL
nnm_url_base    http://HostA:8080/OvCgi/
jovw.exe?MapName=default

# JP1EVENT SEVERITY
severity normal  to Information
severity warning to Warning
severity minor   to Error
severity major   to Critical
severity critical to Alert
severity unknown to Information

# SNMP AGENT HOST NAMES
snmp-filter
  source hostA hostB hostC 10.208.aa.bbb
end-filter

# $ VARIABLES EXPANSION PARAMETERS
var_expand   1

# $ VARIABLES OPTION PARAMETERS
var_option  $E $e
```

(2) SNMP trap conversion filter file (snmpfilter.conf)

Format

```
[+triangle.tif]enterprise-name.event-name
[+triangle.tif]enterprise-name.*
!enterprise-name.event-name
```

Storage destination directory

In Windows:

installation-folder`\conf\evtgw\snmpfilter.conf`

In UNIX:

`/etc/opt/jp1base/conf/evtgw/snmpfilter.conf`

Description

The SNMP trap conversion filter file specifies whether SNMP traps are to be converted into JP1 events. Make sure that the enterprise name and event name you define in the filter file for converting SNMP traps (`snmpfilter.conf`) match those defined in the `trapd.conf` file of NNM. The enterprise name and event name are case sensitive. Note that the settings entered in this file differ according to the language environment in which NNM is running.

Application of settings

When you perform one of the following operations, the settings take effect:

- Start the SNMP trap converter.
- Start the NNM alarm browser (`xnmevents`).
- Change a setting in the NNM event settings dialog box, and then click the **Save** button.
- Execute the NNM-supplied `xnmevents -event` command.
- Execute the NNM-supplied `xnmtrap -event` command.

Definition statement

- A hash mark (`#`) at the start of a line indicates a comment.
- The content of the SNMP trap conversion filter file (`snmpfilter.conf`) must not exceed 900 bytes, as shown in the expression below.

  ((a1+1)+(a2+1)+(a3+1)+(a4+1)...(**an**#+1))+34 < 900 bytes

  #: Length of the object ID for a SNMP trap defined in the filter file (`snmpfilter.conf`). For example, if an object ID is `.1.2.3.4.5`, **an** is 10 bytes long.

  When you define generic traps in the filter file (`snmpfilter.conf`), use the following expression: (*result-of-the-above-expression*) + (*number-of-general-traps* **x** 2) < 900

Definition details

`+`

Specify this option if you want to convert *variable binding attributes* of SNMP traps into program-specific information of the extended attributes for JP1 events. Insert one or more spaces or tab characters between `+` and the enterprise name. Do not include both `+` and `!` in the same line. If so, the line will become invalid.

Notes on converting variable binding attributes into JP1 events

- The maximum size of the value of a variable binding attribute that can be converted is 1,023 bytes. The 1,024th and subsequent bytes are not converted if specified.

- The maximum size of a JP1 event is 10,000 bytes. If converting variable binding attributes into JP1 event-specific attributes results in the JP1 event size exceeding 10,000 bytes, some variable binding attributes will be left unconverted.
- The maximum number of variable binding attributes that can be converted into JP1 event-specific attributes is 28.

enterprise-name

Specify `OID_ALIAS` for the SNMP trap to be converted.

event-name

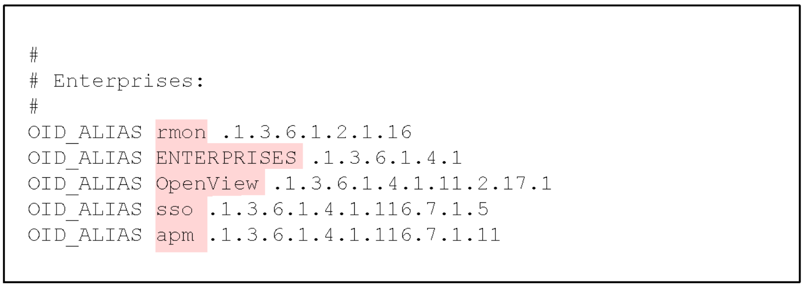
Specify the event name for the SNMP trap you want to convert.

Enterprise and event name examples

The enterprise and event names are described below.

The enterprise names are specified as follows in the `trapd.conf` file.

Figure I-3: Example of specifying an enterprise name defined in trapd.conf



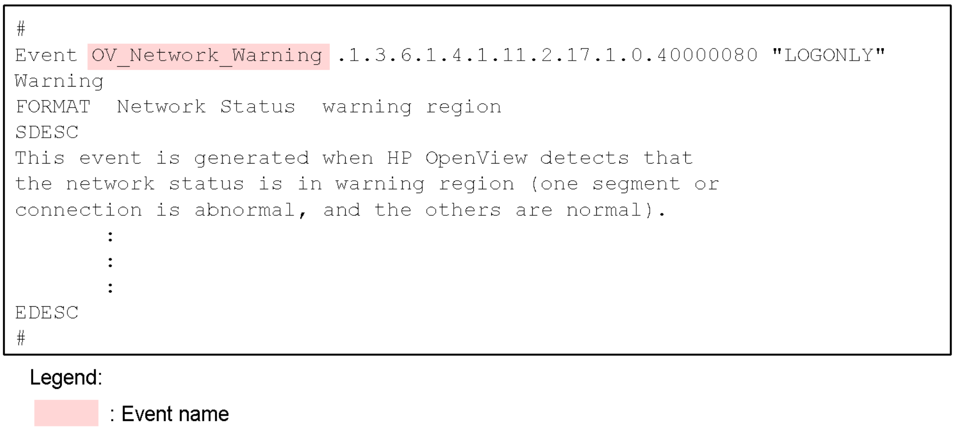
```
#
# Enterprises:
#
OID_ALIAS rmon .1.3.6.1.2.1.16
OID_ALIAS ENTERPRISES .1.3.6.1.4.1
OID_ALIAS OpenView .1.3.6.1.4.1.11.2.17.1
OID_ALIAS sso .1.3.6.1.4.1.116.7.1.5
OID_ALIAS apm .1.3.6.1.4.1.116.7.1.11
```

Legend:

▨ : Enterprise name

The event names are specified as follows in the `trapd.conf` file. Here, `OV_Network_Warning` is the event name.

Figure I-4: Example of specifying an event name defined in trapd.conf



```
#
Event OV_Network_Warning .1.3.6.1.4.1.11.2.17.1.0.40000080 "LOGONLY"
Warning
FORMAT  Network Status  warning region
SDESC
This event is generated when HP OpenView detects that
the network status is in warning region (one segment or
connection is abnormal, and the others are normal).
       :
       :
       :
EDESC
#
```

Legend:

▨ : Event name

*

Specify an asterisk to exclude all SNMP traps with the specified enterprise name from being converted into JP1 events.

!

Specify an exclamation mark to exclude the specified SNMP trap (among those specified in the form `[+Δ]`*enterprise-name*`.*` or `[+Δ]`*enterprise-name*`.`*event-name*) from being converted into a JP1 event. This specification is invalid when both `[+Δ]`*enterprise-name*`.*` and `[+Δ]`*enterprise-name*`.`*event-name* are omitted.

Notes

- When converting SNMP traps into JP1 events, the SNMP trap converter compares the SNMP traps in the order in which they were defined in the filter file for converting SNMP traps (`snmpfilter.conf`). In this filter file, define SNMP traps in the order of priority for conversion into JP1 events.
- You cannot specify a period in enterprise name or event name in the filter file for converting SNMP traps (`snmpfilter.conf`). If a period is included in the enterprise name or event name of any of the SNMP traps to be converted, change that name in NNM to a name that does not contain a period.

Definition examples

An SNMP trap that satisfies the following conditions is converted into a JP1 event:

- The enterprise name is `OpenView`, `snmpTraps`, or `sso`.
- The enterprise name is `OpenView`, and the event name is

`OV_Network_Critical`.

If an SNMP trap satisfies the first condition, but its enterprise name is `snmpTraps`, and its event name is `SNMP_Authen_Failure`, the SNMP trap is not converted.

```
OpenView.*
snmpTraps.*
sso.*

OpenView.OV_Network_Critical

!snmpTraps.SNMP_Authen_Failure
```

I.5 JP1 events for SNMP trap conversion

This section describes JP1 events that might be issued during SNMP trap conversion. If an SNMP trap is detected, a JP1 event with the event ID "00003A80" is issued. The following table provides detailed information on the event ID "00003A80". For details on JP1 event attributes, see *15.1 JP1 event attributes*.

Table I-3: Details about event ID 00003A80

Attribute type		Item	Attribute name	Contents
Basic attribute		Message	--	NNM message

Extended attribute	Common information	Event level	`SEVERITY`	Value according to severity of the SNMP trap.
				Defaults
				Value: Severity
				`Information`: `Normal`
				`Warning`: `Warning`
				`Error`: `Minor`
				`Critical`: `Major`
				`Alert`: `Critical`

		Product name	`PRODUCT_NAME`	`/HITACHI/JP1/IM/SNMP_TRAP`
		Object type	`OBJECT_TYPE`	`SNMP_TRAP`
		Object name	`OBJECT_NAME`	Event name set with NNM
		Root object type	`ROOT_OBJECT_TYPE`	`SNMP_TRAP`
		Root object name	`ROOT_OBJECT_NAME`	Event name set with NNM
		Occurrence	`OCCURRENCE`	`RECEIVE`

Attribute type		Item	Attribute name	Contents
	Program-specific information	SNMP Object ID	`SNMP_OID`	Object ID of the SNMP trap
		SNMP trap occurrence date and time	`SNMP_DATE`	Date and time of the SNMP trap
		SNMP trap occurrence source	`SNMP_SOURCE`	Source that issued the SNMP trap
		Severity	`SNMP_SEVERITY`	Severity set in the SNMP trap
		NNM submap display URL	`SNMP_URL`	URL used to display an NNM submap
		Variable binding storage results[#1]	`SNMP_VARBIND_RESULT`	Results of converting variable bindings `SUCCESS`: All `$` variables have been converted. `ESTRLEN`: Some `$` variables have resulted in a truncated character string due to the length limit (1,023 bytes). `EVARNUM`: Some `$` variables have been deleted due to the limit placed on the number of `$` variables (28). `EEVENTLEN`: Some `$` variables have been deleted due to the limit placed on the JP1 event length (10,000 bytes). `ESTRVARNUM`: Some `$` variables have been deleted due to the limit of the number of `$` variables (28) and some other `$` variables have been truncated due to the length limit (1,023 bytes). `ESTREVENTLEN`: Some `$` variables have been deleted due to the limit of the JP1 event length (10,000 bytes) and some other `$` variables have resulted in a truncated character string due to the length limit (1,023 bytes).
		Number of variable bindings[#1]	`SNMP_VARBIND_NUM`	Number of variable bindings contained in an SNMP trap

Attribute type		Item	Attribute name	Contents
		Object ID[1,2,3...]#1#2	SNMP_VARBIND_OID[1,2,3...]#2	Object ID for variable binding
		Type[1,2,3...]#1#2	SNMP_VARBIND_TYPE[1,2,3...]#2	Type of variable binding ASN_INTEGER ASN_U_INTEGER ASN_OCTET_STR ASN_OBJECT_ID ASN_IPADDRESS ASN_UNSIGNED32 ASN_COUNTER32 ASN_TIMETICKS ASN_COUNTER64 Unsupport: Other than above
		Value[1,2,3...]#1#2	SNMP_VARBIND[1,2,3...]#2	Value of variable binding

Legend:

--: None

#1: Output if you have set up the SNMP trap converter so that variable bindings are converted into JP1 events.

#2: Three items, SNMP_VARBIND_OID, SNMP_VARBIND_TYPE, and SNMP_VARBIND, are output for a single variable binding. Numbers following each item correspond to $ variables for variable bindings.

J. Linking with Products That Use JP1/SES Events

JP1/SES events are the events issued by JP1/SES and JP1/AJS event servers version 5 or earlier. *JP1/SES* and *JP1/AJS* as discussed in this section refer to the following programs:

JP1/SES

- JP1/SES version 05-10 or earlier
- JP1/AOM versions 05-10 to 05-20 (in UNIX)

JP1/AJS

- JP1/AJS version 05-20 or earlier (in Windows NT)
- JP1/AJS versions 05-10 to 05-20 (in Windows NT)

JP1/SES events are used by the following products:

- JP1/OJE Client for VOS1
- JP1/OJE Client for VOSK
- OSCF/Datareplicator Client (VOSK data linkage function)
- VOSK Datareplicator for HiRDB (VOSK data linkage function)
- JP1/OJE Client for VOS3
- JP1/OJE Client for Mainframe
- JP1/OJE for VOS3
- JP1/OJE for Mainframe (for MVS)
- HiRDB
- JP1/AJS `ajsevput` and `ajsevget` commands (for Windows Server 2003 only)

JP1/Base provides a function (called *V5 compatibility*) used to link with products that use JP1/SES events. V5 compatibilities can only be used with an event server running on a physical host. In such a case, an asterisk (`*`) or an at mark (`@`) is specified as part of the event server name in the event server index file (`index`).

To monitor JP1/SES events from JP1/IM, convert them into JP1 events.

This appendix describes how to link JP1/Base with products that use JP1/SES events, and how to specify JP1/Base to convert JP1/SES events into JP1 events.

J.1 Settings for individual products that use JP1/SES events

This section describes how to link JP1/Base with individual products that use JP1/SES events.

(1) Using the JP1/OJE or VOSK data linkage function of VOS1/VOSK

(a) Using other clients' products

To use another client's product with the JP1/OJE or VOSK data linkage function on a host running JP1/Base, you must perform the following:

- Delete the `options v5-unused` parameter in the event server settings file (`conf`). This parameter inhibits V5 compatibility.
- Specify a TCP port for the service `JP1AutoJob` in the `services` file.

  For details on how to do this, see *C.1 Port numbers for JP1/Base*.

  Examples are shown below:

  ```
  JP1AutoJob  5001/tcp  # JP1/AutoJob Event Service
  ```

  Specify the same number (`5001`) for the port and the destination.

(b) Using the event sending function

To send events from JP1/OJE on VOS1/VOSK to a host running JP1/Base, specify the same settings as described in *(a) Using other clients' products*. For a UNIX client, use `jesrd` as the service specified in the `services` file.

(c) Using the event receiving function

For JP1/OJE on VOS1/VOSK to receive events from a host running JP1/Base, you must perform the following on the JP1/Base host:

- Delete the `options v5-unused` parameter in the event server settings file (`conf`). This parameter inhibits V5 compatibility.
- In the event server settings file (`conf`), specify the host name of VOS1/VOSK as the event server name, `ses` as the communication type for the `remote-server` parameter.
- In the `services` file, specify a TCP port for the service `JP1AutoJob` or `jesrd`.

  For details on how to do this, see *C.1 Port numbers for JP1/Base*.

  Examples are shown below:

  In Windows:

  ```
    JP1AutoJob  5001/tcp  # JP1/AutoJob Event Service
  ```

  In UNIX:

```
jesrd   5001/tcp  # JP1/SES remote management server
```

Specify the same number (`5001`) for the port and destination.

(2) Using VOS3/MVS JP1/OJE

(a) Using SES communication protocol with products from other clients

When you want to use a JP1/OJE client product on a host running JP1/Base, if the JP1/OJE is specified for SES communication protocol on the VOS3/MVS host that uses the job execution function for the event sending and receiving function, you must specify the same settings as described in *(a) Using other clients' products* of *(1) Using the JP1/OJE or VOSK data linkage function of VOS1/VOSK.* These settings are not necessary if the JP1/OJE is specified for IM communication protocol on the VOS3/MVS host, or if the batch job linkage function is used.

V5 compatibility might be discontinued in the future. We recommend migrating to an environment that uses the IM communication protocol, or an environment that uses the batch job linkage function.

(b) Using the event sending function

When you want to send events from JP1/OJE on a VOS3/MVS host to a host running JP1/Base, if the JP1/OJE is specified for SES communication protocol on the VOS3/MVS host, you must specify the same settings as described in *(b) Using the event sending function* of *(1) Using the JP1/OJE or VOSK data linkage function of VOS1/VOSK*. These settings are not necessary if the JP1/OJE is specified for the IM communication protocol on the VOS3/MVS host.

V5 compatibility might be discontinued in the future. We recommend migrating to an environment that uses the IM communication protocol.

(c) Using the event receiving function

When you want JP1/OJE on a VOS3/MVS host to receive events from a host running JP1/Base, if JP1/OJE is specified for SES communication protocol on the VOS3/MVS host, you must specify the same settings as described in *(c) Using the event receiving function* of *(1) Using the JP1/OJE or VOSK data linkage function of VOS1/VOSK*. These settings are not necessary if the JP1/OJE is specified for IM communication protocol on the VOS3/MVS host.

V5 compatibility might be discontinued in the future. We recommend migrating to an environment that uses the IM communication protocol.

(3) Using HiRDB

(a) Using the event notification function

If the `pd_jp1_event_level` operand is set to `1`, specify the same settings as described in *(a) Using other clients' products* of *(1) Using the JP1/OJE or VOSK data linkage function of VOS1/VOSK*. If the `pd_jp1_event_level` operand is set to `2`, these settings are not necessary.

V5 compatibility might be discontinued in the future. If the environment permits it, we recommend setting the `pd_jp1_event_level` operand to be set to `2`.

(4) Using the ajsevput command

Specify the same settings as described in *(a) Using other clients' products* of *(1) Using the JP1/OJE or VOSK data linkage function of VOS1/VOSK*.

The `ajsevput` command might be discontinued in the future. We recommend migrating to an environment that uses the JP1/Base `jevsend` or `jevsendd` command.

(5) Using the ajsevget command

Specify the same settings as described in *(a) Using other clients' products* of *(1) Using the JP1/OJE or VOSK data linkage function of VOS1/VOSK*.

The `ajsevget` command might be discontinued in the future. We recommend migrating to an environment utilizing a user program that uses the JP1/Base event acquisition function.

J.2 Common settings for products that use JP1/SES events

Set the following parameters in the event server settings file (`conf`) as necessary.

(1) `users { * | ` user-name `} ...`

You need to specify user names in this parameter if there are no user names in the file you specified in the `include ses-conf` or `include ajs-conf` parameter. However, note that specifying an asterisk (`*`) does not signify that all users can obtain events.

In Windows, you must specify a `system` or `SYSTEM` user name. If you do not specify a name, the event server cannot start. In UNIX, specify the superuser name (usually `root`) and `adm` as the user name.

(2) `eventids {* | ` basic-code ` | ` basic-code`:`extended-code`}...`

You need to specify user names in this parameter if there are no user names in the file you specified in the `include ses-conf` or `include ajs-conf` parameter. However, note that specifying an asterisk (`*`) does not signify that all event IDs can be obtained.

(3) `buffnum` JP1/SES-event-count

This parameter specifies the number of JP1/SES events to be saved for a program that obtains JP1/SES events. When the number of registered JP1/SES events reaches this value, JP1/SES events are deleted, starting from the oldest ones, and the events can no longer be retrieved. Specify a number from `2500` to `10000` for UNIX, or specify a number from `64` to `2048` for Windows. When no event count is specified, the defaults are 2,500 (in UNIX) and 1,024 (in Windows).

(4) `include ses-conf` *file-name*

This parameter specifies the following items to be included from the JP1/SES environment definition file: the user name (`USER`), the event ID (`EVID`*xxxx*) values, and the number of buffers (`BUFFNUM`). The included `BUFFNUM` value supersedes the `buffnum` parameter value specified in the event server settings file (`conf`). The user name and event ID values are the sum of the included values and the values specified in the event server settings file (`conf`).

In *file-name*, specify a full path for the file name. This specification is invalid in the Windows version of JP1/Base, but valid in the UNIX version.

(5) `include ajs-conf`

This parameter specifies the following items specified in the JP1/ASJ - EE settings dialog box to be included: the UNIX user ID, UNIX group ID, user name, the event ID values, and the maximum number of events. The included maximum event count, UNIX user ID, and UNIX group ID override the values specified in the `buffnum` and `alt-userid` parameters in the event server settings file (`conf`). The user name and event ID values are the sum of the included values and the values specified in the event server settings file (`conf`).

This parameter is valid only in the Windows version of JP1/Base, not in the UNIX version.

(6) `options [conv-off]`

This parameter inhibits the event acquisition function. When you specify `conv-off`, no JP1 events are passed to the JP1/SES compatibility event acquisition functions, which improves the JP1 event receipt and transfer performance. When this flag is set, the JP1/SES compatibility event acquisition functions cannot get JP1 events. Similarly, the JP1/AJS-compatible command, `ajsevget`, cannot get JP1 events. This flag does not affect functions other than the JP1/SES compatibility event acquisition functions and the `ajsevget` command. The following list shows whether events can be received when `conv-off` is specified:

Table J-1: Events to be received when the flag is specified

Event to be received	Receiver	Event receipt (detection)
JP1 event	JP1/SES compatibility event acquisition function `ajsevget` command	Not detected
JP1/SES event	JP1/SES compatibility event acquisition function `ajsevget` command	Detectable

J.3 Notes on using JP1/SES events

Points to be noted when linking with a product that uses JP1/SES events are described below.

(1) Limitation on the number of pseudo operators

The maximum number of pseudo operators that can be connected simultaneously is limited. A pseudo operator signifies a program that obtains JP1/SES events.

For the compatibility function of Windows version 5, no more than 52 pseudo operators can be used together. Among them, a maximum of 20 pseudo operators are used exclusively for the JP1/AJS `ajsevget` command. Ensure that no more than 20 `ajsevget` commands are executed simultaneously. The remaining 32 are reserved for JP1/OJE Client for VOS3/Mainframe/VOS1/VOSK custom jobs. Ensure that no more than 32 custom jobs are executed simultaneously.

For the compatibility function of UNIX version 5, no more than 32 pseudo operators can be used together. Ensure that the number of pseudo operators does not exceed 32. For details on programs that can be pseudo operators, see the appropriate manuals for installed Hitachi products.

(2) Operating systems that do not support V5 compatibilities

The OSs that do not support either some or all V5 compatibilities are shown in the following table.

Table J-2: OSs that do not support some or all V5 compatibilities

OS	Limitation
Windows Server 2008	Only allows event reception through JP1/SES protocol. Event transmission is not allowed.
Solaris non-global zone	None of the V5 compatibilities can be used.

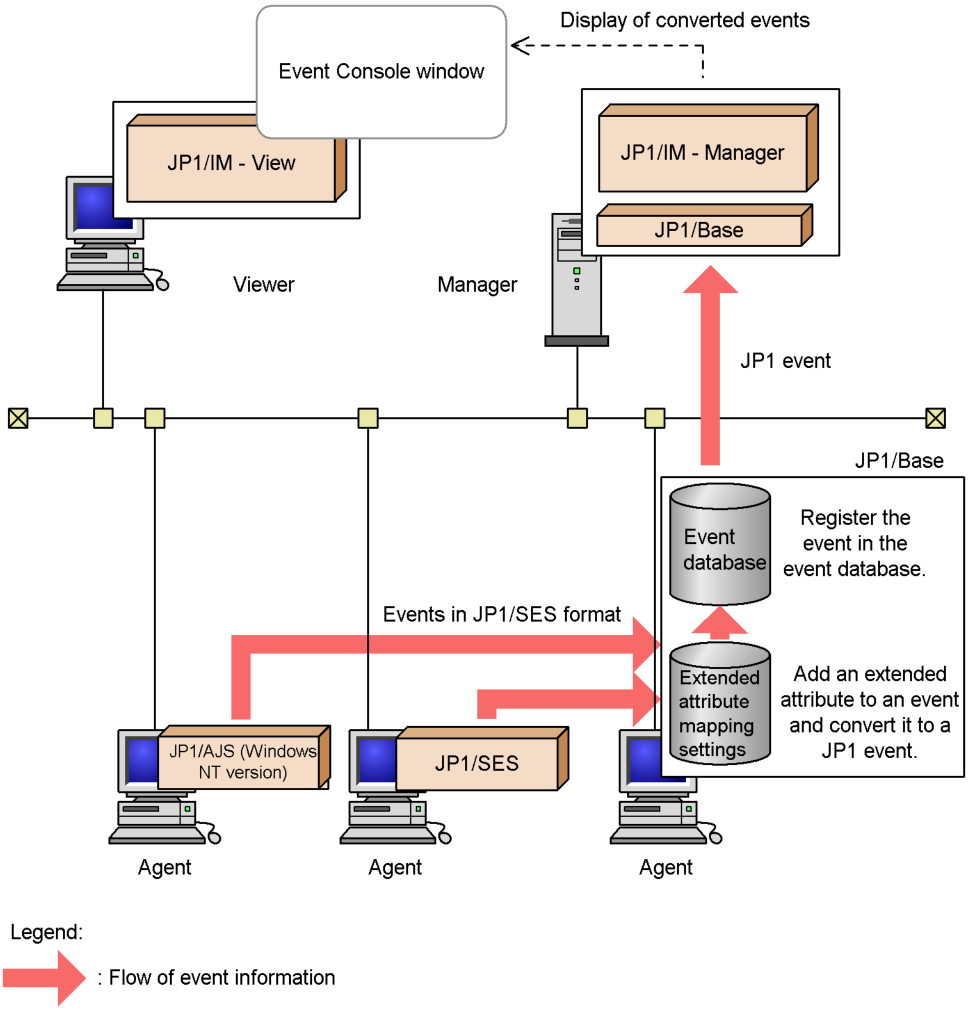
J.4 Converting JP1/SES events into JP1 events

A JP1/SES event only contains a basic set of attributes (such as the event ID and message). It does not contain an extended set of attributes (such as the severity, user name, product name, and object type).

To display an event in the JP1/IM Event Console window, you must specify the extended attributes in that event. To do this, you can use the extended attribute mapping settings file to add extended attributes (such as severity) to the JP1/SES event. To convert a JP1/SES event into a JP1 event, you can add extended attributes to the event. This is called *JP1/SES event conversion*.

The following figure provides an overview of JP1/SES event conversion.

Figure J-1: JP1/SES event conversion


Display of converted events
Event Console window
JP1/IM - View
JP1/IM - Manager
JP1/Base
Viewer
Manager
JP1 event
JP1/Base
Event database
Register the event in the event database.
Events in JP1/SES format
Extended attribute mapping settings
Add an extended attribute to an event and convert it to a JP1 event.
JP1/AJS (Windows NT version)
JP1/SES
Agent
Agent
Agent
Legend:
: Flow of event information

(1) JP1/SES event conversion procedure

This subsection describes how to add extended attributes to a JP1/SES event and convert it into a JP1 event. If necessary, you can add a message with the extended attributes.

The following steps describe how to convert events.

1. Determine the event to be converted, and the extended attributes and message to be added.
2. Create an action definition file.

Create the following definition file on the computer where JP1/Base is installed:

- Extended attribute mapping settings file

3. Restart the event service (JP1/Base)

   If JP1/IM is running, shut it down and restart JP1/Base. Then, restart JP1/IM, if necessary.

(a) Determining the event to be converted, and the extended attributes and message to be added

First, determine which JP1/SES event you want to convert. You can use an event ID or an issuing server name to filter JP1/SES events to reduce the number of events. Filtering only allows a JP1/SES event with a specific event ID, or an event issued by a specific server, to be converted into a JP1 event.

Next, determine the extended attributes and message to be added to the JP1/SES event. To use JP1/IM to monitor an event, the extended attribute `SEVERITY` must be added. For other extended attributes and messages, determine which extended attributes and messages are necessary for JP1/IM to monitor events, and then add those attributes and messages. Guidelines for adding extended attributes are provided in the manual *Job Management Partner 1/Base Function Reference*.

(b) Creating an action definition file

To add extended attributes and a message to a JP1/SES event, create the extended attribute mapping settings file. The following subsection describes how to create the extended attribute mapping settings file.

■ Items to be defined

In the extended attribute mapping settings file, specify an event filer to determine the JP1/SES event to convert, and the extended attribute and message to add to the event.

■ Storage location

Create the extended attribute mapping settings file in the following directory on the computer where JP1/Base is installed.

In Windows:
directory-specified-in-event-server-index`\sesmap\`

This directory is represented in the default event server index as follows:
Base-path`\conf\event\servers\default\sesmap\`

In UNIX:
directory-specified-in-event-server-index`/sesmap/`

This directory is represented in the default event server index as follows:
`/etc/opt/jp1base/conf/event/servers/default/sesmap/`

The `sesmap` directory is not created during standard installation. You first need to create the `sesmap` directory, and then create a text file with a file name (in the format shown below) directly under the directory:
*company-name_product-name*_`map.conf`

The `PRODUCT_NAME` can be `SERIES NAME_PRODUCT NAME`. For the file name, we recommend replacing forward slashes (`/`) (part of the value specified for `PRODUCT_NAME` when issuing a JP1 event) with underscores (_). Because `hitachi` is used as the standard name for the supplied file, we recommend using a company name other than `hitachi` as the *company-name*.

More than one extended attribute mapping settings file can be created. When multiple extended attribute mapping settings files with different names are created directly under the `sesmap` directory, those files are used to convert the JP1/SES events they define. If multiple extended attribute mapping settings files are created, the contents of these files are parsed in ascending order of file name.

Note

Only store definition files in the `sesmap` directory.

If a backup file or model file exists in the directory, the file can be used to perform conversion.

■ Format

An extended attribute mapping settings file is a collection of mapping setting blocks. The format for a mapping setting block is as follows:

```
# Comment
map
[filter-block]
[message]
[extended-attribute-1]
[extended-attribute-2]
       ...
[extended-attribute-n]
end-map
# Comment
```

The comment line starts with a hash mark (`#`) and does not contain any linefeed characters. A comment can be inserted between mapping setting blocks, but cannot be inserted in a block.

`map` and `end-map` declare the start and end of a mapping setting block.

The other components of a mapping setting block are described below.

- ***filter-block***

In the filter block, specify the filter used to determine the JP1/SES event to be

converted into a JP1 event. The file format is as follows:
`filter`
Event-filter
`end-filter`

If no filter block exists, all JP1/SES events are converted. For details, see *Event filter syntax*.

- ***message***

  Specify a message to be added to the JP1/SES event as event information. The format is as follows:
  `B.MESSAGE` *delimiter message-text*

  The text between the delimiter following the `B.MESSAGE` and the linefeed at the end of the line is added as a message. If no message text is specified, no message is added.

  If a JP1/SES event already contains a message, the message is replaced with the message text specified by this parameter. However, if the total size of the message text to be added and the original event information exceeds 1,024 bytes, the message is not added.

- ***extended-attribute***

  Specify one or more extended attributes to be added to event information as necessary. The format is as follows:
  `E.`*extended-attribute-name delimiter extended-attribute-value*

  After `E.`, specify the name of the extended attribute to be added. The character string between the delimiter and the linefeed at the end of the line is treated as the value of the extended attribute. This value cannot be empty (NULL) and it cannot contain any linefeeds.

  To add multiple extended attributes to a single JP1/SES event, repeat this line for each of the extended attributes. A mapping setting block cannot contain extended attributes with the same name. The maximum number of extended attributes that can be added to a JP1/SES event is 100, and the total size for all extended attributes can be no more than 10,000 bytes. If either of these limits is exceed, the entire mapping setting block is ignored.

■ Notes

- The size of a record in the extended attribute settings file can be no more than 1,024 bytes.
- You can omit filter blocks, messages, and extended attributes. If you specify these items, specify them in the order shown. If the order is wrong, or if a block other than an extended attribute block appears two or more times, the entire mapping setting block is invalid.

- The extended attribute mapping settings file does not support exclusion conditions. Do *not* specify an exclusion condition for a filter defined in the filter block.

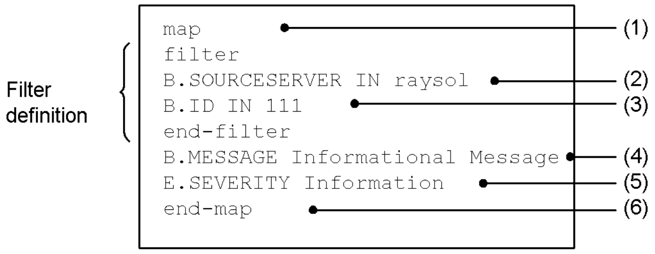
■ Definition examples

• Single mapping

In this example, for JP1/SES events sent to the local host from JP1/SES running on a host named `raysol`, the extended attribute `SEVERITY` (specified `Information`) and the message `Information Message` are added to a JP1/SES event with an event ID of 111.

A text editor is used to create an extended attribute mapping settings file named `company_sample_map.conf`. The extended attribute mapping settings files contain the following definitions:

Figure J-2: Definition example for the extended attribute mapping settings file (single mapping)



```
map
filter
B.SOURCESERVER IN raysol
B.ID IN 111
end-filter
B.MESSAGE Informational Message
E.SEVERITY Information
end-map
```

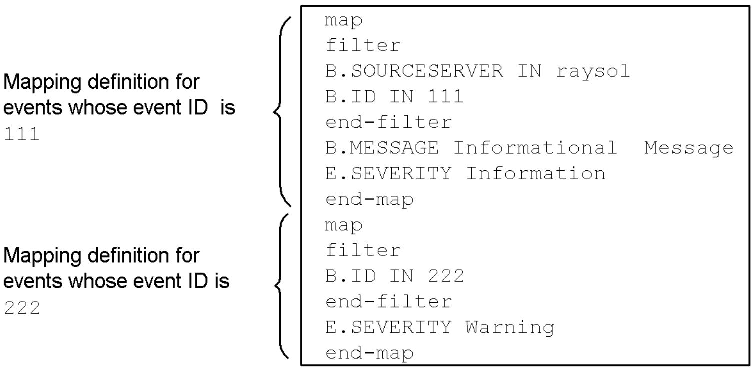
(1) Declare the start of the mapping settings block.
(2) Define that the target events are events that are issued from `raysol`.
(3) Define that the target events are events whose event ID is `111`.
(4) Add a message `Informational Message`.
(5) Set `Information` to the extended attribute `SEVERITY`.
(6) Declare the end of the mapping settings block.

• Multiple mappings

An extended attribute mapping settings file can contain multiple mapping definitions.

For example, in addition to the definition shown in *Single mapping*, another extended attribute SEVERITY (specified to `Warning`) can be added to a JP1/SES event with an event ID of `222`. In this case, the mapping is defined as follows:

Figure J-3: Definition example for the extended attribute mapping settings file (multiple mappings)



Mapping definition for events whose event ID is 111
Mapping definition for events whose event ID is 222

```
map
filter
B.SOURCESERVER IN raysol
B.ID IN 111
end-filter
B.MESSAGE Informational  Message
E.SEVERITY Information
end-map
map
filter
B.ID IN 222
end-filter
E.SEVERITY Warning
end-map
```

If an extended attribute mapping settings file contains multiple mapping definitions, they definitions are parsed in the order that they appear in the file.

K. Operation Log Output

The JP1/Base operation log provides a history of output log information for operations performed on the authentication server. This log records what operation was performed, when it was performed, and who performed it. The operation log is useful for investigating security problems that might occur on the authentication server, such as unauthorized operation. The log also collects information used to safely operate the system.

When JP1 user account or operating permission information (a resource managed by JP1/Base) is added, changed, or deleted, the altered information is output to the JP1/ Base operation log. For example, if a JP1 user password was changed, information on which JP1 user password was changed, when it was changed, and the OS user who changed it, is output to the operation log. Information on the startup and shutdown of the authentication server is also output.

Output to the operation log is supported by JP1/Base version 09-00 or later. Output to the operation log is disabled by default.

The operation log is a CSV text file. You can periodically save the operation log, and edit the saved log with a spreadsheet program to use it for an analysis.

This appendix describes what information can be output to the operation log, and how to specify JP1/Base for operation log output.

K.1 Types of events recorded in the operation log

The table below show the types of events recorded in the operation log, and the trigger conditions for operation log output by JP1/Base. An event type is an identifier used to classify events output to the operation log.

Table K-1: Types of events recorded in the operation log

Event type	Description	Trigger condition for JP1/Base log output
StartStop	Indicates that the software has started up or shut down.	The authentication server starts up or shuts down.
ConfigurationAccess	Indicates that an administrator's authorized operation has succeeded or failed.	• When adding or deleting a JP1 user • Changing the password of a JP1 user • When adding, changing, or deleting JP1 user operating permission • When executing the `jbs_spmd_reload` command • When executing the `jbsaclreload` command

K.2 Storage format of operation log output

This section describes the file format for the operation log. Operation log information is output to the operation log file (`base_log.log`). This log file is a sequential file. When the log file reaches a certain size, it is renamed, and then saved. A new log file is created with the same name as the original, and new log information is written to this file. Specifically, when the file reaches a certain size, the `base_log.log` file is renamed to base_log1.log, and then saved. After the old file is saved, a new `base_log.log` file is created to accept log information. When the new `base_log.log` file reaches a certain size, the saved `base_log1.log` is renamed to `base_log2.log`, and the current `base_log.log` is renamed to `base_log1.log`.

In this way, each time a new log file is created, the number at the end of the old file name is *incremented by 1*. Thus, the file with the higher number is the older file. When the number of saved files exceeds a certain number, the oldest log file is deleted.

Each time the log file is changed, the output destination, and the number of log files to be saved, can be changed in the operation log definition file (`jp1bs_baselog_setup.conf`). The initial size of the log file is 1,024 kilobytes. The initial number of log files that can be saved is four. For details on the range of specifiable values, see *K.5 Settings for outputting operation logs*.

K.3 Operation log output format

An operation log record is output at an operated JP1 user level, or at a JP1 resource group level. For example, if the JP1 authority levels for two JP1 resource groups (`jp1group1` and `jp1group2`) registered by a JP1 user are changed, a record for each JP1 resource group (`jp1group1` and `jp1group2`) is output.

If the setting for the JP1 resource group or JP1 authority level is changed in the user permission level file (`JP1_UserLevel`), and then the `jbsaclreload` or `jbs_spmd_reload` command is executed, the contents of the user permission level file (`JP1_UserLevel`) are compared with the operating permission information on the authentication server. Only the changed definition information is output to the operation log.

The output format, destination, and the items for the operation log output are described below.

(1) Output format

`CALFHM` *x*`.`*x*`,`*output-item-1*`=`*value-1*`,`*output-item-2*`=`*value-2*`,...,`*output-item-n*`=`*value-n*

(2) Output log

In Windows:

installation-folder`\log\BASE\base_log[`*n*#`].log`

In UNIX:

```
/var/opt/jp1base/log/BASE/base_log[n#].log
```

#: *n* is a decimal number from 1 to 16.

(3) Output items

There are two types of output items:

- Common output items

  These items are common to all JP1 products that output operation log information.

- Fixed output items

  These are optionally output by JP1 products that output operation log information.

(a) Common output items

The following table shows the possible common output values and their meanings.

Table K-2: Common output items for the operation log

No.	Output item		Value	Contents
	Item name	Output attribute name		
1	Common specification identifier	--	`CALFHM`	Log format identifier
2	Common specification revision number	--	*x*.*x*	Revision number for log format management
3	Sequence number	`seqnum`	Sequence number	Operation log record sequence number. (Each process is numbered.)
4	Message ID	`msgid`	`KAJP6`*xxx*-*x*	Product message ID
5	Date and time	`date`	*yyyy*-*mm*-*dd*T*hh*:*mm*:*ss*.*sss*T ZD#1	Data and time the operation log record is output, and the time zone
6	Source program name	`progid`	`JP1Base`	Name of the program where the event occurred

No.	Output item		Value	Contents
	Item name	Output attribute name		
7	Source component name	`compid`	`User_management`	Name of the component where the event occurred
8	Source process ID	`pid`	Authentication server's process ID	ID of the process where the event occurred
9	Source location (host name)	`ocp:host`	Authentication server's host name#4	Name of the host where the event occurred
10	Event type	`ctgry`	• `StartStop` • `ConfigurationAccess`	Category name used to classify events recorded in the operation log
11	Event result	`result`	• `Success` • `Failure`	Event result
12	Subject identification	`subj:euid`	• *OS-user-name*#4 • `Unknown`#2 • `Not Support`#3	Name of the OS user that caused the event

Legend:

--: There is no attribute name to be output.

#1: T separates the date from the time. `ZD` is a time zone specifier. One of the following is output:

- `+`*hh*`:`*mm*: Indicates a positive time difference of *hh*`:`*mm* from the UTC time.
- `-`*hh*`:`*mm*: Indicates a negative time difference of *hh*`:`*mm* from the UTC time.
- `Z`: Indicates the same time as the UTC time.

#2: `Unknown` is output if a message (from KAJP6016-I to KAJP6020-I) is output when the `jbs_spmd_reload` command is executed. The name of the OS user executing the command is included in the subject type information for the message (from KAJP6022-I to KAJP6023-W) that immediately follows.

#3: `Not Support` is output if a user authentication command is executed for JP1/Base version 08-00 or earlier. To determine the OS user that executed the command, JP1/Base must be version 09-00 or later.

#4: `None` is output if no value is available.

(b) Fixed output items

The following table shows the possible fixed output values and their meanings.

Table K-3: Fixed output items for the operation log

No.	Output item		Value	Contents
	Item name	Output attribute name		
1	Object information	`obj`	• `JP1user` • `Permission` • `Process` • `Password`	Operation target
2	Operation information	`op`	• `Add` • `Apply` • `Update` • `Delete` • `Start` • `Stop`	Operation type
3	Object location information: *authentication-server-name*	`objloc:authsv`	*authentication-server-name*#1	Name of the authentication server where the operated resource exists
4	Object location information: *JP1-user-name*	`objloc:user`	*JP1-user-name*#1	Name of the JP1 user that has the operated resource
5	Pre-change information: *JP1-resource group-name*	`before:rsrcgrp`	*JP1-resource-group-name*#1	Deleted information output as pre-change information
6	Post-change information: *JP1-resource-group-name*	`after:rsrcgrp`	*JP1-resource-group-name*#1	Post-change information output
7	Post-change information: *JP1-authority-level-name*	`after:prmssn`	*JP1-authority-level-name*#1	Post-change information output

No.	Output item		Value	Contents
	Item name	Output attribute name		

8	Authority information	`auth`	- Windows
			`Administrator`
			- UNIX
			`SuperUser`
				Authority of the operating OS user

9	Requesting host	`from:ipv4`	*IP-address-of-the-command-executing-host*#1#2	IP address of the command executing host
10	Optional description	`msg`	For details on messages#2, see *K.6 Operation log messages*.	Message describing the event

#1: Output of these values depend on the operation log message. See *Table K-4*.

#2: `None` is output if no value is available.

Fixed output items output to the operation log depend on the operation log message. The fixed output items for message IDs are shown in the following table.

Table K-4: Message IDs and fixed output items

Message ID	Object location information: authentication server name	Object location information: JP1 user name	Pre-change information: JP1 resource group name	Post-change information: JP1 resource group name	Post-change information: JP1 authority level name	Requesting host
KAJP6000-I	Y	Y	N	N	N	Y
KAJP6001-W	Y	Y	N	N	N	Y
KAJP6002-I	Y	Y	N	N	N	Y
KAJP6003-W	Y	Y	N	N	N	Y
KAJP6004-I	Y	Y	N	N	N	Y
KAJP6005-W	Y	Y	N	N	N	Y
KAJP6006-I	Y	Y	N	Y	Y	Y
KAJP6007-W	Y	N	N	N	N	Y
KAJP6008-I	Y	Y	N	Y	Y	Y

Message ID	Object location information: authentication server name	Object location information: JP1 user name	Pre-change information: JP1 resource group name	Post-change information: JP1 resource group name	Post-change information: JP1 authority level name	Requesting host
KAJP6010-I	Y	Y	Y	N	N	Y
KAJP6011-W	Y	Y	N	N	N	Y
KAJP6012-I	Y	N	N	N	N	N
KAJP6013-E	Y	N	N	N	N	N
KAJP6014-I	Y	N	N	N	N	N
KAJP6015-E	Y	N	N	N	N	N
KAJP6016-I	Y	Y	N	Y	Y	Y
KAJP6017-W	Y	N	N	N	N	Y
KAJP6018-I	Y	Y	N	Y	Y	Y
KAJP6020-I	Y	Y	Y	N	N	Y
KAJP6022-I	N	N	N	N	N	N
KAJP6023-W	N	N	N	N	N	N

Legend:

Y: Output

N: Not output

(4) Output example

An example of operation log output is shown below.

This output example shows information output to the operation log on the authentication server "server1" when the JP1 user `jp1user1` is added with the `jbsadduser` command.

```
CALFHM
1.0,seqnum=59,msgid=KAJP6000-I,date=2006-09-10T11:05:23.480+09
:00,
progid=JP1Base,compid=User_management, pid=4028,
ocp:host=hostA,ctgry=ConfigurationAccess,result=Success,
subj:euid=Administrator,obj=JP1user,op=Add,objloc:authsv=serve
r1,
objloc:user=jp1user1,auth=Administrator,from:ipv4=206.aa.bb.cc
c,
msg=The JP1 user was added successfully
```

K.4 Trigger conditions for operation log output

This section shows the conditions triggering operation log output, and the associated message IDs. For details on the message texts output by message IDs, see *K.6 Operation log messages*.

Table K-5: Trigger conditions for operation log output and message IDs

Trigger condition			Message ID
Operation	**Result**	**Recorded "Failed" event description**	
When registering a JP1 user	Registration succeeded	--	KAJP6000-I
	Registration failed	An attempt was made to add an already registered JP1 user.	KAJP6001-W
When changing the password of a JP1 user[#1]	Change succeeded	--	KAJP6002-I
	Change failed	• The JP1 user to be changed does not exist. • The old password is wrong.	KAJP6003-W
When deleting a JP1 user	Deletion succeeded	--	KAJP6004-I
	Deletion failed	The JP1 user to be deleted does not exist.	KAJP6005-W
When registering a JP1 resource group	Registration succeeded	--	KAJP6006-I
When changing a JP1 resource group	Change succeeded	--	KAJP6008-I
When deleting a JP1 resource group	Deletion succeeded	--	KAJP6010-I
	Deletion failed	The JP1 user to be deleted does not exist.	KAJP6011-W
When starting an authentication server	Startup succeeded	--	KAJP6012-I
	Startup failed	Startup of the authentication server failed.	KAJP6013-E

Trigger condition			Message ID
Operation	**Result**	**Recorded "Failed" event description**	
When stopping an authentication server	Shutdown succeeded	--	KAJP6014-I
	Shutdown failed	Shutdown of the authentication server failed.	KAJP6015-E
When reloading the JP1/Base process (or executing the `jbs_spmd_reload` command)#2	Registration succeeded	--	KAJP6016-I
	Update failed	Update failed before it was completed.	KAJP6017-W
	Change succeeded	--	KAJP6018-I
	Deletion failed	--	KAJP6020-I
	Command succeeded	--	KAJP6022-I
	Command failed	The `jbs_spmd_reload` command execution failed.	KAJP6023-W
When reloading the user permission levels (or executing `jbsaclreload` command)#3	Registration succeeded	--	KAJP6006-I
	Change succeeded	--	KAJP6008-I
	Deletion succeeded	--	KAJP6010-I
	Update failed	Update failed before it was completed.	KAJP6007-W

Legend:

--: No "Failed" event is recorded.

#1: Attempts to change a linked user password are not recorded in the operation log. Because linked user passwords are managed on the linked directory server, they cannot be changed on the authentication server. If the `jbschgpasswd` command is executed, a KAVA5209-E message is output.

#2: The `jbs_spmd_reload` command reloads the JP1/Base process. When this command is executed, operating permission information is reloaded from the user permission level file (`JP1_UserLevel`). Only the JP1 user information changed from the operating permission information on the authentication server is output to the operation log.

#3: The `jbsaclreload` command reloads operating permission information from the user permission level file (`JP1_UserLevel`). Only the JP1 user information changed from the operating permission information on the authentication server is output to the operation log.

K.5 Settings for outputting operation logs

You can use the operation log definition file (`jp1bs_baselog_setup.conf`) to specify JP1/Base for operation log output. This section describes how to specify JP1/Base for operation log output.

(1) Setup

To specify JP1/Base for operation log output:

1. Edit the operation log definition file (`jp1bs_baselog_setup.conf`).
2. Execute the `jbssetcnf` command.

   The settings are reflected in the common definition information.
3. Enable the setting.

   To enable the automatic restart setting, restart JP1/Base or execute the reload command (`jbs_spmd_reload`).

(2) Operation log definition file (jp1bs_baselog_setup.conf) details

The operation log definition file (`jp1bs_baselog_setup.conf`) is described in detail below.

(a) Storage destination directory

The operation log definition file (`jp1bs_baselog_setup.conf`) is in the following location.

In Windows:

installation-folder`\conf\`

In UNIX:

`/etc/opt/jp1base/conf/`

(b) Format

In the operation log definition file (`jp1bs_baselog_setup.conf`), use the following format to specify whether operation log output is enabled. You can also use this format to specify the output destination and file size of the operation log file (`base_log.log`), the number of files to be saved, and whether the log file is changed automatically.

`"`*item-name*`"=`*value*

(c) Definition details

The items that can be specified in the operation log definition file (`jp1bs_baselog_setup.conf`) are described below. Excluding the output destination of the operation log file (`base_log.log`), specify a hexadecimal value for all. A value in () indicates a decimal value.

ENABLE

Specifies whether to enable operation log output. If you specify a number other than the following numbers, the system assumes that the default is specified.

- Initial value: 00000000
- To disable operation log output: 00000000
- To enable operation log output: 00000001

LOGFILEDIR

Enter the output path of the operation log file (`base_log.log`).

- Initial value

  In Windows: *installation-folder*`\log\BASE`

  In UNIX: `/var/opt/jp1base/log/BASE`

LOGSIZE

Specifies the operation log file (`base_log.log`) size in bytes. If a value smaller than the lower limit of the possible range is specified, the lower limit value is assumed. If a value greater than the upper limit is specified, the upper limit value is assumed.

- Initial value: 00100000 (1,024 KB)
- Possible value range: 00002000 to 00400000 (8 KB to 4,096 KB)

LOGFILENUM

Specifies the number of operation log files (`base_log.log`) to be saved. If a value smaller than the lower limit of the possible range is specified, the lower limit value is assumed. If a value greater than the upper limit is specified, the upper limit value is assumed.

- Initial value: 00000004 (4 files)

- Possible value range: 00000001-00000010 (from 1 to 16 files)

LOGCHANGEOPT

Specifies whether to automatically change the log file when JP1/Base starts. If you specify a number other than one of the following, the system assumes the initial value.

- Initial value: 00000000
- Not to be changed at startup: 00000000
- To be changed at startup: 00000001

(d) Operation log definition file definition example

This subsection provides a definition example for when operation log output is enabled. If the `ENABLE` value is changed to `00000001`, the operation log can store no more than 1 megabyte of output, and save no more than four log files.

```
[JP1_DEFAULT\JP1BASE\BASE_LOG]
"ENABLE"=dword:00000001
"LOGFILEDIR"="/var/opt/jp1base/log/BASE"
"LOGSIZE"=dword:00100000
"LOGFILENUM"=dword:00000004
"LOGCHANGEOPT"=dword:00000000
```

K.6 Operation log messages

This section lists the message IDs and message text that can be output to the operation log.

KAJP6000-I

The JP1 user was registered successfully.

KAJP6001-W

An attempt to register the JP1 user has failed.

KAJP6002-I

The password for the JP1 user was changed successfully.

KAJP6003-W

An attempt to change the password for the JP1 user has failed.

KAJP6004-I

The JP1 user was deleted successfully.

KAJP6005-W

An attempt to delete the JP1 user has failed.

KAJP6006-I

The JP1 resource group was registered successfully.

KAJP6007-W

An attempt to reload the definition information about the JP1 user operating permissions has failed.

KAJP6008-I

The JP1 resource group was changed successfully.

KAJP6010-I

The JP1 resource group was deleted successfully.

KAJP6011-W

An attempt to delete the JP1 resource group has failed.

KAJP6012-I

The authentication server was started successfully.

KAJP6013-E

An attempt to start the authentication server has failed.

KAJP6014-I

The authentication server was stopped successfully.

KAJP6015-E

An attempt to stop the authentication server has failed.

KAJP6016-I

The JP1 resource group was registered successfully.

KAJP6017-W

An attempt to reload the definition information about the JP1 user operating permissions has failed.

KAJP6018-I

The JP1 resource group was changed successfully.

KAJP6020-I

The JP1 resource group was deleted successfully.

KAJP6022-I

The jbs_spmd_reload command was executed successfully.

KAJP6023-W

An attempt to execute the jbs_spmd_reload command has failed.

L. Version Changes

This appendix describes changes between versions.

L.1 Changes in 09-00

- JP1/Base now supports Windows Server 2008.
- JP1/Base now supports Windows Vista.
- The local action function has been added.
- IM configuration management is now supported.
- Operating information can now be collected.
- Login authentication via linkage to a directory server is now available (for Windows only).
- The operation log output function has been added.
- A new option has been added to the `jevlogstart` command. This option allows you to specify a maximum of 1,024 bytes (including one byte of a termination character) for the length of a JP1 event message.
- A new option has been added to the `jbslistuser` command. This option allows you to output the date of the last JP1 user update.
- The system extracts as many valid records as possible from the key ISAM file where an error occurred, and then adds the restore command (`Jisktod`) to a sequential file.
- The `-ds` option has been added to the `jbsadduser` and `jbslistuser` commands (for Windows only).
- The `jbschgds` and `jbschkds` commands have been added (for Windows only).
- The `-e` option has been added to the `jisinfo` command (for UNIX only).
- A monitoring target name can now be specified for the following log file trapping commands:

  `jevlogreload`, `jevlogstart`, `jevlogstat`, `jevlogstop`
- The `-q` option has been added to enhance the usability of the data collection command.
- Descriptions have been added for the following JP1/IM-related commands:

  `jbsrt_del`, `jbsrt_distrib`, `jbsrt_get`, `jbsrt_sync`, `jcocmddef`, `jcocmddel`, `jcocmdlog`, `jcocmdshow`

- The descriptions of the following commands have been changed:

  List of commands, cpysvprm, hntr2getname, jbs_log.bat, jbs_spmd_reload, jbs_spmd_status, jbs_spmd_stop, jbsacllint, jbsaclreload, jbsadduser, jbsblockadesrv, jbschgpasswd, jbsgetcnf, jbsgetumap, jbshostsexport, jbshostsimport, jbslistacl, jbslistsrv, jbslistuser, jbsmkpass, jbsmkumap, jbsrmacl, jbsrmumap, jbsrmumappass, jbsrmuser, jbssetacl, jbssetcnf, jbssetumap, jbsumappass, jbsunblockadesrv, jbsunsetcnf, jcocmdconv, jevdbinit, jevdbswitch, jevdef_distrib, jevdef_get, jeveltreload, jevlogreload, jevlogstart, jevlogstat, jevlogstop, jevregsvc, jevreload, jevstat, Jischk, Jiscond, Jisconv, Jiscpy, Jisext, Jisinfo, Jiskeymnt, Jisktod, Jislckclear, Jislckext, Jislckfree, Jismlcktr, Jisprt
- Output of the message (KAJP1037-E) can now be suppressed.
- Messages have been added and changed.
- A new parameter named restart has been added to the event server settings file (conf). This parameter enables JP1/Base for Unix to restart the event service process if it ends abnormally on a physical host.
- The client parameter has been added to the API settings file.
- An exclusion condition can now be specified for an event filter.
- The JP1 event (00003D04) was added.
- Descriptions for the following JP1/IM-related JP1 events have been added:

  00003FA0, 00003FA1, 00003FA2, 00003FA3, 00003FA5, 00003FA6
- The description of the JP1/IM-related JP1 event (00003A10) has been changed.
- User applications can now be written in the C language.
- SEQ2 files can now also be monitored under Windows.
- An output format description for the integrated trace log has been added.
- The operation log definition file has been added to the list of backed up files.
- The file list has been updated.

L.2 Changes in 08-00

- The $ variables supported by the SNMP trap converter have been expanded. A parameter has been added for specifying whether to expand the information contained in these new $ variables when SNMP events are converted into JP1 events.
- The hosts names of source SNMP agents can now be specified for conversion of

SNMP events into JP1 events by the SNMP trap converter.

- Parameters have been added for specifying target SNMP traps by wildcard for conversion into JP1 events by the SNMP trap converter, and for excluding particular SNMP traps from JP1 event conversion.
- The list of files has been updated for version 08-00.
- Messages have been added and changed.
- The descriptions about memory and disk space requirements have been deleted. For details on these requirements, see the *Readme.txt* in Windows or the *Release Notes* in UNIX.

L.3 Changes in 07-51

- A health check function was added to detect hangups or abnormal termination of JP1/Base processes.
- Functionality was added in the startup management, to enable setting the timing for starting control services, so the system load is reduced when the services start.
- Changes were made to the list of files that users should back up.
- A command for initializing an event database (`jevdbinit`) and a command for manually switching the event database (`jevdbswitch`) were added.
- A JP1 event is issued when a corrupted record is detected in the event database.
- An option for specifying the file to be output was added to the command for outputting the event database in CSV format (`jevexport`).
- An option for outputting the title name of the basic attribute or extended attribute was added to the command for outputting the event database in CSV format (`jevexport`).
- Functionality was added to the log file trapping function so that it issues a JP1 event and retries monitoring when a log file cannot be accessed.
- Multi-process trace file format (`HTRACE`) was added to the log file formats that can be monitored with the log file trapping function.
- The `{EXIT}` option was added to the `ACTDEF` parameter, specified in the action definition file of the log file trapping function.
- Functionality that retries connecting to the event services for the log file trapping function was added.
- An option was added that can read all the logs that have occurred up to the moment the stop command (`jevlogstop`) of the log file trapping function is executed.
- Users can specify a monitoring interval for the event log trapping function.

- A parameter (matching-level) was added to the event log trapping function, enabling users to set a comparison level for applying a filter condition in the action definition file to an event log entry.
- A parameter (filter-check-level) was added to the event log trapping function, enabling users to set a checking level when an invalid log type (log type that does not exist in the system) or invalid regular expression is found in a filter condition.
- Functionality was added to the SNMP trap converter, to enable setting the severity of JP1 events for SNMP trap severity.
- An option for specifying how long to wait for execution to complete was added to the command for checking the activity of event service processes (jevstat).
- The calculation of the capacity for the event service error log, which is specified in the error-size parameter of the event server settings file (conf), was changed.
- An option for displaying a confirmation message before deletion was added to the command for deleting the operating permissions of a JP1 user (jbsrmacl).
- An option for displaying a confirmation message before deletion was added to the command for deleting specific user mapping information (jbsrmumap).
- A command was added for checking and clearing the locked status of ISAM files and records (Jislckclear).
- Functionality was added to enable collecting of troubleshooting information without having to customize the data collection tools (jbs_log.bat, jbs_log.sh).
- The jcocmdcom process was added to the processes used in the process management functionality.
- JP1 events were added.
- The list of files was updated.
- Recovery action was added for responding to the message The port ID for the SES emulator is not defined.
- The list of limits was updated.
- Messages related to command execution were added.
- Messages related to configuration management were added.
- Messages were added, changed, and deleted.

L.4 Changes in 07-00

- Functionality to restart a JP1/Base process that has stopped was supported.

- Functionality to issue a JP1 event when a process ends abnormally or authentication servers are switched was added.
- Commands to register, change, and delete JP1 users, JP1 users' operation authorization, and user mapping information for each user were added.
- Functionality to specify JP1 users who have used commands was added for Windows.
- Functionality to add variable binding attributes to the program-specific information of the extended attribute for JP1 events was added.
- A command to reload the action definition files for file trapping and event log trapping was added.
- Functionality to collect and distribute event service definition information was added (only for JP1/IM).
- Event database switching can be detected while the `jevexport` command is being executed.
- A comparison keyword (`WITHIN`) to write to the filter file specified in the `jevexport` command was added.
- Extended regular expressions were supported for regular expressions used in filters.
- Automatic setup functionality for installation was added. Automatic setup can be selected at installation on Windows only.
- `SEQ2` was added to the log types specifiable as filter conditions in the action definition file for log file trapping.

M. Glossary

agent

A program that is managed by another program on the system, or a host that is managed by another host on the system.

For example, JP1/Base is the agent for JP1/IM, and JP1/AJS - Agent and JP1/Base are the agents for JP1/AJS.

ANY binding method

A communication protocol that permits reception of data sent to all the IP addresses assigned to the hosts. The communication wait process ensures that data sent to all the hosts by using port numbers is received. The connection process ensures that data is sent to all the hosts on the subnetworks even if each host uses multiple subnetworks. If JP1/Base is used for a physical host alone, JP1/Base typically operates by this ANY binding method (without the need to make settings).

authentication server

A server that manages the access permissions of JP1 users. One authentication server is required in each user authentication block. The administrator can centrally manage all JP1 users on this server. When JP1/IM or JP1/AJS is installed in the system, the administrator must register JP1 user names on this server.

basic attribute

An attribute held by all JP1 events.

blocked status

Status where the system does not attempt to reconnect the authentication server after a connection failure. This status might occur when two authentication servers are installed in a single user authentication block.

client

A host that issues instructions for process execution to another host (or program), and receives the execution results from that host (or program). JP1/IM - View acts as a client in a JP1/IM system, and JP1/AJS - View acts as a client in a JP1/AJS system.

cluster system

A system configured with multiple server systems that work together so that job processing can continue if a failure occurs. The process of one system taking over from a failed system is called *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.

common definition information

A set of definitions relating to JP1/Base, JP1/IM, JP1/AJS, and JP1/Power Monitor. This information is managed by JP1/Base. The database containing this information is on a local disk of each server, and the definition parameters are stored on each of the physical hosts and logical hosts to which they apply.

When JP1 is used in a cluster system, the logical hosts definitions in the common definition information stored on the servers must be identical on both the primary and secondary nodes. For this reason, after completing the setup and environment settings on the primary server, you must copy the parameters to the secondary server.

configuration definition

Information defining the configuration of a system run and managed by JP1/IM.

A configuration definition defines the hierarchy of managers and agents in JP1/IM. You can define managers at different levels. For example, you can define a higher-level integrated manager and a lower-level site manager.

The information about host relationships defined in a configuration definition can be utilized in various ways. For example, in JP1/IM, it indicates the manager hosts to which important JP1 events should be forwarded and defines the hosts on which commands can be executed as automated actions.

directory server

A server that provides services required to centrally manage various resources on the network and their respective attributes.

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 manual for that program.

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 log trapping

The *event log trapping* functionality converts Windows event log data into JP1 events.

event server

A program that has functionality for managing JP1 events under JP1/Base. When the event server is active, JP1 events can be collected and distributed.

event service

Functionality for registering and managing the events generated in the system as JP1 events.

extended attribute

An attribute of a JP1 event, optionally set by a source program when issuing a JP1 event. An extended attribute consists of common information and program-specific information. The common information is shared by all JP1 programs. The program-specific information is additional information set by the particular program.

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*.

IP binding method

A communication protocol that permits reception of data sent to a particular IP address. The communication wait process ensures that data sent to a particular IP address only is received. The connection process ensures that data is sent via a NIC that uses a particular IP address only.

If JP1/Base is used in a cluster system, JP1/Base typically operates by this IP binding method. (Making the settings for the cluster system changes the communication protocol to the IP binding method.)

JP1/AJS

A program for running jobs automatically. Using JP1/AJS2, you can execute a sequence of processes according to a predefined schedule, or initiate processing when a specific event occurs.

JP1/Base

A program that provides event services. Using JP1/Base, you can send and receive JP1 events, and control the sequence in which services are activated.

JP1/Base is a prerequisite program for JP1/IM, JP1/AJS, and JP1/Power Monitor. When JP1/IM or JP1/AJS are configured in the system, JP1/Base enables the administrator to restrict the operations that JP1 users can perform.

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 attribute

Held by all JP1 events.

Basic attribute names are expressed as, for example, `B.ID` (or simply `ID`) for the event ID.

Extended attribute

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:

1. Common information (extended attribute information in a format shared by all programs)

2. Program-specific information (other information in a format specific to the program issuing the event)

Extended attribute names are expressed as, for example, `E.SEVERITY` (or simply `SEVERITY`) for the severity level.

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

jp1hosts

Host information specific to JP1/Base. If `jp1hosts` information is defined, JP1/Base has two or more IP addresses assigned to each host, and thus can resolve two or more IP addresses from each host name even when the OS can resolve only one IP address from each host name. `jp1hosts` information is valid when it is registered as a common definition.

JP1/IM - Manager

JP1/IM - Manager (JP1/Integrated Management - Manager) is a program that provides integrated system management through centralized monitoring and operation across the entire system.

JP1/IM - Manager provides two core features: *integrated console* and *integrated scope*.

JP1/IM - View

A program that provides the view functionality for integrated system management in JP1/IM.

JP1/IM - View provides a common graphical user interface for JP1/IM - Manager and JP1/IM - Rule Operation. The user can link JP1/IM - View to these programs as required, and perform system monitoring and management suited to the system's purpose.

JP1 permission level

A level that indicates the types of operations that a JP1 user is allowed to perform on a management target (that is, on a resource). Permissible operations depend on whether the management targets (the resources) are jobs, jobnets, events, or other entities. JP1 users' access permissions are managed as combinations of different permissions set for specific types of resources.

JP1/Power Monitor

A program that starts and stops hosts automatically.

Using JP1/Power Monitor, you can start and stop hosts according to a set schedule, and start and stop hosts remotely.

JP1 resource group

A set of management targets (that is, resources), such as jobs, jobnets, or events, that are managed together in JP1. Each set of resources is a *JP1 resource group*.

JP1/SES

A program in Version 5 and earlier versions of the JP1 series. JP1/SES provides functionality (System Event Service) for managing events issued by applications.

JP1/SES compatibility

Functionality to maintain compatibility with the event service provided by the pre-Version 6 programs, JP1/SES and JP1/AJS.

JP1 user

An identifier for accessing JP1/IM or JP1/AJS. This name is registered on the authentication server, which controls the user's access permissions to a remote host. The JP1 user name might differ from the user account registered on the OS.

A JP1 user whose login is authenticated by an authentication server is called a *standard user*, and a JP1 user whose login is authenticated by a directory server is called a *linked user*.

key definition file

A file that contains the correspondence between data files and key files.

key file

A file that contains the index information in a hierarchical tree structure for retrieving keys. This file also contains keys for retrieving data file records. There are two types of key files: a main key file and a subkey file.

linked user

A JP1 user whose login is authenticated by a directory server. Passwords are managed by the directory server. This allows JP1 users to be registered in an authentication server without entering a password.

local action

A function that automatically executes a command on the local host when a specific JP1 event occurs.

log file trapping function

Functionality that converts log data that was output to a log file by an application program. The log data is converted to JP1 events.

logical host

A logical server that executes JP1 in a cluster system. If a failure occurs, a failover between logical hosts takes place.

Each logical host has a separate IP address and a shared disk. In the event of a failover, a logical host starts operating by inheriting the IP address and shared disk of the failed logical host. Thus, after a physical server is switched into service because of a failure, other hosts can access the server by using the same IP address as that of the failed server. To the host, it seems as if one server is always active.

manager

A program that manages other programs (agents) on the system, or a host that manages other hosts on the system.

For example, JP1/IM - Manager, JP1/IM - Rule Operation, and JP1/AJS - Manager manage either JP1/IM or JP1/AJS. These program manage other programs (agents) on the system.

multi-LAN connectivity

JP1 functionality for a system composed of multiple LANs.

Using this functionality, you can set a JP1 communication LAN on a host connected to multiple hosts. You can also make communication settings specific to JP1, regardless of the system or any other applications. This provides flexibility to adapt to various network configurations and operation methods.

In some cases, a host connected to multiple LANs is called a *multi-home host* or *multi-NIC host*.

JP1/Base can operate in the following multi-LAN connectivity environment:

- Environment divided into multiple networks

NNM

A generic name for the integrated network management programs designed for network configuration, performance, and trouble management.

node switching system

See *cluster system*.

operating information

Definition information loaded by JP1/Base services. This information can be used to check the currently valid definition for JP1/Base.

physical host

A unique environment given to each of the servers that make up a cluster system. The environment for a physical host is not inherited by other servers when a failover takes place.

primary authentication server

One of two authentication servers installed in a single user authentication block. The primary authentication server is the server that is usually used.

process

A Windows service program or UNIX daemon program.

regular expression

A list of characters and special characters corresponding to one or more specific text strings.

secondary authentication server

One of two authentication servers installed in a single user authentication block. The secondary authentication server is used as a backup.

SNMP trap converter

A function that converts SNMP traps issued by NNM into JP1 events.

sparse character

Any character that is specified not to be used as a key. Specify sparse characters for creating a key definition file or for adding a key.

When you add a record, any key that only contains sparse characters will not be added to the key file. This key is called a *sparse key*. Using the sparse key reduces the size of the key file and the time required for processing a duplicate key. This key helps to reduce the time it might take to process duplicate keys.

standard user

A JP1 user whose login is authenticated by an authentication server. Passwords are managed by the authentication server.

user authentication block

The range of hosts managed by one authentication server in a system. JP1 users can run jobs, execute commands, and perform automated actions and other operations on the hosts within an authentication block. When JP1/IM or JP1/AJS is installed in the system, the administrator must decide the configuration of user authentication blocks.

user mapping

Functionality that grants to JP1 users the rights of one or more users registered in the OS.

When user mapping is defined, a user who is registered as a JP1 user on an authentication server is allowed to perform operations on a host using the privileges of a user registered in the OS of that host.

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, if JP1/PFM/SSO detects an error while monitoring an application, the application name can be appended in a variable binding as detailed information when the error is trapped.

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.

viewer

A program that provides windows used to operate managers and agents, and to confirm the information they manage. A host that executes a viewer is also called a process.

For example, JP1/IM - View is the viewer for JP1/IM, and JP1/AJS - View is the viewer for JP1/AJS.

Index

Reader's Comment Form

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

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

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

(For Hitachi use)